TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Mika Kähkönen

Ympyrän neliöimisestä

Matematiikan ja tilastotieteen laitos
Matematiikka
Heinäkuu 2009

Tampereen yliopisto

Matematiikan ja tilastotieteen laitos

KÄHKÖNEN, MIKA: Ympyrän neliöimisestä

Pro gradu -tutkielma, 38 s.

Matematiikka

Heinäkuu 2009

Tiivistelmä

Hakutermit: geometrinen konstruktio, pii, Neperin luku, algebrallinen luku, transkendenttinen luku

Tutkielma käsittelee klassista ympyrän neliöimisen ongelmaa: on geometrisella konstruktiolla eli harpilla ja viivaimella piirrettävä ympyrästä alaltaan yhtä suuri neliö.

Tutkielmassa seurataan ongelman historiaa ja todistetaan neliöiminen mahdottomaksi: Geometrisilla konstruktioilla voidaan piirtää sellaisia pisteitä, joiden koordinaatit ovat tietynlaisia algebrallisia lukuja. Ympyrän neliöimiseksi pitäisi päästä pisteeseen, jonka koordinaatissa on luku π. Koska π on transkendenttinen eikä algebrallinen, on ympyrän neliöiminen mahdotonta.

Tutkielman päälähteet ovat Carl Boyerin *Tieteiden kuningatar* ja E.W. Hobsonin *Squaring the circle and other monographs.*

Sisältö

1 Johdanto

Tutkielmamme tavoite on todistaa klassinen antiikin ajoilta periytyvä ympyrän neliöimisen ongelma mahdottomaksi. Neliöimisessä on harpilla ja viivaimella piirrettävä eli konstruoitava ympyrästä alaltaan yhtä suuri neliö. Geometrista ongelmaa yritettiin ratkoa vuosisatoja, kunnes vuonna 1882 saksalainen Ferdinand Lindemann todisti sen mahdottomuuden algebrallisin keinoin.

Luvussa 2 esittelemme todistamiseen tarvittavia määritelmiä ja lauseita. Luvussa 3 selvitämme tasokonstruktioiden yhteyden algebraan. Osoitamme, että vain tiettyjä algebrallisia lukuja voidaan konstruoida. Luvussa 4 tarkastelemme ongelman ratkaisuun johtanutta matematiikan kehitystä. Lopuksi luvussa 5 todistamme, että neliöidäkseen ympyrän pitäisi konstruoida π. Sitten todistamme luvun π transkendenttisuuden. Koska transkendenttistä lukua ei voi konstruoida, huomaamme, että ympyrän neliöiminen on mahdotonta. Tutkielman ymmärtämiseen lukijalla riittää alkeisgeometrian tuntemus, analyysin ja algebran alkeiden sekä todistamisen logiikan hallinta.

Ympyrän neliöimisestä on suhteellisen paljon kirjallisuutta mutta suomeksi vähän. Ympyrän neliöimisen historia on läheisesti luvun π historiaa. Petr Beckmanin *Pii, erään luvun tarina* käy aihetta ansiokkaasti läpi ja usein myös arvioi historian yhteiskuntia lähinnä matematiikan arvostuksen näkökulmasta. Matematiikan yleishistorioita on suomeksi ilmestynyt kaksi: laaja Carl Boyerin *Tieteiden kuningatar* ja Matti Lehtisen suppeampi *Matematiikan historia*. Lisäksi on joitakin elämäkertakokoelmia ja suppeita opintomonisteita. [15, s. 4]. Englanniksi asiaa käsittelevät muun muassa H. Tietzen *Famous problems of mathematics*, E. Hobsonin *Squaring the circle* ja F. Kleinin *Famous problems of elementary geometry*.

Tutkielman matemaattinen sisältö seuraa Hobsonia [10], jossa esitetään riittävä todistus. Tukena käytämme lisäksi Lindelöfiä [16]. Historian osalta tärkeimmät lähteemme ovat Boyer [4], Beckman [1] ja Hobson [10]. Tarkastelemme historiasta todistusyritysten matematiikkaa ja jätämme yhteiskunnan olojen arvioimisen historioitsijoille.

Ympyrän neliöiminen on mielenkiintoinen tapaus matematiikan historiassa. Se on puhtaasti teoreettinen ongelma, jota monet matemaatikot yrittivät ratkaista vain ratkaisemisen ilosta – ja ehkä kunnianhimonkin vuoksi. Hieman jälkiviisaasti näemme koomisena sen, että mahdotonta yritettiin turhaan tehdä tuhansien vuosien ajan. Neliöiminen nähtiin kuitenkin ajan tuhlaamiseksi jo antiikissa Aristofaneen (450–385 eKr.) näytelmässä [17] ja keskiajan lopulla Dante (1265–1321) kuvaa *Jumalaisen näytelmän* viimeisissä säkeissä, kuinka päähenkilö yrittää turhaan ymmärtää jumalaista näkyä – turhaan kuin matemaatikko ympyrää neliöidessään [7, kolmasneljättä laulu]:

Se kaaristasi, joka näytti mulle
valolta heijastunehelta, koska
ma tuokion sit' olin tuijottanut,

nyt näytti kantavan kuin ihmiskuvaa
sisällään, mutta jumalaistunutta,
siks häneen kääntyi koko katseheni.

Kuin matemaatikko; mi turhaan pyrkii
mittaamaan ympyrätä eikä löydä
aatetta etsimäänsä miettienkään;

niin näyn tuon uuden eessä olin minä:
ma nähdä tahdoin, kuinka kehään sopi
tuo kuva ja mik' oli suhde niiden.

Mut riittäneet ei siihen siivet omat;
salama äkkiä mun halki sielun
löi häikäisten ja täytti toiveheni.

Jo vaipui korkea nyt kuvausvoima;
mut kaihoain ja tahtoain nyt johti
kuin pyörää tasan pyörivää, se Rakkaus,

mi ohjaa Auringon ja kaikki tähdet.

Nyt ryhdymme tutkimaan ympyrän neliöimistä ja päädymme mekin ylimaalliseen, transkendenttiseen[1]. Oppaamme matkalla ei ole Danten Beatrice vaan matematiikan tutkijat ja heidän todistuksensa. Oppaamme antiikin kreikkalaisista aina Lindemanniin asti löytävät meille "aatteen etsimäämme", ratkaisun neliöimisongelmaan.

[1]Transkendenttinen tarkoittaa järjen ja aistien ylittävää ilmiötä, ylimaallista. Termi 'transkendenttinen luku' esiintyy suomeksi myös muodossa 'transsendenttinen luku'. Nimitys 'transkendentaalinen' on Gottfried Leibnizin (1646–1716) käyttöönottama. Vuonna 1682 Leibniz osoitti, että $\sin x$ ei ole x:n algebrallinen funktio. [3, s. 74]

2 Esitietoja

Esittelemme aluksi tutkielmassa käytettyjä merkintöjä. Sitten käsittelemme polynomeja ja määrittelemme algebralliset ja transkendettiset luvut. Luvun lopuksi annamme analyysiin ja lukuteoriaan liittyviä lauseita. Jos jokin apulause tai määritelmä liittyy läheisesti todistukseen, johdamme sen todistuksen yhteydessä.

Merkintä ”luvut C_i” esiintyy tutkielmassa usein lausekkeiden yhteydessä. Tarkoitamme merkinnällä kaikkia niitä lukuja C_1, C_2, ..., jotka esiintyvät viitatussa lausekkeessa.

Käytämme A-keskiselle ja AB-säteiselle ympyrälle merkintää (A, B).

Rationaalilausekkeeksi kutsumme rationaalilukujen lauseketta, jossa käytämme vain rationaalisia operaatioita eli lisäämistä, vähentämistä, jakamista ja kertomista $(+, -, /, \times)$. Esimerkiksi lauseke $3-(5\cdot 3+1)/2$ on rationaalilauseke. Lauseke $3+\sqrt{5}$ taas ei ole rationaalilauseke, koska siinä on käytetty juurenottoa.

2.1 Polynomeista

Oletamme tunnetuiksi polynomiin liittyvät peruskäsitteet (vaikkapa termi ja aste). Annamme tässä määritelmän symmetrisille polynomeille [12, s. 14–16] sekä algebrallisille ja transkendenttisille luvuille [4, s. 44–46].

Määritelmä 2.1. *Symmetrinen polynomi* on polynomi P, joka pysyy samana, vaikka sen muuttujien paikkoja vaihdetaan.

Esimerkki 2.1. Polynomi $P(x, y) = x^2 + 2xy + y^2$ on symmetrinen, sillä $P(y, x) = y^2 + 2yx + x^2 = P(x, y)$.

Määritelmä 2.2. Symmetrisiä polynomeja $s_i = s_i(t_1, \dots, t_n)$, $i = 1, \dots, n$ kutsutaan symmetrisiksi perusfunktioiksi. Ne ovat

$$\begin{aligned} s_1 &= t_1 + t_2 + \cdots + t_n, \\ s_2 &= t_1t_2 + t_2t_3 + \cdots + t_{n-1}t_n, \\ &\vdots \\ s_n &= t_1t_2\cdots t_n. \end{aligned}$$

Esimerkki 2.2. Kolmen muuttujan x_1, x_2 ja x_3 symmetriset perusfunktiot ovat

$$\begin{aligned} s_1 &= x_1 + x_2 + x_3, \\ s_2 &= x_1x_2 + x_1x_3 + x_2x_3, \\ s_3 &= x_1x_2x_3. \end{aligned}$$

Todistuksissa tärkeä polynomeihin liittyvä apukeino on Taylorin polynomi.

Lause 2.1. *Polynomi $f(x)$, jonka aste on n, voidaan esittää kohdassa a Taylorin polynomikehitelmän $T_a(x)$ avulla seuraavasti*

$$f(x) = T_a(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n.$$

Todistus. Ks. [16, s. 81]. □

Määritelmä 2.3. Olkoon kompleksiluku x jonkin n-asteisen kokonaislukukertoimisen polynomiyhtälön

$$P(x) = C_0x^0 + C_1x^1 + \cdots + C_nx^n = 0,$$

juuri. Yhtälössä P ainakin yksi kertoimista C_i ei ole nolla. Sanomme, että tällöin luku x on (n-asteinen) *algebrallinen luku.*

Helposti näemme, että myös rationaalilukukertoimisilla polynomiyhtälöillä on algebrallinen juuri. Voimmehan laventaa rationaalikertoimet kokonaisluvuiksi, jolloin saamme määritelmämme polynomiyhtälön. Kertojamuodon lisäksi voimme algebran peruslauseen nojalla esittää yhtälön juurimuodossa

$$P(x) = c_n(x-x_1)(x-x_2)\cdots(x-x_n) = 0, \tag{2.1}$$

missä luvut c_n ja x_i ovat joitakin algebrallisia lukuja.

Esimerkki 2.3. Kokonaisluvut ovat algebrallisia. Mikä tahansa kokonaisluku k on polynomiyhtälön $-k + x = 0$ juuri. Rationaaliluku on määritelmänsä mukaan ensimmäisen asteen algebrallinen luku, koska mikä tahansa rationaaliluku $\frac{p}{q}$ on kokonaislukukertoimisen polynomiyhtälön $-p + qx = 0$ juuri. Irrationaaliluvuista esimerkiksi $\sqrt{2}$ on algebrallinen, koska se toteuttaa yhtälön $-2 + x^2 = 0$. Kompleksiluvuista yksinkertaisin esimerkki on imaginääriyksikkö i, joka on polynomiyhtälön $1 + x^2 = 0$ juuri.

Määritelmä 2.4. *Transkendenttiluku* on ei-algebrallinen luku eli sellainen kompleksiluku, joka ei ole minkään äärellisen kokonaislukupolynomin juuri.

Esimerkki 2.4. Jokainen transkendenttiluku on myös irrationaalinen, koska kaikki rationaaliluvut ovat algebrallisia lukuja.

2.2 Analyysia

Kompleksianalyysista on tarpeen tuntea muutamia määritelmiä ja lauseita.

Määritelmä 2.5. *Kompleksinen eksponenttifunktio* $\mathrm{e}:\mathbb{C}\to\mathbb{C}$ määritellään

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

Tälle pätevät kaikki tavalliset laskusäännöt (kuten $e' = e$ ja $\mathrm{e}^z\mathrm{e}^w = \mathrm{e}^{z+w}$) ja lisäksi

$$|\mathrm{e}^z| \leq \mathrm{e}^{|z|} \qquad \text{ja} \tag{2.2}$$

$$|z_1 + z_2| \leq |z_1| + |z_2|. \tag{2.3}$$

Lause 2.2 (Eulerin kaava)**.** *Olkoon x reaaliluku. Silloin pätee*

$$\mathrm{e}^{\mathrm{i}x} = \cos x + \mathrm{i}\sin x$$

ja erityisesti kun $x = \pi$

$$\mathrm{e}^{\mathrm{i}\pi} + 1 = 0.$$

Euler johti kaavat luvun e^z sarjakehitelmästä [10, s. 41–42].

Lause 2.3 (Differentiaalilaskennan väliarvolause)**.** *Olkoon f välillä $[a,b]$ derivoituva funktio. Tällöin $\exists c \in (a,b)$, jolle pätee*

$$f'(c) = \frac{f(b) - f(a)}{b - a}.$$

Todistus. Ks. [20, 197–199]. □

Lause 2.4. *Olkoon M jokin reaaliluku. Silloin*

$$\lim_{n\to\infty} \frac{M^n}{n!} = 0.$$

Todistus. Ks. [16, s. 96]. □

Lause 2.5. *Alkulukuja on ääretön määrä.*

Todistus. Ks. [8, IX kirja, väittämä 20]. □

3 Konstruktioiden geometria ja algebra

Siirrymme tässä luvussa kontruktioiden geometriasta niiden algebrallisiin ominaisuuksiin Hobsonin tapaan [10, 47–51].

3.1 Tasokonstruoinnista

Geometrisessa konstruktiotehtävässä pitää annettujen välineiden avulla konstruoida eli piirtää jokin tason piste, kun on annettu jokin alkuehto. Tutkielmassa välineemme ovat harppi ja viivain, ja alkuehtona on, että tasolta tunnetaan kaksi pistettä.

Reaalimaailmassa on tietysti mahdollista konstruoida mittaustarkkuuden rajoissa käytännön tarpeisiin riittävä ratkaisu [10, s. 33–35]. Matemaatikkoa kiinnostaa kuitenkin täsmällisyys. Katsomme siis harpin ja viivaimen ideaalisiksi, kun ongelmien ratkomisessa siirrymme piirustuksista teoreettiseen tarkasteluun. Viivaimella piirtämämme viiva on suora ilman kynän tekemää paksuutta. Samoin ideaalisella harpillamme saamme tarkasti oikeaan paikkaan oikeankokoisen ympyrän, jonka kehällä ei ole paksuutta. Todellisesta maailmasta otamme kuvioiden lisäksi mukaan aikarajoituksen: operaatioita saa tehdä vain äärellisen määrän. [22, s. 92–93]. Annamme nyt tasokonstruoinnin määritelmän.

Määritelmä 3.1. Tunnemme aluksi tasolta vähintään kaksi pistettä.

(Harppipostulaatti) Jos tunnemme kaksi eri pistettä A ja B, voimme piste A keskipisteenä piirtää ympyrän (A, B).

