Helsingin yliopisto

MAST31901 - History of Mathematics

Kurssiessee:

Euler ja lukuteoria

Elli Kiiski

24. huhtikuuta 2024

1 Johdanto

On hankala päättää millä titteleillä hänet esittelisi; ainoastaan hänen ansioluettelonsa läpikäyminen vaatisi oman kymmensivuisen esseensä. Tällä kertaa tarkoitusperiimme kuitenkin sopii tituleerata tätä yleisneroa matemaatikko Leonhard Euleriksi.

Määrittelyongelmat eivät tosin jää siihen, sillä Euler onnistui tuottamaan mullistavia tuloksia myös ällistyttävän monella eri osa-alueella matematiikan alan sisällä. Poistamme hetkeksi mielestämme maailman kauneimman yhtälön[1] sekä Königsbergin siltaongelman[2] ja keskitymme tällä erää matematiikan kuningattareen[3], lukuteoriaan. Eulerin saavutukset yksin tällä sektorilla olisivat varmasti riittäneet nostamaan hänet historiankirjoihin yhtenä historian suurimmista matemaatikoista.

Yhtäläisesti historiallisena kuin matemaattisenakin esseenä tasapainottelemme näiden näkökulmien välillä varoen uppoutumasta liian syvällisesti kumpaankaan. Toisaalta pyrkimyksenä on koota yhteen johdonmukainen[4] kuva Eulerin lukuteoreettisesta elämäntyöstä niin ajallisessa kuin matemaattisessakin kontekstissa. Se kaikki alkaa jo hyvän aikaa ennen Eulerin syntymää.

2 Lukuteoria ennen Euleria

Oikeastaan vielä Eulerinkaan aikana ei puhuttu matematiikan alasta nimeltä lukuteoria [4]. Kuitenkin ongelmia, joiden katsotaan nykyään kuuluvan lukuteorian piiriin, on ratkottu paljon ennen ajanlaskumme alkua. Ensimmäisenä todisteena pidetään babylonialaista Plimpton 322 savitaulua, joka sisältää vaikuttavan määrän yhtälön $a^2+b^2=c^2$ toteuttavia lukukolmikoita, joita kutsutaan tätä nykyä Pythagoraan kolmikoiksi.

Juuri Pythagoraan (n. 580–500 eaa.) nimissä olevat löydökset, joihin kuuluu noiden kolmikoiden ja niihin liittyvän Pythagoraan lauseen lisäksi mm. monikulmioluvut kuten kolmio- ja neliöluvut, ovat ensimmäisiä merkkejä

[1] Eulerin identiteettiä $e^{\pi i}+1=0$ on verrattu Shakespearin sonettin ja testattu maailman kauneimmaksi yhtätlöksi jopa magneettikuvaustutkimuksilla! [11]

[2] Euler todisti, ettei Königsbergissä (nykyinen Kaliningrad) ollut mahdollista tehdä kävelyretkeä, jolla ylittää kunkin kaupungin seitsemästä sillasta täsmälleen kerran [9]

[3] "Mathematics is the queen of the sciences and number theory is the queen of mathematics."
Carl Friedrich Gauss [8]

[4] Varoituksen sananen alaviitteistä: Johtuen kirjoittajan rönsyilevästä ajatuksenkulusta (ja pakonomaisesta tarpeesta selittää kaikki auki) lukijan on syytä varautua ylenpalttiseen määrään lisähuomautuksia, tarkennuksia ja hauskoja faktoja, jotka voi halutessaan myös tyystin sivuuttaa.

lukujen teoreettisemmasta tutkimisesta [1]. Myös myöhemmin tutuksi tulevat täydelliset luvut (*engl. perfect number*) ja ystävälliset lukuparit (*engl. amicable numbers*) yhdistetään häneen ja aikalaisiin seuraajiinsa.

