Miljoonan dollarin palkkio odottaa matemaattisen väittämän todistajaa

Matti K. Sinisalo

Arkhimedes 4/2000

"Es scheinet weningstens, dass eine jede Zahl, die grösser ist als 2, ein aggregatum trium numerorum primorum sey."

Englantilainen matemaatikko **Christian Goldbach** esitti 7. kesäkuuta vuonna 1742 päivätyssä kirjeessään sveitsiläiselle matemaatikolle Leonard Eulerille ongelman, joka on kiehtonut matemaatikoiden mieliä vuosisatojen ajan. Ongelman tekee ajankohtaiseksi se, että englantilainen kirjankustantaja Faber and Faber on äskettäin luvannut miljoonan dollarin palkkion sille, joka seuraavien kahden vuoden kuluessa todistaa tämän yhden tällä hetkellä tunnetuimmista lukuteorian ongelmista, Goldbachin väittämän eli konjektuurin. Lehdistötiedote luvatusta palkinnosta on nähtävillä kustantaja Faberin webbisivuilla osoitteessa "http://www.faber.co.uk". Samoilta sivuilta löytyvät myös kilpailun säännöt.

Goldbachin väittämässä on kysymys positiivisten kokonaislukujen esittämisestä alkulukujen summana. Sen alkuperäisen muodon mukaan jokainen kokonaisluku, joka on suurempi kuin 5, voidaan esittää kolmen alkuluvun summana. Helposti voidaan todeta, että tämä on yhtäpitävää sen kanssa, että jokainen lukua 2 suurempi parillinen kokonaisluku voidaan esittää kahden alkuluvun summana.

Alkuluku on lukua 1 suurempi luonnollinen luku, joka on jaollinen vain luvulla 1 ja itsellään. Pienimmät kahdeksan näistä luvuista ovat 2, 3, 5, 7, 11, 13, 17 ja 19. Toistaiseksi suurin tunnettu alkuluku on $2^{756839} - 1$. Suuria alkulukuja, joskin vähän pienempiä, muutaman sadan numeron pituisia, käytetään viestien salaamiseen mm. RSA-salakirjoitusjärjestelmässä.

Goldbachin väittämän mukaan jokainen lukua 2 suurempi parillinen kokonaisluku voidaan siis esittää ainakin yhdellä tavalla kahden alkuluvun summana. Esimerkiksi luku 4 voidaan esittää alkulukujen summana muodossa $4 = 2 + 2$, luku 6 muodossa $6 = 3 + 3$, $8 = 3 + 5$, $10 = 3 + 7 = 5 + 5$, $12 = 5 + 7$, $14 = 3 + 11 = 7 + 7$ jne.

Lukua 500 pienemmät alkuluvut ovat 2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 ja 499.

Goldbachin väittämän heikomman muodon, ns. *ternäärisen Goldbachin konjektuurin* mukaan, että jokainen pariton kokonaisluku, joka on suurempi kuin 7, voidaan esittää kolmen parittoman alkuluvun summana. **Vinogradov** todisti, että tämä pitää paikkansa jokaiselle tiettyä, hyvin suurta lukua suuremmalle kokonaisluvulle.

Pieniä alkulukuja voidaan etsiä ns. **Eratostheneen** seulaa apuna käyttäen. Eratostheneen seulaa käytettäessä muodostetaan ensin luettelo kaikista tiettyä lukua pienemmistä mutta lukua 1 suuremmista kokonaisluvuista. Esimerkiksi 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30. Tämän jälkeen joukosta poistetaan kaikki luvulla 2 tasan jaolliset mutta sitä suuremmat kokonaisluvut. Luettelomme tulee nyt muotoon 2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29. Seuraava jäljelle jäänyt luku on 3, joka siis on alkuluku. Poistamme luettelostamme lukua 3 suuremmat sillä tasan jaolliset kokonaisluvut. Saamme luettelon muotoon 2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29. Toteamme, että seuraava luku luettelossamme on luku 5, joka on siis myös alkuluku. Poistamme luettelostamme lukua 5 suuremmat sillä tasan jaolliset luvut, jolloin luettelomme tulee muotoon 2, 3, 5, 7, 11, 13, 17, 19, 23, 29. Näin olemmekin muodostaneet luettelon kaikista lukua 30 pienemmistä alkuluvuista. Seuraava luku luettelossamme olisi luku 7, mutta sillä tasan jaollisia mutta sitä suurempia kokonaislukuja ei luettelossamme enää esiinny. Itseasiassa Eratostheneen seulamenetelmää käytettäessä riittää käydä läpi jakajan arvot suurimman luvun neliöjuureen asti. Luku 7 korotettuna neliöön olisi jo 49.

