Tampereen yliopisto

Ida Saari

TÄYDELLISET LUVUT JA MERSENNEN JA FERMAT'N LUVUT

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Lokakuu 2021

Tiivistelmä

Ida Saari: Täydelliset luvut ja Mersennen ja Fermat'n luvut
Kandidaattitutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Lokakuu 2021

Tutkielmassa tutustutaan matemaattisen kirjallisuuden pohjalta kolmentyyppisiin lukuihin, joita kutsutaan täydellisiksi luvuiksi, Mersennen luvuiksi ja Fermat'n luvuiksi. Täydellisiksi luvuiksi on nimetty sellaiset luvut, joiden kaikkien positiivisten jakajien summa on yhtä suuri kuin kaksi kertaa luku itse, Mersennen luvuiksi muotoa $2^m - 1$ olevat luvut ja Fermat'n luvuiksi puolestaan luvut, jotka voidaan kirjoittaa muodossa $2^{2^m} + 1$.

Täydellisten lukujen osuudessa todistetaan, että parillisten täydellisten lukujen on oltava muotoa $2^{m-1}(2^m - 1)$, jossa luku $2^m - 1$ on alkuluku, ja kaikki tällaiset luvut ovat täydellisiä lukuja. Lisäksi käsitellään hieman parittomien täydellisten lukujen olemassaoloa.

Mersennen lukuja, jotka ovat alkulukuja, kutsutaan luonnollisesti Mersennen alkuluvuiksi. Mersennen lukujen osuudessa keskitytäänkin juuri Mersennen alkulukujen tutkimiseen. Aluksi todistetaan, että jotta Mersennen luku voisi olla alkuluku, on eksponentin m oltava alkuluku. Lisää keinoja Mersennen alkulukujen tutkimiseen antavat lause, jonka mukaan Mersennen luvun alkulukujakajien on oltava tiettyä muotoa, sekä Lucas-Lehmerin testiksi kutsuttu lause, joka antaa suoran ehdon sille, onko tutkittu Mersennen luku alkuluku. Mersennen luvut ovat olleet tärkeässä roolissa suurten alkulukujen etsinnässä, ja tälläkin hetkellä suurin tunnettu Mersennen alkuluku on samalla suurin tunnettu alkuluku. Suurten Mersennen alkulukujen etsimiseksi on perustettu internetissä toimiva Great Internet Mersenne Prime Search, josta käytetään lyhennettä GIMPS ja jonka nettisivuja on käytetty kirjallisuuden lisäksi tutkielman lähteenä.

Viimeisenä tutustutaan hieman Fermat'n lukuihin. Selviää, että Fermat'n alkuluvut, eli Fermat'n luvut, jotka ovat lisäksi alkulukuja, voidaan esittää

myös muodossa $2^m + 1$. Alun perin esitettiinkin, että kaikki Fermat'n luvut olisivat alkulukuja, mutta todellisuudessa viiden ensimmäisen Fermat'n luvun lisäksi ei ole vieläkään löydetty muita Fermat'n alkulukuja.

Avainsanat: täydellinen luku, Mersennen luku, Fermat'n luku, suuret alkuluvut

Sisällys

1 Johdanto

Tässä tutkielmassa tutustutaan kolmentyyppisiin lukuihin: täydellisiin lukuihin, eli lukuihin, joiden tekijöiden summa on yhtä suuri kuin kaksi kertaa luku itse, Mersennen lukuihin, jotka ovat lukuja muodossa $2^n - 1$, sekä Fermat'n lukuihin, jotka puolestaan ovat lukuja, jotka voidaan kirjoittaa muodossa $2^{2^n} + 1$.

Täydellisiä lukuja käsitellään luvussa 3. Se on jaettu kahteen alalukuun, joista toisessa todistetaan parillisia täydellisiä lukuja koskeva lause, jonka mukaan jokainen parillinen täydellinen luku on esitettävissä tietyssä muodossa ja kaikki lauseen ehdot täyttävät luvut ovat täydellisiä lukuja, ja huomataan, että parillisilla täydellisillä luvuilla on yhteys Mersennen alkulukuihin. Toisessa käsitellään parittomien täydellisten lukujen olemassaoloa.

Luku 4 käsittelee nimensä mukaisesti Mersennen luvuiksi kutsuttuja lukuja. Sekin on jaettu kahteen alalukuun, jotka käsittelevät molemmat pääasiassa Mersennen alkulukuja. Ensin todistetaan lause, jonka mukaan Mersennen alkuluvussa esiintyvän eksponentin n on oltava alkuluku, ja tutustutaan sitten hieman lisää Mersennen alkulukujen etsimiseen. Toinen alaluku käsittelee suurten alkulukujen etsintää.

Luvussa 5 perehdytään vielä hieman Fermat'n lukuihin sekä alkulukuihin. Luvussa esimerkiksi osoitetaan, että kun kyseessä on Fermat'n alkuluku, merkinnän $2^{2^n} + 1$ sijaan on mahdollista käyttää myös merkintää $2^n + 1$.

Lukijan oletetaan tuntevan ainakin hieman alkulukuja ja niiden ominaisuuksia, sillä alkulukuihin ei perehdytä tutkielmassa erikseen. Kongruenssin käsitteen tunteminen helpottaa tutkielman lukemista, vaikka kongruenssin määritelmä ja joitakin siihen liittyviä ominaisuuksia esitelläänkin esitiedoissa luvussa 2. Esitietoja-luvussa on esitelty varsin kattavasti sellaiset tutkielmassa käytettävät määritelmät ja lauseet, joita ei käsitellä varsinaisissa sisältöluvuissa.

