

Helsingin yliopisto

MAST31901 - History of Mathematics

Kurssiessee:

Euler ja lukuteoria

Elli Kiiski

6. toukokuuta 2024

1 Johdanto

On hankala päättää millä titteleillä hänet esittelisi; ainoastaan hänen ansioluettelonsa läpikäyminen vaatisi oman kymmensivuisen esseensä. Tällä kertaa tarkoituspärimme 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 yhtälön¹ sekä Königsbergin siltaongelman² ja keskitymme tällä erää matematiikan kuningattareen³, 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 johdonmukainen⁴ 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

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

²Euler 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]

⁴Varoituksen sanan 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 tulivat 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 vaikuttavasta⁵ 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 tekijän⁶ 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 täydellinen⁷.

Maanmiestensä tapaan antiikin Kreikan lopputaipaleen aikaan⁸ 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 Diofantoksen yhtälö, kun sen rarkaisuksi etsitään Pythagoraan kolmikkoa.

Seuraavilta vuosisadoilta näyttää puuttuvan kaikki nimekkäät lukuteoreetikot, joiden löydökset ja keksinnöt olisivat tulleet laajalle yleisölle tutuksi. Näkökanta on kuitenkin varsin Eurooppa-keskeinen. Nimittäin noina aikoina esimerkiksi Intiassa kehitettiin nykyinen kantalukujärjestelmä sekä otettiin muita edistysaskelia, eikä islamilaisenaan maailman panosta ole syytä väheksyä. Kuitenkaan Brahmaguptan⁹ tai Thābit ibn Qurran¹⁰ kaltaiset nimet

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

⁶Luku 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 $d = \text{sy}(a, b)$.

⁷Täydellinen luku määritellään ihan pian luvussa 3.

⁸Diofantoksen 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.

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

¹⁰Thābit 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 ylipäättään 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 lauseelle¹¹ (*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 päteviksi¹² 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. Kansantajuimmasta 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 täydellisten lukujen ja

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

¹¹Fermat’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 onnistitiin todistamaan vasta vuonna 1995. Andrew Wiles käytti ratkaisussaan varsin modernia matematiikkaa, mikä vahvasti vihjaa siihen suuntaan, ettei Fermatilla tainnutkaan olla tiedossaan virheetöntä todistusta.

¹²Luku 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. Tällainen 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 siitä yhdestä 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 näytettyistä (ja ehkä myös yksi kiinnosta-

vimmista¹³) 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 $\phi : \mathbb{N} \rightarrow \mathbb{N}$

$\phi(1) = 1$ sekä kaikilla $n \geq 2$, $\phi(n)$ on sellaisten lukujen $1, 2, \dots, n$ määrä, joiden suurin yhteinen tekijä luvun n kanssa on 1.

Eulerin ϕ -funktioita käytetään laajasti lukuteoriassa ja jopa käytännön sovelluksissa, kuten luvussa 7 kuuullaan.

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).

Menemättä tarkemmin neliöjäännösten teoriaan ja Legendren symboliin¹⁵ mainittakoon tässä kohtaa niin kutsuttu Eulerin kriteeri (engl. *Euler's criterion*). Tarkemmin ajatellen kriteerin esittely tuskin juuri lämmittää lukijaa ilman näitä taustietoja, mutta vuonna 1748 todistettu yhteys kuuluu kaikessa kontekstin puutteessaan seuraavasti.

Eulerin kriteeri $\left(\frac{a}{n}\right) \equiv a^{\frac{p-1}{2}} \pmod{n}$

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.

5 Fermat'n töille jatkoa

Fermatin, viimeisimmän häntä edeltäneen nimekkään lukuteoreetikon, työt olivat Eulerille tuttuja ja innoittivatkin häntä jatkamaan niistä useita. Kos-

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

¹⁴Suomeksi 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 $e = \sum_{n=0}^{\infty} \frac{1}{n!} = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots$ [10].

