TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Petri Laaksonen

Täydellisistä luvuista

Matematiikan ja tilastotieteen laitos
Matematiikka
Huhtikuu 2008

Tampereen yliopisto

Matematiikan ja tilastotieteen laitos

LAAKSONEN, PETRI: Täydellisistä luvuista

Pro gradu -tutkielma, 22 s.

Matematiikka

Huhtikuu 2008

Tiivistelmä

Täydelliseksi luvuksi kutsutaan lukua, joka on itseään pienempien tekijöidensä summa. Luku 6 on täydellinen, koska $6 = 1 + 2 + 3$ ja luvut 1, 2 ja 3 ovat luvun 6 itsensä lisäksi sen ainoat tekijät. Suuruusjärjestyksessä seuraava täydellinen luku on 28, sillä $28 = 1 + 2 + 4 + 7 + 14$ ja luvut 1, 2, 4, 7 ja 14 ovat lukua 28 pienemmät luvun 28 tekijät. Seuraavat kolme täydellistä lukua ovat 496, 8128 ja 33550336. Täydelliset luvut ovat hyvin harvinaisia, ja niitä onkin löytynyt tähän päivään mennessä vain 44 kappaletta.

Ennen kuin tämän tutkielman luvusta 3 eteenpäin perehdytään varsinaisesti täydellisiin lukuihin käydään luvussa 2 läpi kaikki tarvittavat lukuteorian peruskäsitteet, jotta asiasta kiinnostuneet koulutustaustastaan riippumatta voisivat seurata ja ymmärtää esitettäviä todistuksia. Tutkielman luvussa 4 tutustutaan *parittomiin* täydellisiin lukuihin liittyvään tutkimukseen. Mielenkiintoiseksi tämän tutkimuksen tekee etenkin se, että tähän päivään mennessä ei ole löytynyt yhtään paritonta täydellistä lukua. Ei edes tiedetä, onko sellaisia olemassa. Tutkimus on kuitenkin ahkeraa, ja siinä on saavutettu monia mielenkiintoisia tuloksia.

Sisältö

1 Johdanto

> Olisi vaikea löytää kokonaislukujen joukkoa, jolla olisi kiehtovampi historia ja hienostuneemmat ominaisuudet syvempiin mysteereihin kiedottuina – ja jolla olisi vähemmän käyttöä – kuin täydellisillä luvuilla.
>
> –Martin Gardner [10, s. 1]

Täydellinen luku on positiivinen kokonaisluku, joka on itseään pienempien tekijöidensä summa. Ensimmäinen täydellinen luku on luku 6, jonka tekijät ovat 1, 2, 3 ja 6, ja siis $1 + 2 + 3 = 6$. Suuruusjärjestyksessä seuraavat kolme täydellistä lukua ovat 28 ($1+2+4+7+14 = 28$), 496 ja 8128. Jo muinaiset kreikkalaiset tunsivat nämä neljä ensimmäistä täydellistä lukua. [13, s. 88]

Apostol toteaa kirjassaan [1, s. 4] tunnetun tosiasian noin 300 vuotta ennen ajanlaskumme alkua eläneen kreikkalaisen matemaatikon Eukleideen keskeisestä osasta täydellisten lukujen historiassa. Eukleideen *Alkeiden* kolmestatoista kirjasta kolme oli omistettu lukuteorialle, ja näistä etenkin kirja numero yhdeksän on keskeinen aiheemme käsittelyssä. Tämä sisälsi myös kuuluisan todistuksen alkulukujen joukon äärettömyydestä, joka on sisällytetty tämän tutkielmaan lukuun 2.3. Vielä oleellisempaa tämän työn aiheelle on kuitenkin se, että tässä kirjassa Eukleides löysi kaikki *parilliset* täydelliset luvut. *Parittomat* täydelliset luvut ovat aivan oma lukunsa, mihin palaamme luvussa 4.

> Jos muodostamme ykkösestä aloittaen summan, jossa jokainen summan termi on sitä edeltävä luku kaksinkertaisena, ja tästä summasta muodostuu alkuluku, ja kerromme tämän summan sen viimeisellä termillä, niin tämä tulo on täydellinen.
>
> –Eukleides [13, s. 88]

Edeltävä lainaus toisin sanoen, jos esimerkiksi $1+2+4+8+16$ on alkuluku, niin kuin se onkin, sillä se on $2^5 - 1 = 31$, niin 31×16 on täydellinen. Sitä se todella on, sillä tämä tulos saa arvon 496, joka on suuruusjärjestyksessä kolmas täydellinen luku. Sitä edeltävät $28 = 2^2(2^3-1)$ ja $6 = 2(2^2-1)$. Jokaisessa tapauksessa suluissa oleva tulon tekijä, edellä $2^2(2^3 - 1)$ ja $2(2^2 - 1)$, jotka ovat Mersennen lukuja (katso alaluku 3.2), on alkuluku. Tämä onkin kriittinen ehto. [13, s. 88] Eukleides siis todisti, että parillinen luku on täydellinen, jos sillä on muoto $2^{p-1}(2^p - 1)$, missä sekä p että $2^p - 1$ ovat alkulukuja.

Eukleides todisti vain, että hänen sääntönsä on riittävä parillisen täydellisen luvun löytämiseksi. Vasta kaksi tuhatta vuotta myöhemmin sveitsiläinen matemaatikko ja fysiikko Euler todisti Eukleideen teoreeman käänteisesti, eli että jokaisen parillisen täydellisen luvun täytyy olla Eukleideen esittämää muotoa. Syvennymme edellä mainittuihin todistuksiin luvussa 3.

Täydellisillä luvuilla on monia mielenkiintoisia – jopa "mystisinä" pidettyjä – ominaisuuksia, joihin on aikojen saatossa liittynyt myös vääriä luuloja. Ajanlaskumme kolmantena ja neljäntenä vuosisatana eläneen Jamblikhosin oletus siitä, että jokainen (parillinen) täydellinen luku päättyy joko lukuun 6 tai 8 on sittemmin osoitettu todeksi (ks. lause 3.8), mutta hänen toinen oletuksensa lukujen 6 ja 8 vuorottelusta ei pidä paikkaansa: täydellisten lukujen viimeisten numeroiden jono alkaa $6, 8, 6, 8, 6, 6, 8, 8, 6, 6, 8, 8, 6, 8, 8, \ldots$. [13, s. 88] Luvussa 3 tutustumme myös moniin muihin näistä erikoislaatuisista ominaisuuksista.

Merkittävää uusien täydellisten lukujen löytämiselle on niiden jo aiemmin todettu vastaavuus Mersennen alkulukujen kanssa. Ajankohtaiseksi tämän jo tuhansia vuosia vanhan aiheen tekeekin moderni tietotekniikka, jonka avulla on verrattain suuriksi kasvaneiden laskentatehojen ansiosta pystytty suhteellisen pienin väliajoin löytämään monia uusia Mersennen alkulukuja. Tässä hienoa on siis se, että aina samalla kertaa on löydetty myös uusi täydellinen luku! Myös tähän uusia yhä suurempia Mersennen alkulukuja löytämään pyrkivään tutkimukseen tutustumme myöhemmin tässä tutkielmassa.