Tutkielmassa on käytetty lähteinä Kenneth H. Rosenin kirjaa *Elementary number theory and its applications*, David M. Burtonin kirjaa *Elementary number theory*, James J. Tattersallin kirjaa *Elementary number theory in nine chapters*, Cindy Tsangin opinnäytettä *Fermat numbers* sekä Great Internet Mersenne Prime Search -projektin nettisivuja.

2 Esitietoja

Tässä luvussa esitellään sellaisia määritelmiä ja tuloksia, jotka helpottavat myöhempien lukujen määritelmien tai lauseiden ymmärtämistä tai joihin viitataan myöhempien lukujen lauseiden todistuksissa. Tämän luvun lauseita ja apulauseita ei todisteta, mutta niihin annetaan lähdeviitteet, jolloin kiinnostuneet voivat itse perehtyä todistuksiin halutessaan.

Määritelmä 2.1 (Positiivisen kokonaisluvun jakajien summa, vrt. [4, s. 86], [3, s. 232])**.** Olkoot n ja d positiivisia kokonaislukuja. Määritellään funktio σ seuraavasti:

$$\sigma(n) = \sum_{d|n} d.$$

Apulause 2.1. Olkoon luku p alkuluku ja luku n positiivinen kokonaisluku. Silloin

$$\sigma(p^n) = 1 + p + p^2 + \cdots + p^n = \frac{p^{n+1} - 1}{p - 1}.$$

Todistus. Ks. [3, s. 234]. □

Määritelmä 2.2 (Suhteelliset alkuluvut, vrt. [3, s. 80])**.** Kokonaisluvut a ja b ovat *suhteellisia alkulukuja*, jos niiden suurin yhteinen tekijä on 1.

Määritelmä 2.3 (Multiplikatiivinen funktio, vrt. [3, s. 222])**.** Olkoon f funktio positiivisten kokonaislukujen joukolta reaalilukujen joukkoon. Funktio f on *multiplikatiivinen*, jos on voimassa yhtälö $f(mn) = f(m)f(n)$ aina, kun luvut m ja n ovat suhteellisia alkulukuja.

Apulause 2.2. Funktio σ on multiplikatiivinen funktio.

Todistus. Ks. [3, s. 234]. □

Lause 2.1. *Olkoon funktio f multiplikatiivinen, luku n positiivinen kokonaisluku ja $n = p_1^{k_i} p_2^{k_2} \cdots p_r^{k_r}$ luku n jaettuna alkulukutekijöihin. Tällöin*

$$f(n) = f(p_1^{k_i}) f(p_2^{k_2}) \cdots f(p_r^{k_r}).$$

Todistus. Ks. [3, s. 222] □

Apulause 2.3. Olkoot m, n ja l sellaisia positiivisia kokonaislukuja, että lukujen m ja n suurin yhteinen tekijä on 1 ja $m \mid nl$. Tällöin myös $m \mid l$.

Todistus. Ks. [3, s. 97]. □

Määritelmä 2.4 (Kongruenssi, vrt. [3, s. 128])**.** Olkoon luku m positiivinen kokonaisluku ja olkoot luvut a ja b kokonaislukuja. Luku a on *kongruentti luvun b kanssa modulo m*, jos $m \mid (a - b)$. Tällöin käytetään merkintää $a \equiv b \pmod{m}$.

Apulause 2.4. Olkoot luvut a, b, c ja d kokonaislukuja, olkoon m positiivinen kokonaisluku ja $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m}$. Tällöin

$$a + c \equiv b + d \pmod{m}$$

ja

$$ac \equiv bd \pmod{m}.$$

Todistus. Ks. [3, s. 131] □

Apulause 2.5. Kongruenssilla modulo m on refleksiivisyys-, symmetrisyys- ja transitiivisuusominaisuudet.

Todistus. Ks. [3, s. 129] □

Määritelmä 2.5 (vrt. [1, s. 147])**.** Olkoot a ja n sellaisia lukuja, että niiden suurin yhteinen tekijä on 1 ja $n > 1$. Tällöin pienintä sellaista positiivista kokonaislukua k, jolle pätee $a^k \equiv 1 \pmod{n}$ kutsutaan luvun a *kertaluvuksi modulo n*.

Lause 2.2. *Olkoon k kokonaisluvun a kertaluku modulo n. Tällöin $a^h \equiv 1 \pmod{n}$, jos ja vain jos $k \mid h$.*

Todistus. Ks. [1, s. 148]. □

Lause 2.3 (Fermat'n pieni lause)**.** *Olkoon p alkuluku ja n sellainen positiivinen kokonaisluku, että $p \nmid n$. Silloin $n^{p-1} \equiv 1 \pmod{p}$.*

Todistus. Ks. [3, s. 199–200]. □

3 Täydelliset luvut

Täydelliset luvut ovat lukuja, jotka ovat kiinnostaneet ihmisiä jo pitkään, sillä ne tunnettiin jo muinaisten kreikkalaisten keskuudessa [3, s. 239]. Tämän luvun kahdessa alaluvussa perehdytään lyhyesti sekä parillisiin että parittomiin täydellisiin lukuihin. Tutustutaan kuitenkin ensin täydellisen luvun määritelmään.

Määritelmä 3.1 (Täydellinen luku, vrt. [3, s. 239])**.** Olkoon luku n positiivinen kokonaisluku. Jos $\sigma(n) = 2n$, luku n on *täydellinen luku.*

Esimerkki 3.1 (vrt. [3, s. 239])**.** Luku 6 on täydellinen luku, koska $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6$.

