ALKULUKUJA JA MELKEIN ALKULUKUJA

MINNA TUONONEN

Versio: 12. heinäkuuta 2011.

Sisältö

1. Johdanto

Tutkielmani koostuu neljästä aiheesta, jotka kaikki liittyvät lukuteoriaan. Varsinaisesti aiheet eivät liity toisiinsa, mutta läpi tutkielman etsitään tapoja tutkia onko jokin luku alkuluku. Lukujen kolme ja viisi välille saadaan konkreettinen yhteys, josta tarkemmin luvun viisi esittelyssä.

Toiseen lukuun olen koonnut määritelmiä ja lauseita, joihin viittaan läpi tutkielmani. Selkeyden vuoksi nämä esitellään erillisessä luvussa.

Kolmannessa luvussa käsitellään Mersennen alkulukuja ja täydellisiä lukuja. Mersennen luvut ovat muotoa $M_p = 2^p - 1$, missä p on alkuluku. Jos Mersennen luku M_p on alkuluku, niin lukua kutsutaan Mersennen alkuluvuksi. Täydelliset luvut ovat lukuja, jotka saadaan aidosti itseään pienempien jakajien summana. Esimerkki täydellisestä luvusta on luku kuusi. Luvun tärkein tulos on Lause 3.13, jossa todistetaan Mersennen alkulukujen ja parillisten täydellisten lukujen yhteys. Lauseessa todistetaan, että jokaiselle Mersennen alkuluvulle löytyy sitä vastaava parillinen täydellinen luku. Vastaavasti myös parilliselle täydelliselle luvulle löytyy sitä vastaava Mersennen alkuluku.

Neljännessä luvussa aiheena on Eulerin funktio. Luku aloitetaan määrittelemällä Eulerin funktio, ϕ. Eulerin funktiolla $\phi(n)$ saadaan niiden kokonaislukujen määrä, joille $\text{syt}(a, n) = 1$ ja $1 \leq a \leq n$. Luvun tuloksista tärkein on Lause 4.1 eli Eulerin lause, jossa todistetaan, että keskenään jaottomille luvuille a ja n pätee $a^{\phi(n)} \equiv 1 \pmod{n}$. Luvun toiseksi tärkein tulos on Eulerin lauseen erikoistapaus Fermat´n pieni lause 4.8. Lauseessa todistetaan, että kun kokonaisluku a ja alkuluku p ovat keskenään jaottomia, niin $a^{p-1} \equiv 1 \pmod{p}$. Fermat´n pieneen lauseeseen tullaan viittaamaan myös tutkielman viimeisissä luvuissa.

Viidennessä luvussa aiheena ovat pseudoalkuluvut ja Carmichaelin luvut. Luvun alussa käydään läpi muutamia lauseita, joilla voidaan tutkia onko luku alkuluku. Pseudoalkuluvut ja Carmichaelin luvut eivät ole alkulukuja, mutta toteuttavat kongruenssiyhtälöt, jotka alkuluvut toteuttavat. Jos luku n ei ole alkuluku ja toteuttaa kongruenssiyhtälön $2^{n-1} \equiv 1 \pmod{n}$, niin luku n on pseudoalkuluku. Jos luku n, joka ei ole alkuluku toteuttaa kongruenssiyhtälön $a^{n-1} \equiv 1 \pmod{n}$ kaikilla a, joille $\text{syt}(a, n) = 1$, niin n on Carmichaelin luku. Tästä luvusta saadaan yhteys Lauseella 5.6 tutkielman kolmanteen lukuun. Lauseessa todistetaan Mersennen luvun olevan pseudoalkuluku, jos se ei ole alkuluku.

Viimeisessä eli kuudennessa luvussa käsitellään Pythagoraan kolmikoita eli lukuja, jotka toteuttavat Pythagoraan lauseen, $a^2 + b^2 = c^2$. Luvun Lauseessa 6.4 todistetaan, että vain lukua kolme suuremmat tai yhtäsuuret luvut voivat esiintyä Pythagoraan kolmikossa. Luvussa esitellään Lause 6.9, jossa todistetaan kaavat luvuille a, b ja c, joilla saadaan primitiivinen Pythagoraan kolmikko eli jossa kaikki luvut a, b ja c ovat keskenään jaottomia.

2. Tutkielmassa tarvittavia määritelmiä ja apulauseita

Tässä luvussa käydään läpi tutkielmassa tarvittavia määritelmiä ja apulauseita. Selkeyden vuoksi nämä esitellään erillisessä luvussa, koska joitakin näistä tuloksista tullaan tarvitsemaan useammassa tutkielman luvussa.

Määritelmä 2.1. Jos kokonaisluku d jakaa kokonaisluvut a ja b, niin luku d on lukujen a ja b yhteinen tekijä. Jos ainakin toinen luvuista a, b on erisuuri kuin nolla, niin lukua

$$\text{syt}(a,b) = \max\{d \in \mathbb{N} : d|a \text{ ja } d|b\}$$

sanotaan lukujen a ja b suurimmaksi yhteiseksi tekijäksi.

Lause 2.2. *Olkoon* $\text{syt}(a,b)=1$.
1) Jos $a|c$ *ja* $b|c$, *niin* $ab|c$.
2) Jos $a|bc$, *niin* $a|c$.

Todistus. [3], Seuraus 1.11. □

Lause 2.3. *Jos* $a|b$ *ja* $b|c$, *niin* $a|c$.

Todistus. Lähde [5], Lause 1.2. □

Lause 2.4. *Olkoot* a *ja* b *positiivisia kokonaislukuja.*
Jos $a|b$, *niin* $a \leq b$.

Todistus. [5], Lause 1.2. □

Lemma 2.5. *Olkoot luvut* n *ja* m *luonnollisia lukuja. Tällöin*
1) kun $\text{syt}(m,n) = 1$ *ja jos* $c|mn$, *niin on yksikäsitteiset luonnolliset luvut* d *ja* e, *joille* $c=de$ *sekä* $d|m$ *ja* $e|n$.
2) jos $a|m$ *ja* $b|n$, *niin* $ab|mn$.

Todistus. 1)Ensin todistetaan, että $c = de$. Todistetaan tämä kahdessa osassa siten, että ensin näytetään, että $de \leq c$. Tämän jälkeen näytetään, että $c \leq de$.

Lopuksi osoitetaan lukujen d ja e yksikäsitteisyys.

Olkoon $d=\text{syt}(m,c)$ ja $e=\text{syt}(n,c)$, tällöin

$$d|c \text{ ja } e|c.$$

Nyt myös $d|m$ ja $e|n$. Olkoon

$$\text{syt}(d,e) = s, \text{ missä } s \in \mathbb{N} \setminus \{1\},$$

tällöin $s|d$ ja $s|e$. Nyt myös $s|m$ ja $s|n$, mikä on ristiriita, sillä $\text{syt}(m,n) = 1$.

On siis oltava $\text{syt}(d,e) = 1$.

Aloitetaan todistamalla, että $de \leq c$. Nyt $\text{syt}(d,e) = 1$ sekä $d|c$ ja $e|c$. Tällöin Lauseen 2.2 nojalla $de|c$. Nyt Lauseen 2.4 nojalla $de \leq c$.

Todistetaan toiseksi, että $c \leq de$. Olkoot luvut $m‘$ ja $c‘$ luonnollisia lukuja siten, että

$$m = dm‘ \text{ ja } c = dc‘.$$

Näytetään, että on oltava $\text{syt}(m‘,c‘) = 1$. Jos olisi

$$\text{syt}(m‘,c‘) = s, \text{ missä } s \in \mathbb{N} \setminus \{1\},$$

niin $s|m‘$ ja $s|c‘$. Tällöin

$$sd|m \text{ ja } sd|c,$$

mikä on ristiriita, sillä $\text{syt}(m,c) = d$ ja $sd > d$.

Joten on oltava $\text{syt}(m', c') = 1$.

Koska

$$d|c, e|c \text{ ja } \text{syt}(d, e) = 1$$

niin Lauseen 2.2 nojalla

$$de|c \text{ ja } c = dc', \text{ niin } de|dc'.$$

Nyt supistamalla luvulla $d \neq 0$ saadaan $e|c'$.

Oletuksen mukaan $c|mn$, joten on

$$mn = kc \text{ jollain luonnollisella luvulla } k.$$

Nyt saadaan yhtälö sijoituksilla $m = dm'$ ja $c = dc'$ muotoon

$$dm'n = kdc',$$

josta supistamalla luvulla $d \neq 0$ saadaan

$$m'n = kc' \text{ eli } c'|m'n.$$

Koska $\text{syt}(m', c') = 1$, niin Lauseen 2.2 nojalla $c'|n$. Koska

$$e = \text{syt}(n, c), c'|n \text{ ja } c'|c,$$

niin on $c' \leq e$. Siten on

$$c = dc' \leq de.$$

Todistetaan seuraavaksi lukujen d ja e yksikäsitteisyys. Olkoot d, e, d' ja e' luonnollisia lukuja siten, että

$$de = de', d|m, d'|m, e|n \text{ ja } e'|n.$$

Koska $\text{syt}(d, e')=1=\text{syt}(d', e)$, niin $d|d'$ ja $d'|d$. Siten $d=d'$ ja $e=e'$.

2) Koska luku m on jaollinen luvulla a ja luku n on jaollinen luvulla b, niin tällöin on kokonaisluvut k ja l siten, että

$$m = ka \text{ ja } n = lb.$$

Tällöin on

$$mn = kalb = (kl)ab$$

eli luku ab jakaa luvun mn. □

Määritelmä 2.6. Olkoon n luonnollinen luku ja luvut a ja b kokonaislukuja. Luku a on kongruentti luvun b kanssa modulo n,

$$a \equiv b \pmod{n}$$

jos $n \mid (a - b)$.

Jos $n \nmid (a - b)$, niin merkitään $a \not\equiv b \pmod{n}$. Lukua n sanotaan moduliksi.

Lause 2.7. *(Kiinalainen jäännöslause) Olkoot $n_1, n_2, \ldots, n_k$ positiivisia kokonaislukuja, joille $\text{syt}(n_i, n_j)=1$ aina, kun $i \neq j$. Olkoot $a_1, a_2, \ldots, a_k$ kokonaislukuja. Tällöin lineaarisella kongruenssiyhtälöryhmällä*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ x \equiv a_3 \pmod{n_3} \\ \ldots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

on yksikäsitteinen ratkaisu kongruenssiluokkana mod n, missä $n = n_1n_2n_3...n_k$.

Todistus. Lähde [3], Lause 3.10. □

Lause 2.8. *(Kongruenssin laskusääntöjä)*
1) Olkoon n luonnollinen luku ja luvut a, b ja c kokonaislukuja, joille

$$ac \equiv bc \pmod{n}.$$

Jos $\text{syt}(n, c)=1$, *niin* $a \equiv b \pmod{n}$.
Yleisemmin;

$$\textit{Jos } \text{syt}(n, c) = d, \textit{ niin } a \equiv b \pmod{\frac{n}{d}}.$$

2) Olkoon n luonnollinen luku ja olkoot luvut a, b ja c kokonaislukuja. Kaikilla $n \geq 1$ *on voimassa*
a) $a \equiv a \pmod{n}$.
b) Jos $a \equiv b \pmod{n}$, *niin* $b \equiv a \pmod{n}$.
c) Jos $a \equiv b \pmod{n}$ *ja* $b \equiv c \pmod{n}$, *niin* $a \equiv c \pmod{n}$.
3) Olkoon n luonnollinen luku ja olkoot luvut a, b, c ja d kokonaislukuja. Tällöin, jos

$$a \equiv b \pmod{n} \textit{ ja } c \equiv d \pmod{n},$$

niin

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

Todistus. 1) Lähde [5], Lause 2.3.
2)Lähde [3], Lemma 3.2.
3) Lähde [5], Lause 2.1. □

Lause 2.9. *Jos* $m > 1$ *ja* $a^m - 1$ *on alkuluku, niin* $a = 2$ *ja m on alkuluku.*

Todistus. Jos $a > 2$, niin

$$a^m - 1 = (a-1)(a^{m-1} + a^{m-2} + \cdots + 1) \tag{2.1}$$

eli $(a-1)|(a^m-1)$.
Siten luku $a^m - 1$ on alkuluku vain jos $a = 2$.
Jos $m = rs$, missä $s, r > 1$, niin

$$2^m - 1 = (2^r)^s - 1 = (2^r - 1)((2^r)^{s-1} + (2^r)^{s-2} + \cdots + 1)$$

eli luku 2^m-1 on jaollinen luvulla 2^r-1. Tämä on ristiriita, sillä $1 < 2^r-1 < 2^m-1$.
Täten luku $a^m - 1$ on alkuluku vain jos m on alkuluku. □

Lause 2.10. *(Bézout) Olkoot luvut a ja b nollasta eroavia kokonaislukuja. Tällöin on olemassa kokonaisluvut u ja v siten, että*

$$\text{syt}(a, b) = au + bv.$$

Todistus. Lähde [3], Lause 1.7. □

Lause 2.11. *Olkoot a, b ja c kokonaislukuja siten, että* $a \neq 0$ *tai* $b \neq 0$. *Tällöin*

$$c = ka + lb, \textit{ jollain kokonaisluvuilla } k \textit{ ja } l$$

jos ja vain jos $\text{syt}(a, b)$ *jakaa luvun c.*

Todistus. Lähde [3], Lause 1.8. □

Lemma 2.12. *Olkoot a, b ja n kokonaislukuja. Jos*

$$\text{syt}(a,n) = 1 \text{ ja } \text{syt}(b,n) = 1,$$

niin

$$\text{syt}(ab,n) = 1.$$

Todistus. Olkoon $\text{syt}(ab,n) = d$. Koska

$$\text{syt}(a,n) = 1 = \text{syt}(b,n),$$

niin

$$\text{syt}(a,d) = 1 = \text{syt}(b,d).$$

Koska $d|ab$, niin Lauseen 2.2 nojalla $d|b$.