Jotta mahdollisimman moni voisi koulutustaustastaan riippumatta perehtyä tämän tutkielman avulla täydellisten lukujen moniin kiehtoviin ominaisuuksiin, on luvussa 2 käyty läpi kaikki peruslukiomatematiikan lisäksi vaadittava algebra ja lukuteoria, jota tarvitaan luvussa 3 esitettyjen todistusten ymmärtämiseen. Käytössä olevat merkinnät on esitelty määritelmien yhteydessä, joten niitä emme lähde tässä käymään läpi. Toteamme kuitenkin vielä, että tämä tutkielma sijoittuu matematiikan osa-aluista lukuteorian piiriin, joten se liikkuu koko ajan kokonaislukujen joukossa (merkitsemme sitä symbolilla $\mathbb{Z}$) ja useimmiten nimenomaan sen osajoukossa positiiviset kokonaisluvut ($\mathbb{Z}^+$).

2 Lukuteorian peruskäsitteitä

Tutustumme tässä luvussa joihinkin keskeisiin algebran ja lukuteorian peruskäsitteisiin, joita tarvitsemme myöhemmin täydellisiä lukuja matemaattisen eksaktisti määritellessämme ja niiden ominaisuuksia käsitellessämme. Seuraamme tässä luvussa määritelmien osalta Pentti Haukkasen luentomonisteita *Algebra 1* [5] ja *Lukuteoriaa* [6].

2.1 Jaollisuus

Määritelmä 2.1. Olkoot a ja b kokonaislukuja. Luku a on luvun b *tekijä* (eli luku b on *jaollinen* luvulla a eli luku a jakaa luvun b), jos on olemassa sellainen $c \in \mathbb{Z}$, että $b = ac$. Merkitsemme tätä $a \mid b$.

Esimerkki 2.1. Luvun 6 positiiviset tekijät ovat luvut 1, 2, 3 ja 6. Voimme siis kirjoittaa $1 \mid 6$, $2 \mid 6$, $3 \mid 6$ ja $6 \mid 6$.

2.2 Suurin yhteinen tekijä

Määritelmä 2.2. Olkoot a ja b kokonaislukuja, joista ainakin toinen on erisuuri kuin 0. Silloin kokonaisluku c on lukujen a ja b *suurin yhteinen tekijä* (syt), jos

$$\begin{aligned} &1) \quad c \mid a, c \mid b \quad \text{ja} \\ &2) \quad d \mid a, d \mid b \Rightarrow d \leq c \end{aligned}$$

eli luku c on lukujen a ja b tekijä, ja jos luku d on toinen näiden lukujen tekijä, niin se ei ole lukua c suurempi. Merkitsemme tätä $(a, b) = c$.

Esimerkki 2.2. Luvun 4 positiiviset tekijät ovat 1, 2 ja 4, ja luvulle 6 ne ovat 1, 2, 3 ja 6. Lukujen 4 ja 6 suurin yhteinen tekijä on siis 2 eli $(4, 6) = 2$.

Esimerkki 2.3. Luvun 5 positiiviset tekijät ovat 1 ja 5, ja luvulle 10 ne ovat 1, 2, 5 ja 10. Lukujen 5 ja 10 suurin yhteinen tekijä on siis 5 eli $(5, 10) = 5$.

2.3 Alkuluvuista

Määritelmä 2.3. Luku p (> 1) on *alkuluku*, jos sen ainoat positiiviset tekijät ovat 1 ja p. Merkitsemme alkulukujen joukkoa symbolilla $\mathbb{P}$.

Esimerkki 2.4. (Vrt. [5, s. 12].) Lukua 20 pienemmät alkuluvut ovat 2, 3, 5, 7, 11, 13, 17 ja 19. Luku 2 on ainoa parillinen alkuluku.

Lause 2.1. *Jokainen kokonaisluku $n > 1$ on joko alkuluku tai kahden tai useamman alkuluvun tulo.*

Todistus. (Vrt. [1, s. 16].) Käytämme induktiota luvun n suhteen. Väite on selvästi tosi, kun $n = 2$. Teemme induktio-oletuksen, että väite pätee kaikille lukua n pienemmille kokonaisluvuille. Jos n ei ole alkuluku, niin se on muotoa $n = cd$, missä $1 < c, d < n$. Tällöin induktio-oletuksen nojalla luvut c ja d ovat alkulukujen tuloja, joten niin on myös luku n. □

Lause 2.2 (Eukleides)**.** *Alkulukuja on ääretön määrä.*

Todistus. (Vrt. [1, s. 17].) Teemme vastaoletuksen, että alkulukuja on vain äärellinen määrä. Olkoot ne $p_1, p_2, \ldots, p_n$ ja olkoon $N = 1 + p_1 p_2 \cdots p_n$. Lauseen 2.1 mukaan luku $N > 1$ on joko alkuluku tai alkulukujen tulo. Luku N ei kuitenkaan voi olla alkuluku, sillä $N > p_i$ aina, kun $i = 1, 2, \ldots, n$, eikä se myöskään ole alkulukujen tulo, sillä mikäli jokin p_i ($i = 1, 2, \ldots, n$) jakaisi luvun N, jakaisi se myös erotuksen $N - p_1 p_2 \cdots p_n = 1$, mikä on mahdotonta. Vastaoletus on siis väärin ja väite on oikein. □

Määritelmä 2.4. Luvut a ja b ovat *suhteellisia alkulukuja*, jos $(a, b) = 1$. Käytetään myös sanontaa *keskenään jaottomia*.

Esimerkki 2.5. Luvut 4 ja 9 ovat suhteellisia alkulukuja, sillä $(4, 9) = 1$. Kumpikaan näistä luvuista ei kuitenkaan ole *alkuluku*.

2.4 Kongruenssi

Määritelmä 2.5. Olkoon $m \in \mathbb{Z}^+$. Tällöin luku a on *kongruentti* luvun b kanssa *modulo* m, jos

$$m \mid (a - b)$$

eli jos luku m jakaa lukujen a ja b erotuksen. Käytämme tällöin merkintää

$$a \equiv b \pmod{m}.$$

Esimerkki 2.6.

$$10 \mid (16 - 6) \quad \text{ja} \quad 10 \mid (28 - 8),$$

joten

$$16 \equiv 6 \pmod{10} \quad \text{ja} \quad 28 \equiv 8 \pmod{10}.$$

Kuten edellisestä esimerkistä huomaamme, voimme kongruenssin ja modulon 10 avulla selvittää luvun viimeisen numeron. Tarvitsemme tätä myöhemmin lauseen 3.8 todistuksessa.