3.1 Parilliset täydelliset luvut

Tämä alaluku sisältää oikeastaan vain yhden, mutta parillisten täydellisten lukujen kannalta merkittävän lauseen todistuksineen. Hieman lisää tietoa parillisista täydellisistä luvuista on löydettävissä esimerkiksi Burtonin kirjan [1] sivuilta 219 – 223.

Lause 3.1. *Olkoon luku n positiivinen (ja parillinen) kokonaisluku. Luku n on parillinen täydellinen luku, jos ja vain jos*

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

missä luku m on sellainen kokonaisluku, että $m \geq 2$, ja $2^m - 1$ on alkuluku.

Todistus (vrt. [3, s. 239–240]). Olkoon luku n positiivinen (ja parillinen) kokonaisluku. Oletetaan ensin, että luku $2^m - 1$ on alkuluku, $m \geq 2$ ja $n = 2^{m-1}(2^m - 1)$, ja osoitetaan, että tällöin luku n on täydellinen luku. Täydellisen luvun määritelmän perusteella on siis osoitettava, että $\sigma(n) = 2n$.

Luku 2^{m-1} on jaollinen vain luvuilla $1, 2, 2^2, \ldots, 2^{m-1}$ [4, s. 127] ja luku $2^m - 1$ on pariton, joten lukujen 2^{m-1} ja $2^m - 1$ suurin yhteinen tekijä on 1. Määritelmän 2.2 perusteella luvut 2^{m-1} ja $2^m - 1$ ovat siis suhteellisia alkulukuja. Lisäksi apulause 2.2 kertoo, että funktio σ on multiplikatiivinen, joten määritelmän 2.3 nojalla

$$\sigma(n) = \sigma(2^{m-1}(2^m - 1)) = \sigma(2^{m-1})\sigma(2^m - 1). \tag{3.1}$$

Koska luku 2 on alkuluku ja $m \geq 2$, apulauseen 2.1 perusteella

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

Oletuksen perusteella luku $2^m - 1$ on alkuluku, joten voidaan jälleen hyödyntää apulausetta 2.1 ja saadaan

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

Sijoittamalla nämä yhtälöön (3.1) saadaan

$$\sigma(n) = \sigma(2^{m-1})\sigma(2^m - 1) = 2^m(2^m - 1) = 2 \cdot 2^{m-1}(2^m - 1) = 2n,$$

eli luku n on täydellinen luku.

Oletetaan sitten, että luku n on parillinen täydellinen luku, ja osoitetaan, että tällöin se voidaan kirjoittaa muodossa

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

missä luku $2^m - 1$ on alkuluku ja $m \geq 2$.

Olkoot s ja t positiivisia kokonaislukuja, t pariton ja $n = 2^s t$. Koska luku 2 on alkuluku, apulauseen 2.1 perusteella

$$\sigma(2^s) = \frac{2^{s+1} - 1}{2 - 1} = 2^{s+1} - 1.$$

Lukujen 2^s ja t suurin yhteinen tekijä on 1, joten määritelmän 2.3 ja edellisen yhtälön perusteella

$$\sigma(n) = \sigma(2^s t) = \sigma(2^s)\sigma(t) = (2^{s+1} - 1)\sigma(t). \tag{3.2}$$

Oletuksen mukaan n on täydellinen luku, joten määritelmän nojalla

$$\sigma(n) = 2n = 2 \cdot 2^s t = 2^{s+1} t. \tag{3.3}$$

Yhtälöiden (3.2) ja (3.3) perusteella

$$(2^{s+1} - 1)\sigma(t) = 2^{s+1} t. \tag{3.4}$$

Myös lukujen 2^{s+1} ja $2^{s+1} - 1$ suurin yhteinen tekijä on 1, ja yhtälöstä (3.4) nähdään, että $2^{s+1} \mid (2^{s+1} - 1)\sigma(t)$, joten apulauseen 2.3 perusteella $2^{s+1} | \sigma(t)$.

On siis olemassa sellainen positiivinen kokonaisluku q, että $\sigma(t) = 2^{s+1}q$. Sijoitetaan tämä yhtälöön (3.4), jolloin saadaan

$$(2^{s+1} - 1)2^{s+1}q = 2^{s+1}t \Leftrightarrow (2^{s+1} - 1)q = t. \tag{3.5}$$

Luku t on siis jaollinen luvulla q ja $q \neq t$. Sijoittamalla luvun t paikalle luku $(2^{s+1} - 1)q$ yhtälöstä (3.5) huomataan, että

$$t + q = (2^{s+1} - 1)q + q = (2^{s+1} - 1 + 1)q = 2^{s+1}q = \sigma(t). \tag{3.6}$$

Osoitetaan sitten, että $q = 1$. Tehdään vastaoletus, jonka mukaan $q \neq 1$. Koska $q \mid t$ ja $q \neq t$, luku t on jaollinen ainakin kolmella erisuurella positiivisella kokonaisluvulla, luvuilla q, t ja 1. Tällöin määritelmän 2.1 perusteella $\sigma(t) \geq q + t + 1$, mikä ei voi pitää paikkaansa, koska $\sigma(t) = t + q$. Vastaoletus on siis väärä, joten $q = 1$.

Koska osoitettiin, että $q = 1$, ja aiemmin osoitettiin, että $t = (2^{s+1} - 1)q$, saadaan yhtälö

$$t = 2^{s+1} - 1.$$

Sijoitetaan $2^{s+1} - 1$ yhtälöön $n = 2^s t$, jolloin on osoitettu, että

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

Luku s on positiivinen kokonaisluku, joten $s \geq 1$. Kun luvun s paikalle sijoitetaan luku $m - 1$, saadaan haluttu muoto

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

jossa $m - 1 \geq 1$ eli $m \geq 2$.