Oletuksen mukaan $\text{syt}(b,n) = 1$, joten on oltava $d = 1$ eli

$$\text{syt}(ab,n) = 1.$$

□

Lause 2.13. *Olkoon p alkuluku. Jos*

$$p|a_1a_2\cdots a_k,$$

niin luku p jakaa luvun a_i jollain i.

Todistus. [3], Seuraus 2.2. □

Lause 2.14. *Olkoon n luonnollinen luku, olkoot a ja b kokonaislukuja ja* $\text{syt}(a,n) = d$

1) Jos $d \nmid b$, niin lineaarisella kongruenssilla $ax \equiv b \pmod{n}$ ei ole kokonaisluku ratkaisua x.

2) Jos $d \mid b$, niin lineaarisella kongruenssilla $ax \equiv b \pmod{n}$ on d ratkaisua (kongruenssiluokkaa modulo n).

Todistus. [3], Lause 3.7. □

Lause 2.15. *Jokaisella kokonaisluvulla $n \geq 2$, on yksikäsitteinen alkutekijäesitys siten, että*

$$n = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r},$$

missä luvut $p_1,\ldots,p_r$ ovat alkulukuja siten, että $p_1 < p_2 < \cdots < p_r$ ja luvut $e_1,\ldots,e_r$ ovat positiivisia kokonaislukuja.

Todistus. Lähde [3], Lause 2.3. □

3. Mersennen alkuluvut ja täydelliset luvut

Tässä luvussa käsitellään Mersennen alkulukujen ja täydellisten lukujen yhteyttä. Mersennen luvut ovat saaneet nimensä Marin Mersennen mukaan, joka tutki kyseisiä lukuja 1600-luvulla. Mersennen alkulukuja tiedetään tällä hetkellä 47 kappaletta, joista suurin on $M_{43112609}$. Tällä hetkellä tiedossa oleva suurin Mersennen alkuluku löydettiin 23. elokuuta 2008 ja siinä on 12 978 189 numeroa. Luvussa päästään käsiksi parillisiin täydellisiin lukuihin ja niiden ongelmanratkaisuun. Parillisia täydellisiä lukuja on yhtä paljon kuin Mersennen alkulukuja. Uskotaan, että niitä on ääretön määrä, mutta uskomusta ei olla onnistuttu ainakaan toistaiseksi todistamaan. Yhtään paritonta täydellistä lukua ei tunneta, mutta ei olla pystytty todistamaan etteikö niitä olisi olemassa. Parittomien täydellisten lukujen olemassaolo lienee matematiikan yksi vanhimmista ratkaisemattomista ongelmista.

Luku pohjautuu lähteisiin [1], [3], [4], [7] ja [9].

Määritelmä 3.1. Aritmeettinen funktio f: $\mathbb{N} \to \mathbb{C}$ on funktio, joka on määritelty luonnollisille luvuille $\mathbb{N}$ ja saa arvoksi kompleksilukuja $\mathbb{C}$.

Seuraavaksi määritellään multiplikatiivisuus. Myöhemmin tutkielmassa todistetaan multiplikatiivisuus tietyille funktioille.

Määritelmä 3.2. Aritmeettinen funktio f on multiplikatiivinen, jos

$$f(mn) = f(m)f(n), \tag{3.1}$$

aina kun $\text{syt}(m, n) = 1$.

Määritelmä 3.3. Funktio $\sigma : \mathbb{N} \to \mathbb{N}$,

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

on tekijäfunktio. Tekijäfunktiolla saadaan siis luvun n jakajien summa.

Esimerkki 3.4. Olkoon $n = 12$. Luvun 12 jakajat ovat $1, 2, 3, 4, 6$ ja 12, joten

$$\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28.$$

Lemma 3.5. *Olkoon p alkuluku ja k luonnollinen luku. Tällöin*

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

Erityisesti

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

Todistus. Luvun p^k jakajat ovat 1,p,...,p^k, koska luku p on alkuluku ja Lauseen 2.15 nojalla luvun alkutekijäesitys on yksikäsitteinen. Tällöin jakajien summaksi tulee geometrinen summa, jonka arvo saadaan suoraan geometrisen summan kaavasta, joten

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

□

Esimerkki 3.6. Olkoon $p = 7$, tällöin

$$p^2 = 7^2 = 49.$$

Lemmassa 3.5 annetulla kaavalla saadaan

$$\sigma(7^2) = \frac{1 - 7^{2+1}}{1 - 7} = \frac{1 - 7^3}{-6} = \frac{-342}{-6} = 57.$$

Vastaavaan tulokseen päästään laskemalla

$$\sigma(7^2) = \sigma(49) = 1 + 7 + 49 = 57.$$

Lause 3.7. *Jos* $\text{syt}(m, n) = 1$, *niin*

$$\sigma(mn) = \sigma(m)\sigma(n).$$

Siis σ *on multiplikatiivinen.*

Todistus. Oletetaan, että $\text{syt}(m, n) = 1$. Nyt Lemman 2.5 nojalla, jos tulo mn on jaollinen luvulla d, niin on olemassa yksikäsitteiset luonnolliset luvut a ja b siten, että $d = ab$, luku m on jaollinen luvulla a ja luku n on jaollinen luvulla b. Tällöin on

$$\sigma(mn) = \sum_{d|mn} d = \sum_{a|m} \sum_{b|n} ab = \sum_{a|m} a \cdot \sum_{b|n} b = \sigma(m)\sigma(n).$$

□

Seuraavassa esimerkissä käytetään hyödyksi tietoa, että funktio σ on multiplikatiivinen.

Esimerkki 3.8. Olkoon $n = 25$ ja $m = 22$. Tällöin

$$\text{syt}(25, 22) = 1, \sigma(25) = 31 \text{ ja } \sigma(22) = 36.$$

Nyt Lauseen 3.7 nojalla

$$\sigma(25 \cdot 22) = \sigma(25) \cdot \sigma(22) = 31 \cdot 36 = 1116.$$

Huomautus 3.9. On oltava $\text{syt}(m, n) = 1$, että multiplikatiivisuus on voimassa.
Esimerkiksi

$$\text{syt}(2, 4) = 2, \sigma(2) = 3 \text{ ja } \sigma(4) = 7,$$

jolloin

$$\sigma(2) \cdot \sigma(4) = 3 \cdot 7 = 21.$$

Kun taas

$$\sigma(2 \cdot 4) = \sigma(8) = 15.$$

Näin ollen

$$\sigma(8) \neq \sigma(2) \cdot \sigma(4),$$

joten multiplikatiivisuus ei päde, koska luvut 2 ja 4 ovat jaollisia keskenään.

Alkujaan Eukleides tutkittuaan täydellisiä lukuja löysi yhteyden lukuihin, jotka myöhemmin nimettiin Mersennen luvuiksi. Täydellisiin lukuihin palataan myöhemmin tässä luvussa ja Mersennen luvut määritellään seuraavaksi. Mersennen luvut on nimetty niitä tutkineen ranskalaisen munkin Marin Mersennen mukaan. Hän julkaisi listan Mersennen alkuluvuista aina eksponenttiin 257 asti. Tosin hänen kirjoittamansa lista ei ollut virheetön, koska hän sisällytti luvut M_{67} ja M_{257} listaan, vaikka ne eivät ole alkulukuja. Listasta taas puuttuivat Mersennen alkuluvut M_{89} ja M_{107}. Mersenne ei antanut paljon vihjeitä, kuinka hän päätyi luetteloonsa ja listan todistaminen suoritettiin noin kaksi vuosisataa myöhemmin sen ilmestymisestä.

Määritelmä 3.10. Lukuja, jotka ovat muotoa

$$M_p = 2^p - 1,$$

missä p on alkuluku kutsutaan Mersennen luvuiksi.

Jos Mersennen luku on alkuluku, tällöin lukua kutsutaan Mersennen alkuluvuksi.

Esimerkki 3.11. Lasketaan Mersennen lukuja aloittaen pienimmästä alkuluvusta,

$$M_2 = 2^2 - 1 = 3$$
$$M_3 = 2^3 - 1 = 7$$
$$M_5 = 2^5 - 1 = 31$$
$$M_7 = 2^7 - 1 = 127.$$

Kaikki yllä olevat luvut ovat Mersennen alkulukuja, joten näyttäisi että kaavalla saadaan pelkkiä alkulukuja. Jatketaan laskemista edelleen,

$$M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89,$$

jolloin löydetään Mersennen luku, joka ei ole alkuluku. Jatketaan laskemista edelleen ja huomataan, että

$$M_{13} = 8191,$$
$$M_{17} = 131071,$$
$$M_{19} = 524287$$

ja

$$M_{31} = 2147483647$$

ovat kaikki Mersennen alkulukuja. Näyttäisi siltä, että Mersennen alkulukuja esiintyy melko tiheästi, mutta alkulukujen kasvaessa Mersennen alkulukujen esiintyminen harvenee todella paljon. Kuten luvun alussa mainitaan, niin Mersennen alkulukuja tiedetään tällä hetkellä vain 47 kappaletta, joista kahdeksan on esitettynä jo yllä.

Kreikkalaiset, kuten Eukleides, olivat kiinnostuneita täydellisistä luvuista sekä niiden ominaisuuksista ja tutkivat niitä jo muinoin. Seuraavaksi määritellään täydelliset luvut, jotka ovat tämän luvun toinen pääaihe.

Määritelmä 3.12. Luonnollinen luku n on täydellinen, jos se on aidosti itseään pienempien jakajiensa summa. Tällöin siis pätee $\sigma(n) = 2n$.

Esimerkiksi luku 6 on täydellinen, koska $1 + 2 + 3 = 6$. Tällöin

$$\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6.$$

Ei olla onnistuttu todistamaan vielä tänäkään päivänä, että onko olemassa parittomia täydellisiä lukuja. Tällä hetkellä tiedetään, että ei ole olemassa lukua 10^{300} pienempiä parittomia täydellisiä lukuja.
Täydellisten lukujen rinnalle on myös määritelty lähes täydelliset luvut, joille pätee

$$\sigma(n) = 2n - 1.$$

Esimerkki lähes täydellisestä luvusta on luku 4, koska

$$1 + 2 + 4 = 7 = 2 \cdot 4 - 1.$$

Lisäksi on olemassa moninkertaisesti täydellisiä lukuja, joille pätee

$$\sigma(n) = kn, \text{ missä } k \text{ on kokonaisluku.}$$

Esimerkiksi luku 120 on kolminkertaisesti täydellinen, koska luvun jakajien summa on 360, joka voidaan esittää luvun 120 monikertana eli $3 \cdot 120$.