2.5 Aritmeettinen funktio

Määritelmä 2.6. Reaaliarvoista funktiota, jonka määrittelyjoukko on positiivisten kokonaislukujen joukko ($\mathbb{Z}^+$), sanotaan *aritmeettiseksi funktioksi.*

Esimerkki 2.7. (Vrt. [6, s. 27].) Olkoon $\alpha \in \mathbb{R}$. Symbolilla N^α merkitään sellaista aritmeettista funktiota, että $N^\alpha(n) = n^\alpha$, kun $n \in \mathbb{Z}^+$. Erityisesti merkitään $N^1 = N$, siis $N(n) = n$, kun $n \in \mathbb{Z}^+$.

2.6 Multiplikatiivisuus

Määritelmä 2.7. Aritmeettista funktiota f sanotaan *multiplikatiiviseksi*, jos $f(1) = 1$ ja $f(mn) = f(m)f(n)$ aina, kun $(m, n) = 1$.

Esimerkki 2.8. Aritmeettinen funktio N^α on multiplikatiivinen, sillä

$$N^\alpha(1) = 1^\alpha = 1,$$

ja kun oletamme, että $(m, n) = 1$, niin

$$N^\alpha(mn) = (mn)^\alpha = m^\alpha n^\alpha = N^\alpha(m)N^\alpha(n).$$

2.7 Tekijäfunktio

Määritelmä 2.8. Olkoon $\alpha \in \mathbb{R}$. *Tekijäfunktio* σ_α on sellainen aritmeettinen funktio, että

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha.$$

Huomautus 2.1. Tekijäfunktion arvo $\sigma_1(n) = \sigma(n)$ ilmaisee luvun n positiivisten tekijöiden summan. Joskus merkitään lyhyesti $\sigma_1 = \sigma$. Arvo $\sigma_0(n)$ taas ilmaisee näiden tekijöiden lukumäärän.

Lause 2.3. *Tekijäfunktio σ_α on multiplikatiivinen.*

Todistus. Selvästi

$$\sigma_\alpha(1) = \sum_{d|1} d^\alpha = 1^\alpha = 1.$$

Oletetaan nyt, että $(m, n) = 1$. Jos $d \mid mn$, niin d voidaan esittää muodossa $d = ab$, missä $a \mid m$ ja $b \mid n$. Näin ollen

$$\begin{aligned}\sigma_\alpha(mn) &= \sum_{d|mn} d^\alpha = \sum_{\substack{a|m \\ b|n}} (ab)^\alpha = \sum_{\substack{a|m \\ b|n}} a^\alpha b^\alpha \\ &= \sum_{a|m} a^\alpha \sum_{b|n} b^\alpha = \sigma_\alpha(m)\sigma_\alpha(n).\end{aligned}$$

Multiplikatiivisuuden määritelmän nojalla olemme nyt todistaneet lauseen. $\square$

Kuten edellisestä huomautuksesta käy ilmi on tekijäfunktio keskeinen tutkielman pääaiheen käsittelyssä, kun $\alpha = 1$. Tarkastelemmekin jatkossa funktiota σ yksinkertaistaaksemme tarkasteluja, mikä tulee esille jo seuraavan lauseen käsittelyssä. Lauseen tulosta tarvitaan lauseen 3.3 todistuksessa.

Lause 2.4. *Jos p on alkuluku ja $k \in \mathbb{Z}^+$, niin*

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}.$$

Todistus. (Vrt. [1, s. 39].) Olkoon p alkuluku ja k positiivinen kokonaisluku. Potenssin p^k tekijät ovat $1, p, p^2, \ldots, p^k$, joten

$$\sigma(p^k) = \sum_{d|p^k} d = 1 + p + p^2 + \cdots + p^k. \tag{2.1}$$

Kun kerrotaan yhtälö (2.1) puolittain luvulla p saadaan

$$p\sigma(p^k) = p + p^2 + p^3 + \cdots + p^{k+1}.$$

Vähentämällä tästä nyt puolittain yhtälö (2.1) saadaan

$$p\sigma(p^k) - \sigma(p^k) = p^{k+1} - 1.$$

Ottamalla nyt $\sigma(p^k)$ yhteiseksi tekijäksi saamme yhtälön muotoon

$$\sigma(p^k)(p-1) = p^{k+1} - 1,$$

jolloin jakaminen puolittain luvulla $p - 1$ ($\neq 0$) tuottaa toivotun muodon

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}.$$

□

3 Täydellinen luku

3.1 Määritelmä

Määritelmä 3.1. Olkoon $n \in \mathbb{Z}^+$. Lukua n kutsutaan *täydelliseksi luvuksi*, jos se on itseään pienempien tekijöidensä summa. Toisin sanoen luku n on täydellinen, jos $\sigma(n) = 2n$.

Esimerkki 3.1. Neljä ensimmäistä täydellistä lukua, jotka kerrotaan tunnetun jo ennen ajanlaskumme alkua [2], ovat

$$
\begin{aligned}
6 \quad & \left(\sigma(6) = \sum_{d|6} d = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6\right), \\
28 \quad & \left(\sigma(28) = \sum_{d|28} d = 1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 \cdot 28\right), \\
496 \quad & \left(\sigma(496) = \sum_{d|496} d = 1 + 2 + \cdots + 248 + 496 = 992 = 2 \cdot 496\right) \text{ ja} \\
8128 \quad & \left(\sigma(8128) = \sum_{d|8128} d = 1 + 2 + \cdots + 4064 + 8128 = 16256 = 2 \cdot 8128\right).
\end{aligned}
$$

3.2 Mersennen alkuluku

Tutustumme nyt tietyntyyppisiin alkulukuihin, joita kutsutaan *Mersennen alkuluvuiksi* niitä vuonna 1644 tutkineen Marin Mersennen mukaan. [1, s. 4]

Aikana ennen tietokoneita oli toimittava ihmisen suorituskyvyn rajoissa, ja etenkin suurten Mersennen alkulukujen löytäminen vaati valtavasti työtä. Käytössä oli kyllä yksinkertaisia tuloksia, joiden avulla lukujen testaustyö voitiin rajoittaa vain tietyn tyyppisten tekijöiden tutkimiseen. Mersenne oli itsekin sitä mieltä, että koko iäisyys ei riittäisi sen selvittämiseen, onko jokin 15- tai 20-numeroinen luku alkuluku. [13, s. 89]

Tietokoneiden aikakausi on kuitenkin muuttanut kaiken, ja Mersennen luvun toteaminen alkuluvuksi on nykyään nopeaa tietokoneella Lucasin-Lehmerin testin avulla (ks. tarkemmin [12]). Monet suurimmista tunnetuista alkuluvuista ovatkin tästä syystä juuri Mersennen alkulukuja. Alaluvussa 3.4 tutustumme tietokoneita ja tätä testiä hyödyntävään projektiin. Mersennen alkuluku kulkee käsi kädessä parillisten täydellisten lukujen kanssa, kuten tulemme huomaamaan luvussa 3.3, ja tästä syystä edellä mainittu projekti liittyy Mersennen alkulukuihin liittyvästä nimestään huolimatta hyvin läheisesti myös uusien täydellisten parillisten lukujen etsimiseen.

