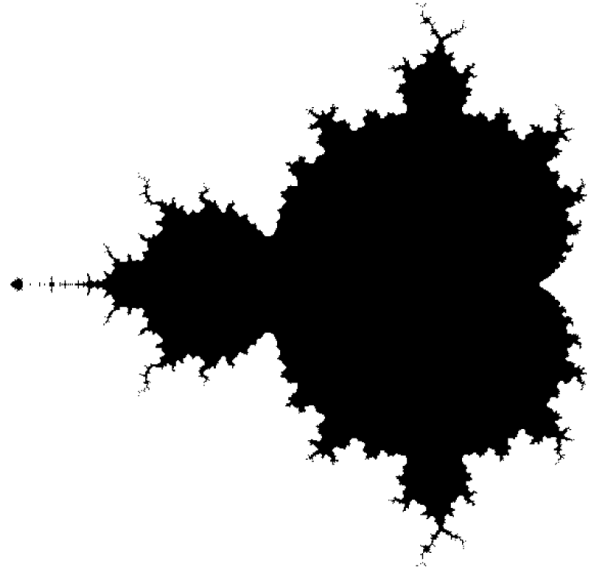


Janne Hakkarainen

Tarinoita matematiikasta



Alkuluvuista Elämän peliin

Tietokirja

Tarinoita matematiikasta

Janne Hakkarainen

Tarinoita matematiikasta

ALKULUVUISTA ELÄMÄN PELIIN

Books on Demand

Copyright © 2019 Janne Hakkarainen

KUSTANTAJA: BOD – BOOKS ON DEMAND, HELSINKI, SUOMI

VALMISTAJA: BOD – BOOKS ON DEMAND, NORDERSTEDT, SAKSA

ISBN: 978-952-80-0745-6

*"Äiti, mikä on ääretön?" Äiti: "Mistä
kuulit?" Matias: "Isiltä!"*

Osa I

**Alkuluvuista Riemannin
hypoteesiin**

Alkuluvut

ALKULUVUT voidaan nähdä muiden lukujen rakennuspalikoina ja siksi ne ovat kiehtoneet matematiikan harrastajia jo ennen ajanlaskun alkua. Alkuluvuiksi kutsutaan lukua 1 suurempia kokonaislukuja, jotka ovat jaollisia vain luvulla 1 ja itsellään. Ensimmäiset 15 alkulukua ovat

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 ja 47.

Muita lukuja kuin alkulukuja ja lukua 1 kutsutaan *yhdistetyiksi* luvuiksi, sillä ne voidaan kirjoittaa muiden lukujen tulona (lukua 1 ei pidetä alkulukuna eikä yhdistettynä lukuna). Näiden lukujen ei tarvitse välttämättä olla alkulukuja, sillä esim. luku 8 voidaan kirjoittaa muodossa $8 = 4 \cdot 2$. Toki tulossa oleva yhdistetty luku voidaan aina kirjoittaa edelleen kahden luvun tulona ja lopulta pelkkiä alkulukuja käyttäen. Siis esimerkiksi $8 = 2 \cdot 2 \cdot 2$. Osoittautuu, että niin kutsutun aritmetiikan peruslauseen mukaan jokaisen luvun alkutekijähajotelma on yksikäsitteinen. Muun muassa tästä syystä lukua 1 ei pidetä alkulukuna.

Euklideen¹ lause eli teoreema sanoo: *alkulukua on äärettömän monta*.

Esitetään Euklideen lauseelle todistus. Tehdään vastaoletus ja oletetaan, että väite ei pidä paikkaansa. Vastaoletuksen mukaan alkulukuja on äärellinen määrä, joten ne voidaan listata muodossa $p_1, p_2, \dots, p_k$. Muodostetaan uudet luvut $a = p_1 \cdot p_2 \cdots p_k$ ja $b = a + 1$. Jos luku $b > 1$ on alkuluku se ei ole mukana alkuperäisessä listassa, joten sen pitää siis olla yhdistetty luku, joten sille voidaan kirjoittaa alkutekijähajotelma. Olkoon q joku luvun b alkutekijöistä. Luvun q pitää siis olla joku luvuista $p_1, p_2, \dots, p_k$. Nyt luku q jakaa sekä luvun a , että luvun b eli se jakaa myös niiden erotuksen $b - a$. Koska $b - a = 1$, niin q siis jakaa luvun 1. Tästä syntyy ristiriita eli vastaväitteen pitää olla epätosi ja alkuperäisen väitteen tosi. Tämä todistaa Euklideen lauseen.

Tämä todistus saattaa tuntua hämmentävältä, sillä todistus ei itessään kerro alkuluvuista mitään eikä anna esimerkiksi kaavaa tai

¹ Eukleides Aleksandrialainen (n. 300 eaa.) oli kreikkalainen matemaatikko, joka kirjoitti oppikirjan *Alkeet* (lat. *Elementa*).

keinoa, jolla generoida loputtomasti uusia alkulukuja. Todistus perustuukin ns. epäsuoran todistuksen periaatteeseen, jonka tarkoituksena on aiheuttaa vasta oletuksesta syntyvä ristiriita. Se on yleinen keino matematiikasta.