Mersennen alkulukujen ja parillisten täydellisten lukujen välillä on yhteys, joka todistetaan seuraavassa lauseessa. Lauseen a)-kohdan on osoittanut Euler ja b)-kohdan Eukleides.

Lause 3.13. *a) Jos n on parillinen täydellinen luku, niin n on muotoa*

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

missä $2^p - 1$ on Mersennen alkuluku.
b) Jos $2^p - 1$ on Mersennen alkuluku, niin luku

$$n = 2^{p-1}(2^p - 1)$$

on täydellinen.

Todistus. a) Oletetaan, että n on parillinen täydellinen luku. Koska n on parillinen, niin se voidaan esittää muodossa

$$n = 2^k m, \text{ missä } k \geq 1 \text{ ja } m \text{ on pariton.}$$

Koska funktio σ on multiplikatiivinen, $\text{syt}(2^k, m) = 1$ ja Lemman 3.5 nojalla

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

niin

$$\sigma(n) = \sigma(2^k m) = \sigma(2^k)\sigma(m) = (\frac{2^{k+1} - 1}{2 - 1})\sigma(m) = (2^{k+1} - 1)\sigma(m). \tag{3.2}$$

Koska luku n on täydellinen, niin

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

Yhtälöiden (3.2) ja (3.3) perusteella on

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

Luku $2^{k+1} - 1$ on pariton. Tulo $(2^{k+1} - 1)\sigma(m)$ on jaollinen luvulla 2^{k+1} yhtälön (3.4) perusteella. Nyt koska $\text{syt}(2^{k+1}, 2^{k+1} - 1) = 1$, niin Lauseen 2.2 nojalla luku $\sigma(m)$ on jaollinen luvulla 2^{k+1}. Toisin sanoen on jokin luku c siten, että

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

Kun tämä sijoitetaan yhtälöön (3.4), niin saadaan

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

Siten

$$m = (2^{k+1} - 1)c.$$

Näytetään, että luku c=1.
Jos olisi $c > 1$, niin tällöin

$$m = (2^{k+1} - 1)c$$

olisi jaollinen luvuilla 1, c ja m. Nyt

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

Koska $\sigma(m) = 2^{k+1} c$, niin on

$$2^{k+1} c \geq 2^{k+1} c + 1.$$

Tämä on mahdotonta, joten c=1.

Tällöin m= $2^{k+1}-1$ ja

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

Siten m on alkuluku.

Ollaan todistettu, että jos luku n on parillinen täydellinen luku, niin silloin se on muotoa

$$n = 2^k(2^{k+1}-1), \text{ missä } 2^{k+1}-1 \text{ on alkuluku.}$$

Lauseen 2.9 nojalla tiedetään, että jos luku $2^{k+1}-1$ on alkuluku, niin luvun $k+1$ oltava alkuluku eli $k+1=p$, jollain alkuluvulla p. Siten jokainen täydellinen luku voidaan esittää muodossa

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

missä 2^p-1 on Mersennen alkuluku.

b)Oletetaan, että luku 2^p-1 on alkuluku. Silloin on

$$\sigma(2^p-1) = (2^p-1)+1 = 2^p.$$

Nyt funktion σ multiplikatiivisuuden ja Lemman 3.5 nojalla on

$$\sigma(n) = \sigma(2^{p-1})\cdot\sigma(2^p-1) = (2^p-1)\cdot 2^p = 2n.$$

Siten luku n on täydellinen. □

Esimerkki 3.14. a) Luku $n=28$ on täydellinen luku, sillä

$$\sigma(28) = 1+2+4+7+14+28 = 56 = 2\cdot 28.$$

Etsitään sitä vastaava Mersennen alkuluku. Nyt n on muotoa

$$n = 28 = 2^{p-1}(2^p-1), \text{ missä } p \text{ ja } 2^p-1 \text{ ovat alkulukuja.}$$

Kokeilemalla nähdään, että alkuluku $p=3$ toteuttaa yhtälön.

Täydellistä lukua 28 vastaava Mersennen alkuluku on

$$M_3 = 2^3-1 = 7.$$

b) Luku

$$M_7 = 2^7-1 = 127$$

on Mersennen alkuluku. Lasketaan sitä vastaava täydellinen luku. Koska $p=7$, niin

$$n = 2^{p-1}(2^p-1) = 2^6(2^7-1) = 8128.$$

Näin ollen Mersennen alkulukua 127 vastaava täydellinen luku on 8128, sillä

$\sigma(8128) = 1+2+4+8+16+32+64+127+254+508+1016+2032+4064+8128 = 16256 = 2\cdot 8128.$

4. Eulerin funktio

Tässä luvussa käsitellään Eulerin funktiota sekä todistetaan sen multiplikatiivisuus. Multiplikatiivisuuden todistamisessa käytetään kiinalaista jäännöslausetta, jonka avulla saadaan ratkaistuksi kongruenssiyhtälöryhmiä. Luvussa käydään läpi myös Eulerin lause, joka on yleistys Fermat'n pienestä lauseesta. Luku pohjautuu lähteisiin [3], [4] ja [8].

Määritelmä 4.1. Eulerin funktio $\phi : \mathbb{N} \to \mathbb{N}$ antaa niiden kokonaislukujen määrän, joille pätee $\text{syt}(a, n)=1$ eli luvut a ja n ovat keskenään jaottomia sekä $1 \leq a \leq n$.

$$\phi(n) = \sharp\{a \in \mathbb{N} : 1 \leq a \leq n \text{ ja } \text{syt}(a, n) = 1\}. \tag{4.1}$$

Seuraava esimerkki havainnollistaa Eulerin funktion käyttöä.

Esimerkki 4.2. Määritetään $\phi(12)$. Selvitetään kuinka moni kokonaisluku yhdestä kahteentoista on jaoton luvun 12 kanssa. Luvut 1, 5, 7 ja 11 täyttävät ehdon, joten

$$\phi(12) = 4.$$

Lause 4.3. *Jos* $\text{syt}(m, n)=1$*, niin*

$$\phi(mn) = \phi(m)\phi(n).$$

Siis Eulerin funktio ϕ *on multiplikatiivinen.*

Todistus. Olkoot joukot

$$A = \{a : 1 \leq a \leq mn \text{ ja } \text{syt}(a, mn) = 1\}$$

ja

$$B = \{(b, c) : 1 \leq b \leq m \text{ ja } \text{syt}(b, m) = 1, 1 \leq c \leq n \text{ ja } \text{syt}(c, n) = 1\}.$$

Näytetään, että joukoissa on yhtä monta alkiota.

Osoitetaan ensin, että jokaista joukon A alkiota vastaa täsmälleen yksi alkio joukosta B ja että jokainen alkio "kuvautuu"eri alkioiksi. Tämä tarkastelu osoittaa funktion injektiivisyyden.

Määritellään kuvaus $f : A \to B$ asettamalla $f(a) = (b, c)$, kun

$$\begin{cases} a \equiv b \pmod{m} \\ a \equiv c \pmod{n}. \end{cases}$$

Kongruenssin ominaisuuksien ja joukkojen A ja B määritelmien nojalla kaikilla a on täsmälleen yksi lukupari (b, c) joukosta B, jolle $f(a) = (b, c)$. Olkoot luvut a_1 ja a_2 joukosta A, joille $f(a_1) = f(a_2) = (b, c)$. Tällöin

$$\begin{cases} a_1 \equiv b \pmod{m} \\ a_1 \equiv c \pmod{n} \end{cases} \tag{4.2}$$

ja

$$\begin{cases} a_2 \equiv b \pmod{m} \\ a_2 \equiv c \pmod{n}. \end{cases} \tag{4.3}$$

Nyt Lauseen 2.8 nojalla saadaan kongruenssiyhtälöpari (4.3) muotoon

$$\begin{cases} b \equiv a_2 \pmod{m} \\ c \equiv a_2 \pmod{n}, \end{cases} \tag{4.4}$$

ja edelleen Lauseen 2.8 nojalla kongruenssiyhtälöpareista (4.2) ja (4.4) saadaan

$$\begin{cases} a_1 \equiv a_2 \pmod{m} \\ a_1 \equiv a_2 \pmod{n}. \end{cases} \tag{4.5}$$

Nyt

$$m|(a_1 - a_2) \text{ ja } n|(a_1 - a_2),$$

niin Lauseen 2.2 nojalla

$$mn|(a_1 - a_2)$$

toisin sanoen

$$a_1 \equiv a_2 \pmod{mn}.$$

Näin ollen funktio f on injektio.

Toiseksi todistetaan, että jokaiselle joukon B alkiolle $y = (b, c)$ on joukon A alkio, joka kuvautuu alkioksi y. Olkoon lukupari (b, c) joukosta B. Täytyy siis näyttää, että kongruenssiyhtälöpari

$$\begin{cases} a \equiv b \pmod{m} \\ a \equiv c \pmod{n} \end{cases} \tag{4.6}$$

toteutuu jollain kokonaisluvulla a joukosta A. Koska m ja n ovat positiivisia kokonaislukuja, joille syt(m, n)=1, niin kiinalaisen jäännöslauseen nojalla kongruenssiparilla on yksikäsitteinen ratkaisu modulo mn. Kiinalaisen jäännöslauseen nojalla ratkaisu on välillä $0 \leq a < mn$, joten löytyy luku a, joka toteuttaa kongruenssiparin. Siis funktio f on surjektio.

Joukossa A on $\phi(mn)$ kappaletta lukuja. Vastaavasti joukossa B on $\phi(m)$ vaihtoehtoa luvulle b ja $\phi(n)$ vaihtoehtoa luvulle c. Näin ollen lukuparille (b, c) on siis vaihtoehtoja $\phi(m)\phi(n)$ kappaletta. Koska kuvaus f on injektio ja surjektio, niin se on bijektio, jolloin

$$\phi(mn) = \phi(m)\phi(n).$$

□

Seuraavassa esimerkissä käytetään hyödyksi Eulerin funktion multiplikatiivisuutta.

Esimerkki 4.4. Määritetään $\phi(26)$. Luku 26 voidaan esittää lukujen 2 ja 13 tulona. Nyt koska syt$(2, 13)$=1, niin Lauseen 4.3 nojalla

$$\phi(26) = \phi(2) \cdot \phi(13) = 1 \cdot 12 = 12.$$

Lemma 4.5. *Olkoon p alkuluku ja k luonnollinen luku. Nyt*
1) $\phi(p) = p - 1$
2) $\phi(p^k) = p^k - p^{k-1}$.

Todistus. 1) Koska oletetaan, että p on alkuluku, niin kaikki kokonaisluvut $1 \leq a < p$ ovat jaottomia luvun p kanssa eli syt$(a, p) = 1$. Lukuja on $p - 1$ kappaletta, joten

$$\phi(p) = p - 1.$$

2) Olkoon $m = p^k$, missä p on alkuluku ja k on kokonaisluku. Nyt haetaan kaikki luvut a väliltä $1 \leq a \leq p^k$, jotka ovat jaottomia luvun p^k kanssa eli syt$(a, p^k) = 1$. Koska luvun p^k ainoat tekijät ovat luvun p potenssit, niin näiden lukumäärä saadaan selville vähentämällä luvusta p^k niiden lukujen lukumäärä, joille $p|a$ eli

$$\phi(p^k) = p^k - \sharp\{a : 1 \leq a \leq p^k \text{ ja } p|a\}.$$

Luvun p monikertoja välillä $1, \ldots, p^k$ ovat

$$p, 2p, 3p, 4p, \ldots, (p^{k-1}-2)p, (p^{k-1}-1)p, p^k$$

ja niitä on p^{k-1} kappaletta. Näin ollen

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

□

Lause 4.6. *Olkoon n luonnollinen luku. Olkoot luvut $r_1, \ldots, r_{\phi(n)}$ jaottomia luvun n kanssa sekä olkoot luvut $r_1, \ldots, r_{\phi(n)}$ eri lukuja modulo n. Jos* $\text{syt}(a, n) = 1$*, niin luvut*

$$ar_1, ar_2, ar_3, \ldots, ar_{\phi(n)} \pmod{n}$$

ovat samoja kuin luvut

$$r_1, r_2, r_3, \ldots, r_{\phi(n)} \pmod{n},$$

vaikka luvut olisivat eri järjestyksessä.