Määritelmä 3.2. Olkoon $m \in \mathbb{Z}^+$. Tällöin luku $M_m = 2^m - 1$ on järjestyksessä m. Mersennen luku.

Määritelmä 3.3. Olkoon $p \in \mathbb{P}$. Tällöin lukua $M_p = 2^p - 1$ kutsutaan *Mersennen alkuluvuksi*, jos myös $M_p \in \mathbb{P}$.

Esimerkki 3.2. Neljä ensimmäistä Mersennen alkulukua ovat 3, 7, 31 ja 127, joita kaavassa $2^p - 1$ vastaa luvun $p \in \mathbb{P}$ arvot 2, 3, 5 ja 7.

Lause 3.1. *Jos $m \in \mathbb{Z}^+$ ja $2^m - 1$ on alkuluku, niin m on alkuluku*

Todistus. ([9, s. 224]) Teemme vastaoletuksen, että luku m ei ole alkuluku. Tällöin se on muotoa $m = ab$, missä $1 < a < m$ ja $1 < b < m$. Nyt

$$2^m - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1).$$

Koska molemmat tulon tekijät oikealla puolella ovat suurempia kuin 1, näemme selvästi, että $2^m - 1$ ei olisi alkuluku, mikäli luku m ei olisi alkuluku. Siksi luvun m täytyy olla alkuluku aina, kun luku $2^m - 1$ on alkuluku. □

Lause 3.2. *Olkoot $a, m \in \mathbb{Z}^+$ siten, että $a > 1$ ja $m > 1$. Jos $a^m - 1$ on alkuluku, niin $a = 2$ ja m on alkuluku.*

Todistus. Seuraa melko suoraan lauseesta 3.1. □

Lauseessa 2.2 esitimme Eukleideen kuuluisaa tulosta mukailevan todistuksen, jonka mukaan alkulukuja on ääretön määrä. Mersennen alkulukujen määrää ei tiedetä, mutta niitä epäillään myös olevan ääretön määrä, vaikkei tätä ole pystyttykään todistamaan. [9, s. 227]

Seuraavan sivun taulukossa on kaikki tähän mennessä löydetyt Mersennen alkuluvut järjestysnumeroineen ja löytämisvuosineen. Taulukossa on myös luvun $p \in \mathbb{P}$ arvot, joilla vastaavat muotoa $M_p = 2^p - 1$ olevat Mersennen alkuluvut voi laskea; on tosin hyvä huomata, että suurimmat näistä ovat todella suuria, kuten sarakkeen "Numeroita" (luvussa M_p) arvoista voi todeta. Huomattavaa on, että ei ole tiedossa, onko järjestyksessä 39. luvun ja suurimman löydetyn luvun välissä vielä löytämättömiä Mersennen alkulukuja; tästä syystä viimeisten lukujen järjestyslukuja on merkitty kysymysmerkeillä. Lähteenä taulukon tiedoille on käytetty www-sivun [2] taulukkoa.

	p	$M_p = 2^p - 1$	Numeroita	Vuosi
1	2	$2^2 - 1$	1	
2	3	$2^3 - 1$	1	
3	5	$2^5 - 1$	2	
4	7	$2^7 - 1$	3	
5	13	$2^{13} - 1$	4	1456
6	17	$2^{17} - 1$	6	1588
7	19	$2^{19} - 1$	6	1588
8	31	$2^{31} - 1$	10	1772
9	61	$2^{61} - 1$	19	1883
10	89	$2^{89} - 1$	27	1911
11	107	$2^{107} - 1$	33	1914
12	127	$2^{127} - 1$	39	1876
13	521	$2^{521} - 1$	157	1952
14	607	$2^{607} - 1$	183	1952
15	1279	$2^{1279} - 1$	386	1952
16	2203	$2^{2203} - 1$	664	1952
17	2281	$2^{2281} - 1$	687	1952
18	3217	$2^{3217} - 1$	969	1957
19	4253	$2^{4253} - 1$	1 281	1961
20	4423	$2^{4423} - 1$	1 332	1961
21	9689	$2^{9689} - 1$	2 917	1963
22	9941	$2^{9941} - 1$	2 993	1963
23	11213	$2^{11213} - 1$	3 376	1963
24	19937	$2^{19937} - 1$	6 002	1971
25	21701	$2^{21701} - 1$	6 533	1978
26	23209	$2^{23209} - 1$	6 987	1979
27	44497	$2^{44497} - 1$	13 395	1979
28	86243	$2^{86243} - 1$	25 962	1982
29	110503	$2^{110503} - 1$	33 265	1988
30	132049	$2^{132049} - 1$	39 751	1983
31	216091	$2^{216091} - 1$	65 050	1985
32	756839	$2^{756839} - 1$	227 832	1992
33	859433	$2^{859433} - 1$	258 716	1994
34	1257787	$2^{1257787} - 1$	378 632	1996
35	1398269	$2^{1398269} - 1$	420 921	1996
36	2976221	$2^{2976221} - 1$	895 932	1997
37	3021377	$2^{3021377} - 1$	909 526	1998
38	6972593	$2^{6972593} - 1$	2 098 960	1999
39	13466917	$2^{13466917} - 1$	4 053 946	2001
??	20996011	$2^{20996011} - 1$	6 320 430	2003
??	24036583	$2^{24036583} - 1$	7 235 733	2004
??	25964951	$2^{25964951} - 1$	7 816 230	2005
??	30402457	$2^{30402457} - 1$	9 152 052	2005
??	32582657	$2^{32582657} - 1$	9 808 358	2006

3.3 Parillinen täydellinen luku

Jo muinaiset kreikkalaiset tiesivät, miten voidaan etsiä kaikki parilliset täydelliset luvut [9, s. 223]. Seuraavan lauseen avulla voimme tämän tehdä.

Lause 3.3. *Luku $n \in \mathbb{Z}^+$ on parillinen täydellinen luku, jos ja vain jos*

$$n = 2^{k-1}(2^k - 1),$$

missä $k \geq 2$, ja $2^k - 1$ on alkuluku.

Todistus. (Vrt. [2].) Olkoon $p = 2^k - 1$ alkuluku, ja olkoon $n = 2^{k-1}(2^k - 1)$. Näyttääksemme, että n on täydellinen luku, meidän on osoitettava, että

$$\sigma(n) = 2n.$$

Koska σ on multiplikatiivinen, ja lauseen 2.4 mukaan

$$\sigma(2^{k-1}) = \frac{2^{k-1+1} - 1}{2 - 1} = \frac{2^k - 1}{1} = 2^k - 1,$$

sekä selvästi

$$\sigma(p) = \sum_{d|p} d = p + 1 = 2^k - 1 + 1 = 2^k,$$

niin tiedämme, koska $(2^{k-1}, 2^k - 1) = 1$, että

$$\begin{aligned}\sigma(n) &= \sigma(2^{k-1}(2^k - 1)) = \sigma(2^{k-1})\sigma(2^k - 1) \\ &= \sigma(2^{k-1})\sigma(p) = (2^k - 1)2^k \\ &= 2 \cdot 2^{k-1}(2^k - 1) = 2n.\end{aligned}$$

Olemme nyt näyttäneet, että n on täydellinen luku.