On vielä osoitettava, että $2^{s+1} - 1$ on alkuluku. Koska yhtälön (3.6) mukaan $\sigma(t) = t + q$, ja osoitettiin, että $q = 1$,

$$\sigma(t) = t + 1.$$

Määritelmän 2.1 mukaan luku t on siis jaollinen vain luvuilla t ja 1, joten se on alkuluku. □

Sellaisiin alkulukuihin, jotka voidaan kirjoittaa muodossa $2^m - 1$, perehdytään tarkemmin luvussa 4.

3.2 Parittomat täydelliset luvut

Alaluvussa 3.1 käsiteltiin parillisia täydellisiä lukuja. Tässä alaluvussa perehdytään lyhyesti parittomien täydellisten lukujen ongelmaan. Alaluku perustuu kokonaisuudessaan Burtonin kirjan [1] sivuihin 231 – 233.

Esimerkissä 3.1 annettiin esimerkki ainoastaan parillisesta täydellisestä luvusta. Tähän on syynä se, että parittomia täydellisiä lukuja ei tunneta toistaiseksi yhtäkään. Ei ole kuitenkaan pystytty myöskään todistamaan, ettei niitä olisi olemassa. Sen sijaan on onnistuttu löytämään ehtoja sille, millainen luvun n tulisi olla, jotta se voisi olla pariton täydellinen luku. Todistetaan seuraavaksi yksi sellainen.

Lause 3.2. *Jos on olemassa pariton täydellinen luku n, se voidaan kirjoittaa muodossa*

$$n = p_1^{k_1} p_2^{2j_2} \cdots p_r^{2j_r},$$

missä luvut $p_1, \ldots, p_r$ ovat erisuuria parittomia alkulukuja ja

$$p_1 \equiv k_1 \equiv 1 \pmod 4.$$

Todistus. Oletetaan, että on olemassa pariton täydellinen luku n. Olkoon $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ luku n jaettuna alkulukutekijöihin. Tällöin täydellisen luvun määritelmän sekä apulauseen 2.2 ja lauseen 2.1 perusteella

$$2n = \sigma(n) = \sigma(p_1^{k_1})\sigma(p_2^{k_2}) \cdots \sigma(p_r^{k_r}).$$

Luku n on pariton kokonaisluku, joten voidaan merkitä $n = 2m + 1$. Tällöin $2n = 2(2m + 1) = 4m + 2$. Nyt huomataan, että $4 \mid 4m + 2 - 2 = 4m$, joten kongruenssin määritelmän perusteella jokaiselle parittomalle kokonaisluvulle n pätee $2n \equiv 2 \pmod 4$. Luku $2n$ ei voi siis olla jaollinen luvulla 4, mutta koska se on parillinen, se on jaollinen luvulla 2. Yhden luvuista $\sigma(p_i^{k_i})$ täytyy siis olla parillinen ja muiden lukujen $\sigma(p_i^{k_i})$ parittomia, koska muuten luku $2n$ olisi jaollinen luvulla 4. Valitaan parilliseksi luvuksi $\sigma(p_1^{k_1})$. Edelleen koska luku $2n$ ei voi olla jaollinen luvulla 4, myöskään luku $\sigma(p_1^{k_1})$ ei voi olla jaollinen luvulla 4, jolloin sitä voidaan merkitä $\sigma(p_1^{k_1}) = 2m$, missä luku m on pariton kokonaisluku. Tästä seuraa, kuten aiemmin osoitettiin, että $\sigma(p_1^{k_1}) \equiv 2 \pmod 4$.

Luku n on pariton, joten jokaisen luvuista $p_1, p_2, \ldots, p_r$ on oltava pariton. Joka toinen parillinen luku on jaollinen luvulla 4, joten joko $4 \mid 2m$ tai $4 \mid$

$2m-2$. Jokaiselle parittomalle luvulle $2m+1$ pätee siis joko $4 \mid 2m+1-1 = 2m$ tai $4 \mid 2m+1-3 = 2m-2$, joten kongruenssin määritelmän perusteella jokaiselle luvulle p_i pätee joko $p_i \equiv 1 \pmod 4$ tai $p_i \equiv 3 \pmod 4$. Lisäksi koska p_i on alkuluku, määritelmän 2.1 perusteella

$$\sigma(p_i^{k_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{k_i}. \tag{3.7}$$

Oletetaan nyt, että $p_i \equiv 3 \equiv -1 \pmod 4$. Tästä seuraa yhtälön (3.7) ja apulauseen 2.4 perusteella, että

$$\begin{aligned}\sigma(p_i^{k_i}) &\equiv 1 + (-1) + (-1)^2 + \cdots + (-1)^{k_i} \pmod 4 \\ &\equiv \begin{cases} 0 \pmod 4, & \text{kun } k_i \text{ on pariton,} \\ 1 \pmod 4, & \text{kun } k_i \text{ on parillinen.} \end{cases}\end{aligned}$$

Huomataan ensin, että koska $\sigma(p_1^{k_1}) \equiv 2 \pmod 4$, ei ole mahdollista, että $p_1 \equiv 3 \pmod 4$. Siispä $p_1 \equiv 1 \pmod 4$.