Todistus. Olkoot $\text{syt}(a, n) = 1$ ja $\text{syt}(r, n) = 1$, tällöin Lemman 2.12 nojalla

$$\text{syt}(ar, n) = 1.$$

Joten jokainen luku listasta

$$ar_1, ar_2, ar_3, \ldots, ar_{\phi(n)} \pmod{n}$$

on kongruentti yhden luvun kanssa listasta

$$r_1, r_2, r_3, \ldots, r_{\phi(n)} \pmod{n}.$$

Molemmissa listoissa on $\phi(n)$ kappaletta lukuja. Jos voidaan osoittaa, että kaikki luvut ensimmäisessä listassa ovat eri lukuja modulo n, niin nämä kaksi listaa ovat samoja.
Otetaan luvut $r_j a$ ja $r_k a$ ensimmäisestä listasta, jotka toteuttavat kongruenssiyhtälön

$$r_j a \equiv r_k a \pmod{n}.$$

Tällöin $n|(r_j - r_k)a$. Koska $\text{syt}(a, n) = 1$, niin Lauseen 2.2 nojalla

$$n|(r_j - r_k).$$

Toisaalta luvut r_j ja r_k ovat lukuja väliltä yhdestä lukuun $n-1$ eli

$$0 \leq |r_j - r_k| \leq n - 1.$$

On olemassa vain yksi lukua n pienempi luku, joka on jaollinen luvulla n. Tämä luku on 0, joten oltava

$$r_j = r_k.$$

Näin ollen kaikki luvut listasta

$$ar_1, ar_2, ar_3, \ldots, ar_{\phi(n)} \pmod{n}$$

ovat eri lukuja modulo n, joten lause todistettu. □

Seuraavaksi käydään läpi Eulerin lause, jossa oletuksena on $\text{syt}(a, n) = 1$. Lauseen jälkeen käydään läpi, onko tämä oletus lukujen a ja n keskenään jaottomuudesta välttämätön.

Lause 4.7. *(Eulerin lause) Jos* $\text{syt}(a, n) = 1$*, niin*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Todistus. Olkoon

$$R = \{r_1, r_2, r_3, ..., r_{\phi(n)}\} = \{r : 1 \leq r \leq n-1, \text{syt}(r, n) = 1\}$$

$$\text{ja } aR = \{ar_1, ar_2, ar_3, ..., ar_{\phi(n)}\}.$$

Koska syt(r_i, n)=1, niin

$$r_i \not\equiv 0 \pmod{n},$$

kaikilla $i = 1, \ldots, \phi(n)$.

Jos olisi

$$ar_i \equiv 0 \pmod{n} \text{ eli } n|ar_i,$$

niin Lauseen 2.2 nojalla $n|r_i$, koska syt$(a, n) = 1$. Tämä on ristiriita, sillä syt$(r_i, n) = 1$, joten

$$ar_i \not\equiv 0 \pmod{n},$$

kaikilla $i = 1, \ldots, \phi(n)$. Nyt Lauseiden 2.8 ja 4.6 nojalla pätee

$$ar_1 ar_2 \cdots ar_{\phi(n)} \equiv r_1 r_2 \cdots r_{\phi(n)} \pmod{n},$$

mikä saadaan muotoon

$$a^{\phi(n)} r_1 r_2 \cdots r_{\phi(n)} \equiv r_1 r_2 \cdots r_{\phi(n)} \pmod{n}$$

Koska syt$(r_i, n) = 1$, niin Lemman 2.12 nojalla

$$\text{syt}(r_1 r_2 \cdots r_{\phi(n)}, n) = 1.$$

Nyt Lauseen 2.8 nojalla saadaan tulo $r_1 r_2 \cdots r_{\phi(n)}$ supistettua pois ja saadaan

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

□

Edellisessä lauseessa on siis oletuksena, että syt$(a, n) = 1$, tällöin

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Toteutuuko kongruenssiyhtälö, jos syt$(a, n) \neq 1$?

Olkoon syt$(a, n) = d$. Jos

$$a^k \equiv 1 \pmod{n},$$

niin

$$a^k = 1 + ln, \text{ jollain } l.$$

Nyt d jakaa luvun $a^k - ln = 1$, jolloin on oltava $d = 1$.

Jotta Eulerin lause toimisi, niin on oltava syt$(a, n) = 1$.

Seuraavaksi Fermat'n pieni lause, joka on Eulerin lauseen erikoistapaus. Lause on perustana Fermat´n alkulukutestaukselle, josta tarkemmin luvun viisi alkupuolella. Fermat ei itse todistanut lausetta tarkemmin kuten ei yleensäkään. Euler julkaisi todistuksen lauseelle 1736, mutta myös Leibniz lienee todistanut lauseen jo 1680-luvulla.

Lause 4.8. *Olkoon p alkuluku ja* syt(a, p)=1. *Tällöin*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Todistus. Koska luku p on alkuluku, niin Lemman 4.5 nojalla $\phi(p) = p - 1$. Nyt koska syt(a, p)=1, niin Eulerin lauseen 4.7 nojalla

$$a^{\phi(n)} = a^{p-1} \equiv 1 \pmod{p}.$$

□

Seuraavassa esimerkissä käytetään Eulerin lausetta.

Esimerkki 4.9. a) Olkoot luvut n=13 ja a=5, tällöin

$$\text{syt}(5, 13) = 1.$$

Nyt

$$\phi(n) = \phi(13) = 12.$$
$$a^{\phi(n)} = 5^{\phi(13)} = 5^{12} = 244140625 \equiv 1 \pmod{13}.$$

Tarkastellaan myös tilannetta, missä luku n ei ole alkuluku.
b) Olkoot $a = 5$ ja $n = 26$, tällöin

$$\text{syt}(5, 26) = 1.$$

Esimerkissä 4.4 laskettiin

$$\phi(26) = 12.$$

Näin ollen

$$a^{\phi(n)} = 5^{\phi(26)} = 5^{12} = 244140625 \equiv 1 \pmod{26}.$$

Seuraava lause osoittaa, että summa kaikista luvun n jakajien Eulerin funktioista antaa luvun n itse.

Lause 4.10. *Olkoon $n \geq 1$ kokonaisluku. Tällöin*

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

Todistus. Olkoon S={1, 2, ..., n}. Jokaiselle luvun n jakajalle d olkoon

$$S_d = \left\{ a \in S \mid \text{syt}(a, n) = \frac{n}{d} \right\}.$$

Tällöin $S = \bigcup_{d|n} S_d$ ja joukot S_d ovat erillisiä.

$\supset$: Olkoon d luvun n jakaja ja olkoon luku b joukosta S_d. Nyt joukon S_d määritelmästä nähdään, että luku b kuuluu joukkoon S.

$\subset$: Olkoon luku a joukosta S ja olkoon $c = \text{syt}(a, n)$. Nyt $c|n$, joten

$$n = dc \text{ jollain yksikäsitteisellä luonnollisella luvulla } d.$$

Näin ollen luku a kuuluu joukkoon S_d.

Edelliset kaksi tarkastelua osoittavat, että joukko S_d jakaa joukon S erillisiin osajoukkoihin, joiden yhdiste on S.

Merkitään joukon S alkioiden lukumäärää eli joukon kokoa merkinnällä | S |. Tällöin

$$\sum_{d|n} \mid S_d \mid = \mid S \mid = n,$$

joten riittää osoittaa että

$$\mid S_d \mid = \phi(d) \text{ kaikilla } d.$$

Määritellään luku $a^*=\frac{ad}{n}$ kaikilla kokonaisluvuilla a. Jos luku a kuuluu joukkoon S_d, niin $\frac{n}{d}|a$ ja siten luku a^* on luonnollinen luku.

Joukon S_d määritelmän mukaan luku $a^*\frac{n}{d} = a$ kuuluu joukkoon S_d jos ja vain jos luku a^* on luonnollinen, välillä $1 \leq a^* \leq d$ ja $\text{syt}(a^*, d) = 1$: Ehto $1 \leq a^* \leq d$ on selvä. Ehto $\text{syt}(a^*, d) = 1$ seuraa, sillä

$$\text{syt}(a^*\frac{n}{d}, n) = \frac{n}{d}$$

ja Bézoutin lauseen 2.10 nojalla

$$a^*\frac{n}{d}x + ny = \frac{n}{d} \text{ joillain kokonaisluvuilla } x \text{ ja } y.$$

Nyt kertomalla luvulla d ja jakamalla luvulla n saadaan

$$a^*x + dy = 1.$$

Nyt Lauseen 2.11 nojalla $\text{syt}(a^*, d)|1$, josta nähdään että $\text{syt}(a^*, d) = 1$.

Nyt siis päästiin Eulerin funktion määritelmään;

luku a^* on luonnollinen luku, $1 \leq a^* \leq d$ ja $\text{syt}(a^*, d)=1$, joten

$$| S_d |= \phi(d).$$

□

Esimerkki 4.11. Olkoon n=10. Luvun 10 jakajia ovat luvut 1, 2, 5 ja 10.

Nyt joukko $S = \{1, 2, \ldots, 10\}$ ja joukot S_d ovat

$$S_1 = \{a \mid \text{syt}(a, 10) = \frac{10}{1} = 10\} = \{10\}$$

$$S_2 = \{a \mid \text{syt}(a, 10) = \frac{10}{2} = 5\} = \{5\}$$

$$S_5 = \{a \mid \text{syt}(a, 10) = \frac{10}{5} = 2\} = \{2, 4, 6, 8\}$$

$$S_{10} = \{a \mid \text{syt}(a, 10) = \frac{10}{10} = 1\} = \{1, 3, 7, 9\}.$$

Nyt katsotaan kuinka monta alkiota on kussakin joukossa,

$$| S_1 |= 1, | S_2 |= 1, | S_5 |= 4 \text{ ja } | S_{10} |= 4.$$

Lasketaan

$$\sum_{d|n} | S_d |=| S_1 | + | S_2 | + | S_5 | + | S_{10} |= 10 = n.$$

Lasketaan Eulerin funktion arvot jokaiselle luvun 10 jakajalle,

$$\phi(1) = 1, \phi(2) = 1, \phi(5) = 4 \text{ ja } \phi(10) = 4.$$

Lasketaan

$$\sum_{d|n} \phi(d) = \phi(1) + \phi(2) + \phi(5) + \phi(10) = 10 = n.$$

5. Pseudoalkuluvut ja Carmichaelin luvut

Tässä luvussa tarkastellaan pseudoalkulukuja sekä Carmichaelin lukuja. Ne ovat lukuja, jotka toteuttavat tietynlaiset kongruenssiyhtälöt. Nämä kongruenssiyhtälöt ovat eräänlaisia erikoistapauksia Fermat'n pienestä lauseesta, joka esiteltiin edellisessä luvussa lauseena 4.8. Pienin pseudoalkuluku on 341 ja pienin Carmichaelin luku on 561. Molempia lukuja on ääretön määrä, mutta tässä työssä todistetaan tämä väittämä vain pseudoalkulukujen kohdalta. Luku pohjautuu pseudoalkuluvuissa lähteeseen [3] ja Carmichaelin luvuissa lähteeseen [4].

Esitellään luvun alkuun muutama lause, joiden avulla voidaan tutkia, onko jokin tietty luku alkuluku.

Lause 5.1. *(Wilsonin lause) Luku p on alkuluku jos ja vain jos*

$$(p-1)! \equiv -1 \pmod{p}.$$

Todistus. Oletetaan, että $(p-1)! \equiv -1 \pmod{p}$ pätee, mutta p ei ole alkuluku. Tällöin luvulla p on Lauseen 2.15 mukaan yksikäsitteinen alkutekijäesitys.

Olkoon q yksi luvun p alkutekijöistä, tällöin

$$1 < q \leq p-1.$$

Nyt

$$q \mid (p-1)!,$$

josta seuraa että

$$q \nmid ((p-1)!+1).$$

Koska $q \nmid ((p-1)!+1)$ on totta kaikille luvun p alkutekijöille q, niin

$$p \nmid ((p-1)!+1).$$

Siten

$$(p-1)! \not\equiv -1 \pmod{p},$$

mikä on ristiriita. Luku p on siis alkuluku.