Oletamme seuraavaksi, että n on mikä tahansa parillinen täydellinen luku ja kirjoitamme sen muodossa $n = 2^{k-1}m$, missä $m \in \mathbb{Z}^+$, $k \geq 2$ ja $(2, m) = 1$. Koska σ on multiplikatiivinen, niin

$$\sigma(2^{k-1}m) = \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m).$$

Koska n on täydellinen luku, tiedämme myös, että

$$\sigma(n) = 2n = 2^k m.$$

Nyt siis

$$2^k m = (2^k - 1)\sigma(m), \tag{3.1}$$

joten $2^k - 1$ jakaa tulon $2^k m$, ja koska se ei parittomana lukuna voi jakaa lukua 2^k, jakaa se siis luvun m. Merkitsemme tätä $m = (2^k - 1)c$, missä $c \in \mathbb{Z}^+$. Nyt kun sijoitamme tämän yhtälöön (3.1) ja jaamme yhtälön puolittain luvulla

$2^k - 1$, saamme $2^k c = \sigma(m)$. Koska c ja m ovat molemmat luvun m tekijöitä, tiedämme, että

$$\begin{aligned} 2^k c = \sigma(m) &\geq c + m \\ &= c + (2^k - 1)c = c + 2^k c - c \\ &= 2^k c. \end{aligned}$$

Siis $\sigma(m) = c+m$. Nyt siis luvulla m on vain kaksi tekijää, joiden on oltava 1 (c) ja luku itse (m). Tämä todistaa, että $m = (2^k - 1)c = (2^k - 1) \cdot 1 = 2^k - 1$ on alkuluku ja että luku n on muotoa $n = 2^{k-1}m = 2^{k-1}(2^k - 1)$. □

Lauseista 3.1 ja 3.3 seuraa, että parillisten täydellisten lukujen tutkimus on uusien parillisten täydellisten lukujen etsimisen osalta pelkistynyt uusien Mersennen alkulukujen etsimiseen. Tähän palaamme alaluvussa 3.4.

Parillisilla täydellisillä luvuilla on monia mielenkiintoisia ominaisuuksia, joihin tutustumme seuraavaksi. Kun käytämme jatkossa käsitettä *täydellinen luku*, tarkoitamme kuitenkin tämän luvun loppuun saakka vain *parillisia* täydellisiä lukuja.

Lause 3.4. *Täydellisen luvun n kaikkien tekijöiden (myös itse luvun) käänteislukujen summa on kaksi, ts.*

$$\sum_{d|n} \frac{1}{d} = 2.$$

Todistus. (Vrt. [11].) Olkoot positiiviset kokonaisluvut $1, 2, \ldots, n$ (luvut 1 ja 2 ovat selvästi kaikkien täydellisten lukujen tekijöitä) täydellisen luvun n kaikki tekijät. Nyt määritelmän mukaan

$$\begin{aligned} 1 + 2 + \cdots + n &= 2n \\ n + \cdots + 2 + 1 &= 2n \\ \frac{n}{1} + \frac{n}{2} + \cdots \frac{n}{n} &= 2n \\ n(\frac{1}{1} + \frac{1}{2} + \cdots \frac{1}{n}) &= 2n \\ \frac{1}{1} + \frac{1}{2} + \cdots \frac{1}{n} &= 2 \\ \sum_{d|n} \frac{1}{d} &= 2. \end{aligned}$$

□

Seuraavassa lauseessa todistamme, että jokainen täydellinen luku on *kolmioluku*. Kolmioluku saa nimensä siitä, että sen osoittamasta määrästä pisteitä voidaan muodostaa kolmion muotoinen kuvio.

Lause 3.5. *Jokainen täydellinen luku on kolmioluku eli positiivinen kokonaisluku, joka on muotoa*

$$\frac{a(a-1)}{2},$$

missä $a > 1$ on positiivinen kokonaisluku.

Todistus. ([10, s. 7]) Lauseen 3.3 mukaan jokainen (parillinen) täydellinen luku n on muotoa

$$n = 2^{k-1}(2^k - 1).$$

Nyt

$$n = 2^{k-1}(2^k - 1) = \frac{2^k(2^k - 1)}{2},$$

missä siis nyt 2^k on positiivinen kokonaisluku. Olemme näin todistaneet lauseen. □

Huomautus 3.1. Kolmioluku on kirjallisuudessa usein määritelty positiiviseksi kokonaisluvuksi, joka on muotoa

$$\frac{b(b+1)}{2},$$

missä $b \in \mathbb{Z}^+$. Tämä muoto on kuitenkin lauseessa 3.5 käyttämäämme vastaava, kun valitsemme $b = a - 1$, missä $a > 1$ on positiivinen kokonaisluku.

Voimme kirjoittaa jokaisen täydellisen luvun, paitsi luvun 6, myös kuutioiden summana, kuten seuraavasta lauseesta käy ilmi. Tarkemmin sanottuna kyse on sarjan $1^3 + 3^3 + 5^3 + 7^3 + 9^3 + \ldots$ osasummasta.

Lause 3.6. *Jos luku $n = 2^{k-1}(2^k - 1)$, missä $k > 2$, on täydellinen, niin*

$$n = 1^3 + 3^3 + \cdots + (2 \cdot 2^{(k-1)/2} - 1)^3.$$

Todistus. (Vrt. [10, s. 7].) Kuutioiden summalle on olemassa kaava

$$\sum_{i=1}^{a} i^3 = \frac{a^2(a+1)^2}{4}, \tag{3.2}$$

jonka todistamme induktiolla luvun a suhteen. Perusaskel on voimassa eli

$$\sum_{i=1}^{1} i^3 = 1^3 = 1 \quad \text{ja} \quad \frac{1^2(1+1)^2}{4} = \frac{1 \cdot 4}{4} = 1,$$

joten teemme induktio-oletuksen, että kaava (3.2) pätee, kun $a = b$, ja induktioväitteen

$$\sum_{i=1}^{b+1} i^3 = \frac{(b+1)^2(b+2)^2}{4},$$

jonka todistamme. Nyt siis

$$\begin{aligned}\sum_{i=1}^{b+1} i^3 &= 1^3 + 2^3 + \cdots + b^3 + (b+1)^3 = \sum_{i=1}^{b} i^3 + (b+1)^3 \\ &= \frac{b^2(b+1)^2 + 4(b+1)^3}{4} = \frac{(b^2+2b+1)(b^2+4(b+1))}{4} \\ &= \frac{(b^2+2b+1)(b^2+4b+4)}{4} = \frac{(b+1)^2(b+2)^2}{4},\end{aligned}$$

joten induktioperiaatteen nojalla kuutioiden summan kaava (3.2) pätee.