(Viivainpostulaatti) Jos tunnemme kaksi eri pistettä A ja B, voimme piirtää niiden kautta suoran $l = AB$.

(Äärellisyys) Voimme toistaa näitä kahta operaatiota äärellisen määrän.

Sanomme tätä menetelmää *harppi–viivain-konstruktioinniksi* tai lyhyesti *konstruktioksi.*

Voimme nimittää konstruktiota myös *tasokonstruoinniksi*, *geometriseksi konstruoinniksi* tai *euklidiseksi konstruktioksi.* Pisteet A ja B voivat olla jonkin yksikköjanan kaksi päätepistettä. Konstruoinnissa saamme konstruoitua uusia pisteitä, kun toistuvasti piirrämme ympyröitä ja suoria. Leikkaavista suorista saamme yhden uuden pisteen. Kahden ympyrän tai ympyrän ja suoran leikkauksesta saamme yksi tai kaksi uutta pistettä. Näiden uusien pisteiden avulla voimme piirtää uusia ympyröitä tai suoria ja saada uusia pisteitä kunnes lopulta päädymme pisteeseen P. [10, s. 48].

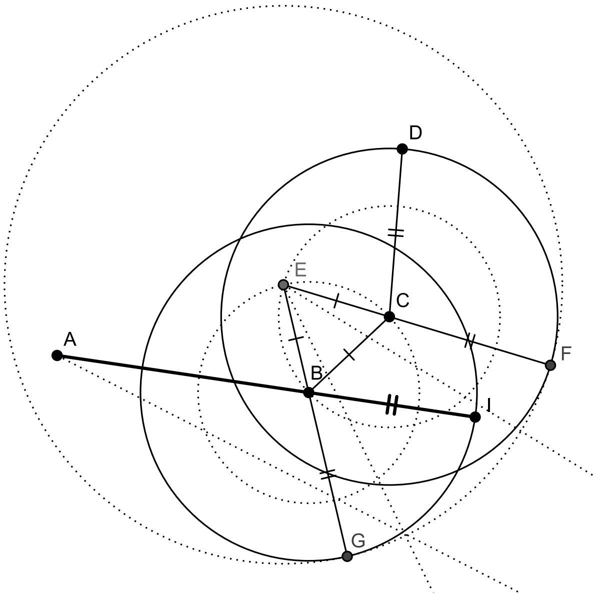
Tämän tutkielman konstruktiotehtävä on ympyrän neliöiminen.

Tehtävä 3.1. Olkoon annettu ympyrä kahtena pisteenä, joista toinen on ympyrän keskipiste, toinen sen kehällä oleva piste. Tästä janasta eli ympyrän säteestä on konstruoitava sellainen neliö, jolla on täsmälleen sama pinta-ala kuin annetulla ympyrällä. Kutsumme tätä *ympyrän neliöimiseksi.*

Ratkeavan konstruointiongelman täydellinen käsittely koostuu ratkaisun eli konstruktion vaiheiden esittämisestä, ratkaisun todistuksesta sekä olemassaolon ja ratkaisujen lukumäärän tarkastelusta [14, s. 80]. Koska tämä ongelma ei kuitenkaan ole ratkeava, meidän pitääkin todistaa se mahdottomaksi. Teemme sen johdannossa jo mainitsemallamme tavalla. Todistamme toisaalta, että vaaditun neliön kontruoimiseksi pitäisi konstruoida π, ja toisaalta, että lukua π ei voi konstruoida. Tarkastelemme seuraavaksi, mitä tarkoittaa luvun konstruoiminen.

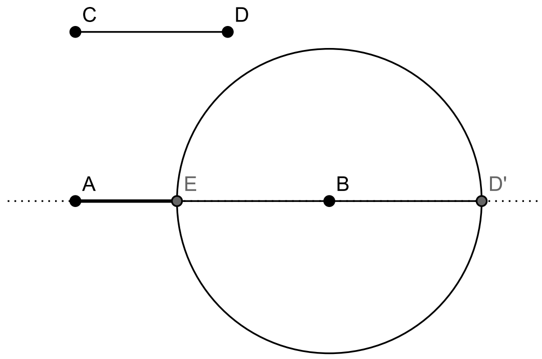
3.2 Peruslaskutoimitusten konstruktiot

Peruslaskutoimitusten geometriset vastineet todisti jo Eukleides Aleksandrialainen (300-luvulla eKr.) klassisessa *Alkeet*-teoksessaan (kreikaksi *Stoikheia*, latinaksi *Elementa*). Tässä luvussa esittelemme ratkaisut ja vain viittaamme niiden todistuksiin.



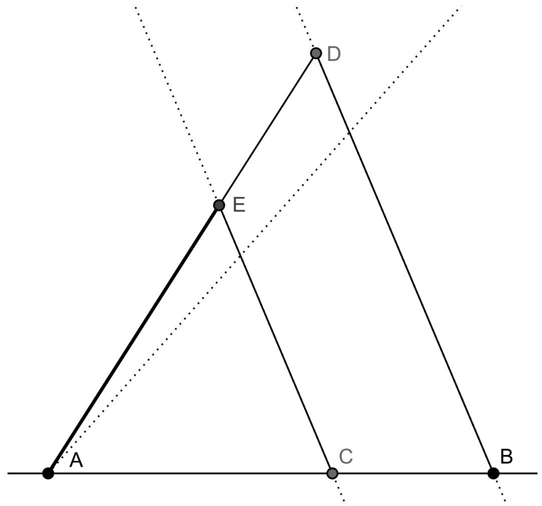
Kuva 1: Janojen yhteenlasku

Ratkaisu. Kahden janan AB ja CD **yhteenlasku** (kuva 1) konstruoidaan siten, että ensin muodostamme tasasivuisen kolmion piirtämällä ympyrät (B, C) ja (C, B) ja leikkauspisteeseen E janat BE ja CE. Piirrämme janan EC jatkeen ja ympyrän (C, D). Niiden leikkauspiste olkoon F. Piirrämme ympyrän (E, F), joka leikkaa janan EB jatkeen pisteessä G, ja piirrämme ympyrän (B, G). Sen ja janan AB jatkeen leikkauspiste olkoon I. Nyt AI on haluttu summa $AB + CD \cong AI$, koska BI on yhtenevä janan CD kanssa. Yhteenlasku on siis mahdollinen konstruointi. Todistuksen esittää Eukleides *Alkeissaan* [8, I kirja, 2. väittämä].



Kuva 2: Janojen vähennyslasku

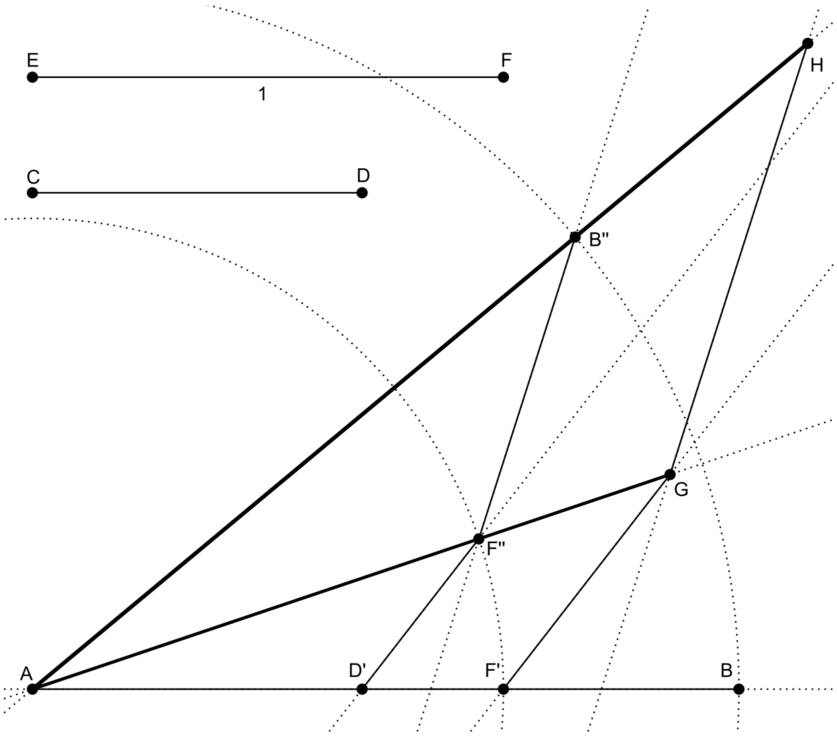
Ratkaisu. Oletamme ensin, että $AB \geq CD$. **Vähennyslaskussa** (kuva 2) voimme edellisen kohdan tapaan siirtää toisen janan ensimmäisen jatkeeksi. Siirrämme janan CD janan AB jatkeeksi, jolloin $CD \cong BD'$. Piirrämme ympyrän (B, D'). Suoran AD' ja ympyrän leikkauspiste olkoon E. Nyt erotus $AB - CD$ on yhtenevä janan AE kanssa. Vähennyslasku on siis mahdollinen konstruointi. [8, I kirja, 3. väittämä.].



Kuva 3: Janojen jakolasku

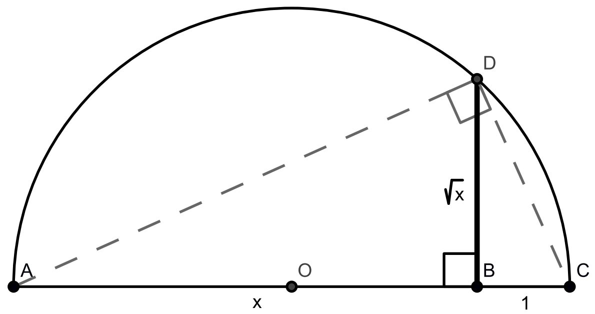
Ratkaisu. Kahden janan **jakolaskussa** AD/AB (kuva 3) olkoon AC yksikköjana. Piirrämme ensin suoran BD ja sitten yhdensuuntaisen suoran pisteen C kautta. Tämä suora leikkaa suoran AD pisteessä E. Nyt yhdenmuotoisista kolmioista saamme $AE/AC \cong AD/AB$ eli että $AE \cong AD/AB$. Jakolasku on siis mahdollinen konstruointi. [14, s. 81].

Ratkaisu. Janojen **kertolaskussa** (kuva 4) $AB \cdot CD$ käytämme hyväksi sitä lukujen ominaisuutta, että tulo on yhtäsuuri kuin tekijän käänteisluvulla jakaminen. Olkoon janat AB, CD ja yksikköjana EF. Siirrämme ensin



Kuva 4: Janojen kertolasku

janat CD ja EF samalle suoralle AB jolloin $AD' \cong CD$ ja $AF' \cong EF$. Sitten jakolaskun piirtomenetelmällä jaamme janan $CD \cong AD'$ suhteeseen $EF/CD \cong AG$, jonka jälkeen jaamme taas suhteelle $AB/AG \cong AH$. Nyt on $AH \cong AB \cdot CD$ ja kertolasku on siis mahdollinen konstruointi.



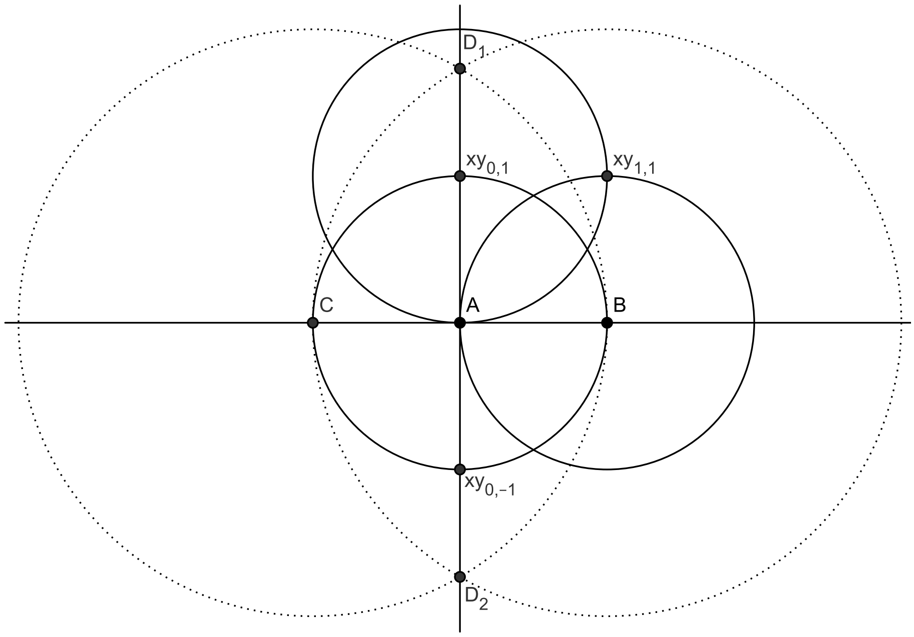
Kuva 5: Janan neliöjuuri

Ratkaisu. **Neliöjuuren** (kuva 5) janasta AB saamme, kun lisäämme janan jatkeelle yksikköjanan BC. Puolitamme sitten janan AC, josta saamme keskipisteen O. Piirrämme puoliympyrän (O, C) ja janan AC normaalin pisteen B kautta. Nimeämme normaalin ja puoliympyrän leikkauspisteen pisteeksi D. Nyt luvun $|AB| = x$ neliöjuuri on $|BD| = \sqrt{x}$. Neliöjuuren otto on siis mahdollinen konstruointi. [14, s. 82].

Näin olemme yllä osoittaneet, että voimme konstruoida kaikki peruslaskutoimitukset ja neliöjuuren oton.

3.3 Koordinaatisto

Määritelmä 3.2. Sanomme, että piste P on *konstruoituva*, jos on olemassa sellainen konstruktio, jolla piste saadaan määritettyä.



Kuva 6: Koordinaatiston konstruoiminen.

Piste P voidaan esittää myös koordinaatteina. Konstruktiotehtävässä on annettu kaksi tason pistettä A ja B. Voimme pitää niitä yksikköjanana ja konstruoida niistä tasolle koordinaatiston.

Kun piirrämme (kuva 6) annettuihin pisteisiin ympyrän (A, B) ja suoran AB, saamme pisteen C. Kun piirrämme ympyrät (C, B) ja (B, C), saamme ympyröiden leikkauspisteisiin uudet pisteet D_1 ja D_2. Piirtämällä suoran D_1D_2 saamme y-akselin. Tämän ja x-akselin eli suoran AB leikkauspiste A on origo. Ympyrän (A, B) ja y-akselin leikkauspisteet olkoot $xy_{0,1}$ ja $xy_{0,-1}$. Ympyröiden $(xy_{0,1}, A)$ ja (B, A) toiseen leikkauspisteeseen saamme koordinaattipisteen $xy_{1,1}$ akseleiden ulkopuolelle. Näiden ympyröiden piirtämistä jatkamalla saisimme kokonaislukupisteet. Jos selvittäisimme sitten näiden pisteiden keskipisteet ja jatkaisimme jakamista äärettömästi, saisimme lopulta piirrettyä kaikki pisteet.

Voimme pitää pistettä koordinaattiparina (x, y). Pisteen P konstruoinnissa saamme siis konstruoitua kaksi lukua, pisteen koordinaatit.