Olkoon p alkuluku. Lause pätee luvuilla $p = 2$ ja $p = 3$. Oletetaan, että $p \geq 5$. Nyt

$$(p-1)! \equiv -1 \pmod{p}$$

voidaan esittää muodossa

$$1 \cdot 2 \cdot 3 \cdots (p-3)(p-2)(p-1) \equiv -1 \pmod{p}.$$

Nyt

$$(p-1) \equiv -1 \pmod{p}.$$

Tarkastellaan siis lukujen $1, 2, 3, \ldots, (p-3), (p-2)$ käyttäytymistä kongruenssiyhtälössä. Lauseen 2.14 nojalla on olemassa yksikäsitteinen ratkaisu $0 \leq i \leq p-1$ siten, että

$$ji \equiv 1 \pmod{p},$$

kun $\text{syt}(j,p) = 1$ kaikilla $1 \leq j \leq p-1$. Tarkastellaan nyt tilanteet, jos $i = 0$, $i = j$ ja $i = 1$.

Olkoon $i = 0$, tällöin $p| - 1$, mikä on ristiriita. Näin ollen on $i \neq 0$.

Jos $i = j$, niin kongruenssiyhtälö tulee muotoon

$$j^2 \equiv 1 \pmod{p},$$

jolloin $p \mid (j^2 - 1)$, josta edelleen saadaan

$$p \mid (j+1)(j-1).$$

Koska $\text{syt}(j-1, p) = 1$, niin tällöin Lauseen 2.2 nojalla

$$p \mid (j+1),$$

mikä pätee vain jos $j = p - 1$ eli

$$p \mid j + 1,$$

jolloin

$$p \mid p.$$

Jos $i = 1$, kun $1 < j < p - 1$, niin

$$j \equiv 1 \pmod{p}.$$

Tällöin $p \mid (j-1)$, mikä on ristiriita, koska $\text{syt}(j-1, p) = 1$. Tämä kuitenkin pätee, jos $j = 1$. Täten oltava $i \neq 1$, kun $1 < j < p - 1$.

Edellisten tarkastelujen nojalla kun $2 \leq j \leq p-2$, niin on yksikäsitteinen ratkaisu $2 \leq i \leq p - 2$ siten, että

$$ij \equiv 1 \pmod{p}.$$

Näin ollen Lauseen 2.8 nojalla saadaan

$$(p-1)! = (p-1) \cdot (p-2) \cdot (p-3) \cdots 2 \cdot 1 \equiv -1 \cdot 1 \cdot 1 \cdots 1 \cdot 1 = -1 \pmod{p}.$$

Näin ollen alkuluvulle p on voimassa kongruenssiyhtälö

$$(p-1)! \equiv -1 \pmod{p}.$$

□

Wilsonin lause 5.1 ei ole kovin käytännöllinen tutkittaessa onko luku alkuluku, sillä kertomat kasvavat huimaa vauhtia hyvinkin pienillä luvuilla.

Seuraavaksi esitellään toinen tulos, jolla voidaan tutkia onko luku alkuluku.

Lause 5.2. *Olkoon luku a luonnollinen luku siten, että*

$$a^{n-1} \equiv 1 \pmod{n}$$

ja

$$a^d \equiv 1 \pmod{n} \text{ aina kun } d \mid (n-1) \text{ ja } 1 < d < n - 1.$$

Tällöin luku n on alkuluku.

Todistus. [5], Lause 2.28. □

Edellisessä luvussa käsiteltyä Fermat'n pientä lausetta voidaan käyttää tutkittaessa, onko luku alkuluku vai ei. Tämä onkin Wilsonin lausetta käytännöllisempi tulos, koska kongruenssiyhtälöiden ratkaiseminen onnistuu kätevästi isommillekin potensseille, koska ne voidaan muokata siten, että päästään käsiksi luvun pienempiin potensseihin, joiden kautta päästään ratkaisuun.

Jos p on alkuluku, niin se toteuttaa

$$a^p \equiv a \pmod{p}$$

kaikilla kokonaisluvuilla a.

Vastaavasti jos

$$a^p \not\equiv a \pmod{p}$$

jollain kokonaisluvuilla a, niin luku p ei ole alkuluku.

Kiinalaiset olivat tietoisia Fermat'n pienestä lauseesta ja he ajattelivat, että kun luku n toteuttaa lauseen luvulla $a = 2$, niin luku on alkuluku. Kuitenkin myöhemmin löydettiin lukuja (esimerkiksi $n = 341$), jotka eivät ole alkulukuja ja toteuttavat Fermat'n pienen lauseen luvulla $a = 2$. Tällaisia lukuja alettiin kutsua pseudoalkuluvuiksi, jotka seuraavaksi määritellään.

Määritelmä 5.3. Jos

$$2^{n-1} \equiv 1 \pmod{n},$$

ja n ei ole alkuluku, niin sanotaan, että n on pseudoalkuluku.

Seuraavassa esimerkissä testataan, että tietty luku on pseudoalkuluku eli toteuttaa edellä esitellyn määritelmän.

Esimerkki 5.4. Näytetään, että luku n=341 on pseudoalkuluku.

Nyt

$$n = 341 = 11 \cdot 31.$$

Fermat'n pienen lauseen nojalla, koska p_1=11 on alkuluku, joka ei jaa lukua 2 niin on voimassa

$$2^{11-1} = 2^{10} \equiv 1 \pmod{11}.$$

Kongruenssin laskusääntöjen nojalla

$$2^{340} = (2^{10})^{34} \equiv 1 \pmod{11}.$$

Laskemalla saadaan

$$2^5 \equiv 1 \pmod{31},$$

josta edelleen kongruenssin laskusääntöjen nojalla

$$2^{340} = (2^5)^{68} \equiv 1 \pmod{31}.$$

Koska

$$\text{syt}(11, 31) = 1, 11|2^{340} - 1 \text{ ja } 31|2^{340} - 1,$$

niin Lauseen 2.2 nojalla luku $341 = 11 \cdot 31$ jakaa luvun $2^{340} - 1$ eli

$$2^{340} \equiv 1 \pmod{341},$$

joten luku n=341 on pseudoalkuluku.

Lause 5.5. *Pseudoalkulukuja on ääretön määrä.*

Todistus. Osoitetaan, että jos n on pseudoalkuluku, niin myös luku $2^n - 1$ on pseudoalkuluku. Jos n on pseudoalkuluku, tällöin luku n ei ole alkuluku. Lauseen 2.9 perusteella tällöin myöskään luku $2^n - 1$ ei ole alkuluku.

Todistetaan seuraavaksi, että luku $2^n - 1$ on pseudoalkuluku eli että se toteuttaa kongruenssiyhtälön

$$2^{2^n-1} \equiv 2 \pmod{2^n - 1}.$$

Koska

$$2^n \equiv 2 \pmod{n},$$

niin $2^n = nk + 2$ jollain kokonaisluvulla $k \geq 1$. Sijoitetaan

$$x = 2^n \text{ ja } m = k$$

Lauseen 2.9 todistuksessa esiintyneeseen yhtälöön (2.1) ja saadaan

$$x^m - 1 = (2^n)^k - 1 = 2^{nk} - 1 = (2^n - 1)(2^{n(k-1)} + 2^{n(k-2)} + ... + 1).$$

Yllä olevasta yhtälöstä nähdään, että luku $2^n - 1$ on luvun $2^{nk} - 1$ tekijä, joten

$$2^{nk} \equiv 1 \pmod{2^n - 1}.$$

Näin ollen

$$2^{2^n-1} = 2^{nk+2-1} = 2^{nk+1} = 2^{nk} \cdot 2 \equiv 2 \pmod{2^n - 1},$$

joten myös luku $2^n - 1$ on pseudoalkuluku. Tämä tarkastelu osoittaa, että pseudoalkulukuja on ääretön määrä. □

Seuraavassa lauseessa osoitetaan, että edellisessä luvussa määritellyt Mersenneluvut sekä pseudoalkuluvut ovat yhteydessä toisiinsa.

Lause 5.6. *Mersenneluku*

$$M_p = 2^p - 1$$

on pseudoalkuluku, jos se ei ole alkuluku.

Todistus. Fermat'n pienen lauseen 4.8 perusteella, koska luku p on alkuluku niin

$$2^p \equiv 2 \pmod{p}.$$

Nyt

$$2^p = pk + 2 \text{ jollain kokonaisluvulla } k \geq 1.$$

Todistus jatkuu kuten Lauseen 5.5 todistus ja lopulta päästään kongruenssiyhtälöön

$$2^{2^p-1} = 2^{pk+2-1} = 2^{pk+1} = 2^{pk} \cdot 2 \equiv 2 \pmod{2^p - 1},$$

joten Mersenneluku M_p on pseudoalkuluku, jos se ei ole alkuluku. □

Esimerkki 5.7. Mersennen luku

$$n = M_{11} = 2047 = 23 \cdot 89$$

ei ole alkuluku. Näytetään, että se on pseudoalkuluku. Nyt

$$2^{11} \equiv 1 \pmod{2047},$$

jolloin kongruenssin laskusääntöjen nojalla

$$2^{n-1} = 2^{2046} = (2^{11})^{186} \equiv 1 \pmod{2047}.$$

Näin ollen luku $M_{11} = 2047$ on pseudoalkuluku.

Seuraavaksi esitellään määritelmä Carmichaelin luvuille, jotka ovat saaneet nimensä lukuja tutkineen matemaatikon R. Carmichaelin mukaan. Hän tutki lukuja 1910-luvulla. Fermat'n pienessä lauseessa todetaan, että jos n on alkuluku, niin pätee

$$a^n \equiv a \pmod{n} \text{ kaikilla kokonaisluvuilla } a.$$

Seuraavaksi määritellään Carmichaelin luvut, jotka toteuttavat yllä olevan kongruenssiyhtälön, mutta eivät ole alkulukuja.

Määritelmä 5.8. Jos luku n ei ole alkuluku ja

$$a^{n-1} \equiv 1 \pmod{n}.$$

kaikilla a, joille $\text{syt}(a, n)=1$, niin sanotaan, että n on Carmichaelin luku.

Lause 5.9. *Kaikki Carmichaelin luvut ovat parittomia.*

Todistus. Olkoon n Carmichaelin luku. Määritelmän 5.8 mukaan on voimassa kongruenssiyhtälö

$$a^n \equiv a \pmod{n} \text{ luvulle } a = n - 1.$$

Koska

$$n - 1 \equiv -1 \pmod{n},$$

niin

$$(-1)^n \equiv -1 \pmod{n}.$$

Tämä osoittaa, että luku n on pariton (tai $n = 2$). Siis kaikki Carmichaelin luvut ovat parittomia. □

Seuraavassa esimerkissä näytetään, että tietty luku toteuttaa Carmichaelin määritelmän.

Esimerkki 5.10. Näytetään, että luku n=561 on Carmichaelin luku.

Nyt

$$n = 561 = 3 \cdot 11 \cdot 17.$$

Koska oltava $\text{syt}(a, 561) = 1$, niin myös

$$\text{syt}(a, 3) = \text{syt}(a, 11) = \text{syt}(a, 17) = 1.$$

Koska luku p_1=3 on alkuluku, niin Fermat'n pienen lauseen 4.8 nojalla

$$a^{3-1} = a^2 \equiv 1 \pmod{3}$$

ja kongruenssin laskusääntöjen nojalla

$$a^{560} = (a^2)^{280} \equiv 1 \pmod{3}.$$

Vastaavalla tavalla alkuluvuille p_2=11 ja p_3=17 Fermat'n pienen lauseen 4.8 ja kongruenssin laskusääntöjen nojalla

$$a^{10} \equiv 1 \pmod{11},$$

josta edelleen

$$a^{560} = (a^{10})^{56} \equiv 1 \pmod{11}.$$

Nyt

$$a^{16} \equiv 1 \pmod{17},$$

josta edelleen

$$a^{560} = (a^{16})^{35} \equiv 1 \pmod{17}.$$

Nyt koska

$$\text{syt}(3, 11, 17) = 1, 3|a^{560-1}, 11|a^{560-1} \text{ ja } 17|a^{560-1},$$

niin Lauseen 2.2 nojalla luku $561 = 3 \cdot 11 \cdot 17$ jakaa luvun a^{560-1} eli

$$a^{560} \equiv 1 \pmod{561},$$

joten luku n=561 on Carmichaelin luku.