¹⁵Luku a on neliöjäännös modulo n , jos on olemassa kokonaisluku x , jolla pätee $x^2 \equiv a \pmod{n}$. Puolestaan Legendren symbolin $\left(\frac{a}{n}\right)$ arvo on 1, jos a on neliöjäännös modulo n (sekä -1 jos näin ei ole ja nolla jos n on jaollinen a :lla)

ka Fermat ei itse ollut järin tuottelias todistaja, saattoi Euler joitakin hänen töitään loppuun osoittamalla ne todeksi ja toisinaan kehitti niitä yleisemmän muotoon. Toisaalta Euler myös kumosi muutamia Fermat'n hypoteeseja ja konjektuureja.

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

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.

Osaa löydöksistään Fermat ei ilmeisesti edes väittänyt todistaneensa, ja niihin viitataan asianmukaisesti konjektuureina. Yksi tällainen oli Fermat'n otaksuma siitä, että kaikki luvut muotoa $F_n = 2^{2^n}$ (missä n on positiivinen kokonaisluku) ovat alkulukuja [4]. Euler onnistui kuitenkin kumoamaan väitteen näyttämällä, että luku $F_5 = 4294967297 = 642 \cdot 6700417$ ei kuulu alkulukuihin¹⁶.

Toinen Fermat'n konjektuuri, jota Euler tutki ja tällä kertaa todisti todeksi, liittyy lukujen esittämiseen kahden neliön summana. Konjektuurin mukaan kaikki alkuluvut muotoa $p = 4n + 1$ ja vain tällaiset luvut voidaan esittää muodossa $a^2 + b^2$. Euler jatkoi havaintojaan osoittamalla vastaavanlaisen yhteyden¹⁷ esityksille $a^2 + 2b^2$ ja $x^2 + 3b^2$.

Kuuluisa Fermat'n suuri lause (*engl. Fermat's last theorem*) ei myöskään jäänyt Eulerilta rauhaan. Hän nimittäin todisti, ettei tapaukselle $x^3 + y^3 = z^3$ löydy ratkaisua positiivisten kokonaislukujen joukosta. Moisessa hän onnistui tutkimalla algebrallisten lukujen ominaisuuksia ja hyödyntämällä tietä-

¹⁶Konjektuurin kumoamisesta huolimatta kyseistä muotoa olevat luvut F_n on kuitenkin nimetty Fermat'n luvuiksi.[4]

¹⁷Euler näytti, että alkuluvut muotoa $p = 8n + 1$ ja $p = 8n + 3$, ja vain tällaiset voidaan esittää muodossa $a^2 + 2b^2$ sekä alkuluvut muotoa $p = 6n + 1$, ja vain tällaiset voidaan esittää muodossa $a^2 + 3b^2$.

mättään aritmetiikan peruslausetta¹⁸, josta tuli lause vasta Gaussin todistettua sen vuosia myöhemmin.

6 Vielä vähän alkuluvuista

Voiko lukuteoreetikosta puhua ilman, että käsittelee tämän suhdetta alkulukuihin? Jo esimerkiksi hänen mukaansa nimettyjä "onnenlukuja" pikaisesti käsitellessämme saattoi arvella, ettei myöskään Euler karttanut uransa aikana alkulujen pyörittelyä vaikka vain omaksi huvikseenkin. Aikaisemmissa luvuissa tarkasteltujen tapausten, jotka suurin osa (kuten koko lukuteoria) liittyvät tiiviisti alkulukuihin, jälkeen onkin yhä jäljellä ainakin yksi mainitsemisen arvoinen sekä alkulukuihin että Euleriin liittyvä tulos.