Määritelmä 3.3. Kutsumme konstruoituvan pisteen P koordinaatteja *konstruoituviksi luvuiksi.*

Koska rajoitumme tekemään vain äärellisen määrän piirtoja, saamme konstruoitua vain tietyt pisteet. Seuraavaksi todistamme, millaisia lukuja nämä konstruoituvat luvut oikein ovat.

3.4 Analyyttista geometriaa ja algebraa

Tässä todistamme konstruoinnin yhteydestä algebraan, joka pohjautuu koordinaatiston avulla saatuun analyyttiseen geometriaan.

Lause 3.1. *Piste P on konstruoituva jos ja vain jos sen koordinaatit saadaan esitettyä annettujen pisteiden koordinaattien funktiona käyttämällä äärellisen määrän operaatioita $+$, $-$, $/$, $\times$ ja $\sqrt{}$.*

Todistus. Kun meille annetaan r pistettä, on koordinaatteja silloin $2r$ eli $a_1, a_2, \ldots, a_{2r}$. Jotta saisimme ympyröiden ja suorien leikkauspisteet, meidän tulee asettaa kahdeksan koordinaattia (neljästä eri pisteestä) joko kahden suoran, kahden ympyrän tai suoran ja ympyrän yhtälöihin.

Suoran yleinen yhtälö on

$$y = kx + b, \tag{3.1}$$

missä k ja b ovat tiedettyjen pisteiden muodostamia rationaalilausekkeita: Luku k voidaan laskea suoran koordinaattimuodosta $y_1 - y_2 = k(x_1 - x_2)$, jossa k on kulmakerroin $\Delta y/\Delta x = (y_1 - y_2)/(x_1 - x_2)$. Luku b on $k \cdot x_2 + y_2$. Kahden muotoa (3.1) olevan yhtälön ratkaisuna saamme kahden leikkauspisteen koordinaatit, jotka ovat rationaalilausekkeita.

Ympyrän yleinen yhtälö taas on koordinaattimuodossa

$$(x - k_x)^2 + (y - k_y)^2 = (r_x - k_x)^2 + (r_y - k_y)^2, \tag{3.2}$$

missä vakiot k_i ovat keskipisteen ja r_i kehältä tunnetun pisteen koordinaatit. Suoran ja ympyrän leikkauksessa teemme yhtälöparin ja ratkaisemme sijoittamalla yhtälön (3.1) yhtälöön (3.2). Saamme eliminoitua toisen muuttujan, ensin vaikkapa muuttujan y. Koordinaatti x on siten muotoa $A \pm \sqrt{B}$. Myös y on samaa muotoa. Yhtälössä A ja B ovat rationaalilausekkeita.

Kahden ympyrän leikatessa on kyseessä kaksi kaavan (3.2) muotoista yhtälöä. Ratkaisemalla yhtälöparin saamme kaksi leikkauspistettä. Tilanne on ympyrän ja suoran leikkauksen kaltainen ja myös tässä koordinaatit ovat muotoa $A \pm \sqrt{B}$.

Pisteen P ja sen koordinaattien konstruoimisessa näitä toimintoja yhdistetään äärellinen määrä. Kuten yllä totesimme, konstruoinnit käsittävät rationaalisia operaatioita ($+$, $-$, $/$, $\times$) tai juurenottoa ($\sqrt{}$). Saimme todistettua seuraavaa: jos piste saadaan konstruoitua, käytetään rationaalioperaatioita ja juurenottoa.

Väite on tosi myös toiseen suuntaan (jos käytetään rationaalioperaatioita ja juurenottoa, saadaan konstruoitua piste), koska rationaalioperaatiot ja juurenotto kuuluvat sallittuihin tasokonstruktioihin (ks. luku 3.2). □

Lause 3.2. *Annetuista pisteistä konstruoituva piste on sellainen, jonka koordinaatit ovat asteeltaan luvun 2 potenssia olevien polynomien juuria. Tällaisen polynomin termien kertoimet ovat annettujen pisteiden koordinaattien rationaalilausekkeita.*

Todistus. Lauseen todistus (vrt. [10, s. 51–52]) on jatkoa edellisestä todistuksesta, jossa totesimme, että leikkausten tuloksena saatavan pisteen koordinaatit ovat lausekkeen $A \pm \sqrt{B}$ muotoisia. Jonkin leikkauspisteen x-koordinaatti voisi esimerkiksi olla

$$x = \frac{\sqrt{a + \sqrt{c + ef}} + \sqrt{d + \sqrt{b}}}{\sqrt{a} + \sqrt{b}} + \frac{b + \sqrt{q}}{\sqrt{r}}, \tag{3.3}$$

missä $a, b, \ldots, r$ ovat rationaalilausekkeita [13, s. 5].

Kun operaatioita on tehty paljon, niiden yhdistelmänä saamme konstruoidun pisteen x- ja y-koordinaateiksi lausekkeen

$$x = a + b\sqrt{c_1 \pm \sqrt{c_2 \pm \sqrt{c_3 + \cdots}}} + b'\sqrt{c'_1 \pm \sqrt{c'_2 \pm \sqrt{c'_3 + \cdots}}} + \cdots \tag{3.4}$$

muotoisia lausekkeita. Oikean puolen kirjaimet kuvaavat annettujen koordinaattien rationaalilausekkeita. Sisäkkäisiä neliöjuuria on äärellinen määrä, koska operaatioita on tehty äärellinen määrä. Lausekkeesta olemme kertomalla poistaneet nimittäjät, ja luvut a, b, c_i, b', c'_i, ... ovat rationaalilausekkeita.

Merkitkäämme nyt sisäkkäisten neliöjuurien määrää vakiolla m ja nimittäkäämme sitä juuriluvuksi[2]. Merkitkäämme x-koordinaatin lauseke

$$x = a + b\sqrt{C} + b'\sqrt{C'} + \cdots, \tag{3.5}$$

missä a, b, C, b', C', ... ovat rationaalilausekkeita. Muuttujien C, C', ... juuriluku on siten enintään $m - 1$.

Lausekkeen C:n ympäriltä voimme poistaa neliöjuuren, kun siirrämme muut termit vasemmalle puolelle ja korotamme yhtälön toiseen potenssiin

$$(x - a - b'\sqrt{C'} + \cdots)^2 = b^2 C. \tag{3.6}$$

Kun laskemme vasemman puolen auki, saamme polynomin, jossa x:n korkein potenssi on 2. Siirrämme vielä termin b^2C vasemmalle, niin saamme polynomin muotoon $P + P'\sqrt{C'} = 0$. Binomilauseen perusteella, siis kertomalla polynomin lausekkeella $P - P'\sqrt{C'}$, voimme merkitä $P^2 - P'^2C' = 0$. Nyt polynomin aste on $2^2 = 4$ eikä tässä polynomissa enää ole neliöjuurta $\sqrt{C'}$ vaan vain C'. Kun jatkamme tätä prosessia, saamme eliminoitua kaikki

[2]Lähde [10] käyttää sanaa rank, jonka suora suomennos olisi 'aste'. Koska 'aste' on jo varattu polynomin ominaisuudelle, käytämme tässä kuvaavampaa nimeä 'juuriluku'.

uloimmat neliöjuuret ja siis juuriluvun yhden pienemmäksi. Näin tuloksena on polynomi, joka on asteeltaan luvun 2 potenssi (2^s) ja jonka kertoimet ovat muuttujien a, b, C, b', C', ... rationaalilausekkeita. Lauseke on muotoa

$$L_1 x^{2^s} + L_2 x^{2^s - 1} + \cdots = 0 \tag{3.7}$$

ja siinä L_1, L_2, ... ovat juuriluvultaan enintään $m - 1$.

Jos neliöjuuria yhä löytyy, jatkamme eliminoimista. Jos joillakin kertojilla L_1, L_2, ... on jokin juuri $\sqrt{K}$, kaava tulee muotoon

$$\sqrt{K}(b_1 x^{2^s} + \cdots) + (b_1' x^{2^s} + \cdots) = 0. \tag{3.8}$$

Kun taas teemme edellä kuvatun eliminointiprosessin, niin polynomi tulee muotoon, jossa ei ole neliöjuurta $\sqrt{K}$. Polynomin aste on silloin 2^{s+1}. Kun teemme prosessin jokaiselle juurelle $\sqrt{K}$, eliminoimme ne kaikki. Saamme polynomin, jossa jokaisen kertoimen juuriluku on $\leq m - 2$. Polynomin aste on jokin luvun 2 potenssi. Jatkamme prosessia ja lopulta saamme polynomin muotoon, jossa neliöjuuria ei esiinny. Silloin jokaisen termin kertoimen juuriluku on 0.

Tällaisen polynomin aste on jokin luvun 2 potenssi. Termien kertoimet ovat annettujen pisteiden koordinaattien rationaalilausekkeita. Polynomin juuri on konstruoidun pisteen koordinaatti. Siis lause on tosi. □

4 Ympyrän neliöimisen historia

Matemaatikot kertovat usein oikeutetusti ylpeillen antiikin kreikkalaisten geometriasta ja muista tuhansia vuosia vanhoista mutta silti yhtä pätevistä matematiikan saavutuksista. Matematiikan historiassa on silti omat nöyryyttä opettavat tarinansa, joista tutkielmamme aihe ympyrän neliöiminen on kenties merkittävin.

Yhdysvaltalainen matematiikan historioitsija Florian Cajori (1859–1930) piti matematiikan historiaa nimenomaan opettavaisena. Matematiikan historiakirjansa [6] esipuheessa hän kirjoittaa, että historia opettaa matemaatikkoja muun muassa välttämään aiempien tekijöiden virheitä ja käymään ongelmiin käsiksi epäsuorasti, jos suora hyökkäys ei onnistu.

Hän nostaa ympyrän neliöimisen esimerkiksi matematiikan ongelmasta, jossa tämä metodi ei pitkään toteutunut. Yli kahdentuhannen vuoden ajan ”ympyränneliöijien armeija” yritti geometrian keinoin todistaa neliöimistä, kunnes 1600-luvulta alkaen analyysi tarjosi toisen reitin ongelman luo ja lopulta auttoi selvittämään sen 1800-luvun lopulla. [6, s. 2–3].

Ympyrän neliöiminen voidaan ajatella joko geometrisen konstruktion keksimiseksi tai ympyrän alan suuruuden tai kehän pituuden mittaamiseksi [22, s. 92–93]. Hobson aloittaakin ympyrän neliöimisen historian egyptiläisestä Rhindin papyruksesta noin vuodelta 1600 eKr. Siinä kirjuri Ahmose kertoo, että ympyrän ala on sama kuin sellaisen neliön, jonka sivu on $\frac{8}{9}$ ympyrän halkaisijasta. Tämä vastaa piin arvoa $\frac{256}{81} \approx 3,16049\ldots$ [10, s. 11].

Intialaisissa Veda-teksteihin kuuluvissa Baudhayanan, Manavan, Apastamban ja Katyayanan sulvasutroissa (köyden säännöt), joista varhaisin tehtiin noin 800 eKr., annetaan ohjeita alttarien rakentamisesta ja niihin liittyvästä geometriasta. Niissä jokaisessa käsitellään myös ympyrän muunnosta neliöksi ja neliön muunnosta ympyräksi. Sutrojen tekijöistä ei tiedetä juuri mitään muuta kuin nimen ja ajoituksen. Tekijät eivät tehneet tarkkojen ja likimääräisten ratkaisujen välille mitään eroa eivätkä todistaneet menetelmiään. [4, s. 299–301], [19].

Ensimmäiseksi matemaatikoksi kutsutaan silti Thales Miletolaista (n. 636–546 eKr.), koska hänen kerrotaan ensimmäisenä todistaneen lauseita. Tiedon todenperäisyys on epävarma mutta matemaattisen todistamisen tiedetään silti alkaneen Kreikassa noin 600-luvulla eKr. [4, s. 80].

Me sivuutamme niin ympyränmittaajat, joista Hobson kirjoittaa, kuin sulvasutrojen rakennusohjeet, joiden tuloksia ei todisteta. Emme kuvaile Arkhimedeen ja hänen seuraajiensa, intialaisten, kiinalaisten ja myöhemmin eurooppalaisten saavutuksia piin likiarvon laskemisessa. Nämä ratkaisut monesti perustuvat ympyrän sisään ja ympärille piirrettyihin monikulmioihin. [10, s. 16–24]. Sivuutamme heidät ja keskitymme yrityksiin löytää ja todistaa täsmällinen geometrinen konstruktio sekä käsittelemme ratkaisuun johtaneiden matematiikan alueiden historiaa.

4.1 Antiikki

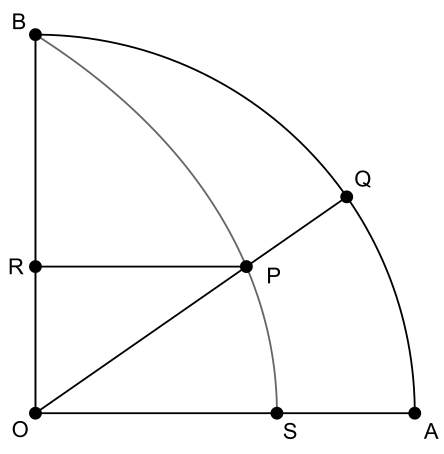
400-luvun puolivälin jälkeen antiikin kreikkalaiset alkoivat pohtia geometriassa kolmea kuuluisaa ongelmaa: ympyrän neliöimistä, kulman kolmiajakoa ja kuution kahdentamista. Kaikkien niiden konstruoiminen harpilla ja viivaimella todistettiin mahdottomaksi vasta yli 2000 vuotta ensimmäisten ratkaisuyritysten jälkeen. [4, s. 107].

Tiettävästi ensimmäisenä ympyrää yritti neliöidä kreikkalainen Anaksagoras Klatsomenailainen (n. 500–428 eKr.). Plutarkhos mainitsee, että tämä oli vangittuna viruessaan noin vuonna 450 eKr. syventynyt ongelmaan. Ei ole tiedossa, millainen ja kuinka likimääräinen tai väärä Anaksagoraan ratkaisu oli. [18], [10, s. 14], [4, s. 105–106].

Heathin mukaan Oinopides Khioslainen (n. 490 – n. 420 eKr.) saattoi olla ensimmäinen joka rajoitti geometristen konstruktioiden ratkaisemisen harpin ja viivaimen käyttöön [9, s. 175–176]. Boyer ja Hobson eivät mainitse Oinopidesta vaan toteavat, että Platon (427–347 eKr.) luultavasti vaikutti siihen, että konstruoinneissa sai käyttää vain ympyrää ja suoraa, jotka vastaavat käytännön tasolla harppia ja viivainta. [10, s. 16], [4, s. 138].

Plutarkhos kertoo Platonin olleen närkästynyt mekaanisten apuvälineiden käyttämisestä geometriassa. Tämä halusi pitää eron puhtaan ajattelun geometrian ja käytännön maailman mekaniikan välillä. Boyer arvelee, että Platonin halun takana oli pikemmin muotojen symmetria kuin harpin ja viivaimen yksinkertaisuus. [10, s. 16], [4, s. 138]. Beckmanin mielestä tämä tulkinta on roskaa. Hän toteaa, että kreikkalaisia kiinnosti vain totuus ja se, kuinka lauseet saadaan johdettua aksioomista. [1, s. 52–54].