Määritelmä 5.11. Olkoot m ja a kokonaislukuja siten, että $\text{syt}(a, m) = 1$ ja olkoon $\mathbb{N} = \{1, 2, ...\}$. Pienintä lukua $k \in \mathbb{N}$, jolle pätee

$$a^k \equiv 1 \pmod{m},$$

kutsutaan luvun a kertaluvuksi modulo m. Tätä merkitään

$$ord_m(a) = k.$$

Edellä määriteltiin luvun a kertaluku modulo m. Tarkastellaan seuraavaksi määritelmää esimerkin kautta ja huomataan pari asiaa. Lasketaan luvulle kolme ja sen potensseille seuraavaksi arvot modulo 7,

$$3^1 \equiv 3 \pmod 7,$$
$$3^2 = 9 \equiv 2 \pmod 7,$$
$$3^2 = 27 \equiv 6 \pmod 7,$$
$$3^4 = 81 \equiv 4 \pmod 7,$$
$$3^5 = 243 \equiv 5 \pmod 7$$

ja

$$3^6 = 729 \equiv 1 \pmod 7.$$

Nyt nähdään, että 3^6 on kongruentti luvun yksi kanssa modulo 7 eli

$$ord_7(3) = 6.$$

Lähteessä [4] on laskettu eri kongruenssiyhtälöitä ja koottu ne taulukoksi 21.2. Taulukosta ja edellä esitetystä esimerkistä huomataan seuraavat asiat:

1. Pienin eksponentti k, joka toteuttaa $a^k \equiv 1 \pmod p$ jakaa aina luvun $p-1$.
2. Joillakin luvuilla a pienin eksponentti, joka toteuttaa $a^k \equiv 1 \pmod p$ on luku $p-1$, joka saadaan Fermat'n pienestä lauseesta $a^{p-1} \equiv 1 \pmod p$.

Lause 5.12. *Olkoon a kokonaisluku ja p alkuluku siten, että* $\text{syt}(a,p) = 1$.
Olkoon $a^n \equiv 1 \pmod p$, tällöin $ord_p(a)$ jakaa luvun n.
Erityisesti $ord_p(a)$ jakaa aina luvun $p-1$.

Todistus. Lähde [4], Lause 21.1. □

Määritelmä 5.13. Jos $\phi(m)$ on luvun a kertaluku modulo m, niin silloin lukua a kutsutaan primitiiviseksi juureksi modulo m eli

$$ord_m(a) = \phi(m).$$

Lause 5.14. *Jokaisella alkuluvulla p on primitiivinen juuri. Tarkemmin sanottuna, alkuluvulla p on täsmälleen $\phi(p-1)$ primitiivistä juurta modulo p.*

Todistus. Lähde [4], Lause 21.2. □

Esimerkki 5.15. Etsitään primitiiviset juuret modulo a) 5 b) 7 ja c) 11.

Olkoon $m = 5$. Täytyy siis etsiä luvut $1 \leq a \leq 5$, joille $\text{syt}(a,5) = 1$. Luvut $1, 2, 3$ ja 4 täyttävät ehdon, joten $\phi(5) = 4$. Laskemalla nähdään, että

$$1^1 \equiv 1 \pmod 5$$
$$2^4 \equiv 1 \pmod 5$$
$$3^4 \equiv 1 \pmod 5$$
$$4^2 \equiv 1 \pmod 5.$$

Lukujen 2 ja 3 pienemmät potenssit eivät ole kongruentteja luvun 1 kanssa modulo 5. Siten luvut 2 ja 3 ovat primitiivisiä juuria modulo 5.

Olkoon $m = 7$. Nyt

$$\phi(7) = 6,$$

koska luvut $1, 2, 3, 4, 5$ ja 6 ovat jaottomia luvun 7 kanssa. Laskemalla nähdään, että

$$1^1 \equiv 1 \pmod 7$$

$$2^3 \equiv 1 \pmod 7$$
$$3^6 \equiv 1 \pmod 7$$
$$4^3 \equiv 1 \pmod 7$$
$$5^6 \equiv 1 \pmod 7$$
$$6^2 \equiv 1 \pmod 7.$$

Lukujen 3 ja 5 pienemmät potenssit eivät ole kongruentteja luvun 1 kanssa modulo 7. Siten luvut 3 ja 5 ovat primitiivisiä juuria modulo 7.

Olkoon $m = 11$. Luku 11 on alkuluku, niin Lauseen 4.5 nojalla

$$\phi(11) = 11 - 1 = 10.$$

Kaikki luvut yhdestä lukuun 10 ovat jaottomia luvun 11 kanssa. Laskemalla nähdään, että

$$1^1 \equiv 1 \pmod{11}$$
$$2^{10} \equiv 1 \pmod{11}$$
$$3^5 \equiv 1 \pmod{11}$$
$$4^5 \equiv 1 \pmod{11}$$
$$5^5 \equiv 1 \pmod{11}$$
$$6^{10} \equiv 1 \pmod{11}.$$
$$7^{10} \equiv 1 \pmod{11}$$
$$8^{10} \equiv 1 \pmod{11}$$
$$9^5 \equiv 1 \pmod{11}$$
$$10^2 \equiv 1 \pmod{11}$$

Lukujen $2, 6, 7$ ja 8 pienemmät potenssit eivät ole kongruentteja luvun 1 kanssa modulo 11. Siten luvut $2, 6, 7$ ja 8 ovat primitiivisiä juuria modulo 11.

Lause 5.16. *(Korseltin lause) Olkoon luku n kokonaisluku, joka ei ole alkuluku. Luvulle n pätee*

$$a^n \equiv a \pmod n \text{ kaikilla } 1 \leq a \leq n. \tag{5.1}$$

jos ja vain jos se on pariton ja jokainen luvun n jakava alkuluku p toteuttaa seuraavat ehdot:
1) Luku p^2 ei jaa lukua n.
2) Luku $p - 1$ jakaa luvun $n - 1$.

Todistus. Olkoon n pariton kokonaisluku, joka ei ole alkuluku. Tällöin luvulla n on Lauseen 2.15 mukainen alkutekijäesitys. Oletetaan, että luvun n kaikki alkutekijät p_i toteuttavat ehdot 1) ja 2). On osoitettava, että luku n toteuttaa kongruenssiyhtälön (5.1). Nyt voidaan jakaa luku n tekijöihin seuraavasti

$$n = p_1 p_2 p_3 \cdots p_r.$$

Kohdan 1) perusteella tiedetään, että kaikki luvut $p_1, p_2, \ldots, p_r$ ovat kaikki eri lukuja. Tiedetään myös kohdan 2) perusteella, että $p_i - 1$ jakaa luvun $n - 1$ kaikilla i. Näin ollen on voimassa

$$n - 1 = (p_i - 1)k_i \text{ jollain kokonaisluvulla } k_i. \tag{5.2}$$

Nyt valitaan jokin kokonaisluku a ja lasketaan arvoja $a^n \pmod{p_i}$. Jos luku p_i jakaa luvun a, niin

$$a^n \equiv 0 \equiv a \pmod{p_i}.$$

Jos taas luku p_i ei jaa lukua a, niin käytetään Fermat'n pientä lausetta 4.8 ja yhtälöä (5.2), niin saadaan

$$a^n = a^{(p_i-1)k_i+1} = (a^{p_i-1})^{k_i} \cdot a \equiv 1^{k_i} \cdot a = a \pmod{p_i}.$$

Nyt

$$a^n \equiv a \pmod{p_i} \text{ kaikilla } i = 1, 2, \ldots, r$$

eli

$$p_i | a^n - a \text{ kaikilla } i = 1, 2, \ldots, r$$

ja $\text{syt}(p_i, p_j) = 1$, kun $i \neq j$, koska alkuluvut $p_1, \ldots, p_r$ ovat kaikki eri lukuja kohdan 1) nojalla. Nyt Lauseen 2.2 nojalla lukujen $p_1, \ldots, p_r$ tulo eli luku n jakaa luvun $a^n - a$ toisin sanoen

$$a^n \equiv a \pmod{n}.$$

Näin todistettiin, että luku n toteuttaa kongruenssiyhtälön (5.1).

Toiseksi täytyy todistaa, että luku n, joka toteuttaa kongruenssiyhtälön (5.1), toteuttaa ehdot 1) ja 2). Lauseen 5.9 todistuksen nojalla luku n on pariton.

Ehdon 1) mukaan millään luvulla, joka toteuttaa kongruenssiyhtälön (5.1), ei ole kahta samaa alkulukutekijää. Oletetaan, että luku n toteuttaa kongruenssiyhtälön (5.1). Olkoon luku p luvun n alkulukutekijä. Olkoon e suurin potenssi, jolle p^{e+1} on luvun n tekijä. Näytetään, että luvun e on oltava 0. Luvun n määritelmän mukaan

$$a^n \equiv a \pmod{n} \text{ kaikilla } 1 \leq a \leq n.$$

Tämä toteutuu myös luvulla $a = p^e$, sillä luku p^e on luvun n tekijä ja siten $p^e < n$. Näin ollen

$$p^{en} \equiv p^e \pmod{n}.$$

Koska luku n jakaa luvun $p^{en} - p^e$ ja luku p^{e+1} jakaa luvun n, niin Lauseen 2.3 nojalla luku p^{e+1} jakaa luvun $p^{en} - p^e$. Tällöin luvun

$$\frac{p^{en} - p^e}{p^{e+1}} = \frac{p^{en-e} - 1}{p}$$

on oltava kokonaisluku. Tämä toteutuu vain silloin, kun $e = 0$, joten luvuilla, jotka toteuttavat kongruenssiyhtälön (5.1), alkulukutekijät esiintyvät vain kerran.

Todistetaan kohta 2) eli luku $p - 1$ jakaa luvun $n - 1$. Oletetaan, että luku n toteuttaa kongruenssiyhtälön (5.1) ja p on luvun n alkulukutekijä. Lauseen 5.14 nojalla jokaisella alkuluvulla on primitiivinen juuri. Olkoon a primitiivinen juuri modulo p, tällöin Määritelmän 5.13 nojalla

$$a^{\phi(p)} \equiv 1 \pmod{p},$$

ja Lemman 4.5 nojalla $\phi(p) = p - 1$, joten

$$a^{p-1} \equiv 1 \pmod{p}. \tag{5.3}$$

Nyt Lauseen 2.8 nojalla saadaan kongruenssiyhtälö (5.3) muotoon

$$1 \equiv a^{p-1} \pmod{p}. \tag{5.4}$$

Nyt luvun n määritelmän mukaan

$$a^n \equiv a \pmod{n},$$

mikä saadaan Lauseen 2.8 nojalla muotoon

$$a^{n-1} \equiv 1 \pmod{n}. \tag{5.5}$$

Lauseen 2.8 nojalla saadaan kongruenssiyhtälöistä (5.5) ja (5.4) kongruenssiyhtälö

$$a^{n-1} \equiv a^{p-1} \pmod{p}.$$

Nyt $n-1 > p-1$, joten on $k > 0$ siten, että $n-1 = p-1+k$. Nyt

$$a^{n-1} - a^{p-1} \equiv 0 \pmod{p},$$

mikä saadaan muotoon

$$a^{p-1}(a^k - 1) \equiv 1(a^k - 1) \equiv (a^k - 1) \pmod{p}.$$

Näin ollen

$$a^k \equiv 1 \pmod{p}.$$

Nyt koska $\text{syt}(a, p) = 1$, niin Lauseen 5.12 nojalla

$$\phi(p)|k, \text{ missä } \phi(p) = p-1.$$

Nyt $n-1 = p-1+s(p-1)$, jollain s. Tällöin $p-1|n-1$. □

Seuraus 5.17. *Olkoon luku n kokonaisluku, joka ei ole alkuluku. Luku on n on Carmichaelin luku jos ja vain jos se on pariton ja jokainen luvun n jakava alkuluku p toteuttaa seuraavat ehdot:*
1) Luku p^2 ei jaa lukua n.
2) Luku $p-1$ jakaa luvun $n-1$.

Todistus. Seuraa Lauseesta 5.16 sekä lähteen [3] Lemmasta 4.8 ja Lauseesta 6.15. □

Esimerkki 5.18. Etsi muotoa $7 \cdot 23 \cdot p$ oleva Carmichaelin luku, missä luku p on alkuluku.

Korseltin lauseen 5.16 nojalla luvun $n-1$ on oltava jaollinen luvuilla 6, 22 ja $p-1$.