Todistamme nyt itse lauseen. Olkoon $m = 2^{(k-1)/2}$. Tällöin

$$\begin{aligned}1^3 + 3^3 + \cdots + (2m-1)^3 &= \Big(1^3 + 2^3 + \cdots + (2m)^3\Big) - \Big(2^3 + 4^3 + \cdots + (2m)^3\Big) \\ &= \frac{(2m)^2(2m+1)^2}{4} - 2^3\frac{m^2(m+1)^2}{4} \\ &= m^2(2m+1)^2 - 2m^2(m+1)^2 \\ &= m^2(4m^2 + 4m + 1 - 2m^2 - 4m - 1) \\ &= m^2(2m^2 - 1) = 2^{k-1}(2^k - 1).\end{aligned}$$

Olemme siis näin ollen todistaneet lauseen. □

Esimerkki 3.3. Järjestyksessä toinen täydellinen luku 28 on kolmioiden summana ja siis sarjan $1^3+3^3+5^3+7^3+9^3+\ldots$ osasummana 1^3+3^3 ja kolmannen täydellisen luvun 496 voimme kirjoittaa muodossa $1^3+3^3+5^3+7^3$. Summa $1^3+3^3+5^3 = 153$ ei puolestaan selvästikään ole täydellinen luku.

Täydellisillä luvuilla on monia ainutlaatuisia esitystapoja. Huomaamme esimerkiksi, että binäärimuodossa neljä ensimmäistä täydellistä lukua ovat $6 = 110_2$, $28 = 11100_2$, $496 = 111110000_2$ ja $8128 = 1111111000000_2$. Yleisestä tapauksesta saamme seuraavan lauseen.

Lause 3.7. *Jos luku $n = 2^{k-1}(2^k-1)$ on täydellinen ja n kirjoitetaan binäärimuodossa, niin siinä on $2n-1$ numeroa, joista n ensimmäistä ovat ykkösiä ja viimeiset $n-1$ ovat nollia.*

Todistus. (Vrt. [10, s. 7].) Tulos seuraa suoraan binääriluvun muodostamistavasta ja kaavasta $2^p - 1 = 1 + 2 + \cdots + 2^{p-1}$, jonka todistuksen nyt sivuutamme. Voimme kuitenkin todeta tuloksen seuraavan myös suoraan lauseesta 3.3, sillä jokainen täydellinen luku on Mersennen alkuluvun ja luvun 2 potenssin tulo. Koska Mersennen alkuluku on muotoa 2^p-1 ($p \in \mathbb{P}$), on sen binääriesitys ykkösten jono, ja sellaisen kertominen luvun 2 potenssilla tekee vain "siirron" eli lisää nollia ykkösten oikealle puolelle. □

Lause 3.8. *Jokainen parillinen täydellinen luku päättyy joko numeroon* 6 *tai numeroon* 8.

Todistus. (Vrt. [10, s. 8].) Olkoon $n = 2^{p-1}(2^p - 1)$ täydellinen luku (missä siis $p \in \mathbb{P}$ ja $2^p - 1$ on Mersennen alkuluku). Jos $p = 2$, niin

$$n = 2^{2-1}(2^2 - 1) = 2 \cdot 3 = 6.$$

Jos taas $p > 2$, niin tiedetään, että jokainen tällainen alkuluku on joko muotoa $4m + 1$ tai $4m + 3$ ($m \in \mathbb{Z}^+$), sillä jokainen positiivinen kokonaisluku on selvästi muotoa $4m$, $4m + 1$, $4m + 2$ tai $4m + 3$, joista ensimmäiseksi ja kolmanneksi mainittu ovat kahdella jaollisia. Ensimmäisessä tapauksessa

$$\begin{aligned} n &= 2^{4m}(2^{4m+1} - 1) = 16^m(2 \cdot 16^m - 1) \equiv 6^m(2 \cdot 6^m - 1) \\ &\equiv 6(12 - 1) \equiv 6 \cdot 11 \equiv 6 \pmod{10}, \end{aligned}$$

koska $6^m \equiv 6 \pmod{10}$ kaikilla $m \in \mathbb{Z}^+$. Vastaavasti toisessa tapauksessa

$$\begin{aligned} n &= 2^{4m+2}(2^{4m+3} - 1) = 4 \cdot 16^m(8 \cdot 16^m - 1) \equiv 4 \cdot 6^m(8 \cdot 6^m - 1) \\ &\equiv 24(48 - 1) \equiv 4(8 - 1) \equiv 4 \cdot 7 \equiv 28 \equiv 8 \pmod{10}. \end{aligned}$$

Olemme nyt käsitelleet kaikki mahdolliset tapaukset ja todistaneet lauseen. □

Huomautus 3.2. Numerot 6 ja 8 eivät kuitenkaan vuorottele parillisten täydellisten lukujen viimeisinä numeroina, kuten viidestä ensimmäisestä täydellisestä luvusta 6, 28, 496, 8128 ja 33550336 voisi virheellisesti olettaa. Järjestyksessä kuudes täydellinen luku on nimittäin 8589869056.

Listaamme seuraavan sivun taulukossa kaikki tähän mennessä löydetyt täydelliset luvut, jotka kaikki ovat parillisia. Taulukossa on järjestysnumeron lisäksi luvun $p \in \mathbb{P}$ arvo sekä täydellisen luvun n arvo, joka on luvun p avulla laskettu. Lisäksi taulukossa on kunkin täydellisen luvun numeroiden lukumäärä. Ei ole tiedossa, onko järjestyksessä 39. täydellisen luvun ja suurimman löydetyn täydellisen luvun välissä vielä löytämättömiä täydellisiä lukuja; tästä syystä viimeisten lukujen järjestyslukuja on merkitty kysymysmerkeillä. Lähteenä taulukon tiedoille on käytetty www-sivun [2] taulukkoa.