Antiikin Kreikassa keksittiin erilaisia apuvälineitä tai käyriä ja saatiin niillä neliöityä ympyrä. Dinostratus (n. 390 – n. 320 eKr.) käytti ratkaisuissaan Hippiaan (n. 460 – n. 400 eKr.) noin vuonna 420 eKr. kehittämää kvadratrix-käyrää ja Arkhimedes (287–212 eKr.) spiraalikäyrää.



Kuva 7: Kvadratrix on pisteen P piirtämä ura.

Olkoon P janan OQ ja janan OB pisteen R kautta kulkevan normaalin leikkauspiste. Kvadratrix (kuva 7) on pisteen P piirtämä ura, kun pisteet Q ja R lähtevät alkupisteistään A ja O tasaisella nopeudella siten, että ne saavuttavat pisteen B yhtäaikaa. Käyrä leikkaa janan OA kohdassa $2OA/\pi = OS$. Luvun π voisi nyt konstruoida piirtämällä jakolaskun $2OA/OS$. [10, s. 4].

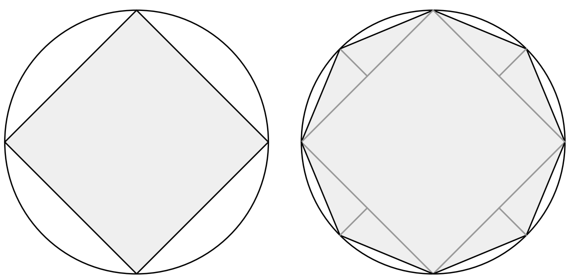
Tällaiset konstruktiot ovat mahdollisia harpilla ja viivaimella, jos tehdään ääretön määrä piirtoja. Kreikkalaisille äärettömyys oli käsittämätöntä eikä tällaisia ratkaisuja voinut johtaa aksioomista. Siksi ne eivät kelvanneet kreikkalaisille ongelman todelliseksi ratkaisuksi vaan etsintä jatkui ja samalla keksittiin uusia käyriä. Etsintä ei ollut turhaa vaan samalla matematiikka kehittyi. [4, s. 113–115, 150–152], [1, s. 52–54].

Täsmälliseen todistukseen antiikki ei kyennyt, mutta antiikin lopulla Pappos Aleksandrialainen (n. 290 – n. 350 jKr.) jo aavisti, että ongelmaa ei voi ratkaista sallituin menetelmin. Noin vuonna 320 hän kirjassaan *Kokoelma* (*Synagoge*) jakaa konstruoitavat ongelmat "taso-, avaruus- ja viivaongelmiin". Taso-ongelmat selviävät ympyrällä ja suoralla, avaruusongelmiin tarvitaan muita kartioleikkauksia ja viivaongelmiin muita käyriä. Hän luetteli erilaisia kolmen suuren ongelman onnistuneita konstruktioita, joissa käytettiin muita välineitä kuin harppia ja viivainta. Sitten hän esittää, että kulman kolmiajako ja kuution kahdentaminen kuuluvat avaruusongelmiin ja ympyrän neliöiminen taas viivaongelmiin. [4, s. 269].

Tarkastelemme seuraavaksi kahta virheellistä antiikin konstruktiota 400-luvulta eKr.

4.2 Antifon ja Hippokrates

Antifon sofisti (480–411 eKr.) oli Anaksagoraan aikalainen. Ympyrän neliöimisen historiaan hän on jäänyt virheellisen neliöinnin ansiosta. Hän piirsi ympyrän sisään neliön (kuva 8). Sitten hän puolitti sivut, piirsi sivuille keskinormaalit ja leikkauspisteiden kautta janat. Hän sai näin kahdeksankulmion. Sivujen lisääminen vastaavalla tavalla näytti muuttavan monikulmion piirin yhtä suureksi kuin ympyrän kehän.

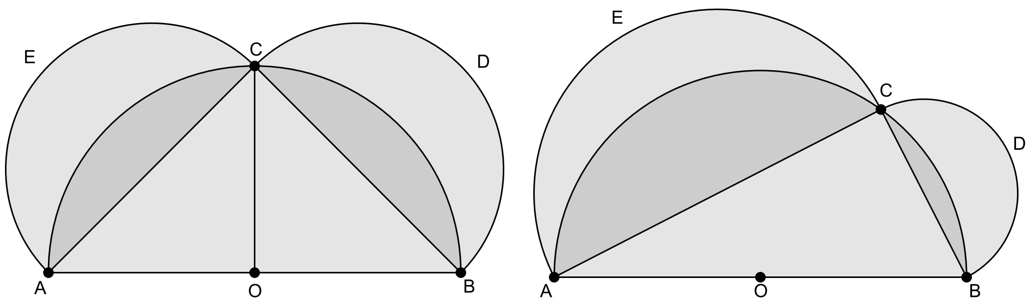


Kuva 8: Antifonin konstruktion ensimmäiset vaiheet.

Antifon arveli siten saavansa monikulmiosta yhtä suuren kuin ympyrä oli. Koska monikulmion saattoi neliöidä, niin hän päätteli, että ympyränkin voisi. Bryson Herakleialainen (469–399 eKr.) kehitti Antifonin todistusta ja arveli, että ympyrän ala olisi ympyrän ulkopuolelle ja sisäpuolelle piirrettyjen monikulmioiden alan keskiarvo. [10, s. 15].

Antifonin tarkastelun huomasivat virheelliseksi jo aikalaiset. Aristoteles (384–322 eKr.) huomauttaa *Fysiikassaan*, ettei pidä olla huolissaan Antifonin todistuksen kumoamisesta, koska todistus on matematiikan periaatteiden vastainen. Hippokrateen puolikuutodistuksen kumoamiseen hän kuitenkin kehottaa. [17].

Hippokrates Khioslainen (n. 470 – n. 410 eKr.) oli kauppias, joka joutui ryöstön kohteeksi ja ryhtyi rahansa menettäneenä tutkimaan geometriaa. Hän oli ensimmäinen, joka teki geometrian lauseiden yleisesityksen *Alkeet*-teoksessaan. Kirja on sittemmin kadonnut, mutta tieto Hippokrateen kuunsirpeistä on jäänyt jälkipolville. Hippokrates onnistui vuonna 430 eKr. neliöimään kahden erisäteisen ympyrän rajaamat kuunsirpin muotoiset alueet. [4, s. 108–112].

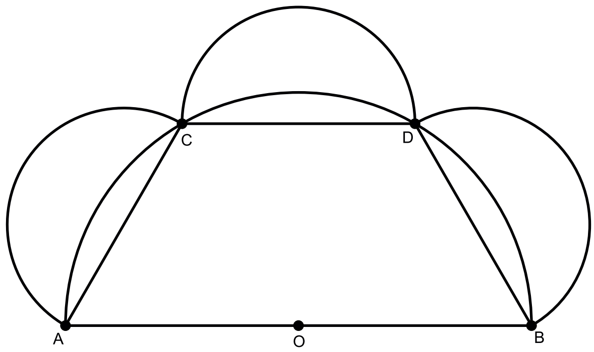


Kuva 9: Hippokrateen kuunsirpit.

Kuvan 9 kolmio ΔABC on suorakulmainen ja tasakylkinen. Sen kyljille on piirretty kaksi puoliympyrää. Kaaren $A\overset{\frown}{C}E$ ja tummanharmaan segmentin väliin jäävä vaaleanharmaa kuunsirpin muotoinen alue on vaaleanharmaan suorakulmaisen ja tasakylkisen kolmion ΔAOC alan kokoinen. Jos kolmio ΔABC ei ole tasakylkinen, molempien kuunsirppien yhteenlaskettu ala on kolmion ΔABC kokoinen. Kolmion alan voi neliöidä, joten samalla neliöidään myös kuunsirpit. [10, 15], [4, s. 108–112].

Hippokrates yritti löytää muitakin neliöitäviä kuunsirppejä. Jos sellainen löytyisi, hän ehkä voisi neliöidä ympyränkin. Kuvan 10 nelikulmiossa on $AB = BC = CD = OA$. Suunnikkaan ala on yhtä suuri kuin kolmen kuunsirpin ja lisäksi yhden pienen puoliympyrän alan summa. Jos tämän saisi neliöityä, niin koko ympyränkin voisi.

On epävarmaa, luuliko Hippokrates pystyvänsä neliöimään ympyrän. Yhden näkemyksen mukaan hän luuli kykenevänsä neliöimään kaikki kuunsirpit ja siten myös ympyrän. Toiset taas arvelevat, että hän tiesi että vain tietyt kuunsirpit voi neliöidä. Mielikuvituksellisin ehdotus on, että Hippokrates olisi



Kuva 10: Hippokrateen kolme kuunsirppiä.

huijannut muita ja uskotellut onnistuneensa. [10, s. 15], [4, s. 108–112].

4.3 Antiikista uuteen aikaan

Antiikin kreikkalaiset eivät olleet ainoita neliöijiä. Myös intialaiset, kiinalaiset ja arabialaiset matemaatikot tutkivat ongelmaa ympyränmittaajina ja saivat yhä tarkempia likiarvoja piille. [10, 22–24].

Antiikin jälkeen matematiikka kehittyi muualla kuin Euroopassa. Noin kuusisataa vuotta Pappoksen jälkeen arabialainen ibn al-Haytham eli tunnetummin Alhazen (965–1039) eräässä teoksessaan lupasi neliöivänsä ympyrän. Koska todistusta ei koskaan ilmestynyt, hän luultavasti luovutti huomattuaan, ettei pysty ratkaisemaan ongelmaa. [17].

Keskiajan eurooppalaisen matematiikan tasoa kuvaa vuoden 1050 yritys neliöidä ympyrä. Franco von Lüttich (de Liège) julkaisi tuolloin kirjansa *De quadratura circuli*, jossa esiintyneen todistuksen perustana oli että piin lukuarvo on 22/7. Hän aloitti ympyrästä, jonka halkaisija oli 14, kehä $14 \cdot 22/7 = 44$ ja ala $1/2 \cdot 7 \cdot 44 = 154$. Ongelma oli nyt saada piirrettyä samankokoisen neliön sivu, nimittäin $\sqrt{154}$. Hän totesi, ettei saa tehtyä sitä numeerisesti, mutta esitti geometrisen konstruktion. [5, s. 9–10]. Euroopan matematiikka tarvitsi selvästi antiikin Kreikan tietämystä kehittyäkseen [17].

Keskiajan lopulla matematiikan kehityksen painopiste siirtyi taas Eurooppaan. 1100- ja 1200-luvulla käännettiin ahkerasti antiikin viisaiden ja arabialaisten kirjoituksia ja arabialaisten välityksellä nykyisin käytetyt numeromerkit levisivät Eurooppaan. [4, s. 357–362].

Nikolaus Cusalainen (1401–1464) oli ensimmäisiä neliöimiseen ryhtyneitä uuden ajan eurooppalaisia. Hän esitti ratkaisuyrityksen, joka perustui ajatukseen siitä, että minimillä ja maksimilla on yhteys. Monikulmiot kolmio, jossa sivuja pienin määrä, ja ympyrä, jossa niitä on eniten, olivat Cusalaisen filosofiassa toisiinsa yhteydessä. Hän kehitteli niistä ympyrän sisään ja ympärille piirrettyihin monikulmioihin perustuvan neliöinnin, jonka Regiomontanus (1436–1476) osoitti virheelliseksi. [4, s. 385].

Algebran ja geometrian yhteys vahvistui, kun Rene Descartes (1596–1650) julkaisi *Metodin esityksen* ja *Geometrian*. Descartes esitti jälkimmäisessä kirjassaan peruslaskutoimitusten konstruoinnit ja keskittyi algebran soveltamiseen geometrisissa ongelmissa. Descartesin ja muiden aikalaisten ansiosta koordinaatisto ja analyyttinen geometria kehittyivät. Descartes lisäksi todisti, vaikkakin vajavaisesti, kaksi muuta antiikin suurta ongelmaa eli kulman kolmijaon ja kuution kahdentamisen mahdottomiksi. [4, s. 474–479]. Täsmällinen todistus näistä saatiin yhtälöteorian kehityttyä 1700- ja 1800-luvun vaihteessa. Todistuksen teki ranskalainen Pierre Wantzell (1814-48) vuonna 1837. [15]

1600-luvulla monikin teki virheellisiä konstruointeja erityisesti vasta keksittyjen differentiaali- ja integraalianalyysin innoittamina, muiden muassa Gregorius St. Vincentläinen (1584–1667). Tasomenetelmistä eroavia ratkaisuja tehtiin onnistuneestikin mutta varsinaisessa neliöimisessä ei tietenkään onnistuttu. Skotti James Gregory (1638–1675) piti neliöintiä mahdottomana. Hän oli ensimmäinen, joka yritti todistaa neliömistä mahdottomaksi piin algebrallisten ominaisuuksien nojalla. Christiaan Huygens (1629–1695) sen sijaan piti neliöimistä mahdollisena ja uskoi että π olisi algebrallinen. Hän osoitti todistuksen virheet ja asiasta kehkeytyi pieni kiista heidän välilleen. Se ratkesi oikean otaksuman mutta väärän todistuksen tehneen Gregoryn hyväksi 1800-luvun lopulla. [10, s. 31], [17], [4, s. 543–544].

Suurempi kiista oli englantilaisten filosofi Thomas Hobbesin (1588–1679) ja matemaatikko John Wallisin (1616–1703) välinen. Boyer ja Beckman sivuuttavat Hobbesin mainitsemalla yliolkaisesti, että Hobbes omahyväisenä mutta kehnona matemaatikkona julkaisi vääriä neliöintejä ja että Wallis olisi jättänyt Hobbesin huomioimatta. [4, s. 541], [1, s. 135]. Douglas Jesseph kertoo kiistasta enemmän kirjassaan *Squaring the circle: the war between Hobbes and Wallis*. Wallis lyttäsi Hobbesin konstruoinnit ja monta muutakin Hobbesin teosta. Tarinaan liittyy myös uskonnollis-poliittisia sävyjä. Wallis presbyteerinä halusi vastustaa Hobbesin ateistisina ja turmiollisina pitämiään ajatuksia. [11]. Jessephin kirjan liitteinä on myös Hobbesin virheellisiä neliöintejä, esimerkiksi [11, s. 380].

Kaikki ratkeavat tasokonstruktiotehtävät voi ratkaista myös pelkästään harpilla tai jopa käyttämällä harppia vain kerran ja muuten viivainta. Viivaimen tarpeettomuuden keksi ensimmäisenä vuonna 1672 tanskalainen Georg Mohr (1640–1697). Mohr jäi kuitenkin vaille huomiota ja kunnian tarpeettomuuden osoittamisesta sai italialainen Lorenzo Mascheroni (1750–1800), joka todisti asian vasta vuonna 1797. [4, s. 521–522]. Harpin tarpeettomuuden, sen jälkeen kun sitä on käytetty kerran, taas todisti saksalainen Jakob Steiner (1796–1863). [4, s. 753], [14, s. 130].