Nyt

$$n = 7 \cdot 23 \cdot p \equiv 1 \pmod{6},$$

jos ja vain jos $p \equiv 5 \pmod{6}$.

Nyt

$$n = 7 \cdot 23 \cdot p \equiv 1 \pmod{22},$$

jos ja vain jos $p \equiv 8 \pmod{11}$ ja

$$n = 7 \cdot 23 \cdot p \equiv 1 \pmod{p-1},$$

jos ja vain jos $161 \equiv 1 \pmod{p-1}$ toisin sanoen $(p-1)|160$.

Alkuluku p=41 toteuttaa kaikki ehdot, joten luku

$$n = 7 \cdot 23 \cdot 41 = 6601$$

on Carmichaelin luku.

6. Pythagoraan kolmikot

Tässä luvussa käsitellään Pythagoraan lauseen toteuttavia kolmikoita. Luvun alussa esitellään Pythagoraan lause. Luvussa näytetään myös, että millaista muotoa Pythagoraan lauseen toteuttavien kokonaislukujen a, b ja c tulee olla. Pythagoraan lauseen yhteydessä täytyy mainita myös Fermat'n suuresta lauseesta, jossa käsitellään yhtälöä

$$a^n + b^n = c^n,$$

jolla ei ole ratkaisua, kun $n \geq 3$. Tämä Lause on aiheuttanut päänvaivaa monelle matemaatikolle läpi historian aina 1600-luvulta 1990-luvulle asti, jolloin lause saatiin vihdoin aukottomasti todistettua. Lause on merkittävä siinä mielessä, että se oli viimeinen todeksi osoitettu Fermat'n luoma teoreema. Luvun lähteenä käytetty [3], [4] ja [6].

Lause 6.1. *(Pythagoras) Olkoon $\triangle ABC$ suorakulmainen kolmio. Merkitään kolmion kateetteja kirjaimin a ja b sekä kolmion hypotenuusaa kirjaimella c. Tällöin on voimassa yhtälö*

$$a^2 + b^2 = c^2.$$

Todistus. Lähde [3], Kuva 11.1. □

Esimerkki 6.2. Olkoot $a = 3$, $b = 4$ ja $c = 5$. Nämä luvut toteuttavat Pythagoraan lauseen

$$a^2 + b^2 = 3^2 + 4^2 = 9 + 16 = 25 = 5^2 = c^2.$$

Määritelmä 6.3. Pythagoraan lauseen toteuttavia luonnollisia lukuja a, b ja c kutsutaan Pythagoraan kolmikoiksi, (a, b, c). Kun luvut ovat keskenään jaottomia, $\text{syt}(a, b, c) = 1$, niin kolmikon sanotaan olevan primitiivinen.

Lause 6.4. *Luvut 1 ja 2 eivät voi olla Pythagoraan kolmikossa, mutta luvut $k \geq 3$ voivat olla.*

Todistus. Luku c ei voi olla 1 tai 2, koska luvut

$$1^2 = 1 \text{ ja } 2^2 = 4$$

eivät ole minkään kahden luvun neliön summa. Näin ollen on oltava $c \geq 3$.

Koska

$$a^2 < a^2 + 1^2 < (a+1)^2,$$

niin luku $a^2 + 1^2$ ei ole neliö, joten oltava $b \geq 2$. Vastaavasti

$$b^2 < b^2 + 1^2 < (b+1)^2,$$

joten luku $b^2 + 1^2$ ei ole neliö, joten oltava $a \geq 2$.

Jos $b = 2$, niin

$$a^2 < a^2 + b^2 = a^2 + 4 < (a+1)^2 = a^2 + 2a + 1,$$

kun $a \geq 2$. Luku $a^2 + b^2$ ei siis ole neliö, kun $b = 2$, joten $b \neq 2$.
Vastaavasti, jos $a = 2$, niin

$$b^2 < b^2 + a^2 = b^2 + 4 < (b+1)^2 = b^2 + 2b + 1,$$

kun $b \geq 2$. Luku $a^2 + b^2$ ei siis ole neliö, kun $a = 2$, joten $a \neq 2$.

Näin ollen on oltava $a, b, c \geq 3$. □

Lause 6.5. *Jokaisella kokonaisluvulla k on äärellinen määrä Pythagoraan kolmikoita, joissa luku k esiintyy.*

Todistus. Jos $c = k$, niin $a, b \leq k - 1$ eli luvuille a ja b on äärellinen määrä mahdollisuuksia.

Jos $a = k$, niin

$$k^2 = c^2 - b^2 \geq c^2 - (c-1)^2 = c^2 - (c^2 - 2c + 1) = c^2 - c^2 + 2c - 1 = 2c - 1,$$

joten

$$b < c \leq \frac{k^2 + 1}{2}.$$

Näin ollen on äärellinen määrä mahdollisuuksia luvuille b ja c. □

Esimerkki 6.6. Etsitään kaikki Pythagoraan kolmikot, jotka sisältävät kokonaisluvut $k \leq 7$.

Lauseen 6.4 nojalla on oltava $k \geq 3$.

Vaatimukset täyttäviä kolmikoita ovat

$$(3, 4, 5), (5, 12, 13), (6, 8, 10) \text{ ja } (7, 24, 25).$$

Pythagoraan lauseen toteutuminen ensimmäisen kolmikon osalta on näytetty Esimerkissä 6.2, joten näytetään tämä myös muiden kolmikoiden osalta. Käydään kolmikot läpi järjestyksessä,

$$5^2 + 12^2 = 25 + 144 = 169 = 13^2,$$

$$6^2 + 8^2 = 36 + 64 = 100 = 10^2$$

ja

$$7^2 + 24^2 = 49 + 576 = 625 = 25^2.$$

Lause 6.7. *Olkoon (a, b, c) primitiivinen Pythagoraan kolmikko. Tällöin toinen luvuista a ja b on parillinen ja yksi luvuista a, b ja c on jaollinen luvulla 3. Luvuista, a, b ja c, yksi on jaollinen luvulla 5.*

Todistus. Primitiivisyyden nojalla, koska

$$\text{syt}(a, b, c) = 1,$$

niin molemmat luvut a ja b eivät voi olla parillisia.

Jos molemmat luvut ovat parittomia, niin

$$a^2 + b^2 \equiv 2 \pmod 4.$$

Nyt c voi olla parillinen tai pariton. Tarkastellaan ensin tilannetta, että c on parillinen eli muotoa

$$c = 2k, \text{ jollain kokonaisluvulla } k,$$

jolloin

$$c^2 = 4k^2 \equiv 0 \pmod 4.$$

Jos taas c on pariton, niin se on muotoa

$$c = 2k + 1, \text{ jollain kokonaisluvulla } k.$$

Nyt

$$c^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4.$$

Näin ollen

$$c^2 \equiv 0 \pmod 4 \text{ tai } c^2 \equiv 1 \pmod 4.$$

Täten toinen luvuista a ja b on pariton ja toinen parillinen.

Jos luvut a ja b eivät ole jaollisia luvulla kolme, niin ne ovat muotoa

$$a = 3k+1 \text{ tai } a = 3k+2 \text{ ja } b = 3l+1 \text{ tai } b = 3l+2, \text{ joillain kokonaisluvuilla } k \text{ ja } l.$$

Tällöin

$$a \not\equiv 0 \pmod 3 \text{ ja } b \not\equiv 0 \pmod 3.$$

Nyt laskemalla saadaan

$$a^2 + b^2 \equiv 2 \pmod 3.$$

Luku c voi olla jaollinen luvulla kolme, jolloin se on muotoa

$$c = 3k, \text{ jollain kokonaisluvulla } k.$$

Tällöin

$$c^2 = 9k^2 \equiv 0 \pmod 3.$$

Jos taas c ei ole jaollinen luvulla kolme, niin se on muotoa

$$c = 3k + 1 \text{ tai } c = 3k + 2, \text{ jollain kokonaisluvulla } k,$$

jolloin

$$c^2 \equiv 1 \pmod 3.$$

Näin ollen siis

$$c^2 \equiv 0 \pmod 3 \text{ tai } c^2 \equiv 1 \pmod 3.$$

Primitiivisyys osoittaa, että korkeintaan yksi luvuista a, b ja c voi olla jaollinen luvulla 5. Sillä

$$x^2 \equiv 0 \pmod 5 \text{ tai } x^2 \equiv \pm 1 \pmod 5.$$

Kolmikosta siis yhden oltava jaollinen luvulla 5. □

Seuraavassa lauseessa todistetaan, että mikään tasakylkinen suorakulmainen kolmio, jonka sivujen pituudet ovat kokonaislukuja, eivät toteuta Pythagoraan lausetta.

Lause 6.8. *Ei ole olemassa Pythagoraan kolmikkoa* (a, b, c) *siten, että* $a = b$.

Todistus. Oletetaan, että on olemassa Pythagoraan kolmikko (a, a, c), jolloin

$$a^2 + a^2 = c^2 \text{ eli } 2a^2 = c^2.$$

Näin ollen c^2 on parillinen ja myös luku c on parillinen. Merkitään lukua $c = 2c_1$, missä c_1 on kokonaisluku. Nyt saadaan

$$2a^2 = c^2 = (2c_1)^2 = 4c_1^2,$$

josta edelleen saadaan

$$a^2 = 2c_1^2.$$

Näin ollen luku a^2 on parillinen ja niin on myös luku a.

Olkoon nyt $a = 2a_1$. Nyt yhtälö $2a^2 = c^2$ voidaan kirjoittaa muodossa

$$2 \cdot (2a_1)^2 = (2c_1)^2,$$

mistä saadaan

$$c_1^2 = 2a_1^2.$$

Näin ollen saatiin toinen Pythagoraan kolmikko (a_1, a_1, c_1), missä termit ovat pienempiä kuin alkuperäisessä kolmikossa. Jatkamalla vastaavasti löydetään kolmikko (a_2, a_2, c_2), jolla edelleen pienemmät termit. Jatkamalla saadaan aidosti vähenevä jono (a_i) positiivisia kokonaislukuja. Lukua a pienenpiä positiivisia kokonaislukuja on $a - 1$ kappaletta, mikä on ristiriita.

$$a > a_1 > a_2 > a_3 ...$$

Näin ollen ei voi olla Pythagoraan kolmikoita, joissa sama termi kahteen kertaan. □

Seuraavassa lauseessa todistetaan, että millaisia Pythagoraan kolmikkojen tulee olla.

Lause 6.9. *Olkoon Pythagoraan kolmikko primitiivinen eli* $\text{syt}(a,b,c)=1$*. Tällöin luku* a *on pariton sekä luku* b *parillinen ja luvut ovat muotoa*

$$a=st, b=\frac{s^2-t^2}{2}, c=\frac{s^2+t^2}{2},$$

missä $1\leq t<s$*, luvut* s *ja* t *ovat parittomia ja* $\text{syt}(s,t)=1$*.*

Todistus. Todistetaan ensin, että luvun a on oltava pariton ja luvun b oltava parillinen.

Oletetaan ensin, että molemmat luvut ovat parillisia eli $a=2k$ ja $b=2l$. Nyt Pythagoraan lauseen nojalla pätee

$$c^2=(2k)^2+(2l)^2=4k^2+4l^2=2(2k^2+2l^2),$$

mistä nähdään, että c on muotoa $2m$ eli parillinen. Nyt koska kaikki luvut a, b ja c ovat parillisia, niin $\text{syt}(a,b,c)\geq 2$, jolloin kolmikko ei ole primitiivinen. Tämä on vastoin oletusta, joten molemmat luvuista a ja b eivät voi olla parillisia.

Oletetaan toiseksi, että molemmat luvut ovat parittomia. Parittoman luvun neliö on pariton eli luvut a^2 ja b^2 ovat parittomia. Kahden parittoman luvun summa on parillinen eli luku $a^2+b^2=c^2$ on parillinen. Luvun neliön c^2 ollessa parillinen, niin myös itse luku c on parillinen. Olkoot l ja k kokonaislukuja. Tällöin Pythagoraan lauseen nojalla

$$(2k+1)^2+(2l+1)^2=(2z)^2$$

eli

$$4k^2+4k+4l^2+4l+2=2z^2,$$

joka kahdella jakamalla ja hieman järjestelemällä saadaan muotoon

$$2(k^2+k+l^2+l)+1=2z^2,$$

mikä on ristiriita. Näin ollen molemmat luvuista a ja b eivät voi olla parittomia. Täten luvun a on oltava pariton ja luvun b oltava parillinen, jolloin Pythagoraan lauseen nojalla pätee

$$(2k+1)^2+(2l)^2=4k^2+4k+1+4l^2=2^2(k^2+l^2+k)+1=c^2.$$

Koska luku c^2 on pariton, niin tällöin myös luku c on pariton.