Tarkastellaan sitten lukuja $p_2, \ldots, p_r$. Mikäli $\sigma(p_i^{k_i}) \equiv 0 \pmod 4$, kongruenssin määritelmän mukaan $4 \mid \sigma(p_i^{k_i})$, mikä ei voi pitää paikkaansa, sillä luku $2n = \sigma(p_1^{k_1})\sigma(p_2^{k_2}) \cdots \sigma(p_r^{k_r})$ ei ole jaollinen luvulla 4. Tästä seuraa, että jos $i \neq 1$, niin $\sigma(p_i^{k_i}) \equiv 1 \pmod 4$, jolloin luku k_i on parillinen.

Siirrytään nyt tarkastelemaan vaihtoehtoa $p_i \equiv 1 \pmod 4$. Tällöin jälleen yhtälön (3.7) sekä apulauseen 2.4 perusteella

$$\sigma(p_i^{k_i}) \equiv 1 + 1 + 1^2 + \cdots + 1^{k_i} \equiv k_i + 1 \pmod 4.$$

Aiemmin todettiin, että $p_1 \equiv 1 \pmod 4$ ja $\sigma(p_1^{k_1}) \equiv 2 \pmod 4$. Apulauseen 2.5 mukaisesti siis $2 \equiv k_1 + 1 \pmod 4$ eli $4 \mid 2 - k_1 - 1 = 1 - k_1$, joten $k_1 \equiv 1 \pmod 4$. Luvut $\sigma(p_2^{k_2}), \ldots, \sigma(p_r^{k_r})$ puolestaan ovat parittomia, joten kun $i \neq 1$, niin joko $\sigma(p_i^{k_i}) \equiv 1 \pmod 4$, jolloin $k_i \equiv 0 \pmod 4$, tai $\sigma(p_i^{k_i}) \equiv 3 \pmod 4$, jolloin $k_i \equiv 2 \pmod 4$. Tämä voidaan perustella samoin kuin edellä tehtiin. Luku k_i $(i \neq 1)$ on siis parillinen myös, jos $p_i \equiv 1 \pmod 4$.

Nyt on siis osoitettu, että kun $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ on luku n jaettuna alkulukutekijöihin, voidaan valita luvuksi $p_1^{k_1}$ sellainen luku, että $p_1 \equiv 1 \pmod 4$ ja $k_1 \equiv 1 \pmod 4$. Lisäksi tällöin luvut $k_2, \ldots, k_r$ ovat parillisia, jolloin voidaan merkitä $k_2 = 2j_2, \ldots, k_r = 2j_r$. □

4 Mersennen luvut

Tämä luku käsittelee 1500 – 1600 -lukujen vaihteessa eläneen Marin Mersennen mukaan nimettyjä lukuja [3, s. 241]. Luvussa keskitytään Mersennen alkulukujen tutkimiseen: alaluku 4.1 johdattelee lauseillaan ja esimerkeillään Mersennen alkulukujen etsimiseen, ja alaluku 4.2 tutustuttaa lukijan siihen, miten Mersennen alkuluvut liittyvät suurten alkulukujen etsimiseen. Kuten luvussa 3 mainittiin, Mersennen alkuluvuilla on myös yhteys parillisten täydellisten lukujen etsimiseen.

4.1 Mersennen luvut ja alkuluvut

Määritelmä 4.1 (vrt. [3, s. 241])**.** Olkoon luku m positiivinen kokonaisluku. Luku $2^m - 1$ on m:s *Mersennen luku* ja siitä käytetään merkintää M_m. Jos luku M_m on lisäksi alkuluku, sitä kutsutaan *Mersennen alkuluvuksi*.

Esimerkki 4.1. Luku $2^6 - 1 = 63$ on 6. Mersennen luku eli M_6. Se ei kuitenkaan ole Mersennen alkuluku, sillä esimerkiksi $3 \cdot 21 = 63$.

Lause 4.1. *Olkoon luku m positiivinen kokonaisluku. Jos luku $2^m - 1$ on alkuluku, myös luku m on alkuluku.*

Todistus (vrt. [3, s. 240–241]). Oletetaan, että luku $2^m - 1$ on alkuluku, ja tehdään vastaoletus, jonka mukaan luku m ei ole alkuluku. Koska m ei ole alkuluku, voidaan kirjoittaa yhtälö $m = ab$, jossa $1 < a < m$ ja $1 < b < m$. Koska $m = ab$,

$$\begin{aligned} 2^m - 1 &= 2^{ab} - 1 \\ &= 2^{ab} + 2^{ab-a} + \cdots + 2^{2a} + 2^a - 2^{ab-a} - 2^{ab-2a} - \cdots - 2^a - 1 \\ &= 2^a \cdot 2^{a(b-1)} + 2^a \cdot 2^{a(b-2)} + \cdots \\ &\qquad + 2^a \cdot 2^a + 2^a \cdot 1 - 2^{a(b-1)} - 2^{a(b-2)} - \cdots - 2^a - 1 \\ &= (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1). \end{aligned}$$

Koska $a > 1$, myös $(2^a - 1) > 1$, ja $(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1) > 1$, joten luku $2^m - 1$ ei voi olla alkuluku, mikä on ristiriidassa oletusten kanssa. Vastaoletus ei siis pidä paikkaansa, eli luku m on alkuluku. □

Esimerkki 4.2. Luku 3562 on jaollinen ainakin luvulla 2. Mersennen luku $M_{3562} = 2^{3562} - 1$ ei siis ole alkuluku, koska luku 3562 ei ole alkuluku. Sen sijaan luvut 7 ja 11 ovat alkulukuja, joten lauseen 4.1 perusteella ei voida päätellä, ovatko M_7 ja M_{11} alkulukuja.