Euleria ei laajalti tunneta konjektuuristaan, jonka mukaan jokaisen positiivisen kokonaisluvun n (pois lukien 1) ja oman tuplauksensa $2n$ välille mahtuu ainakin yksi alkuluku. Lausetta kutsutaankin yleensä Bertrandin postulaatiksi¹⁹ ranskalaisen matemaatikon mukaan, joka onnistui näyttämään väitteen pitävän paikkansa ainakin kolmeen miljoonaan saakka. Sittenkin koko väitteen ovat todistaneet Tšebyšov ja vaihtoehtoisia helpompia tapoja esittäneet Ramanujan ja Erdős.

7 Eulerin perintö

Euler kuoli aivoverenvuotoon vuonna 1783 Pietarissa, minne hänet myös haudattiin (kuva 7). Hän kuulemma luhistui keskustellessaan erään aikalaisensa astronomin kanssa äskettäin löydetyistä uudesta planeetasta, Uranuksesta. Loppuun asti aktiivisena tiedeyhteisön jäsenenä toimineena yleisnerona hän jätti jälkeensä valtaisan perinnön.

Edeltäjänsä kuoleman aikaan kuusivuotias Carl Friedrich Gauss (1777-1855) pääsikin ensin vähän vartuttuaan jatkamaan siitä mihin Euler jäi. Hän mm. todisti Eulerin kriteerin pohjalta neliöjäännöslauseen ja olipa hän itse asiassa se, joka alkoi käyttää Eulerin ϕ -funktioista puhuttaessa nimenomaan symbolia ϕ [4]. Saavutuksissankin hän ylsi elämänsä aikana Euleriin verrattavalle tasolle.

¹⁸Aritmetiikan peruslauseen mukaan jokainen ykköstä suurempi kokonaisluku voidaan ilmaista alkulukujen summana täsmälleen yhdellä tavalla.

¹⁹Kirjoittajan asiaton välikommentti: Miksi Fermat on saanut pitää nimissään kaikki arvailunsa ja muka todistamansa väitteet, mutta Eulerin aikaansaannoksista osa ei kanna nykypäivänä hänen nimeään? Tai onhan tässä jo paasattukin, kuinka Eulerin nimellä löytyy ties kuinka monia tuloksia, joten kaikei kritiikki oikeastaan kohdistuu enemmän Fermat'n nimen ylenpalttiseen viljelyyn.

Gaussin jälkeen tulivat Dirichlet (1805-1859), Hadamard (1865-1963), Ramanujan (1887-1920), Wiles (1953-)... Ja lukuteoria on jatkanut kehittymistään. Jotkin asiat eivät tosin ole selvinneet edes tietokoneiden käsittämättömän laskentatehon avulla: Euler epäili aikanaan, ettei parittomia täydellisiä lukuja ole olemassa. Tuohon otaksumaan ei osata varmuudella sanoa juuta eikä jaata vielä vuoden 2024 toukokuussakaan.