Näin ollen luvun a on oltava pariton, luvun b parillinen (ja luvun c pariton).

Todistetaan seuraavaksi lukujen a, b ja c kaavat. Koska $\text{syt}(a,b,c)=1$, niin luku a^2 voidaan jakaa tekijöihin seuraavasti

$$a^2=c^2-b^2=(c-b)(c+b).$$

Nyt täytyy osoittaa, että luvut $c-b$ ja $c+b$ ovat neliöitä. Olkoon $\text{syt}(c-b,c+b)=d$. Tällöin

$$d|(c-b) \text{ ja } d|(c+b).$$

Nyt luku d jakaa myös lukujen $c-b$ ja $c+b$ summan ja erotuksen eli luvut

$$c-b+c+b=2c \text{ ja } c+b-(c-b)=2b.$$

Nyt $\text{syt}(b,c)=1$, koska luvut kuuluvat primitiiviseen kolmikkoon. Täten luvun d on oltava 1 tai 2. Nyt, koska

$$d|(c-b)(c+b)=a^2$$

ja parittoman luvun a neliö on myös pariton, niin oltava $d = 1$. Tiedetään, että $\text{syt}(c-b, c+b) = 1$ ja $(c-b)(c+b) = a^2$. Tämä toteutuu vain, jos luvut ovat neliöitä eli

$$c - b = s^2 \text{ ja } c + b = t^2,$$

josta saadaan ratkaistua luvut b ja c. Luvuille saadaan kaavat $b = \frac{s^2-t^2}{2}$ ja $c = \frac{s^2+t^2}{2}$. Näiden avulla saadaan ratkaistua $a = \sqrt{(c-b)(c+b)} = st$. □

Lause 6.10. *Kaikki primitiiviset Pythagoraan kolmikot (a,b,c) saadaan kaavoilla*

$$a = u^2 - v^2, b = 2uv \text{ ja } c = u^2 + v^2,$$

missä $0 < v < u$, $\text{syt}(u, v) = 1$ *joista toinen luvuista* u *ja* v *on pariton ja toinen parillinen.*

Todistus. Kaavojen todistus kuten Lauseessa 6.9.

Todistetaan, että kaavoilla saadaan primitiivinen Pythagoraan kolmikko. Luvut a, b ja c ovat positiivisia kokonaislukuja, jolloin

$$(u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2 \text{ kaikilla kokonaisluvuilla } u \text{ ja } v.$$

Nyt siis (a, b, c) on Pythagoraan kolmikko.

Oletetaan, että kolmikko ei ole primitiivinen, jolloin luvut a, b ja c ovat jaollisia jollain alkuluvulla p.

Jos $p = 2$, niin a on parillinen ja $a = u^2 - v^2$, jolloin lukujen u ja v tulisi olla parillisia. Tämä on kuitenkin ristiriita, sillä oltava $\text{syt}(u, v) = 1$. Jos p on pariton, niin se jakaa luvun $\frac{a+c}{2} = u^2$, joten luku p jakaa myös luvun u. Edelleen luku p jakaa luvun $u^2 - a = v^2$, joten luku p jakaa myös luvun v. Tämä johtaa myös ristiriitaan, sillä $\text{syt}(u, v) = 1$. Näin ollen molemmissa tapauksissa päädyttiin ristiriitaan, joten Pythagoraan kolmikon (a, b, c) on oltava primitiivinen. □

Seuraus 6.11. *Yleinen muoto Pythagoraan kolmikolle* (a, b, c) *on*

$$a = m(u^2 - v^2), b = 2muv \text{ ja } c = m(u^2 + v^2),$$

missä $\text{syt}(u, v) = 1$, $v < u$ *ja* m *on positiivinen kokonaisluku.*

Kaikki Pythagoraan kolmikot (ma, mb, mc) ovat primitiivisen Pythagoraan kolmikon (a, b, c) monikertoja, jollain kokonaisluvulla $m \geq 1$. Kun löydetään primitiiviset Pythagoraan kolmikot, niin löydetään myös kaikki Pythagoraan kolmikot näiden monikertoina.

Seuraavassa esimerkissä testataan, onko annettu kolmikko Pythagoraan kolmikko.

Esimerkki 6.12. Onko seuraava kolmikko $(4961, 6480, 8161)$ primitiivinen Pythagoraan kolmikko?

Tarkastellaan ensin, onko lukujen $\text{syt}(4961, 6480, 8161) = 1$ ja tämän jälkeen testataan toteuttaako kolmikko Pythagoraan lauseen. Jos nämä kaksi ehtoa toteutuvat, niin kyseessä on primitiivinen Pythagoraan kolmikko.

Aloitetaan laskemalla lukujen 6480 ja 8161 suurin yhteinen tekijä Eukleideen algoritmin avulla.

$$8161 = 1 \cdot 6480 + 1681$$
$$6480 = 3 \cdot 1681 + 1437$$
$$1681 = 1 \cdot 1437 + 244$$
$$1437 = 5 \cdot 244 + 217$$
$$244 = 1 \cdot 217 + 27$$

$$217 = 8 \cdot 27 + 1$$

$$27 = 27 \cdot 1$$

Nyt lukujen suurin yhteinen tekijä on Eukleideen algoritmin mukaan viimeinen jakojäännös, joten $\text{syt}(6480, 8161) = 1$. Nyt koko kolmikon suurin yhteinen tekijä saadaan lähteen [3] tehtävän 1.9 nojalla seuraavalla tavalla

$$\text{syt}(4961, 6480, 8161) = \text{syt}(4961, \text{syt}(6480, 8161)) = \text{syt}(4961, 1) = 1$$

eli kolmikko on primitiivinen.

Toteuttaako primitiivinen kolmikko Pythagoraan lauseen, $a^2 + b^2 = c^2$.

$$4961^2 + 6480^2 = 66601921 = 8161^2.$$

Lause toteutuu, joten kolmikko $(4961, 6480, 8161)$ on primitiivinen Pythagoraan kolmikko.

Esimerkki 6.13. Pythagoraan kolmikko $(4961, 6480, 8161)$ on primitiivinen Esimerkin 6.12 nojalla. Etsitään kolmikolle Lauseessa 6.9 esitetty esitys lukujen s ja t avulla. Luku a voidaan esittää tulona

$$a = 4961 = 41 \cdot 121.$$

Nyt

$$s = 121 \text{ ja } t = 41, \text{ jolloin } \text{syt}(121, 41) = 1.$$

Luvut s ja t ovat parittomia, jolloin kaikki Lauseessa 6.9 olevat ehdot luvuille s ja t täyttyvät. Nyt luku b saadaan kaavalla

$$b = \frac{s^2 - t^2}{2} = \frac{121^2 - 41^2}{2} = \frac{14641 - 1681}{2} = \frac{6480}{2} = 6480.$$

Vastaavasti luku c saadaan kaavalla

$$c = \frac{s^2 + t^2}{2} = \frac{121^2 + 41^2}{2} = \frac{14641 + 1681}{2} = \frac{16322}{2} = 8161.$$

Nyt lukujen s ja t avulla päästiin vastaavaan primitiiviseen Pythagoraan kolmikkoon kuin Esimerkissä 6.12 eli $(4961, 6480, 8161)$.

Etsitään kolmikolle myös Lauseessa 6.10 esitetty esitys lukujen u ja v avulla. Luku b voidaan esittää tulona

$$b = 6480 = 2 \cdot 40 \cdot 81.$$

Nyt

$$u = 81 \text{ ja } v = 40, \text{ jolloin } \text{syt}(81, 40) = 1.$$

Luku u on pariton ja luku v on parillinen, jolloin kaikki Lauseessa 6.10 olevat ehdot luvuille u ja v täyttyvät. Nyt luku a saadaan kaavalla

$$a = u^2 - v^2 = 81^2 - 40^2 = 6561 - 1600 = 4961.$$

Vastaavasti luku c saadaan kaavalla

$$c = u^2 + v^2 = 81^2 + 40^2 = 6561 + 1600 = 8161.$$

Myös näin päästiin primitiiviseen Pythagoraan kolmikkoon $(4961, 6480, 8161)$.

Lause 6.14. *Ei ole positiivisia kokonaislukuja x, y ja z siten, että*

$$x^4 + y^4 = z^2. \tag{6.1}$$

Todistus. Jakamalla tarvittaessa mahdollisella yhteisellä tekijällä, voidaan olettaa että kolmikko (x, y, z) on primitiivinen. Nyt myös kolmikko (x^2, y^2, z) on primitiivinen, jolloin pätee Lauseessa 6.10 esiintyneet kaavat

$$x^2 = u^2 - v^2, y^2 = 2uv, z = u^2 + v^2,$$

missä toinen luvuista u ja v on pariton ja toinen parillinen siten, että $\text{syt}(u, v) = 1$. Nyt ensimmäinen yhtälö voidaan kirjoittaa muotoon

$$x^2 + v^2 = u^2.$$

Näin ollen myös kolmikko (x, v, u) on primitiivinen, sillä $\text{syt}(u, v) = 1$. Koska x on pariton, niin Lauseen 6.10 nojalla pätee kaavat

$$x = u_1^2 - v_1^2, v = 2u_1v_1, u = u_1^2 + v_1^2,$$

missä $\text{syt}(u_1, v_1) = 1$. Nyt luvulle $y^2 = 2uv$ voidaan laskea uusi kaava lukujen u_1 ja v_1 avulla.

$$y^2 = 2uv = 2(u_1^2 + v_1^2)(2u_1v_1) = 4u_1v_1(u_1^2 + v_1^2).$$

Nyt luvut u_1, v_1 ja $u_1 + v_1$ ovat keskenään jaottomia ja neliöitä, joten

$$u_1 = x_1^2, v_1 = y_1^2, u_1^2 + v_1^2 = z_1^2,$$

joten

$$x_1^4 + y_1^4 = z_1^2.$$

Nyt kolmikko (x_1, y_1, z_1) on toinen ratkaisu yhtälölle 6.1 ja

$$z_1 < z_1^4 = (u_1^2 + v_1^2)^2 = u^2 < u^2 + v^2 = z.$$

Jatkamalla näin saadaan aina pienempiä ja pienempiä ratkaisua, joka johtaa ristiriitaan. Näin ollen yhtälöllä (6.1) ei ole positiivisia kokonaislukuratkaisuja.

□

Viimeisenä lauseena Fermat'n suuri lause.

Seuraus 6.15. *Yhtälöllä*

$$a^4 + b^4 = c^4 \tag{6.2}$$

ei ole kokonaislukuratkaisuja.

Todistus. Oletetaan, että yhtälöllä olisi ratkaisu. Sijoittamalla luvut $a = x$, $b = y$ ja $c^2 = z$ saadaan yhtälö (6.2) muotoon

$$x^4 + y^4 = z^2,$$

jolla ei ole ratkaisua Lauseen 6.14 nojalla. Näin ollen päädyttiin ristiriitaan, joten yhtälöllä $a^4 + b^4 = c^4$ ei ole kokonaislukuratkaisuja. □

==========

Viitteet

[1] Coppel, *Number theory*, Springer, 2009
[2] Hardy ja Wright, *An introduction to the theory of numbers*, Oxford University Press, 2008
[3] Jones ja Jones, *Elementary number theory*, Springer, 2008
[4] Silverman, *A friendly introduction to number theory*, Pearson Education, 3. painos, 2006
[5] Redmond, *An Introduction Number Theory*, Marcel Dekker, 1996
[6] http://fi.wikipedia.org/wiki/Fermat'nsuurilause, (27.4.2011)
[7] http://en.wikipedia.org/wiki/Mersenneprime, (24.5.2011)
[8] http://en.wikipedia.org/wiki/Fermat'slittletheorem (24.5.2011)
[9] http://www.mersenne.org/ (24.5.2011)

Jyväskylän yliopisto
E-mail address: minna.tuononen@jyu.fi