Lause 4.2. *Olkoon p pariton alkuluku. Tällöin jokainen Mersennen luvun M_p alkulukujakaja voidaan kirjoittaa muodossa $2kp + 1$.*

Todistus (vrt. [1, s. 228]). Olkoon q jokin Mersennen luvun $M_p = 2^p - 1$ alkulukujakaja. Tarkoituksena on siis todistaa, että luvun q on oltava muotoa $2kp + 1$.

Koska $q \mid M_p$, kongruenssin määritelmän mukaisesti $2^p - 1 \equiv 0 \pmod{q}$ eli $2^p \equiv 1 \pmod{q}$. Olkoon s määritelmän 2.5 mukainen luvun 2 kertaluku modulo q. Tällöin lauseen 2.2 perusteella $s \mid p$.

Luku p on alkuluku, joten joko $s = 1$ tai $s = p$. Oletetaan ensin, että $s = 1$. Tällöin siis $2^1 \equiv 1 \pmod{q}$, mistä kongruenssin määritelmän perusteella seuraa, että $q \mid 2 - 1 = 1$. Tämä ei voi pitää paikkaansa, joten $s = p$.

Koska luku $M_p = 2^p - 1$ on pariton ja $q \mid M_p$, ei voi pitää paikkaansa, että $q = 2$. Siispä $q \nmid 2$, jolloin lauseen 2.3 perusteella $2^{q-1} \equiv 1 \pmod{q}$. Koska aiemmin merkittiin luvulla s luvun 2 kertalukua modulo q, lauseen 2.2 perusteella $s \mid q - 1$. Koska lisäksi $s = p$, myös $p \mid q - 1$. Tämän perusteella voidaan kirjoittaa yhtälö $q - 1 = pt$, jolloin $q = pt + 1$.

Osoitetaan vielä, että luvun t on oltava parillinen eli että $t = 2k$. Oletetaan, että luku t on pariton. Koska myös p on pariton, luku pt on pariton, jolloin $pt + 1 = q$ on parillinen. Tämä ei voi pitää paikkaansa, koska q on alkuluku ja $q \neq 2$. Luvun t on siis oltava parillinen. Kun merkitään $t = 2k$, huomataan, että $q = 2kp + 1$. □

Huomattiin, että kun halutaan selvittää, onko Mersennen luku M_m alkuluku, lauseesta 4.1 on hyötyä vain silloin, kun luku m ei ole alkuluku. Annetaan seuraavaksi muutama esimerkki siitä, miten lausetta 4.2 voidaan käyttää apuna, kun halutaan päätellä, onko Mersennen luku M_p alkuluku silloin, kun luku p on pariton alkuluku. Esimerkit on keksitty käyttäen apuna esimerkkejä lähteestä [3, s. 242].

Esimerkki 4.3. Luku 11 on pariton alkuluku. Voidaan siis selvittää lausetta 4.2 käyttäen, onko Mersennen luku $M_{11} = 2^{11} - 1 = 2047$ Mersennen alkuluku.

Jokaisen luvun M_{11} alkulukujakajan on oltava muotoa $2kp + 1$. Koska $p = 11$, jokaisen alkulukujakajan on oltava muotoa $2 \cdot k \cdot 11 + 1 = 22k + 1$. Nyt huomataan, että luku $22 \cdot 1 + 1 = 23$ toteuttaa ehdon. Huomataan myös, että $23 \cdot 89 = 2047 = M_{11}$, joten M_{11} ei ole alkuluku.

Esimerkki 4.4. Päätellään, onko $M_7 = 2^7 + 1 = 127$ alkuluku. Lauseen 4.2 perusteella jokaisen luvun M_7 alkulukujakajan on oltava muotoa $2 \cdot k \cdot 7 + 1 = 14k + 1$. Jos 127 ei ole alkuluku, sillä täytyy olla lukua $\sqrt{127} \approx 11,27$ pienempi alkulukujakaja. Huomataan kuitenkin, että $14k + 1 > 11,27$, kun $k \geq 1$, joten M_7 on Mersennen alkuluku. Luku 127 on toki niin pieni luku, että on muutenkin helppoa selvittää, onko se alkuluku, mutta lause 4.2 antaa yhden yksinkertaisen keinon sen selvittämiseksi.

4.2 Suurten alkulukujen etsintä

Sen selvittämiseksi, onko tietty Mersennen luku alkuluku, on olemassa vain Mersennen luvuille soveltuvia alkulukutestejä. Niiden avulla voidaan löytää hyvinkin suuria Mersennen alkulukuja, mistä johtuen suurin tunnettu alkuluku on usein Mersennen alkuluku. Mersennen alkulukujenkaan etsiminen ei kuitenkaan ollut helppoa ennen tietokoneiden keksimistä ja niistä esitettiin myöhemmin epätosiksi osoittautuneita väitteitä. Esimerkiksi 1800-luvulla eräs matemaatikko esitti uskomuksen, ettei lukua M_{31} suurempaa Mersennen alkulukua koskaan tultaisi löytämään.

Tietokoneiden yleistyttyä uusien Mersennen alkulukujen etsintä helpottui, ja vuosina 1952–1996 löydettiin yhteensä 22 uutta Mersennen alkulukua tietokoneavusteisesti. Sitten avuksi otettiin internet, kun vuonna 1996 perustettiin the Great Internet Mersenne Prime Search, lyhennettynä GIMPS. Sen avulla yksittäiset ihmiset voivat osallistua uusien Mersennen alkulukujen etsintään liittämällä tietokoneensa osaksi etsintää. Ensimmäinen alkuluku löydettiin GIMPS-projektin avulla jo vuonna 1996.