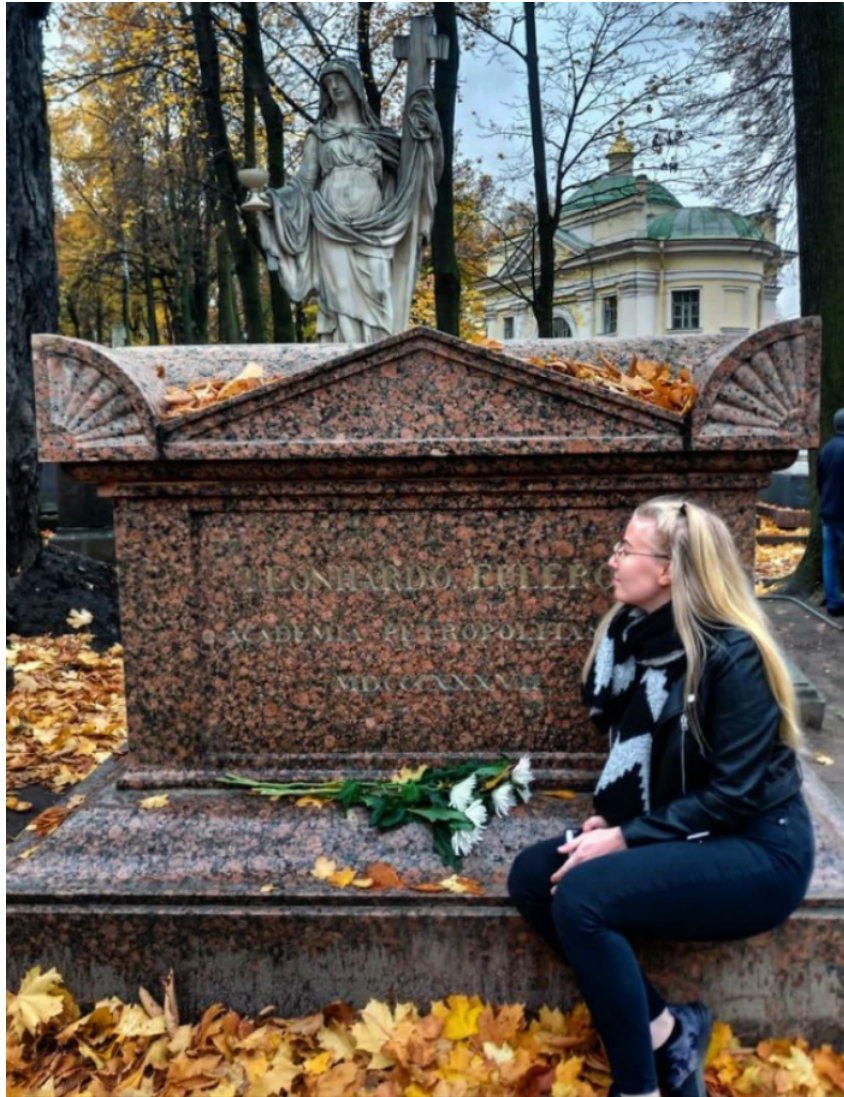
Lukuteorian perustavanlaatuisen ja toisaalta abstraktin luonteen takia on varsin harvinaista, että sen tuloksia sovelletaan suuremmin käytännössä. Siitä huolimatta maailmaa mullistanut ja vieläkin tärkeää osaa kyberturvallisuudessa näyttelevä RSA-salaus perustuu nimenomaan lukuteoriaan. Unohattamatta kenestä tässä essee oikeastaan olikaan kyse, ovat Eulerin panokset avainasemassa salausalgoritmin toiminnassa.

Eulerin ϕ -funktion, sen ominaisuudet sekä paikka Eulerin lauseessa (käsiteltiin luvussa 5) mahdollistavat suunnattoman suurien lukujen pyörittelyn ilman, että jopa tietokoneiden laskimille liian isoja lukuja tarvitsee oikeasti hajottaa alkutekijöihin. Hauska ajatella, kuinka Euler ei aikanaan villeimmissä houreissaankaan olisi voinut arvata, mihin hänen aikaansaannoksensa vielä jonakin päivänä suoraan kytkeytyvät.

Ei pidä luulla, että edellä olisi missään nimessä katettu kaikkea sitä, mitä Euler sai lukuteorian saralla aikaan. Monia hänen tuotoksistaan sivuutettiin joko liian hankalan matematiikan ymmärtämisen tai selitystaitojen ontuessa tai yksinkertaisesti tilan puutteen tähden²⁰. Toisaalta Euler vaikutti töillään yleisemmin myös analyyttisen ajattelun hyödyntämisessä lukuteoriassa, mikä kantanut hedelmää kaikissa hänen jälkeensä tulleissa lukuteoreetikoissa.

Jospa siis vihdoinkin hyväksytään, ettei Eulerin panosta lukuteorialle voi mitata.

²⁰Oikeastaan turha myöskään kuvitella, että kaikki hänen löydyksensä olisivat edes tätä kirjoittaessa tulleet vastaan.



Kuva 1: Eulerin haudalla Pietarissa syksyllä 2019.

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*, Wolfram 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.