4.4 Uuden ajan keinot

Skotlantilainen John Napier (1550–1617) keksi logaritmit 1500-luvun lopulla ja julkaisi tulokset vuonna 1615 teoksessaan *Mirifici logarithmorum canonis descriptio* eli *Ihmeellisen logaritmisäännön kuvaus*. Napier kehitti sanan 'logarithm' kreikan sanoista 'logos' ja 'arthimos', suhde ja luku. Napierin logaritmin määritelmästä logaritmijärjestelmän kantaluvuksi saadaan noin 1/e. [4, s. 440–443]. Lukua e kutsutaan Neperin (Napierin) luvuksi ja sen kantaisia logaritmeja luonnollisiksi logaritmeiksi.

Nimitystä "luonnollinen logaritmi" käytti Nicolaus Mercator (1620–1687) kirjassaan *Logarithmotechnia*, jonka hän julkaisi vuonna 1668. Hän esittää siinä sarjan (Mercatorin sarjan)

$$\ln(1+x) = \frac{x}{1} - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots$$

ja kutsui sarjan antamia arvoja luonnollisiksi logaritmeiksi. [4, s. 545–546]. Koska sarjassa ovat luonnolliset luvut eksponenteissa ja nimittäjissä, on nimitys varsin luonnollinen. Boyerin mukaan Mercator omaksui termin Pietro Mengolilta (1625–1686), joka vuoden 1672 kirjassaan *Il problema della quadratura del circolo* havaitsi sarjan pätevän, kun $x = 2$ [4, s. 522].

Kompleksilukujen olemassaoloa ounasteli jo Gerolamo Cardano (1501–1576), kun hän vuoden 1545 kirjassaan *Ars magna* (suuri taide eli algebra) esitti negatiivisia juuria sisältäviä lukuja yhtälöiden ratkaisuksi. *Ars magnalla* oli myös valtava innostava vaikutus, jopa niin, että vuotta 1545 saatetaan joskus pitää nykymatematiikan alkuna. [4, 399–405]. 1700-luvulle tultaessa kompleksilukujen teoria oli kehittynyt tarpeeksi, jotta Euler pääsi vaikuttamaan ympyrän neliöimisen historiaan.

Sveitsiläinen Leonhard Euler (1707–1783) johti luvun e^z sarjakehitelmästä Eulerin kaavan $\mathrm{e}^{\mathrm{i}\pi} + 1 = 0$. Hän julkaisi kaavan yleistetyn version $\mathrm{e}^{\mathrm{i}x} = \cos x + \mathrm{i} \sin x$ vuonna 1748 tunnetuimmassa oppikirjassaan *Introductio in analysin infinitorum*. Neperin luvun yhteys piihin ja ympyrän neliöimiseen selvisi kompleksilukujen avulla. Kaavaa on kutsuttu myös matematiikan kauneimmaksi kaavaksi. Se yhdistää yhteenlaskulla, kertolaskulla ja potenssiinkorotuksella samaan kaavaan viisi tärkeää matematiikan vakiota: Neperin luvun e, piin π, imaginääriyksikön i, ykkösen 1 ja nollan 0. Tämä tutkielmamme on Eulerille velkaa myös merkinnöistä. Muun muassa merkinnät e, i, $\sum$ ja $f(x)$ ovat hänen käyttöönottamiaan ja paljolti hänen ansiostaan π vakiintui tarkoittamaan ympyrän kehän suhdetta halkaisijaan. Merkintää käytti ensimmäisenä William Jones (1675–1749) vuonna 1706. [4, s. 621–624], [10, s. 41–42].

Eulerin aikaan alettiin arvella, olisiko olemassa lukuja, joita ei voi esittää algebrallisen yhtälön juurina eli transkendenttilukuja. Olisiko π transkendenttiluku? Euler tutki asiaa ensimmäisenä, vuonna 1755 ollessaan jo sokea. Silloin piin irrationaalisuuttakaan ei vielä oltu todistettu, mutta Euler piti jo varmana, että π oli transkendenttinen. Hän kirjoitti tutkielmassaan *De relatione inter ternas pluresve quantitates instituenda*: "Näyttää melko varmalta, että yksikköympyrän kehän pituudella on niin outoja transsendenttisia ominaisuuksia, ettei sitä voi verrata sellaisiin suureisiin kuin juuriin tai muihin transsendenttilukuihin." Kirja julkaistiin vasta kymmenen vuotta myöhemmin, sillä kustantamo ei vielä ollut ehtinyt julkaista tuotteliaan Eulerin edellisiä teoksia. [1, s. 162–164, 173–174].

Johann Lambert (1728–1777) todisti vuonna 1761 että π on irrationaalinen. Hän osoitti, että $\tan x$ ei ole rationaalinen, jos x on nollasta poikkeava rationaaliluku. Tästä seuraa, että x on irrationaalinen tai nolla, jos $\tan x$ on rationaalinen. Koska $\tan \frac{\pi}{4} = 1$, niin $\frac{\pi}{4}$ ja siten myös π on irrationaalinen. Tämän hän julkaisi vuonna 1767 kirjassaan *Vorläufige Kenntnisse fûr die, so die Quadratur und Rektification des Zirkles suchen* eli Perustietoa niille, jotka yrittävät neliöidä ja suoristaa ympyrän. [1, s. 176–177].

Lambertin tulos ei suinkaan lopettanut neliöintiyrityksiä, sillä eräitä irrationaalilukuja kuten $\sqrt{2}$ saattoi hyvinkin konstruoida. Tulos vain lisäsi neliöintiyrityksiä mutta viimeistään tässä vaiheessa ammattimatemaatikot kuitenkin näyttävät kääntyneen sen kannalle, että neliöiminen on mahdotonta. Vuonna 1775 Pariisin tiedeakatemia Académies des Sciences päätti, ettei ympyrän neliöintejä enää tarkasteta virallisesti. Joitakin vuosia myöhemmin Lontoon Royal Society teki saman päätöksen. [17], [4, s. 651].

Ansio geometristen konstruktioiden ratkeavuuden selvittämisestä lankeaa algebraa 1700- ja 1800-lukujen vaihteessa kehittäneille saksalaiselle Gaussille, norjalaiselle Abelille ja ranskalaiselle Galoisille. Epäonninen Évariste Galois (1812–1832) kuoli kansintaistelussa 20-vuotiaana ja Niels Henrik Abel (1802–1829) kärsi arvostuksen puutteesta ja kuoli tuberkuloosiin alle 30-vuotiaana. Matematiikkojen kuninkaaksikin sanottu Carl Friedrich Gauss (1777–1855) taas eli pitkään ja arvostettuna. Hän konstruoi 17-sivuisen säännöllisen monikulmion vuonna 1796. Toinen hänen saavutuksensa on algebran peruslauseen neljä todistusta, joista ensimmäisen hän esitti väitöskirjassaan 1799. Galois yleisti Gaussin tuloksen säännöllisten monikulmioiden ratkeavuudesta ja esitti yhtälön $C_0x^0 + C_1x^1 + \cdots + C_nx^n = 0$ ratkeavuuden ehdot. Abel tutki hänkin algebrallisten yhtälöiden ratkeavuutta. [4, s. 696–701, 731–733, 738–741], [10, s. 47], [1, s. 176].

Ongelma pysyi suosittuna ja yritelmiä oli paljon. Muun muassa Augustus De Morgan (1806–1871) yritti vakuuttaa, että yrittäjät ovat tehneet päättelyssään virheitä. Hän kertoo kirjassaan *A Budget of Paradoxes*, joka julkaistiin postuumisti vuonna 1872, useista virheistä neliöimisyrityksistä. [17].

Vuonna 1844 Joseph Liouville (1809–1882) todisti, että transkendenttilukuja on olemassa. Muutaman kymmenen vuoden päästä siitä vuonna 1873 ranskalainen matemaatikko Charles Hermite (1822-1901) todisti Neperin luvun e transkendenttisuuden Académie des Sciencesin tiedelehden *Comptes Rendusin* artikkelissaan *La Fonction Exponentielle.* Hermite piti vastaavaa todistusta piistä vaikeana ja kirjoittikin ystävälleen, että jättää piin transkendentaalitodistuksen mielihyvin muille. [2, s. 456]. Lopullisesti reaalilukujen jaon jaon algebrallisiin ja transkendentaalisiin todisti Georg Cantor (1845–1918) vuonna 1874 [10, s. 46], [4, s. 800].

Yhdeksän vuotta myöhemmin saksalainen Ferdinand Lindemann (1852–1939) käytti hyvin samanlaista menetelmää piin transkendenttisuuden todistamiseen. *Mathematische Annalenissa* vuonna 1882 ilmestyneessä artikkelissaan *Über die Zahl* π hän todisti samalla ympyrän neliöimisen mahdottomaksi, kuten luvussa 5 huomaamme. [4, s. 800–801].

Tämä ei pysäyttänyt matemaatikoksi haluavia. Tietze [22, s. 93] ja Lehtinen [15, s. 16] toteavat, että yhä vielä saapuu matemaatikoille ratkaisuyrityksiä. Niissä on kuitenkin ymmärretty tehtävä väärin tai unohdettu jokin yksityiskohta. Tai sitten matemaattiset perusteet ovat olleet täysin pielessä. ”Indiana Pi Bill” oli tällainen.

Indianan osavaltiossa 1897, 15 vuotta Lindemannin todistuksen jälkeen, harrastelijamatematiikko Edwin J. Goodwin luuli keksineensä ympyrän neliöimiseen ratkaisun. Se perustui ajatukseen siitä, että neliö, jonka lävistäjä on yhtä pitkä kuin ympyrän halkaisija, on pinta-alaltaan yhtäsuuri kuin ympyrä. Hän oli jo saamassa ratkaisulle lain voiman, mutta ennen ratkaisevaa käsittelyä edustuslaitoksessa vieraillut yliopiston matematiikan professori Clarence Abiathar Waldo ehti valaista lainsäätäjiä Lindemannin saavutuksesta. [1, s. 175].

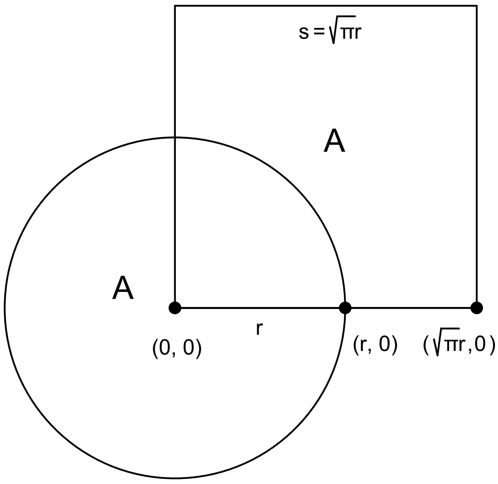
Jotta emme sortuisi ylimielisyyteen tai matemaattiseen elitismiin, mistä eräs ympyränneliöijä Becmanin kirjassa matemaatikkoja syyttää, emme käsittele 1900-luvun vääriä neliöintejä. Ne kyllä ovat matemaattiselta mielettömyydeltään mielenkiintoisia, sillä niiden alkuoletukset ovat Lüttichin Francon oletusten tasoa. Ne kertovatkin enemmän ihmisten yltiöpäisyydestä kuin yleisestä matematiikan ymmärtämisen tasosta. Suosittelemme kiinnostuneita lukemaan niistä Beckmanin teoksesta. Jatkamme matematiikan parissa ja käymme seuraavaksi Hermiten ja Lindemannin esimerkin rohkaisemina ympyrän neliöimisen kimppuun.

5 Ympyrän neliöimisen mahdottomuus

Mahdottomuustodistuksemme pohjautuu luvussa 3 konstruoimisesta saatuihin tuloksiin, ympyrän ja neliön geometriaan sekä luvun π algebrallisiin ominaisuuksiin.

Lause 5.1. *Ympyrän voi neliöidä jos ja vain jos π on konstruoituva.*

Todistus. Tehtävänantomme 3.1 mukaan meidän pitää neliöidä ympyrä eli saada konstruoitua alaltaan samankokoinen neliö kuin ympyrä on. Tiedämme jo alkeisgeometriasta, että r-säteisen ympyrän pinta-ala on πr^2. Samoin tiedämme, että s-sivuisen neliön pinta-ala on s^2. Jotta näiden pinta-ala olisi sama, pitäisi neliön sivun s olla $\sqrt{\pi r^2} = r\sqrt{\pi}$.



Kuva 11: Ympyrän neliöimisessä pitää piirtää ympyrän kokoinen neliö.

Tällainen etäisyys pitää siis saada konstruoitua kahden pisteen välille. On sama, mitkä pisteet valitsemme, sillä janan voi aina siirtää alkamaan toisesta pisteestä. Pisteet voivat olla vaikkapa origo ja piste, jonka toinen koordinaatti on $r\sqrt{\pi}$. Ympyrän neliöiminen vaatii siis luvun $r\sqrt{\pi}$ konstruoimista.

Lause 3.1 sanoo, että yksi konstruoimismenetelmä on kertominen ja yksi juurenotto. Jos siis voi konstruoida luvun $r\sqrt{\pi}$, voi konstruoida myös luvun π ja päinvastoin.

Ympyrän neliöiminen on siis yhtäpitävää luvun π konstruoimisen kanssa. Toisin sanoen: π on konstruoituva, jos ja vain jos ympyrän voi neliöidä. $\square$

Konstruktiotehtävässä meille on annettu yksikköjana, joista voimme konstruoida koordinaatit. Tämän yksikköjanan pisteet ovat $(0,0)$ ja $(1,0)$. Niiden koordinaatit ovat kokonaislukuja. Mitä lukuja ovat konstruoituvien pisteiden koordinaatit?

Lause 5.2. *Konstruoituvan pisteen koordinaatit ovat algebrallisia lukuja.*

Todistus. Annetut koordinaatit ovat kokonaislukuja (0 ja 1). Lauseen 3.2 todistuksessa käsitellyn polynomiyhtälön kertoimet ovat annettujen pisteiden koordinaattien rationaalilausekkeita ja siis rationaalilukuja. Tällaisen yhtälön juuri on määritelmän 2.3 mukaan algebrallinen luku. Konstruoituvan pisteen koordinaatti on siis algebrallinen luku. □

Yhdenkään konstruoituvan pisteen koordinaatti ei ole transkendenttiluku. Toisin sanoen transkendenttilukuja ei voi konstruoida sovituin menetelmin. Todistamme luvussa 5.2, että π on transkendenttinen. Tuloksen avulla saamme todistettua, ettei ympyrää voi neliöidä (tai neliötä ympyröidä). Tuloksen saamiseksi käytämme Eulerin kaavaa 2.2 ja samantapaista menetelmää kuin luvun e transkendenttisuustodistuksessa, jonka teemme ensin. Lopullisen todistuksen neliöimisen mahdottomuudesta annamme viimeiseksi.

5.1 Neperin luku

Todistamme tässä luvussa, että e on transkendenttinen. Todistuksemme seuraa Lindelöfin antamaa todistusta. Sen on saksalainen Adolf Hurwitz yksinkertaistanut Hermiten todistuksesta. [16, s. 101–104].