	p	$n = 2^{p-1}(2^p - 1)$	Numeroita
1	2	$2(2^2 - 1)$	1
2	3	$2^2(2^3 - 1)$	2
3	5	$2^4(2^5 - 1)$	3
4	7	$2^6(2^7 - 1)$	4
5	13	$2^{12}(2^{13} - 1)$	8
6	17	$2^{16}(2^{17} - 1)$	10
7	19	$2^{18}(2^{19} - 1)$	12
8	31	$2^{30}(2^{31} - 1)$	19
9	61	$2^{60}(2^{61} - 1)$	37
10	89	$2^{88}(2^{89} - 1)$	54
11	107	$2^{106}(2^{107} - 1)$	65
12	127	$2^{128}(2^{127} - 1)$	77
13	521	$2^{520}(2^{521} - 1)$	314
14	607	$2^{606}(2^{607} - 1)$	366
15	1279	$2^{1278}(2^{1279} - 1)$	770
16	2203	$2^{2202}(2^{2203} - 1)$	1 327
17	2281	$2^{2280}(2^{2281} - 1)$	1 373
18	3217	$2^{3216}(2^{3217} - 1)$	1 937
19	4253	$2^{4252}(2^{4253} - 1)$	2 561
20	4423	$2^{4422}(2^{4423} - 1)$	2 663
21	9689	$2^{9688}(2^{9689} - 1)$	5 834
22	9941	$2^{9940}(2^{9941} - 1)$	5 985
23	11213	$2^{11212}(2^{11213} - 1)$	6 751
24	19937	$2^{19936}(2^{19937} - 1)$	12 003
25	21701	$2^{21700}(2^{21701} - 1)$	13 066
26	23209	$2^{23208}(2^{23209} - 1)$	13 973
27	44497	$2^{44496}(2^{44497} - 1)$	26 790
28	86243	$2^{86242}(2^{86243} - 1)$	51 924
29	110503	$2^{110502}(2^{110503} - 1)$	66 530
30	132049	$2^{132048}(2^{132049} - 1)$	79 502
31	216091	$2^{216090}(2^{216091} - 1)$	130 100
32	756839	$2^{756838}(2^{756839} - 1)$	455 663
33	859433	$2^{859432}(2^{859433} - 1)$	517 430
34	1257787	$2^{1257786}(2^{1257787} - 1)$	757 263
35	1398269	$2^{1398268}(2^{1398269} - 1)$	841 842
36	2976221	$2^{2976220}(2^{2976221} - 1)$	1 791 864
37	3021377	$2^{3021376}(2^{3021377} - 1)$	1 819 050
38	6972593	$2^{6972592}(2^{6972593} - 1)$	4 197 919
39	13466917	$2^{13466916}(2^{13466917} - 1)$	8 107 892
??	20996011	$2^{20996010}(2^{20996011} - 1)$	12 640 858
??	24036583	$2^{24036582}(2^{24036583} - 1)$	14 471 465
??	25964951	$2^{25964950}(2^{25964951} - 1)$	15 632 458
??	30402457	$2^{30402456}(2^{30402457} - 1)$	18 304 103
??	32582657	$2^{32582656}(2^{32582657} - 1)$	19 616 714

3.4 GIMPS

Englantilainen matemaattisista aiheista kirjoittanut Peter Barlow kirjoitti artikkelissaan julkaisussa *A New Mathematical and Philosophical Dictionary* vuonna 1814 seuraavaa [13, s. 89]:

> Euler varmisti, että $2^{31} - 1 = 2147483647$ on (Mersennen) alkuluku, ja tämä on suurin tällä hetkellä sellaiseksi tunnettu, ja näin ollen viimeisin tunnetuista täydellisistä luvuista, joka riippuu siitä, on suurin täydellinen luku, joka tällä hetkellä tunnetaan, ja todennäköisesti myös sellaiseksi jää, koska ne ovat vain kiehtovia olematta hyödyllisiä ja ei siksi ole luultavaa, että kukaan ihminen yrittäisi löytää enää sitä suurempia.

Kuinka väärässä herra Barlow nykypäivän valossa tuolloin olikaan. On tosin todettava, että hän ei millään voinut ennustaa sitä tietotekniikan voittokulkua, joka kaiken on mahdollistanut.

GIMPS, *the Great Internet Mersenne Prime Search*, on tammikuussa 1996 aloitettu projekti, jonka tarkoituksena on löytää uusia ja aina vain suurempia Mersennen alkulukuja (ks. [3]). Kantavana ideana on valjastaa Internetin avulla asiasta kiinnostuneiden vapaaehtoisten omien kotitietokoneiden laskentateho näiden "neulojen heinäsuovassa" etsimiseen.

Jokainen halukas voi ladata projektin kotisivuilta omalle tietokoneelleen Windows-ympäristössä toimivan Prime95- tai Linuxissa toimivan MPrime-ohjelman, joka käyttää koneen laskentatehoa projektin tarpeisiin silloin, kun käyttäjä ei tee koneelleen itse mitään merkittävää tai laskentatehoja kuluttuvaa, ja näin tietokoneet voidaan valjastaa käyttöön silloinkin, kun niiden näyttöruudulla pyörii korkeintaan näytönsäästäjä. Mies projektin ja näiden ohjelmien takana on MIT:ssä (Massachusetts Institute of Technology) tietojenkäsittelytieteen tutkinnon suorittanut George Woltman.

Projekti on ollut hyvin menestyksellinen, sillä sen avulla on löydetty jo kymmenen Mersennen alkulukua, joista jokainen on ollut löytöhetkellään suurin tunnettu alkuluku. Suurin tällä hetkellä tunnettu alkuluku on $2^{32582657} - 1$, jonka Steven Boone ja Curtis Cooper (University of Central Missouri) löysivät syyskuun 4. päivänä vuonna 2006. Tämä oli siis järjestyksessä kymmenes projektin avulla ja kaiken kaikkiaan 44. löydetty Mersennen alkuluku.

4 Pariton täydellinen luku

Pariton täydellinen luku on aivan oma lukunsa. Pitkällisistä ja ahkerista etsinnöistä huolimatta parittomia täydellisiä lukuja ei nimittäin ole löytynyt vielä yhtään kappaletta! Niiden olemassaoloa ei ole pystytty todistamaan eikä ole myöskään todistettu, että niitä ei ole olemassa. Moderni teknologia tarjoaa erinomaiset työkalut, joilla näitä mahdollisesti vielä löydettävissä olevia lukuja pyritään etsimään. Tähän tutkimukseen tutustumme tässä luvussa.

Yhtään paritonta täydellistä lukua ei siis ole löydetty, mutta siitä huolimatta on pystytty osoittamaan, että jos parittomia täydellisiä lukuja olisi olemassa, olisi niiden oltava tietyntyyppisiä ja -kokoisia. Pitkään on esimerkiksi tiedetty, että pariton täydellinen luku ei voi olla pienempi kuin 10^{300}, ja että sillä täytyy olla ainakin kahdeksan eri alkulukutekijää [9, s. 228].

4.1 Tutkimuksesta

Seuraavaksi käymme läpi parittomien täydellisten lukujen parissa tehtyä tutkimusta seuraten Wellsin kirjaa [13] ja MathWorldin artikkelia [4].

Euler todisti, että parittoman täydellisen luvun, jos sellainen siis on olemassa, on oltava muotoa $p^a q^b r^c \cdots$, missä $p, q, r, \ldots$ ovat keskenään erisuuria parittomia alkulukuja, joista jokainen on muotoa $4n + 1$, a on tätä samaa muotoa, ja $b, c, \ldots$ ovat kaikki parillisia. Steuerwald todisti 1930-luvun lopulla, että jokainen $b, c, \ldots$ ei voi olla 2. Touchard antoi panoksensa 1950-luvulla todistamalla, että parittoman täydellisen luvun täytyy olla muotoa $12k + 1$ tai $36k + 9$.