Antiikin kreikan toinen suuri matemaatikko Euklides (n. 300 eaa.) tunnetaan etenkin vaikuttavasta[5] teoksessaan *Elements* [3], joka käsittelee pääosin geometriaa. Sen kirjoissa VII ja IX esitellään kuitenkin perustavanlaatuisia lukuteorian tuloksia etenkin alkulukuihin liittyen. Merkittävimpiin poimintoihin kuuluvat mm. Euklideen algoritmi (suurimman yhteisen tekijän[6] löytäminen) ja todistus alkulukujen määrän äärettömyydestä. Euklides todisti myös Eulerin myöhemmin täydentämän lauseen

Jos luku a on muotoa $(2^p - 1)2^{p-1}$, missä sekä p että $2p - 1$ ovat alkulukuja, a on täydellinen[7]*.*

Maanmiestensä tapaan antiikin Kreikan lopputaipaleen aikaan[8] elänyt Diofantos (n. 250 jaa.) antoi panoksensa lukuteorialle. Jos Euklides oli geometrian isä, voidaan Diofantosta puolestaan pitää algebran keksijänä. Lukuteorian saralla hänet tunnetaan kuitenkin parhaiten hänen mukaansa nimetyistä kokonaislukukertoimisista yhtälöistä, joissa on vähintään kaksi tuntematonta ja joihin etsitään kokonaislukuratkaisuja. Esimerkiksi $a^2 + b^2 = c^2$ on Diofantuksen yhtälö, kun sen rarkaisuksi etsitään Pythagoraan kolmikkoa.

Seuraavilta vuosisadoilta näyttää puuttuvan kaikki nimekkäät lukuteoreetikot, joiden löydökset ja keksinnöt ovat tulleet laajalle yleisölle tutuksi. Näkökanta on kuitenkin varsin Eurooppa-keskeinen. Nimittäin noina aikoina esimerkiksi Intiassa kehitettiin nykyinen kantalukujärjestelmä sekä otettiin muita edistysaskelia, eikä islamilaisenkaan maailman panosta ole syytä väheksyä. Kuitenkaan Brahmaguptan[9] tai Thābit ibn Qurran[10] kaltaiset nimet

[5]Mitä vähättelyä! *Elements* oli aikansa ensimmäinen (tähän päivään säilynyt) matemaattiseen päättelyyn perustuva teos. Euklides käytännössä keksi geometrian.

[6]Luku d on positiivisten kokonaislukujen a ja b suurin yhteinen tekijä, jos sekä a että b ovat sillä jaollisia ja jokainen molemmat luvut jakava toinen luku jakaa myös luvun d. Tätä merkitään $d = \mathrm{syt}(a, b)$.

[7]Täydellinen luku määritellään ihan pian luvussa 3.

[8]Diofantoksen synnyin- tai kuolinaikaa ei tiedetä edes vuosikymmenen tarkkuudella. Persoonana hänestä ei ylipäätään tiedetä juuri erästä nokkelaa runonpartta enempää: ”*His boyhood lasted for $\frac{1}{6}$ of his life; his beard grew after $\frac{1}{12}$ more; after $\frac{1}{7}$ more he married, and his son was born five years later; the son lived to half his father's age and the father died four years after his son.*”[1] Arvoitusta vastaavan yhtälön $x = \frac{1}{6}x + \frac{1}{12}x + \frac{1}{7}x + 5 + \frac{1}{2}x + 4$ ratkaisemalla voidaan sentään laskea Diofantoksen iäksi 84 vuotta.

[9]Brahmagupta (n. 600 jaa.) edeltäjänsä Āryabhaṭan jalanjäljissä löysi ensimmäisenä yleisen rakaisun lineaariselle Diofantoksen yhtälölle $ax + bx = c$. Oikeastaan nämä intialaiset matematiikot olivat tosiasiassa ne, jotka hyväksyivät Diofantoksen yhtälön ratkaisuksi vain kokonaislukuja. Diofantos itse oli ollut kiinnostunut kaikista rationaalilukuratkaisuista, vaikka määritelmä kantaakin hänen nimeään.[1]

[10]Thābit ibn Qurra (n. 836–901) oli paitsi taitava kääntäjä (hän käänsi useita antiikin Kreikan teoksia arabiaksi) myös hänen oma kirjansa *Book on the Determination of Amicable Numbers* esitteli säännön, jolla voi generoida ystävällisiä lukupareja (jos alaviit-

eivät esiinny historian kirjoissamme yhtä tiuhaan.