Ranskalainen Edouard Lucas kehitti 1870 -luvulla teorian, josta on ollut erityisen paljon hyötyä uusien Mersennen alkulukujen löytämisessä. Yhdysvaltalainen matemaatikko Derrick H. Lehmer kehitti teoriasta yksinkertaisemman testin vuonna 1930, ja kyseinen testi on nimetty Lucas-Lehmerin testiksi. [3, s. 242–246]

Lause 4.3 (Lucas-Lehmerin testi, vrt. [3, s. 243])**.** *Olkoon luku p jokin alkuluku. Tarkastellaan Mersennen lukua $M_p = 2^p - 1$. Olkoon $r_1 = 4$, ja kun $k \geq 2$, olkoon luku r_k sellainen luku, että*

$$r_k \equiv r_{k-1}^2 - 2 \pmod{M_p}, \qquad 0 \leq r_k < M_p.$$

Tällöin Mersennen luku M_p on alkuluku, jos ja vain jos $r_{p-1} \equiv 0 \pmod{M_p}$.

Lauseen todistus sivuutetaan. Tattersallin kirja [4, s. 131] esittää saman asian ehkä hieman helpommin ymmärrettävässä muodossa määrittelemällä luvun r_k jakojäännökseksi, joka saadaan jakamalla luku $r_{k-1}^2 - 2$ luvulla M_p.

Esimerkki 4.5. Osoitetaan Lucas-Lehmerin testin avulla, että luku $M_{13} = 8191$ on alkuluku. Testin mukaan $r_1 = 4$. Huomataan, että $r_1^2 - 2 = 14$. Kun käytetään Tattersallin kirjan muotoilua, huomataan, että kun luku 14 jaetaan luvulla 8191, jakojännös on 14, joten $r_2 = 14$. Huomataan myös, että $14 \equiv 14 \pmod{8191}$, joten se toteuttaa myös lauseessa 4.3 muotoillun ehdon. Jälleen $r_2^2 - 2 = 194$, joten $r_3 = 194$. Lasketaan seuraavaksi, että $r_3^2 - 2 = 37634$. Koska $37634 > M_{13}$, lasketaan jakojäännös, kun luku 37634 jaetaan luvulla M_{13}, ja saadaan $r_4 = 4870$. Jatketaan laskemalla, että $r_5 = 3953$, $r_6 = 5970$, $r_7 = 1857$, $r_8 = 36$, $r_9 = 1294$, $r_{10} = 3470$, $r_{11} = 128$ ja $r_{12} = 0$. Siis $r_{13-1} \equiv 0 \pmod{8191}$, joten M_{13} on Mersennen alkuluku.

Suurin nykyisin tunnettu Mersennen alkuluku löydettiin GIMPS-projektin avulla 7.12.2018. Kyseessä on $M_{82589933}$ eli $2^{82589933} - 1$. Se on 51. tunnettu Mersennen alkuluku ja samalla suurin tunnettu alkuluku. [2]

5 Fermat'n luvut

Fermat'n luvuiksi kutsuttuja lukuja on tutkittu 1600-luvulta lähtien, jolloin ranskalainen matemaatikko Pierre de Fermat, jonka mukaan luvut on myös nimetty, esitti uskomuksen, että ne olisivat kaikki alkulukuja. Tämä osoittatui vääräksi, mutta Fermat'n lukuja on pystytty hyödyntämään esimerkiksi geometristen ongelmien käsittelyssä. [5, s. 2–5]

Tässä tutkielmassa ei kuitenkaan perehdytä geometriaan, vaan todistetaan ensin esimerkkinä kaksi Fermat'n lukujen perusominaisuutta, ja käsitellään sitten hieman sitä, mitä Fermat'n alkuluvuista tiedetään.

Määritelmä 5.1 (Vrt. [4, s. 136])**.** Olkoon luku n ei-negatiivinen kokonaisluku. Tällöin lukua $2^{2^n}+1$ kutsutaan *Fermat'n luvuksi* ja sitä merkitään F_n.

Esimerkki 5.1. Luku $2^{2^8}+1$ on Fermat'n luku F_8.

Lause 5.1. *Olkoon luku n positiivinen kokonaisluku. Tällöin*

$$F_n = (F_{n-1}-1)^2 + 1.$$

Todistus (vrt. [5, s. 7]). Oletetaan, että luku n on positiivinen kokonaisluku, ja todistetaan lause seuraavalla yhtälöketjulla:

$$\begin{aligned}(F_{n-1}-1)^2+1 &\\ = (2^{2^{n-1}}+1-1)^2+1 = (2^{2^{n-1}})^2+1 = 2^{2\cdot 2^{n-1}}+1 &= 2^{2^{1+n-1}}+1\\ &= 2^{2^n}+1 = F_n.\end{aligned}$$

□

Lause 5.2. *Olkoon n positiivinen kokonaisluku. Tällöin*

$$F_n = F_0 \cdots F_{n-1} + 2.$$

Todistus (vrt. [5, s. 7]). Käytetään todistamiseen induktiota. Huomataan ensin, että kun $n=1$, $F_1 = 2^{2^1}+1 = 5$ ja

$$F_0 + 2 = 2^{2^0}+1+2 = 3+2 = 5 = F_1.$$

Väite siis pätee, kun $n=1$.