Stuyvart todisti 1800-luvun lopussa, että parittoman täydellisen luvun täytyy olla kahden neliön summa, ja Gradshtein todisti vuonna 1925 Sylvesterin vuonna 1887 tekemän oletuksen, että jokaisella parittomalla täydellisellä luvulla täytyy olla ainakin kuusi eri alkulukutekijää. Hagis puolestaan näytti 1980-luvulle saavuttaessa, että eri alkulukutekijöitä on ainakin kahdeksan, missä tapauksessa pariton täydellinen luku on jaollinen luvulla 15.

Catalan todisti 1880-luvulla, että jos pariton täydellinen luku ei ole jaollinen alkuluvuilla 3, 5 tai 7, sillä on ainakin 26 eri alkulukutekijää, ja 1900-luvun puolivälin tienoilla Norton laajensi tämän 27 alkulukutekijään. Norton todisti tuolloin myös, että jos pariton täydellinen luku ei ole jaollinen luvuilla 3 ja 5, täytyy sillä olla ainakin 15 eri alkulukutekijää. Nielsen todisti 2000-luvun alussa, että jos pariton täydellinen luku ei ole jaollinen luvulla 3, täytyy sillä olla ainakin 12 eri alkulukutekijää. Nielsen näytti myös, että kaikilla parittomilla täydellisillä luvuilla – jos niitä siis on olemassa – on oltava ainakin yhdeksän eri alkulukutekijää.

Tutkimus käy kuumana yhä 2000-luvullakin ja onkin pystytty löytämään monia rajoja, joiden tarkentamisen kanssa tehdään jatkuvasti työtä. Suurimmalle parittoman täydellisen luvun alkulukutekijälle on yritetty löytää alarajaa. Iannucci ja Jenkins ovat selvittäneet tämän vuosituhannen alussa, että kolmen suurimman alkulukutekijän täytyy olla kooltaan ainakin 100000007, 10007 ja 101.

Hare asetti tutkimustensa perusteella vuonna 2005 rajan sille, kuinka monta alkulukutekijää *yhteensä* parittomalla täydellisellä luvulla on oltava. Tämä rajaluku on 75, ja sen tarkentaminen vaatii lukuisten suurten lukujen tekijöihin jakoa. Tätä työtä tehdään nykyään myös osoitteessa OddPercect.org sijaitsevan projektin nimeltä *Odd Perfect Number Search* nimissä. Nimensä mukaisesti tavoitteena tällä projektilla on etsiä (ja löytää) parittomia täydellisiä lukuja. Pääasiallisena tavoitteena on kuitenkin pyrkiä kasvattamaan pienimmän mahdollisen parittoman täydellisen luvun alarajaa luvusta 10^{300} eli jatkaa tämän rajan varmistaneiden Brentin ja kumppaneiden työtä. Tämän lisäksi käynnissä on useita sivuprojekteja. [7]

4.2 Olemassaolon epäilystä

Parittomien täydellisten lukujen olemassaoloa on epäilty laajalti, eikä aivan syyttä, sillä niitä ei todella ole pitkällisten etsintöjen ja niiden ympärillä tehdyn monia tuloksia tuottaneiden tutkimusten aikana löytynyt yhtään kappaletta. *Odd Perfect Number Search* -projektin sivuilla esitellään epäilijöistä kaksi tunnetuinta, James Joseph Sylvester ja Carl Pomerance, joiden väitteisiin OddPerfect.org-sivuston ylläpitäjä on katsonut tarpeelliseksi perehtyä. Käymme seuraavaksi läpi näistä ensin mainitun mietteitä. Pomerancen heuristiikka (engl. *Pomerance's Heuristic*) sisältää mielenkiintoista kvantitatiivista argumentointia parittomien täydellisten lukujen – ja itse asiassa kaikkien hyvin suurikokoisten täydellisten lukujen – olemassaolon epätodennäköisyydestä mutta myös turhan pitkälle menevää matematiikkaa tässä yhteydessä tarkemmin tarkasteltavaksi.

Sylvesterin ”ehtojen verkko” perustuu ajatukselle, joka käy ilmi hänen vuonna 1888 antamastaan (tässä vapaasti suomennetusta) lausunnostaan:

> ... pitkällinen mietiskely aiheen parissa on vakuuttanut minut, että sellaisen (parittoman täydellisen luvun) olemassaolo – sen pakeneminen, niin sanotusti, monimutkaisten ehtojen verkosta, joka ahdistaa sitä joka puolelta – olisi lähes ihme.

Tätä lainausta seuraa kirjallisuudessa tavallisesti nykytietämyksen mukaan päivitetty lista näistä mainituista ”joka puolelta ahdistavista ehdoista”, joita jo kävimmekin läpi luvussa 4.1. Sylvesterin verkko vihjaa jatkuvista vaikeuksista, joita välttämättä seuraa, kun tehdään tutkimusta yhä suurempien lukujen parissa. [8]

OddPerfect.org-sivuston ylläpitäjä ei ole kuitenkaan lannistunut väitteiden edessä vaan uskoo, että kuinka pieneksi todennäköisyyttä väitettäisiinkin, aina on olemassa mahdollisuus löytää pariton täydellinen luku jossain kokoluokassa.

Viitteet

[1] Apostol, Tom M.: *Introduction to Analytic Number Theory.* Springer-Verlag, New York, 1976.

[2] Caldwell, Chris K.: *Mersenne Primes: History, Theorems and Lists.* http://primes.utm.edu/mersenne (14.1.2008).

[3] *GIMPS - The Great Internet Mersenne Prime Search.* http://www.mersenne.org (18.3.2008).

[4] Greathouse, Charles & Weisstein, Eric W.: *Odd Perfect Number.* MathWorld – A Wolfram Web Resource. http://mathworld.wolfram.com/OddPerfectNumber.html (2.4.2008).

[5] Haukkanen, Pentti: *Algebra 1*, luentomoniste. http://mtl.uta.fi/Opetus/Algebra (14.1.2008).

[6] Haukkanen, Pentti: *Lukuteoriaa*, luentomoniste. http://mtl.uta.fi/Opetus/Algebra/Lukuteoria (14.1.2008).

[7] OddPerfect.org: *Odd Perfect Number Search.* http://www.oddperfect.org/ (2.4.2008).

[8] OddPerfect.org: *The Arguments Against.* http://oddperfect.org/against.html (14.4.2008).

[9] Rosen, Kenneth H.: *Elementary Number Theory and Its Applications.* Addison-Wesley Publishing Company, 1993.

[10] Voight, John: *Perfect Numbers: An Elementary Introduction.* http://www.ima.umn.edu/∼voight/notes/perfelem.pdf (23.1.2008).

[11] Weisstein, Eric W.: *Perfect Number.* MathWorld – A Wolfram Web Resource. http://mathworld.wolfram.com/PerfectNumber.html (14.1.2008).

[12] Weisstein, Eric W.: *Lucas-Lehmer Test.* MathWorld – A Wolfram Web Resource. http://mathworld.wolfram.com/Lucas-LehmerTest.html (18.3.2008).

[13] Wells, David: *The Penguin Dictionary of Curious and Interesting Numbers.* Penguin Books Ltd, London, 1997.