Matematiikan kiinnostus oli ylipäätään ollut vähäistä 1500-luvulla, mutta pian vuosisadan vaihtuessa lukuteorian osalta alaa alkoi elvyttää Pierre de Fermat (1601–1665). Mieleepainuvin häneen yhdistetty seikka lienee "ihmeellinen todistus", jonka hän väittää keksineensä Fermat'n suurelle lauseelle[11] (*engl. Fermat's last theorem*), jonka mukaan mitkään positiiviset kokonaisluvut a, b ja c eivät toteuta yhtälöä $a^n + b^n = c^n$, kun $n > 2$. Moneen muuhunkaan Fermat'n teoreemaan ei ole löydetty hänen omia todistuksiaan (joskin hän ne väitti todistaneensa), mutta myöhemmin muiden näytettyä niitä päteviksi[12] ne kantavat silti keksijänsä nimeä.

Vuihdoin vonna 1707 syntyi Leonhard Euler, joka seuraavana 76 elinvuotenaan kehitti eteenpäin (lähes) jokaisen aikaansa edeltäneen lukuteoreetikon aikaansaannoksia.

3 Täydelliset luvut ja ystävälliset parit

Kuten todettu, tuottoisana matemaatikkona Euler ehti tuottaa lukuisia löytöjä ja todistuksia myös lukuteorian saralla. Vaikka monimutkaisimmat näistä saavat n. vuoden matematiikan opiskelijankin raapimaan päätään, osa puolestaan vaikuttaa nykyihmiselle hyvinkin yksinkertaisilta. Kansantajuisimmasta päästä ovat niin kutsutut täydelliset luvut ja ystävälliset lukuparit.

Täydellinen luku *Positiivinen kokonaisluku, joka on omien itseään pienempien tekijöidensä summa. Esimerkiksi luku* 6 *on täydellinen, koska* $1 + 2 + 3 = 6$.

Palataan nyt aiemmin luvussa 2 esiteltyyn Euklideen täydellisiä lukuja koskevaan lauseeseen, jonka Euler todisti omana aikanaan pätevän myös toiseen suuntaan. Hänen versionsa kuuluu seuraavasti.

Jos luku a on parillinen täydellinen luku se voidaan kirjoittaa muodossa $(2^p - 1)2^{p-1}$, missä sekä p että $2p - 1$ ovat alkulukuja.

Euler siis todisti, että Euklideen todistama yhteys täydelliseten lukujen ja

teellä voisi olla alaviite, kirjoittaisin auki myös kyseisen säännön). Hänen nimissään ei kuitenkaan ole yhtään löydettyä paria.

[11] Fermat'n suuri lause löydettiin hänen jo kuoltua raapustettuna Diofantoksen *Arithmetican* marginaaliin yhdessä (vapaasti suomennetun) huomautuksen "Olen keksinyt tälle ihmeellisen todistuksen, joka ei kuitenkaan mahdu tähän marginaaliin" kera. Lause onnistettiin todistamaan vasta vuonna 1995. Andrew Wiles käytti ratkaisussaan varsin modernia matematiikkaa, mikä vahvasti vihjaa siihen suuntaan, ettei Fermatilla tainnutkaan olla tiedossaan virheetöntä todistusta.

[12] Luku 4 käsittelee Euleri Fermat'n töiden jatkajana. Lisää myös Fermat'sta silloin.

lausekkeen $(2^p - 1)2^{p-1}$ välillä on yhtäpitävä eli pätee molempiin suuntiin. Siinä missä Euklides näytti, että luvun toteuttaessa kyseisen lausekkeen, se on täydellinen, Euler osoitti, että luvun ollessa täydellinen ja parillinen (parittomia täydellisiä lukuja ei ole löydetty tai niiden olemassaolemattomuutta todistettu **??**) se toteuttaa kyseisen lausekkeen.