Eratostheneen seula voidaan ohjelmoida toimimaan tietokoneessa erittäin tehokkaasti. Lukuluettelon laatimisen sijaan jokaista tutkittavalla alueella olevaa luonnollista lukua varten varataan vain yksi looginen muuttuja. Tähän riittää yksi looginen 0/1 tila eli bitti koneen muistissa. Aluksi kaikki bitit asetetaan tilaan 1. Yo. esimerkkiä vastaisi siis bittijono 11111111111111111111111111111111. Bittien numerointi on sellainen, että viimeinen bitti vastaa lukua 0, toiseksi viimeinen lukua 1 jne. Asetetaan luvulla 2 jaollisia lukuja vastaavat bitit tilaan 0. Näin saamme bittijonon 01101010101010101010101010101111. Edelleen asetamme luvuilla 3 ja 5 jaollisia lukuja vastaavat bitit tilaan 0, jolloin saamme bittijonot 01000101000101000101000010101111 ja 01000001000101000101000010101111. Tällaisia bittimatriiseja käyttäen voidaan esimerkiksi kirjoittaa tavalliselle PC-tietokoneelle tietokoneohjelma, joka muodostaa sekunnin murto-osassa luettelon lukua 1000000 pienemmistä alkuluvuista ja ilmoittaa niiden kokonaislukumäärän.

Tällaista lukuun miljoona asti ulottuvaa bittimatriisia voidaan käyttää pitemmälle ulottuvan alkulukuseulonnan jakajien valitsemiseen. Jakamalla bittimatriisi pitemmälle pyrittäessä esimerkiksi miljoonan bitin mittaisiin osiin voidaan seulontaa jatkaa jo luvun miljoona neliöön ts. lukuun 1000000000000 (tuhat miljardia) asti.

Goldbachin konjektuuria voidaan lähteä tarkastamaan muodostamalla esimerkiksi miljoonan bitin lohkoissa tällainen bittimatriisi. Tämän jälkeen liu'utetaan alkupään bittimatriisia tämän matriisin ylitse. Jos lohkon siirrettävän matriisin alkupään kohdalla oleva bitti on 1, niin kaikki siirrettävän matriisin ykkösten kohdalla olevat luvut ovat kahden alkuluvun summia.

Seuraavassa esimerkissä bittivektori A muodostaa alkuperäisen Eratostheneen seulan avulla muodostetun bittijonon. Jokainen bitti vastaa luonnollista lukua, siten, että oikeanpuoleisin bitti vastaa lukua 0, seuraava lukua 1 jne. Bitti on 1, jos luku on alkuluku, muuten 0. Vektori B on aluksi vektorin A kopio, mutta sitä lähdetään sitten siirtämään askel askeleelta vasemmalle. Vektori C koostuu aluksi pelkistä nollista.

```
A...0100000101000100010100010000010100000100010100010100010101100
B...0100000101000100010100010000010100000100010100010100010101100
C...0000000000000000000000000000000000000000000000000000000000000

A...0100000101000100010100010000010100000100010100010100010101100
B...0000010100010001010001000001010000010001010001010001010110000
C...0000010100010001010001000001010000010001010001010001010110000

A...0100000101000100010100010000010100000100010100010100010101100
B...0000010100010001010001000001010000010001010001010001010110000
C...0000111100100010110011000011110000110011110011110011111110000

A...0100000101000100010100010000010100000100010100010100010101100
B...0010100010001010001000001010000010001010001010001010110000
C...0010111110101010111011001011110010111011111011111011111110000

A...0100000101000100010100010000010100000100010100010100010101100
B...1010001000101000100000101000001000101000101000101011000
C...1010111110101010111011101011111010111011111011111011111110000

A...0100000101000100010100010000010100000100010100010100010101100
B...0010001010001000000101000001000101000101000101011000
C...1010111110101010101011101011111010111011111011111011111110000

A...0100000101000100010100010000010100000100010100010100010101100
B...1000101000100000101000001000101000101000101011000
C...1010111110101010101010101011111010111011111011111011111110000
```