Aluksi johdamme apulauseen. Olkoon $f(x)$ astetta n oleva mielivaltainen polynomi ja olkoon polynomi $F(x)$ polynomin $f(x)$ ja sen kaikkien derivaattojen summa

$$F(x) = f(x) + f'(x) + \cdots + f^{(n)}(x). \tag{5.1}$$

Todistus. Viimeinen derivaatta $f^{(n)}(x)$ on vakio. Vakion derivaatta on 0, joten funktion

$$\Phi(x) = \mathrm{e}^{-x} F(x) \tag{5.2}$$

derivaatta on

$$\begin{aligned}\Phi'(x) &= -\mathrm{e}^{-x}F(x) + \mathrm{e}^{-x}F'(x) = -\mathrm{e}^{-x}(F(x) - F'(x)) = \\ &- \mathrm{e}^{-x}(f(x) + f'(x) + \cdots + f^{(n)}(x) - f'(x) - f''(x) - \cdots - f^{(n)}(x) - 0) = \\ &- \mathrm{e}^{-x} f(x).\end{aligned} \tag{5.3}$$

Differentiaalilaskennan väliarvolauseen (lause 2.3) mukaan välillä $(0, x)$ pätee

$$\Phi(x) - \Phi(0) = \mathrm{e}^{-x}F(x) - \mathrm{e}^{-0}F(0) = \Phi'(c) \cdot (x - 0) = -\mathrm{e}^{-c}f(c)x. \tag{5.4}$$

Siirtämällä termejä saamme yllä olevan ensiksi muotoon $F(0) = \mathrm{e}^{-x}F(x) + \mathrm{e}^{-c}f(c)x$. Kun vielä kerromme puolittain luvulla e^{x}, apulauseemme saa lopullisen muotonsa

$$F(0)\mathrm{e}^{x} = F(x) + x\mathrm{e}^{x-c}f(c). \tag{5.5}$$

Tarvitsemme todistuksessa myös seuraavaa apulauseen ominaisuutta.

Lause 5.3. *Polynomi $F(x)$ saadaan polynomin $f(x)$ Taylor-kehitelmästä, kun kehitelmässä korvataan kertoimet $(x-a)^i$ luvun i kertomalla $i!$ (i saa arvot $1, 2, \ldots, n$).*

Teemme ensin funktiosta $f(x)$ kehitelmän ja muutamme sen sitten funktioksi $F(x)$. Verratkaamme lauseketta (5.1) ja polynomin $f(x)$ Taylor-kehitelmää

$$f_a(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n. \tag{5.6}$$

Huomaamme, että $F(x)$ saadaan polynomin $f(x)$ kehitelmästä, kun kehitelmästä korvataan kertoimet $(x-a)^i$ luvun i kertomalla $i!$ (i saa arvot $1, 2, \ldots, n$). Tällöin joka derivaatan kertoimiksi tulee 1 ja muokattu kehitelmä on siis sama kuin (5.1). □

Seuraavassa todistuksessa teemme vastaoletukseksi, että e on polynomiyhtälön juuri. Apulauseella muunnamme yhtälöä ja todistamme, että yhtälön vasen puoli antaa eri tuloksen kuin oikea puoli. Tämä on ristiriita, josta seuraa, että vastaoletus on väärä.

Lause 5.4. *Luku* e *on transkendenttinen.*

Todistus. Todistamme väitteen epäsuorasti vastaoletuksella: e ei ole transkendenttinen. Silloin se on transkendenttiluvun määritelmän 2.4 mukaan algebrallinen ja algebrallisen luvun määritelmän 2.3 mukaan jonkin polynomiyhtälön juuri. Se tarkoittaa, että on olemassa n-asteinen kokonaislukukertoiminen yhtälö

$$C_0 + C_1\mathrm{e} + C_2\mathrm{e}^2 + \cdots + C_n\mathrm{e}^n = 0. \tag{5.7}$$

Yhtälössä kaikki kertoimet eivät ole nollia ja $C_0 \neq 0$. Jos olisi $C_0 = 0$, niin voisimme jakaa luvulla e, kunnes jokin vakiotermiksi tulevista kertoimista olisi $C \neq 0$. Tämän jälkeen vaihtaisimme alaindeksit alkamaan nollasta ja päättymään lukuun n. Siis pätee, että $C_0 \neq 0$, ja voimme jatkaa yhtälön (5.7) käyttämistä.

Olkoon nyt mielivaltainen $v \in \mathbb{Z}_+$. Silloin on olemassa sellainen reaaliluku c_v, että $0 < c_v < v$ ja sijoittamalla yhtälöön (5.5) $x = v$ ja $c = c_v$ saamme $F(0)\mathrm{e}^v = F(v) + v\mathrm{e}^{v-c_v}f(c_v)$. Yhtälössä (5.7) kokonaislukujen kertoimina ovat luvut e^v, missä $v = 1, 2, \ldots, n$. Jos siis kerromme yhtälön luvulla $F(0)$, saamme yhtälön sopivaan muotoon. Termeiksi tulee muotoa $C_vF(0)\mathrm{e}^v = C_v\left(F(v) + v\mathrm{e}^{v-c_v}f(c_v)\right)$ olevia lausekkeita. Ensimmäinen termi, jossa siis $v = 0$, on $C_0\left(F(0) + 0\mathrm{e}^{0-c_0}f(c_0)\right) = C_0F(0)$. Toinen termi on $C_1F(1) + 1C_1\mathrm{e}^{1-c_1}f(c_1)$ ja myös muissa on kaksi termiä. Siirtämällä luvun e potensseja sisältävät termit oikealle puolelle saamme yhtälön

$$\begin{aligned} C_0F(0) &+ C_1F(1) + \cdots + C_nF(n) \\ &= -\left(C_1\mathrm{e}^{1-c_1}f(c_1) + 2C_2\mathrm{e}^{2-c_2}f(c_2) + \cdots + nC_n\mathrm{e}^{n-c_n}f(c_n)\right). \end{aligned} \tag{5.8}$$

Tämän yhtälön vasemman puolen siis todistamme nollasta eroavaksi kokonaisluvuksi, ja oikean puolen välillä $(-1, 1)$ olevaksi luvuksi. Otamme käsittelyyn ensin vasemman puolen.

Alkulukuja on äärettömästi lauseen 2.5 mukaan. Koska siis luvut n, $|C_0|$ ovat äärellisiä, voimme olettaa, että on olemassa sellainen alkuluku p, joka on suurempi lukuja n ja $|C_0|$. Todistamme, että yhtälön vasemman puolen termit ovat kokonaislukuja, joista $C_0F(0)$ ei ole jaollinen luvulla p kun taas loput termit ovat. Vasen puoli kokonaisuudessaan ei siis ole jaollinen luvulla p, joten se on nollasta eroava kokonaisluku.

Olkoon lisäksi

$$f(x) = \frac{1}{(p-1)!} x^{p-1} \left((x-1)(x-2)\cdots(x-n)\right)^p. \tag{5.9}$$

Tämän polynomin aste on $p + np - 1$. Vastaavat polynomit $F(0)$, $F(1)$, $\ldots$, $F(n)$ saamme, kun kehitämme polynomin $f(x)$ tekijän $(x - i)$ potenssien mukaan. Kehittäkäämme ensin tekijän $(x - 0) = x$ potenssien mukaan $f_0(x)$.

Kirjoitamme yhtälön ensin muotoon $f(x) = \frac{1}{(p-1)!} x^{p-1} g(x)$ ja kehitämmekin funktion $g(x) = ((x-1)(x-2)\cdots(x-n))^p = (-1)^{np} n!^p + A_1x^1 + \cdots + A_{np-1}x^{np-1} + x^{np}$, missä A_i ovat kokonaislukuja, koska ne koostuvat vain kokonaislukutekijöitä. Sitten sijoitamme kehitelmän alkuperäiseen funktioon $f(x)$.

Kehitelmän nollas termi $g(0)$ on vakiotermi $(-1)^{np}n!^p$, sillä muut termit eliminoituvat kohdassa nolla. Kehitelmän termin $g(0)x^i/i!$ saamme, kun derivoimme funktiota $g(x)$ i kertaa. Termiksi jää sellainen funktion $g(x)$ termi A_ix^i, jota on derivoitu i kertaa, sillä derivaatan muihin termeihin jää tekijäksi x ja ne eliminoituvat kohdassa nolla. Ainoaksi termiksi tulee $1 \cdot 2 \cdots i \cdot A_i = i!A_i$. Tulokseksi saamme siis $g^{(i)}(0) = i!A_i$. Kokonaisuudessaan Taylor-kehitelmäksi $g_0(x)$ tulee $(-1)^{np}n!^p + \frac{1!A_1}{1!}x^1 + \frac{2!A_2}{2!}x^2 + \cdots + \frac{(np)!A_{np}}{(np)!}x^{np}$. Kun tämän sijoitamme funktioon $f(x) = \frac{1}{(p-1)!}x^{p-1}g(x)$, saamme kehitelmän

$$f_0(x) = \frac{1}{(p-1)!}\Big((-1)^{np}n!^p x^{p-1} + A_1x^p + A_2x^{p+1} + \cdots + A_{np+p-1}x^{np+p-1}\Big), \tag{5.10}$$

missä kertoimet A_i ovat kokonaislukuja.

Nyt kun lauseen 5.3 mukaisesti vaihdamme potenssit x^i kertoimiksi $i!$, niin saamme vastaavan polynomin $F(0)$, joka on

$$\begin{aligned}
F(0) = \frac{1}{(p-1)!}&((-1)^{np}n!^p(p-1)! + \\
&A_1p! + A_2(p+1)! + \cdots + A_{np+p-1}(np+p-1)!) \\
= (-1)^{np}n!^p + A_1p &+ A_2p(p+1) + \cdots + A_{np+p-1}p(p+1)\cdots(np+p-1).
\end{aligned}$$

Koska kertoimia A_i sisältävät termit ovat kokonaislukuja ja jokaisessa on yhteisenä tekijänä p, voimme ilmaista polynomin $F(0)$ muodossa

$$F(0) = (-1)^{np} n!^p + pK_0, \tag{5.11}$$

missä K_0 on jokin kokonaisluku ja mistä huomaamme, että $F(0)$ on kokonaisluku.

Koska $p > n$, niin $p \nmid n!$. Tämä siksi, että p on alkuluku eikä siis ole mikään tekijöiden $1,\ 2,\ \ldots, n$ tulo. Se ei voi siis olla mikään kertoman $n!$ tekijä, koska kertoman kaikki alkulukutekijät ovat lukua p pienempiä. Siispä p ei ole kertoman $n!$ minkään potenssin tekijä, joten $p \nmid n!^p$. Koska siis $p \nmid (-1)^{np} n!^p$ ja triviaalisti $p \mid pK_0$, ei $F(0)$ ole jaollinen luvulla p. Siksi pätee myös $F(0) \neq 0$.

Tarkastellaan nyt loppuja termejä $F(1), F(2), \ldots, F(n)$. Olkoon u mikä tahansa kokonaisluku väliltä $[1, n]$. Kehitämme polynomin $F(u)$ polynomin $f(x)$ tekijän $(x - u)$ potenssien mukaan.

Funktiolla $f(x)$ on tekijä $(x-u)^p$. Derivaatat aina kertalukuun $p-1$ asti siis sisältävät tekijän $(x - u)$. Tällöin $f^{(i)}(u) = 0$. Kertaluvun p derivaatasta alkaen derivaatassa $f^{(i)}(x)$ on vakiotermi $\frac{1}{(p-1)!} \cdot 1 \cdot 2 \cdots i \cdot B_i = \frac{1}{(p-1)!} i! B_i$, missä B_i on kokonaisluku. Muissa termeissä on tekijänä $(x - u)$, joten $f^{(i)}(u) = \frac{1}{(p-1)!} i! B_i$, kun $i \geq p$. Saamme kehitelmäksi

$$f_u(x) = \frac{1}{(p-1)!} \Big(0 + B_p(x-u)^p + B_{p+1}(x-u)^{p+1} + \cdots \Big), \tag{5.12}$$

missä kertoimet B_i ovat kokonaislukuja.

Kun taas vaihdamme tekijät $(x - u)^i$ tekijään $i!$ lauseen 5.3 mukaisesti, saamme polynomin

$$F(u) = \frac{1}{(p-1)!} \left(p! B_p + (p+1)! B_{p+1} + \cdots \right) =$$
$$pB_p + p(p+1)B_{p+1} + \cdots = pK_u,$$

missä K_u on kokonaisluku. Huomaamme, että $F(u) = pK_u$ on kokonaisluku ja triviaalisti $p \mid F(u)$.

Koska $p > |C_0|$ ja $p \nmid F(0)$, niin $p \nmid C_0 F(0)$. Kaikkien polynomien $F(u)$ summa $\sum_1^n F(u)$ taas on jaollinen luvulla p. Näiden summa $C_0 F(0) + \sum_1^n F(u)$ eli yhtälön (5.8) vasen puoli ei siis ole jaollinen luvulla p, mistä seuraa, että summa on nollasta eroava kokonaisluku.

Nyt todistamme, että yhtälön (5.8) oikea puoli on luku välillä $(-1, 1)$. Koska vasen puoli ei yllä todistetun mukaan kuulu tälle välille, seuraa ristiriita.

Koska $c_i > 0$, niin $\mathrm{e}^{i - c_i} < \mathrm{e}^n$, kun i saa arvot $1, 2, \ldots, n$. Jos $0 < x < n$, niin kaikki polynomin (5.9) tekijät $x, x-1, \ldots, x-n$ ovat itseisarvoltaan pienempiä kuin n. Voimme siis merkitä

$$|f(x)| < \frac{1}{(p-1)!} \cdot n^{p-1}(n^n)^p = \frac{n^{p+np-1}}{(p-1)!} = n^n \frac{(n^{n+1})^{p-1}}{(p-1)!}. \tag{5.13}$$

Jokainen c_i on positiivinen ja pienempi kuin n. Erityisesti siis

$$|f(c_v)| < n^n \frac{(n^{n+1})^{p-1}}{(p-1)!}. \tag{5.14}$$

Jos merkitsemme c:llä suurinta arvoa luvuista $|c_0|$, $|c_1|$, $\ldots$, $|c_n|$, niin kaavan (5.8) oikean puolen itseisarvo on pienempi kuin

$$(1+2+\cdots+n)c\mathrm{e}^n n^n \frac{(n^{n+1})^{p-1}}{(p-1)!} = \frac{n(n+1)}{2} c\mathrm{e}^n n^n \frac{(n^{n+1})^{p-1}}{(p-1)!}. \tag{5.15}$$

Koska lauseen 2.4 mukaan $\frac{(n^{n+1})^{p-1}}{(p-1)!} \to 0$, kun $p \to \infty$, ja koska alkuosa $\frac{n(n+1)}{2} c\mathrm{e}^n n^n$ on äärellinen, niin tietystä alkuluvusta $p = p_0$ lähtien oikea puoli on pienempi kuin 1.

Siis kun p on suurempi lukuja n, $|C_0|$ ja p_0, niin yhtälön (5.8) oikean puolen itseisarvo on pienempi kuin 1 eli sen arvo on väliltä $(-1, 1)$.

Päädymme ristiriitaan: yhtälön (5.8) vasen puoli on kokonaisluku, joka ei ole nolla, ja oikea puoli on luku välillä $(-1, 1)$. Vastaoletuksemme on siis väärä ja väitteemme oikea eli Neperin luku e on transkendenttinen. □

5.2 Pii

Todistakaamme ensin pari apulausetta, joiden avulla pääsemme päätodistuksemme alkuun. Todistuksemme seuraa Hobsonin esittämää todistusta, joka perustuu saksalaisen Paul Albert Gordanin antamaan. Gordan oli yksi niistä, jotka yksinkertaistivat Lindemannin todistusta. [10, s. 53–57].