Ystävälliset lukuparit liittyvät läheisesti täydellisiin lukuihin, tavallaan tällaisten lukujen voisi luonnehtia olevan ikään kuin täydellisiä toisilleen. Täsmällinen määritelmä voidaan kirjoittaa seuraavanlaisesti.

Ystävällinen lukupari *Pari* (A, B) *erisuuria positiivisia kokonaislukuja, joille pätee, että luvun* A *itseään pienempien tekijöiden summa on* B *sekä toisinpäin. Esimerkiksi* $(220, 284)$ *on tällainen.*

Ennen Euleria ystävällisiä lukupareja oli löydetty vasta kaksi, niin kutsutut Pythagoraan pari $(220, 284)$ sekä Fermat-Descartesin pari $(17296, 18416)$. Euler kasvatti tätä määrää huimalla 59 parilla, joiden joukossa on myös parittomia lukupareja. Esimerkiksi $(67095 = 3^3 \cdot 5 \cdot 7 \cdot 71, 71145 = 3^3 \cdot 5 \cdot 17 \cdot 31)$ on Eulerin löytämä pariton ystävällinen lukupari.

Ystävällisiä lukupareja tunnetaan nykyään yli miljardi, ja niistä suurimmat ovat tuhansia numeroita pitkiä. Tietokoneiden laskentatehon kehityksellä on tietenkin ollut tähän valtava vaikutus, ja uusien löytöjen algoritmista generointia voi tuskin verrata Eulerilla käytössään olleisiin metodeihin. Tutkimalla lukujen ominaisuuksia Euler kuitenkin huomasi alkuluvuilla olevan hyödyllisiä ominaisuuksia tekijöiden summia laskettaessa, joita hän pystyi käyttämään hyväkseen. [**tarvii kaivaa siitÃď yhdestÃď exam paperista**]

Loppujen lopuksi onkin vähemmän merkittävää, kuinka monta uutta ystävällistä lukuparia tai täydellistä lukua Euler itse onnistui löytämään. Hänen kehittämänsä menetelmät niiden tuottamiseen sen sijaan ovat antaneet työkaluja tulevaisuuden matemaatikoille kasvattaa kyseisiä lukulistoja.

4 Eulerin φ-funktio ja muita nimikkotuotteita

Siltä varalta, ettei Eulerin massiivista aikaansannosten määrää ole vielä alleviivattu tarpeeksi, päästään kyseiseen tavoitteeseen viimeistään tutkimalla Wikipedia-sivua *List of things named after Leonhard Euler* (lista Leonhard Eulerin mukaan nimetyistä asioista) [6]. Pelkästään teoreemoja hänen nimellään löytyy 11 kappaletta. Listalle niin ikään lukeutuva Eulerin identiteetti vilahtikin jo erässä aiemmassa alaviitteessä, mutta listaus sisältää tietysti myös useita merkittäviä lukuteorian tuloksia.

Eulerin vuonna 1763 esittelemä φ-funktio (*engl. Euler's totient function*) [2] on eräs lukuteoriassa usein näyttäytyvistä (ja ehkä myös yksi kiinnostavimmista[13]) funktioista. Sen arvo kertoo lukujen jaollisuudesta, tosin käänteisesti: mitä useammalla luvulla jaollinen luku kokoonsa nähden on, sitä pienempi on ϕ-funktion arvo.

Eulerin ϕ-funktio $\phi : \mathbb{N} \to \mathbb{N}$
$\phi(1) = 1$ *sekä kaikilla* $n \geq 2$, $\phi(n)$ *on sellaisten lukujen* $1, 2, ..., n$ *määrä, joiden suurin yhteinen tekijä luvun* n *kanssa on* 1.

Myöhemmin käsiteltävien tulosten lisäksi ϕ-funktiota käytetään myös MISSÄ.