Bittijonoille B ja C suoritetaan aina alkulukua vastaavan siirroksen jälkeen biteittäinen TAI- (OR-) operaatio ja näin saatu tulos talletetaan vektoriin C. Vektorin C tietyn bitin arvo tulee näin olemaan lopuksi 1, jos vastaava luonnollinen luku on kahden alkuluvun summa. Yo. taulukon viimeiseltä riviltä nähdään mm. (lopusta lukien), että luvut $4 - 10$ samoin kuin kaikki parilliset luvut lukuun 60 asti voidaan esittää kahden alkuluvun summana.

Tällainen menettelytapa voidaan ohjelmoida hyvin nopeaksi tietokoneelle esim. ns. symbolista konekieltä l. assembly-kieltä (joka on hyvin suosittu kieli mm. peliohjelmoinnissa) käyttäen. Myös korkeamman tason ohjelmointikielet, kuten FORTRAN ja C++ sisältävät sellaisia funktioita, joita käyttäen voidaan kirjoittaa tehokkaita, lähellä konekieltä olevia ohjelmia.

Laskennalliset tulokset

A. Desboves tarkasti vuonna 1855 Goldbachin väittämän rajaan 10000 asti. **Cunningham** tarkasteli eräitä erityistyyppejä olevia lukuja vuonna 1906. Digitaalisten tietokoneiden aikakaudella on saavutettu yhä suurempia rajoja:

	Vuosi	**Raja**
N. Pipping	1940	100000
M. K. Shen	1964	3.3×10^7
M. L. Stein, P. R. Stein	1965	10^8
A. Granville, J. van de Lune, H. J. J. te Riele	1989	2×10^{10}
M. K. Sinisalo	1993	4×10^{11}
J.-M. Deshouillers, H. J. J. te Riele	1998	10^{14}

Viimeisimmän tiedon mukaan **Joerg Richstein** Justus-Liebigin yliopiston informatiikan laitokselta on tarkastanut Goldbachin konjektuurin rajaan 4×10^{14} asti. Käytetty ohjelma oli hajautettu useille työasemille. Ohjelma etsi sellaisia lukuja, joilla ns. minimaalisen Goldbach-osituksen pienempi alkuluku on mahdollisimman suuri. Luvulla $n = 389965026819938$ pienin sellainen alkuluku p, jolla myös $n - p$ on alkuluku, on $p = 5569$.

Richteinin selostus tuloksistaan (ja mm. yo. taulukko) löytyy verkosta osoitteesta "http://www.informatik.uni-giessen.de/staff/richstein/ca/Goldbach.html".

Lopuksi

Kustantaja Faberin tavoitteena on edistää **Apostolos Doxiadiksen** kirjoittaman kirjan "Uncle Petros and Goldbach's Conjecture" myyntiä. Kirja on fik-

tiivinen tarina matemaatikosta, joka jää koukkuun tartuttuaan liian vaikeaan matemaattiseen ongelmaan ja menettää lopulta järkensä. Samalla kustantaja noudattaa kuitenkin matematiikassa perinteiseksi muodostunutta tapaa luvata palkkioita matemaattisten väittämien todistajille. Tunnetuimpia esimerkkejä näistä palkkioista lienevät Ranskan ja Saksan tiedeakatemioiden **Fermat**'n teoreeman todistajille lupaamat palkinnot. Äskettäin, vuonna 1996, edesmenneellä **Pal Erdösillä**, yhdellä 1900-luvun tunnetuimmista matemaatikoista, oli tapana luvata pienehköjä palkkioita erilaisten väittämien todistajille. Monet Erdösin ongelmat ovat edelleen ilman ratkaisua.

Lehtiartikkelit

Bruce Schechter: "In the Life of Pure Reason, Prizes Have Their Place", The New York Times, April 25, 2000.
"http://www.mscs.dal.ca/ dilcher/Goldbach/nyt.html"

"A million-dollar maths question", The Times of London, March 16, 2000.
"http://www.the-times.co.uk/news/pages/tim/2000/03/16/timfeafea02004.html"

"Die Eine-Million-Dollar-Frage" (Saksankielinen), Süddeutche Zeitung, May 16,2000.