Tehdään sitten induktio-oletus, jonka mukaan

$$F_n = F_0 \cdots F_{n-1} + 2,$$

ja väitetään, että tällöin myös $F_{n+1} = F_0 \cdots F_n + 2$. Huomataan ensin, että

$$F_0 \cdots F_n + 2 = F_0 \cdots F_{n-1} \cdot F_n + 2.$$

ja että induktio-oletuksen mukaan $F_n = F_0 \cdots F_{n-1} + 2$ eli

$$F_0 \cdots F_{n-1} = F_n - 2$$

Nyt voidaan kirjoittaa yhtälöketju

$$\begin{aligned} F_0 \cdots F_n + 2 &= F_0 \cdots F_{n-1} \cdot F_n + 2 \\ &= (F_n - 2) \cdot F_n + 2 \\ &= (2^{2^n} + 1 - 2)(2^{2^n} + 1) + 2 \\ &= (2^{2^n} - 1)(2^{2^n} + 1) + 2 \\ &= (2^{2^n})^2 + 2^{2^n} - 2^{2^n} - 1 + 2 \\ &= 2^{2^n \cdot 2} + 1 = 2^{2^{n+1}} + 1 = F_{n+1}. \end{aligned}$$

□

Lisää Fermat'n lukujen perusominaisuuksista on luettavissa lähteen [5] sivuilta 7 – 11.

Joskus Fermat'n luvuille käytetään myös määritelmää, jossa luvun $2^{2^n} + 1$ tilalla käytetään lukua $2^n + 1$. Kaikki Fermat'n lukujen ominaisuudet eivät kuitenkaan ole voimassa jälkimmäistä määritelmää käytettäessä. Fermat'n alkulukujen kohdalla molemmat määritelmät ovat kuitenkin yhtä käyttökelpoisia. [5, s. 12] Todistetaan tämä seuraavalla lauseella:

Lause 5.3. *Olkoon $a^n + 1$ alkuluku, jossa $a > 1$ ja $n > 0$. Tällöin luku a on parillinen ja luku n voidaan kirjoittaa muodossa 2^r, jossa luku r on positiivinen kokonaisluku.*

Todistus (vrt. [4, s. 136]). Oletetaan, että luku $a^n + 1$ on alkuluku, jossa $a > 1$ ja $n > 0$. Osoitetaan ensin, että luvun a on oltava parillinen tekemällä vastaoletus, jonka mukaan a on pariton. Tällöin luku a^n on pariton, jolloin luku $a^n + 1$ on parillinen. Koska $a > 1$ ja $n > 0$ ja $a^n + 1$ on parillinen, $a^n + 1 > 3$.

Luku $a^n + 1$ on siis parillinen ja suurempi kuin 3, joten se ei voi olla alkuluku, mikä on ristiriidassa oletuksen kanssa. Luvun a täytyy siis olla parillinen.

Osoitetaan sitten, että luku n voidaan kirjoittaa muodossa 2^r. Oletetaan, että luvulla n on lukua 1 suurempi pariton tekijä, eli voidaan kirjoittaa yhtälö $n = st$, jossa luku s on pariton ja $s > 1$. Siis

$$\begin{aligned} a^n + 1 &= a^{st} + 1 \\ &= a^{st} - a^{t(s-1)} + \cdots - a^{2t} + a^t + a^{t(s-1)} - a^{t(s-2)} + \cdots - a^t + 1 \\ &= a^t \cdot a^{t(s-1)} - a^t \cdot a^{t(s-2)} + \cdots \\ &\qquad - a^t \cdot a^t + a^t + a^{t(s-1)} - a^{t(s-2)} + \cdots - a^t + 1 \\ &= (a^t + 1)(a^{t(s-1)} - a^{t(s-2)} + \cdots - a^{t(s-(s-1))} + 1). \end{aligned}$$

Koska luku s on pariton ja $s > 1$, $s \geq 3$, mistä seuraa, että $a^{t(s-1)} - a^{t(s-2)} + \cdots - a^{t(s-(s-1))} + 1 > 1$. Samoin koska $a > 1$, $a^t + 1 > 1$. Luvulla $2^n + 1$ on siis kaksi lukua 1 suurempaa tekijää, joten se ei voi olla alkuluku, mikä on jälleen ristiriidassa oletuksen kanssa. Luvulla n ei siis voi olla parittomia tekijöitä, joten se voidaan kirjoittaa muodossa 2^r. □

Huomautus. Jos Fermat'n alkuluvulle käytetään merkintää $2^n + 1$, kyseessä ei ole määritelmän 5.1 mukainen Fermat'n luku F_n, vaan luku F_r, kun luku n on kirjoitettu lauseen 5.3 mukaisesti muodossa 2^r.

Fermat'n alkulukuja tunnetaan kuitenkin vain viisi: viisi ensimmäistä Fermat'n lukua eli luvut F_0, F_1, F_2, F_3 ja F_4. Suurin tunnettu Fermat'n alkuluku on siis $2^{2^4} + 1 = 65537$. [5, s. 6] Vaikka ainoat tunnetut Fermat'n alkuluvut ovat viisi ensimmäistä Fermat'n lukua, ei silti tiedetä, onko niitä olemassa äärettömästi [5, s. 19].

Lähteet

[1] Burton, David M. Elementary Number Theory, 6th ed. McGraw-Hill, New York. 2007.

[2] Great Internet Mersenne Prime Search (GIMPS). Luettu 26.5.2021. https://www.mersenne.org/

[3] Rosen, Kenneth H. Elementary Number Theory and Its Applications, 4th ed. Addison-Wesley, Reading, Massachusetts. 1997.

[4] Tattersall, James J. Elementary Number Theory in Nine Chapters. Cambridge University Press, Cambridge. 1999.

[5] Tsang, Cindy. Fermat Numbers. Math414 Number Theorey, University of Washington. 2010.