Myös lukuteorian todistuksissa toisinaan esiintyvä Eulerin-Macheronin vakio $\gamma \approx 0,5772$ kantaa päähenkilömme nimeä. Tätä Eulerin ensimmäistä kertaa vuonna 1734 käyttämää vakiota harmonisen sarjan ja luonnollisen logaritmin erotukselle kutsutaan toisinaan myös pelkästään Eulerin vakioksi. Sitä ei pidä kuitenkaan sekoittaa luonnollisen logaritmin kantalukuun $e \approx 2,71823$ (*engl. Euler's number*[14]).

Alkuluvut 2, 3, 5, 11, 17 ja 41 on puolestaan nimetty Eulerin onnenluvuiksi (*engl. Lucky number of Euler*), koska ne toteuttavat seuraavan ehdon: sijoitettuna termin n tilalle lausekkeeseen $k^2 - k + n$, ne tuottavat alkuluvun jokaisella $1 \leq k < n$ [7]. Kyseinen kuuden numeron listan tosin osoitettiin tyhjentäväksi vasta 1900-luvulla.

Euler's criterion (quatratic root modulo)

Euler's factorization method

5 Fermat'n töille jatkoa

Fermatin, viimeisimmän häntä edeltäneen nimekkään lukuteoreetikon, työt olivat Eulerille tuttuja ja innoittivatkin häntä jatkamaan niistä useita. Koska Fermat ei itse ollut järin tuottelias todistaja, saattoi Euler joitakin hänen töitään loppuun osoittamalla ne todeksi ja toisinaan kehitti niitä yleisempään muotoon. Toisaalta Euler myös kumosi muutamia Fermat'n hypoteeseja ja konjetuureja.

Yksi tusinasta Eulerin lauseesta, omaperäiseltä nimeltään Eulerin lause (*engl. Euler's theorem*), on itse asiassa yleistys Fermat'n pienestä lauseesta.

[13] Kirjoittaja sattui tekemään kandityönsä *The Order of Euler's totient function* kyseisen funktion kasvuvauhdin alarajasta [5].

[14] Suomeksi sekaannuksen vaara ei ole yhtä ilmeinen, sillä lukua e kutsutaan Neperin luvuksi John Napierin mukaan, jonka teksteissä käsiteltiin luonnollisia logaritmeja jo 1618. Euler puolestaan vakiinnutti luvulle symbolin e (tuskin kuitenkaan oman nimikirjaimensa mukaan, kuten jotkut ovat arvelleet) ja todisti vuonna 1748 julkaisussaan *Introductio in Analysin infinitorum* vakiolle summamuodon $e = \sum_{n=0}^{\infty} \frac{1}{n!} = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots$ [10].

Fermat'n pieni lause

Kaikille alkuluvuille p ja kokonaisluvuille a pätee $a^p \equiv a \pmod{p}$. Yhtäpitävästi $a^{p-1} \equiv 1 \pmod{p}$.

Eulerin lause

Kaikilla kokonaisluvuilla a, joiden suurin yhteinen tekijä positiivisen kokonaisluvun n kanssa on 1, pätee $a^{\phi(n)} \equiv 1 \pmod{n}$.

Fermat'n pieni lause on itse asiassa esimerkki lauseesta, jota hän ei nimestä huolimatta itse todistanut. Sen teki sen sijaan Euler vuonna 1736 tekstissään *Theorematum quorundam ad numeros primos spectantium demonstratio.* Myöhemmin, vuonna 1763 muotoiltuaan edellä esitellyn ϕ-funktion, hän todisti sen avulla oman lauseensa, joka yleistää alkuperäisen lauseen koskemaan myös lukuja, jotka eivät kuulu alkulukuihin. Toisin sanoen Fermat'n pieni lause on erikoustapaus Eulerin lauseesta, jossa n on alkuluku.

the quadratic reciprocity law / euler's criterion

6 Alkuluvut

Jokaisen matemaatikon ja etenkin lukuteoreetikon klassikkolemppari

Konjektuuri n 2n keissi

Suhteelliset alkuluvut ehkä voi mainita

Mitä olikin jo aiemmin esim onneluvut

7 Eulerin perintö

Gauss tuli eulerin jälkeen

Konjektuuri, ettei ole parittomia alkulukuja (ei vieläkän todistettu)