Lause 5.5. *Kompleksiluku z on algebrallinen luku jos ja vain jos* iz *on.*

Todistus. (Ks. [12, s. 14].) Olkoon z algebrallinen. Silloin se on jonkin n-asteisen kokonaislukukertoimisen polynomin juuri eli

$$P(z) = C_0 + C_1 z^1 + \cdots + C_n z^n = 0. \tag{5.16}$$

Imaginääriyksikön toinen potenssi on $\mathrm{i}^2 = -1$, joten $P(-\mathrm{i}^2 z) = P(-\mathrm{i}(\mathrm{i}z)) = P(z) = 0$ ja

$$P(-\mathrm{i}(\mathrm{i}z)) = C_0 + C_1(-\mathrm{i}(\mathrm{i}z))^1 + \cdots + C_n(-\mathrm{i}(\mathrm{i}z))^n. \tag{5.17}$$

Imaginääriyksikön kaikki potenssit ovat joko $1, \mathrm{i}, -1$ tai $-\mathrm{i}$, sillä $\mathrm{i}^0 = 1$, $\mathrm{i}^1 = \mathrm{i}$, $\mathrm{i}^2 = -1$, $\mathrm{i}^3 = \mathrm{i} \cdot \mathrm{i}^2 = -\mathrm{i}$ ja muut potenssit tuottavat järjestyksessä samoja arvoja:

$$C_0 - \mathrm{i}C_1(\mathrm{i}z) - C_2(\mathrm{i}z)^2 + \mathrm{i}C_3(\mathrm{i}z)^3 + C_4(\mathrm{i}z)^4 + \cdots + (-\mathrm{i})^n C_n(\mathrm{i}z)^n. \tag{5.18}$$

Siispä polynomi $P(z)$ on muotoa

$$P(z) = Q(\mathrm{i}z) + \mathrm{i}R(\mathrm{i}z) = 0, \tag{5.19}$$

missä Q ja R ovat kokonaislukukertoimisia polynomeja. Kun kerromme tämän lausekkeella $Q(\mathrm{i}z) - \mathrm{i}R(\mathrm{i}z)$, saamme

$$0 = (Q(\mathrm{i}z) + \mathrm{i}R(\mathrm{i}z))\,(Q(\mathrm{i}z) - \mathrm{i}R(\mathrm{i}z)) = Q^2(\mathrm{i}z) - R^2(\mathrm{i}z). \tag{5.20}$$

Tämä on polynomi, jonka kertoimet ovat kokonaislukuja ja ainakin yksi niistä ei ole nolla. Koska iz on sen nollakohta, niin algeballisen luvun määritelmän mukaan iz on algebrallinen. Väite on siis tosi. □

Lause 5.6. *Olkoot eri joukkoihin kuuluvat muuttujat*

$$x_1, x_2, \dots, x_a; \qquad y_1, y_2, \dots, y_b; \qquad z_1, z_2, \dots, z_c; \qquad \dots, \tag{5.21}$$

ja olkoon P symmetrinen polynomi, joka koostuu $a+b+c+\dots$ muuttujasta otettujen p muuttujan tulojen summasta. Polynomi P voidaan esittää näiden eri joukoissa olevien muuttujien symmetristen perusfunktioiden avulla.

Todistus. Todistamme tämän kahden joukon tapauksessa (laajempi todistus, ks. esim. [12, 14–20]).

Olkoon $\sum_p P(x,y)$ haluamamme tulojen summa ja olkoon $\sum_r P(x)$ sellaisten tulojen summa, jonka termeissä on r tekijää muuttujista $x_1, x_2, \dots, x_a$ (vastaavasti summa $\sum_r P(y)$ muuttujista y). Summat $\sum_r P(x)$ ja $\sum_r P(y)$ ovat siis symmetrisiä perusfunktioita s_r.

Kun $p \le a$, niin

$$\sum_p P(x,y) = \sum_p P(x) + \sum_{p-1} P(x) \sum_1 P(y) + \sum_{p-2} P(x) \sum_2 P(y) + \cdots \tag{5.22}$$

ja kun $p > a$, niin

$$\begin{aligned}\sum_p P(x,y) =& \\ \sum_a P(x) \sum_{p-a} P(y) + \sum_{a-1} P(x) &\sum_{p-a+1} P(y) + \sum_{a-2} P(x) \sum_{p-a+2} P(y) + \cdots .\end{aligned} \tag{5.23}$$

Termit oikealla puolella koostuvat siis kaikissa tapauksissa vain kahteen eri joukkoon kuuluvien muuttujien symmetrisistä polynomeista. Apulauseemme siis pätee kahden joukon tapauksessa ja laajennus yleiseen muotoon on nyt ilmeistä. □

Esimerkki 5.1. Olkoot muuttujat x_1, x_2 ja y_1, y_2. Muuttujille x_i ja y_i symmetriset perusfunktiot ovat $\sum_1 P(x) = x_1 + x_2$, $\sum_2 P(x) = x_1x_2$, $\sum_1 P(y) = y_1 + y_2$ ja $\sum_2 P(y) = y_1y_2$. Symmetrinen polynomi $\sum_2 P(x,y) = x_1x_2 + x_1y_1 +$

$x_2y_1+x_1y_2+x_2y_2+y_1y_2$ voidaan esittää perusfunktioiden avulla ($p=2=a$) seuraavasti

$$\sum_2 P(x,y) = \sum_2 P(x) + \sum_1 P(y) \sum_1 P(x) + \sum_2 P(y).$$

Samoin symmetrinen polynomi $\sum_3 P(x,y) = x_1x_2y_1+x_1x_2y_2+x_1y_1y_2+x_2y_1y_2$ on perusfunktioiden avulla ilmaistuna (nyt $p=3>2=a$)

$$\sum_3 P(x,y) = \sum_2 P(x) \sum_1 P(x) + \sum_1 P(y) \sum_2 P(x).$$

Nyt pääsemme todistamaan päälausettamme. Teemme sen samantapaisesti kuin Neperin luvun transkendentaalisuustodistuksen. Vastaolettamalla luvun π algebralliseksi saamme polynomiyhtälön. Muunnamme yhtälön muotoon, josta selvästi näkee, että sen toinen puoli on nolla ja toinen nollasta eroavan kokonaisluvun ja väliltä $(-1,1)$ olevan reaaliluvun summa. Seuraa ristiriita, mistä päättelemme väitteen olevan totta.

Lause 5.7. *Luku π on transkendenttinen.*

Todistus. Ensiksi teemme vastaoletuksen, että π on algebrallinen luku. Tällöin lauseen 5.5 mukaan on yhtäpitävää, että $\mathrm{i}\pi$ on algebrallinen eli se on määritelmän 2.3 mukainen kokonaislukukertoimisen polynomiyhtälön juuri. Se tarkoittaa, että $\mathrm{i}\pi$ olisi yksi polynomiyhtälön

$$C(x-a_1)(x-a_2)\cdots(x-a_s)=0 \tag{5.24}$$

luvuista a. Polynomiyhtälön muuttujille lisäksi pätee, että kertojamuotoon muutettuna yhtälön kertojat

$$\begin{gathered} C, \\ C\sum a_r = C(a_1+a_2+\cdots+a_n), \\ C\sum a_ra_s = C(a_1a_2+a_1a_3+\cdots+a_{n-1}a_n), \\ \vdots \\ Ca_1a_2\cdots a_s \end{gathered}$$

ovat kokonaislukuja. Huomaamme, että ne ovat määritelmän 2.2 mukaisesti muuttujien a_i symmetrisiä perusfunktioita vakiolla C kerrottuna.

Eulerin kaava $\mathrm{e}^{\mathrm{i}\pi}+1=0$ antaa luvan olettaa, että

$$(1+\mathrm{e}^{a_1})(1+\mathrm{e}^{a_2})\cdots(1+\mathrm{e}^{a_s})=0 \tag{5.25}$$

on totta, sillä yksi tulon tekijä on yllä 0. Kun kerromme vasemman puolen lausekkeen tekijät keskenään, niin saamme yhtälön

$$A+\mathrm{e}^{b_1}+\mathrm{e}^{b_2}+\cdots+\mathrm{e}^{b_n}=0, \tag{5.26}$$

missä b_i ovat lukujen a_i summia ja A on positiivinen kokonaisluku, koska se on ykkösten ja arvon 1 antavien potenssien summa. Näitä potensseja ovat mahdolliset potenssit $\mathrm{e}^{a_p+a_q+\cdots}$, joissa $a_p + a_q + \cdots = 0$. Rakennamme nyt kokonaisluvun, jolla kerromme yhtälön puolittain ja saamme aikaan ristiriidan. Ensiksi tarvitsemme tietoa luvuista b_i ja erään apufunktion.

Alkuperäisen polynomiyhtälömme 5.24 kertojat koostuvat vakiolla C kerrotusta muuttujien a tulojen summasta siten, että summattavat tulot sisältävät r määrän tekijöitä. Ne ovat määritelmän 2.2 mukaisia symmetrisiä polynomeja ja ne ovat kokonaislukuja. Osoitamme, että symmetrisillä polynomeilla tuloista $Cb_1, Cb_2, \ldots, Cb_n$ on sama ominaisuus.

Kun kirjoitamme yhtälön (5.26) auki seuraavasti

$$\begin{aligned} A + \mathrm{e}^{b_1} + \mathrm{e}^{b_2} + \cdots + \mathrm{e}^{b_n} =& A+ \\ & \mathrm{e}^{a_1} + \mathrm{e}^{a_2} + \mathrm{e}^{a_3} + \cdots + \mathrm{e}^{a_n} + \\ & \mathrm{e}^{a_1+a_2} + \mathrm{e}^{a_1+a_3} + \cdots + \mathrm{e}^{a_{n-1}+a_n} + \\ & \mathrm{e}^{a_1+a_2+a_3} + \cdots + \\ & \vdots \\ & + \mathrm{e}^{a_1+\cdots+a_n} = 0, \end{aligned}$$

näemme heti, että luvut b_i koostuvat summasta, jossa on r kappaletta lukuja $a_1, a_2, \ldots, a_s$. Sovimme nyt, että kaikki saman verran muuttujia a_i sisältävät muuttujat b_i kuuluvat samaan joukkoon. Yllä olevassa kaavassa samalla rivillä olevat eksponentit eli luvut b_i siis kuuluvat samaan joukkoon. Nyt apulauseemme 5.6 perusteella toteamme, että samaan joukkoon kuuluvien lukujen b_i symmetrinen polynomi voidaan esittää lukujen $a_1, a_2, \ldots, a_s$ symmetristen perusfunktioden avulla.

Lukujen Ca_i symmetrinen polynomi on kokonaisluku. Siispä tuloista Cb_i, missä luvut b_i kuuluvat samaan joukkoon, muodostettu symmetrinen polynomi on kokonaisluku. Käyttämällä tätä päättelyä kaikkiin n:ään lukuun Cb_m huomaamme että kaikki symmetriset tulot, jotka koostuvat kaikista luvuista Cb_m, ovat kokonaislukuja mukaan lukien nollan.

Määrittelimme, että sellaiset termit, joiden eksponentti b_m on nolla, lisätään kokonaislukuun A. Nollapotenssit eivät muuta symmetrisen polynomin arvoa, joten sillä lisätäänkö ne kokonaislukuun A ennen vai jälkeen symmetristen polynomien muodostamista, ei ole väliä.

Määrittelemme nyt tietyn kokonaisluvun rakentamiseen tarvittavan apufunktion Φ. Koska alkulukuja on lauseen 2.5 mukaan ääretön määrä ja koska luvut A, n, C, $|C^n b_1 b_2 \cdots b_n|$ ovat äärellisiä, voimme olettaa, että on olemassa sellainen alkuluku p, joka on suurempi lukuja A, n, C, $|C^n b_1 b_2 \cdots b_n|$. Olkoon funktio Φ sellainen, että

$$\Phi(x) = \frac{x^{p-1}}{(p-1)!} C^{np+p-1} \left((x-b_1)(x-b_2)\cdots(x-b_n)\right)^p . \tag{5.27}$$

Kerromme sulkujen sisällä olevat tekijät keskenään ja järjestelemme termit sopivasti. Saamme funktion Φ yhtäpitävään muotoon

$$\Phi(x) = \frac{C^{p-1}x^{p-1}}{(p-1)!} \Big((Cx)^n - q_1(Cx)^{n-1} + q_2(Cx)^{n-2} - \cdots + (-1)^n q_n\Big)^p , \tag{5.28}$$

missä q_1, q_2, …, q_n ovat kokonaislukuja sillä ne ovat lukujen C ja joidenkin b_i tuloja.

Poistamme vielä sulut. Silloin voimme esittää funktion muodossa

$$\Phi(x) = c_{p-1}x^{p-1} + c_p x^p + \cdots + c_{np+p-1}x^{np+p-1}, \tag{5.29}$$

missä luvuille c_i pätee, että $c_{p-1}(p-1)!$, $c_p p!$, … ovat kokonaislukuja. Luvut ovat muotoa $C^{p-1}/(p-1)!$ kerrottuna tulolla, jonka tekijöitä ovat kokonaislukujen C, q ja -1 jotkin potenssit.

Kun $i < (p-1)$, niin $\Phi^{(i)}(0) = 0$. Funktion Φ kertaluvun $(p-1)$ derivaatan kohdassa 0 näemme helpoimmin muodon (5.28) avulla ja se on

$$\Phi^{(p-1)}(0) = (-1)^{np} C^{p-1} q_n^p. \tag{5.30}$$

Derivaatta on kokonaisluku ja $p \nmid \Phi^{(p-1)}(0)$.

Derivoimalla funktion p kertaa saamme

$$\Phi^{(p)}(x) = pC^{p-1}\frac{d}{dx}\Big((Cx)^n - q_1(Cx)^{n-1} + \cdots\Big)^p , \tag{5.31}$$

mistä päättelemme, että $\Phi^{(p)}(0)$ on muotoa $pC^p q$ oleva kokonaisluku ja selvästi $p \mid \Phi^{(p)}(0)$.

Funktion muodon (5.29) avulla huomaamme melko vaivatta, että myös $\Phi^{(p+1)}(0)$, $\Phi^{(p+2)}(0)$, …, $\Phi^{(np+p-1)}(0)$ ovat kokonaislukuja ja niillä on kertojana luku p. Ne ovat siis luvun p monikertoja.

Kun m on väliltä $[1, n]$, niin $\Phi(b_m)$, $\Phi'(b_m)$, …, $\Phi^{(p-1)}(b_m)$ kaikki antavat arvon 0. Luvun p ja sitä suuremman kertaluvun derivaatat taas

$$\sum_{m=1}^{n} \Phi^{(p)}(b_m), \sum_{m=1}^{n} \Phi^{(p+1)}(b_m), \ldots, \sum_{m=1}^{n} \Phi^{(np+p-1)}(b_m) \tag{5.32}$$

ovat kaikki kokonaislukuja, jotka ovat jaollisia luvulla p. Kokonaislukuja ne ovat siksi, että niiden tuloksessa oleva $\sum_{m=1}^{n}(Cb_m)^r$ voidaan esittää symmetrisinä polynomeina, jotka koostuvat tulojen $Cb_1, Cb_2, \ldots, Cb_n$ summista. Aiemman päättelymme mukaanhan tällaiset luvut ovat kokonaislukuja.