Yksi keskeinen alkulukuihin liittyvä ongelma on määrittäminen milloin joku luku on tai ei ole alkuluku. Monista suurista luvista osataan tämä päätellä vaikka yhdistetyn luvun tapauksessa tekijöitä ei tiedetä. Myös tämä on yleinen ominaisuus matematiikassa. Voidaan sanoa, että johonkin ongelmaan on olemassa ratkaisu vaikka itse ratkaisua ei tunneta! Tarkastellaan seuraavaksi kahta lausetta, jotka ovat peräisin Pierre de Fermat² n² kynästä. Katsotaan kuitenkin ensin ns. kellotauluaritmetiikkaa.

Jakojäännöksellä tarkoitetaan kokonaislukua, joka jää yli kun luku jaetaan jollain toisella luvulla. Esimerkiksi kun luku 19 jaetaan luvulla 12 jakojäännökseksi saadaan 7. Merkitään $19 \equiv 7 \pmod{12}$ ja vastaavasti esim. $21 \equiv 9 \pmod{12}$ ja $48 \equiv 0 \pmod{12}$.

Fermat'n pieni lause sanoo: Jos p on alkuluku ja a on mikä tahansa ei p :llä jaollinen kokonaisluku, niin $a^{p-1} - 1$ on jaollinen luvulla p . Tosin sanoen $a^{p-1} \equiv 1 \pmod{p}$.

Jos esimerkiksi $a = 2$ ja $p = 9$, niin $a^{p-1} = 256$, mutta $256 \equiv 4 \pmod{9}$ eli luku 9 ei ole Fermat'n pienen lauseen nojalla alkuluku. Toisaalta siitä, että $a^{p-1} \equiv 1 \pmod{p}$ pätee *jollain* a ei voi päätellä, että p olisi varmuudella alkuluku. Esimerkiksi $2^{341-1} \equiv 1 \pmod{341}$, mutta $3^{341-1} \equiv 332 \pmod{341}$ eli luku 341 ei ole alkuluku.

Fermat'n joululause³ sanoo: Olkoon p pariton alkuluku. Luku p voidaan kirjoittaa kahden kokonaisluvun neliön summana eli $p = a^2 + b^2$, jos ja vain jos $p = 4n + 1$ jollain n . Käyttäen kellotauluaritmetiikkaa voidaan $p = 4n + 1$ kirjoittaa muodossa $p \equiv 1 \pmod{4}$.

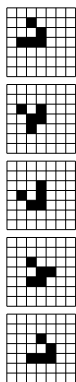
Esimerkiksi $5 = 4 \cdot 1 + 1$ ja $13 = 4 \cdot 3 + 1$, joten ne voidaan kirjoittaa kahden kokonaisluvun neliön summana ($5 = 1^2 + 2^2$ ja $13 = 2^2 + 3^2$). Vastaavasti esimerkiksi alkulukuja 3, 7 ja 11 ei voi kirjoittaa muodossa $p = 4n + 1$ jollain n , joten niitä ei voi esittää kahden kokonaisluvun neliön summana.

Näille molemmille lauseille, kuten myös monille muille Fermat'n lauseille, ensimmäiset (oikeat) todistukset julkaisi sveitsiläinen matemaatikko Leonhard Euler noin sata vuotta myöhemmin.

Alkulukuihin liittyy paljon väittämiä, joita ei ole osattu osoittaa todeksi tai epätodeksi. Tällaisia väittämiä kutsutaan konjektuureiksi. Jos konjektuurille löydetään todistus, siitä tulee teoreema. Joissain erikoistapauksissa konjektuureja kutsutaan hypoteeseiksi (esim. Riemannin hypoteesi) tai jo valmiiksi teoreemoiksi (esim. Fermat'n viimein teoreema, jonka vihdoinkin vuonna 1994 Andrew Wiles todisti oikeaksi). Myös termi konjektuuri saattaa jäädä elämään vaikka kyseinen konjektuuri olisi jo todistettu oikeaksi. Katsotaan seuraavaksi

² Pierre de Fermat (1607–1665) oli ranskalainen lakimies ja matemaatikko. Hänen arkistoistaan on löytynyt muotoillut useille keskeisille lukuteorian tuloksille vaikkakin usein ilman muodollisia todistuksia.

³ Kirje Marin Mersennelle joulupäivänä 1640.



Mikä on suurin tunnettu alkuluku? Miksi Riemannin hypoteesin ratkaisijalle on luvassa miljoonan dollarin Millennium-palkinto? Voidaanko kaikki matematiikan lauseet todistaa oikeiksi?

Tarinoita matematiikasta on huikea seikkailu matematiikan maailmaan. Siinä tarkastellaan, kaavoja kaihtamatta, matematiikan kiinnostavampi tarinoita aina alkuluvuista Elämän peliin.

Kirja on tarkoitettu henkilöille, jotka hallitsevat lukion pitkän matematiikan suhteellisen hyvin. Monet kirjan aiheista soveltuvat kuitenkin kaikille, jotka ovat kiinnostuneita matematiikasta.

Janne Hakkarainen (s. 1981) on filosofian tohtori sovelletussa matematiikassa, ja hän työskentelen erikoistutkijana Ilmatieteen laitoksella mm. inversio-ongelmien ja satelliittihavaintojen parissa. Tarinoita matematiikasta on hänen ensimmäinen kirjansa.



BoDTM
BOOKS on DEMAND

www.bod.fi