Primitive roots ja fii-funktio RSA

Erilaisia irrationaalilukuja

Analyysin käyttö lukuteoriassa ja siten analyyttisen lukuteorian kehittäminen

8 muistiinpanot

8.1 A. A. Karatsuba

In Euler's time there was no such a field of science as "number theory." s.1

Yleisti euklideen lauseen täydellisista luvuista (mersenne prime) ja löysi 59 amicable number pairia (kohta 1)

Frematin konjektuuri että Fn on kaikki alkulukuja, Euler disproves (kohta 2a)

Yleisti fermatin pienen teoreeman fii-funktion avulla (kohta 2b)

Kongruenssin ja quadratic residues, Legendre-juttuja en muista mitään mutta Euler muototoili quadratic reciprocityn mutta ei vielä todistanut (kohta 2c)

Lukujen esittäminen $x^2 + y^2$ jne muodossa, Euler todisti luvuille muotoa 4n+1 jne. (kohta 2d)

Pellin yhtälön ja continued fractions yhdistävä alkgoritmi jotenki en ihan tajuu (kohta 2e)

Jotain neljän neliön summa Lagrangen kanssa ja että kuinka lähelle lukua voi päästä kahden neliön summalla, ilmeisesti jatkoa kohtaan 2d (kohta 2f)

Todisti fremat's last theorem kun n=3, sen innoittamana(?) syntyi algbraic number theory (kohta 2gg)

Euler keppas primitive roots and indices (kohta 3)

Keksi idean transkendenttiluvuista (kohta 4)

Löytyy aina ailkuluku välistä n ja 2n, f(x) = x2 - x+ A antaa alkulukuja, Goldbach problem (kohta 5)

Euler is the author of two methods for solving problems in number theory by means of analysis mut ei kerrota mitkä??? (kohta 6)

Euler ja Bach ??? (kohta 7)

Euler's identity ja Reiamnnin zeta funktio, voi käyttää apuna todistamaan infinitely many primes, myös Dirichlet characters ja Dirichlet's L-function ja Chebyshev's studies of 1848, joista en ymmärtänyt ensilukemalla mitään OKEI tää kohta pitää lukee paremmilla aivoilla uudestaan jos on tarpeellinen (kohta 8)

loput meni ihan yli hilseen (kohta 9)

Viitteet

[1] D.M. Burton. *The History of Mathematics: An Introduction.* Mcgraw-Hill, 2011.

[2] *Euler's totient function, Wikipedia.* URL: https://en.wikipedia.org/wiki/Euler%27s_totient_function.

[3] R. Fitzpatrick J.L. Heiberg. *EUCLID'S ELEMENTS OF GEOMETRY, edited and provided with a modern English translation.*

[4] A.A. Karatsuba. *Euler and Number Theory.* Proceedings of the Steklov Institute of Mathematics, 2009.

[5] Elli Kiiski. *The Order of Euler's totient function.* Kandidaatintutkielma. Saatavilla osoitteessa https://github.com/ellikiiski/Bachelors-thesis-2021/blob/master/Versiohistoria/version-FINAL.pdf. 2021.

[6] *List of things named after Leonhard Euler, Wikipedia.* URL: https://en.wikipedia.org/wiki/List_of_things_named_after_Leonhard_Euler.

[7] *Lucky Number of Euler, Wolram MathWorld.* URL: https://mathworld.wolfram.com/LuckyNumberofEuler.html.

[8] *Quotations, University of St Andrews.* URL: https://mathshistory.st-andrews.ac.uk/Biographies/Gauss/quotations/.

[9] *Seven Bridges of Königsberg, Wikipedia.* URL: https://en.wikipedia.org/wiki/Seven_Bridges_of_K%C3%B6nigsberg.

[10] *The number e, MacTutor.* URL: https://mathshistory.st-andrews.ac.uk/HistTopics/e/.

[11] R. Wilson. *Euler's Pioneering Equation: The Most Beautiful Theorem in Mathematics.* Oxford University Press, 2019.