Derivaattojen summa

$$\Phi^{(p-1)}(0) + \Phi^{(p)}(0) + \cdots + \Phi^{(np+p-1)}(0) \tag{5.33}$$

ei siis ole luvulla p jaollinen, sillä $p \nmid \Phi^{(p-1)}(0)$ mutta $p \mid \sum_p^{np+p-1} \Phi^{(i)}(0)$. Summa

$$\sum_{m=1}^{n} \left(\Phi^{(p)}(b_m) + \Phi^{(p+1)}(b_m) + \cdots + \Phi^{(np+p-1)}(b_m) \right) \tag{5.34}$$

sen sijaan on luvun p monikerta.

Nyt voimme määritellä kokonaislukumme. Olkoon nyt K_p kokonaisluku

$$\sum_{r=p-1}^{np+p-1} r! c_r = (p-1)! c_{p-1} + p! c_p + \cdots + (np+p-1)! c_{np+p-1} \tag{5.35}$$

Funktion (5.29) derivaatoilla kohdassa 0 saamme samat termit, joten K_p voidaan kirjoittaa myös muodossa

$$\Phi^{(p-1)}(0) + \Phi^{(p)}(0) + \cdots + \Phi^{(np+p-1)}(0).$$

Koska tämä summa ei ole jaollinen luvulla p, ei myöskään kokonaislukumme K_p ole.

Tarkastelemme muotoa, johon yhtälö (5.26) eli

$$A + \mathrm{e}^{b_1} + \mathrm{e}^{b_2} + \cdots + \mathrm{e}^{b_n} = 0$$

saadaan, kun kerromme kaikki termit luvulla K_p.

Oletuksemme mukaan $p > A$, joten myöskään $K_p A$ ei ole luvun p monikerta.

Muistakaamme eksponenttifunktion määritelmä 2.5. Siispä e^{b_m} on

$$\sum_{r=0}^{\infty} \frac{b_m^r}{r!}. \tag{5.36}$$

Muiksi termeiksi saamme siis muotoa

$$\begin{aligned} K_p \mathrm{e}^{b_m} = \sum_{r=p-1}^{np+p-1} c_r r! \sum_{k=0}^{\infty} \frac{b_m^r}{r!} = \sum_{r=p-1}^{np+p-1} c_r r! (\sum_{r=0}^{p-1} \frac{b_m^r}{r!} + \sum_{r=p}^{\infty} \frac{b_m^r}{r!}) = \\ \sum_{r=p-1}^{np+p-1} c_r \{ b_m^r + r b_m^{r-1} + r(r-1) b_m^{r-2} + \cdots + r! + \\ \frac{b_m^{r+1}}{r+1} + \frac{b_m^{r+2}}{(r+1)(r+2)} + \cdots \} = \\ \Phi^{(p)}(b_m) + \Phi^{(p+1)}(b_m) + \cdots + \Phi^{(np+p-1)}(b_m) + \\ \sum_{r=p-1}^{r=np+p-1} c_r b_m^r \left\{ \frac{b_m}{r+1} + \frac{b_m^2}{(r+1)(r+2)} + \cdots \right\} \end{aligned} \tag{5.37}$$

olevia lausekkeita.

Lausekkeen (5.37) osana olevan sarjan

$$\frac{b_m}{r+1} + \frac{b_m^2}{(r+1)(r+2)} + \cdots \tag{5.38}$$

summan itseisarvo ei kolmioepäyhtälön (2.3) nojalla ylitä sarjan

$$\frac{|b_m|}{r+1} + \frac{|b_m|^2}{(r+1)(r+2)} + \cdots \tag{5.39}$$

summaa. Tämä on vähemmän kuin $e^{|b_m|}$, sillä eksponenttifunktion sarjassa jokainen astetta i oleva termi on suurempi edellisen sarjan (5.39) astetta i olevaa termiä. Kun kirjoitamme eksponenttifunktion sarjaa auki seuraavasti

$$e^{|b_m|} = \sum_{k=0}^{\infty} \frac{|b_m|^k}{k!} = 1 + \frac{|b_m|}{1} + \frac{|b_m|^2}{2} + \cdots, \tag{5.40}$$

huomaamme, että osoittajat ovat samat mutta eksponenttifunktion termin nimittäjä on aina pienempi ja siis koko termi on arvoltaan suurempi.

Siis saamme, että lausekkeen (5.37) osana oleva sarja on

$$c_r b_m^r \left\{ \frac{b_m}{r+1} + \frac{b_m^2}{(r+1)(r+2)} + \cdots \right\} = \theta_r |c_r b_m^r| e^{|b_m|}, \tag{5.41}$$

missä θ_r on jokin luku väliltä $(-1, 1)$.

Kun jaamme sarjan summan

$$\sum_{r=p-1}^{np+p-1} \theta_r |c_r b_m^r| e^{|b_m|} \tag{5.42}$$

itseisarvon luvulla $|\theta_r|$, saamme summan

$$\sum_{r=p-1}^{np+p-1} |c_r b_m^r| e^{|b_m|} = e^{|b_m|} \sum_{r=p-1}^{np+p-1} |c_r b_m^r|, \tag{5.43}$$

joka on suurempi. Summa on $e^{|b_m|}\Phi(b_m)$, jossa Φ on muodoltaan yhtälön (5.29) kaltainen ja jonka termeistä on otettu itseisarvo. Kun sen muutamme muotoon (5.27), saamme

$$e^{|b_m|} \frac{|b_m|^{p-1}}{(p-1)!} C^{np+p-1} \left((|b_m| + |b_1|)(|b_m| + |b_2|) \cdots (|b_m| + |b_n|) \right)^p. \tag{5.44}$$

Valitsemme suurimman luvun luvuista $|b_1|$, $|b_2|$, ..., $|b_n|$ ja merkitsemme sitä $\bar{b}$. Siten lauseke (5.44) on pienempi tai yhtäsuuri (kun $b_m = \bar{b}$) kuin

$$l = e^{\bar{b}} \frac{\bar{b}^{p-1}}{(p-1)!} C^{np+p-1} \Big((\bar{b} + |b_1|)(\bar{b} + |b_2|) \cdots (\bar{b} + |b_n|) \Big)^p. \tag{5.45}$$

Tässä lausekkeessa ei ole alaindeksillä m olevaa tekijää, joten lausekkeen arvo ei riipu luvusta m. Merkitsemme vielä, että $P = e^{\bar{b}}\bar{b}^{-1}C^{-1}$ ja että $Q^p = (C^{n+1}\bar{b}\prod(\bar{b}+|b_m|))^p$. Tällöin lausekkeen arvo l on muotoa $PQ^p/(p-1)!$, missä lukujen P ja Q arvo ei riipu luvusta p.

Osoittautui siis, että summan

$$L_m = \sum_{r=p-1}^{np+p-1} c_r b_m^r \left\{ \frac{b_m}{r+1} + \frac{b_m^2}{(r+1)(r+2)} + \cdots \right\} \tag{5.46}$$

itseisarvo $|L_m|$ on pienempi kuin luku l oli m mikä hyvänsä väliltä $(1, n)$ ja p miten suuri tahansa.

Kokoamme yllä saamamme tulokset. Luvulla K_p kerromme yhtälön (5.26) muotoon

$$K_p(A + \sum_{m=1}^{n} e^{b_m}) = K_p A + \sum_{m=1}^{n} \left\{ \Phi^{(p)}(b_m) + \cdots + \Phi^{(np+p-1)}(b_m) \right\} + L, \tag{5.47}$$

missä $|L| = |\sum_{m=1}^{n} L_m| < nPQ^p/(p-1)!$. Luku $K_p A$ ei ole alkuluvun p monikerta ja summalauseke on kokonaisluku, joka on jaollinen luvulla p. Lauseen 2.4 mukaan tietystä alkuluvusta $p = p_0$ lähtien lausekkeen

$$nPQ^p/(p-1)! = nPQQ^{(p-1)}/(p-1)!$$

arvo on pienempi kuin 1 eli L on väliltä $(-1, 1)$.

Siis kun p on suurempi lukuja A, n, C, $|C^n b_1 b_2 \cdots b_n|$ ja p_0, niin luku $K_p(A + \sum_{m=1}^{n} e^{b_m})$ on sellaisten lukujen summa, joista toinen on kokonaisluku mutta ei ole nolla ja toinen on reaaliluku väliltä $(-1, 1)$. Niiden summa ei selvästikään ole nolla. Siispä

$$K_p(A + e^{b_1} + e^{b_2} + \cdots + e^{b_n}) = 0 \tag{5.48}$$

on epätosi ja myös yhtälö (5.26)

$$A + e^{b_1} + e^{b_2} + \cdots + e^{b_n} = 0$$

on epätosi. Ne kuitenkin seuraavat suoraan vastaoletuksesta. Tämä on ristiriita, joten väitteemme on oikea eli π on transkendenttinen. □

5.3 Mahdottomuus

Lopetamme tutkielman todistamalla, että ympyrää ei voi neliöidä.

Lause 5.8. *Ympyrää ei voi neliöidä.*

Todistus. Lauseen 5.1 nojalla ympyrän voi neliöidä jos ja vain jos π on konstruoituva. Luku ei ole konstruoituva, koska lauseen 5.2 mukaan konstruoituvat luvut ovat algebrallisia lukuja ja π on lauseen 5.7 perusteella transkendenttinen eli ei-algebrallinen. Ympyrän neliöiminen on siis mahdotonta. □

6 Kirjallisuutta

Ympyrän neliöimistä käsitteleviä teoksia on useita. Niitä on myös verkossa digitoituina joko kokonaisina tai osittain. Esittelen tässä lyhyesti joitakin.

Berggren, Lennart; Borwein, Jonathan M. & Borwein, Peter B.: *Pi, A Source Book*. Springer, 2004.
URL: [http://books.google.com/books?id=QlbzjN_5pDoC].

Kirja sisältää alkuperäisdokumentteja piin historiasta, muun muassa Hermiten ja Lindemannin alkuperäiset transkendenttisuustodistukset sekä Hilbertin yksinkertaistetut todistukset niistä. Kirjasta on tekijänoikeussyiden vuoksi vain rajoitettu esikatselu.

Montucla, Jean Etienne: *Histoire des récherches sur la quadrature du cercle*. Bachelier père et fils, 1831.
URL: [http://books.google.fi/books?id=ieYGAAAAYAAJ].

Tämä alun perin vuonna 1754 julkaistu auttamatta vanhentunut teos kertoo neliöimisongelman historian 1700-luvun puoliväliin asti. Se on merkinnöitään nykyaikainen ja ranskantaitoinen voi tutustua siihen. Kirja on luettavissa kokonaisuudessaan.

De Morgan, Augustus: *A Budget of Paradoxes*. Ayer Publishing, 1969.
URL: [http://www.gutenberg.org/etext/23100].

Morganin vuonna 1872 postuumisti julkaistu teos kertoo muun muassa useista virheellisistä neliömisyritysistä, joita on tehty vuosien saatossa. Project Gutenbergissä kirja on julkaistu kokonaisena.

Viitteet

[1] Beckman, Petr: *π, erään luvun tarina*. Terra Cognita, 2000.

[2] Bell, E.T.: *Matematiikan miehiä*. WSOY, 1963.

[3] Bourbaki, Nicolás. *Elements of the History of Mathematics*. Springer, 1998. Myös verkossa: [http://books.google.com/books?id=Qvo8-KC__VAC].

[4] Boyer, Carl B: *Tieteiden kuningatar: matematiikan historia*. Helsinki: Art House, 1994.

[5] Butzer, Paul L.: *Mathematics in the Region Aachen-Liège-Maastricht from Carolingian Times to the 19th Century*. Bulletin de la Société Royale des Sciences de Liège, 51e année, 1-2, 1982. Myös verkossa: [http://popups.ulg.ac.be/SRSL/docannexe.php?id=1330].

[6] Cajori, Florian: *A history of mathematics*. New York, N.Y. : Chelsea, 1985. Myös verkossa: [http://books.google.com/books?id=mGJRjIC9fZgC].

[7] Dante Alighieri: *Jumalainen näytelmä: Paratiisi*. Suomentanut Eino Leino. Myös verkossa: [http://www.gutenberg.org/etext/12547].

[8] Eukleides: *Elements* (*Alkeet*, alkukielellä kreikaksi *Stoikheia*). Noin 300 eKr. Myös verkossa: [http://aleph0.clarku.edu/~djoyce/java/elements/bookI/bookI.html].

[9] Heath, Thomas Little: *A History of Greek Mathematicians*. Myös verkossa: [http://books.google.com/books?id=drnY3Vjix3kC].

[10] Hobson, Ernest W., Hudson, Hilda P. ym.: *Squaring the circle and other monographs*. New York: Chelsea, 1969.

[11] Jesseph, Douglas Michael: *Squaring the circle: the war between Hobbes and Wallis*. University of Chicago Press, 1999. Myös verkossa: [http://books.google.com/books?id=nMlKxQ0ZUbMC].

[12] Kahanpää, Lauri. *Algebra II, mahdollisuuksia ja mahdottomuuksia* -luentomoniste. Myös verkossa: [http://www.math.jyu.fi/~kahanpaa/Algebrajatko.pdf].

[13] Klein, Felix: *Famous problems of elementary geometry*. New York: Chelsea, 1980.

[14] Lehtinen, Matti: *Johdatus tasogeometriaan* Porvoo Helsinki: WSOY Oppimateriaalit, 2007.

[15] Lehtinen, Matti: *Matematiikan historia*. Matematiikkalehti Solmu, 2000. URL: [http://solmu.math.helsinki.fi/2000/mathist/]. Viitattu 14.7.2009.

[16] Lindelöf, Ernst: *Differentiali- ja integralilasku ja sen sovellutukset*. Helsinki: 1950.

[17] O'Connor, John J. & Robertson, Edmund F.: *Squaring the circle*. MacTutor History of Mathematics archive, 1999.
URL: [http://www-history.mcs.st-andrews.ac.uk/HistTopics/Squaring_the_circle.html]. Viitattu 14.7.2009.

[18] O'Connor, John J. & Robertson, Edmund F.: *Anaxagoras of Clazomenae*. MacTutor History of Mathematics archive, 1999.
URL: [http://www-history.mcs.st-andrews.ac.uk/Biographies/Anaxagoras.html]. Viitattu 14.7.2009.

[19] O'Connor, John J. & Robertson, Edmund F.: *Indian Sulbasutras*. MacTutor History of Mathematics archive, 1999.
URL: [http://www-history.mcs.st-andrews.ac.uk/HistTopics/Indian_sulbasutras.html]. Viitattu 14.7.2009.

[20] Saturnino Salas, Einar Hille, Garrett Etgen. *Calculus*. John Wiley & Sons, Inc., 1990. 9. painos.

[21] Sillanpää, Juha: *Kulman kolmiajaosta ja ympyrän neliöinnistä*. Pro gradu -tutkielma. Tampereen yliopisto, 1993.

[22] Tietze, Heinrich: *Famous problems of mathematics : solved and unsolved mathematical problems from antiquity to modern times*. Baltimore: Graylock Press, 1966.