TAMPEREEN YLIOPISTO

Pro gradu -tutkielma

Tuukka Hyvärinen

Täydelliset totienttiluvut

Informaatiotieteiden yksikkö

Matematiikka

Toukokuu 2015

Tampereen yliopisto
Informaatiotieteiden yksikkö
HYVÄRINEN, TUUKKA: Täydelliset totienttiluvut
Pro gradu -tutkielma, 47 s.
Matematiikka
Toukokuu 2015

Tiivistelmä

Tässä tutkielmassa käsitellään täydellisiä totienttilukuja. Täydellinen totienttiluku on kokonaisluku, joka yhtä suuri siitä iteroitujen Eulerin phi-funktioiden arvojen summan kanssa. Tutkielmassa esitellään erilaisia täydellisiä totienttilukuja ja näytetään, miten ne ovat löydettävissä.

Tutkielman aluksi määritellään Eulerin phi-funktio ja useita siihen liittyviä tuloksia. Lisäksi käydään läpi Eulerin phi-funktioon liittyvä Eulerin lause, joka on Fermat'n pienen lauseen yleistys. Määritellään myös muutamia muita tutkielman kannalta hyödyllisiä käsitteitä.

Ennen täydellisiin totienttilukuihin siirtymistä tarkastellaan Eulerin phi-funktion iterointia. Esitellään phi-funktion iteroinnista nouseva funktio ja käsitellän monia sen ominaisuuksia. Osoitetaan myös, että tälle funktiolle on löydettävissä ylä- ja alaraja.

Tämän jälkeen määritellään täydelliset totienttiluvut ja esitetään niistä muutamia esimerkkejä. Osoitetaan mm., että alkulukupotensseista ainostaan luvun kolme potenssit ovat täydellisiä totienttilukuja. Lisäksi käydään läpi useita lauseita, joiden avulla voidaan löytää täydellisiä totienttilukuja. Tutkielman lopuksi määritellään vielä supertäydelliset totienttiluvut ja näytetään, että ne ovat täydellisesti karakteroitavissa yhden lauseen avulla.

Sisältö

1 Johdanto

Tämän tutkielman tarkoitus on esitellä lukijalle täydellisten totienttilukujen käsite ja joitakin siihen liittyviä tuloksia. Tutkielmassa käydään ensin läpi Eulerin phi-funktio, sen muutamia perustuloksia sekä siihen läheisesti liittyvä Eulerin lause. Sen jälkeen esitetään joitakin Eulerin phi-funktion iteroinnista seuraavia tuloksia. Tämän jälkeen päästään viimein määrittelemään täydelliset totienttiluvut ja voidaan esittää niihin liittyviä tuloksia sekä yrittää etsiä täydellisiä totienttilukuja muutamien lauseiden avulla. Tutkielman lopuksi esitetään vielä supertäydellisten totienttilukujen käsite.

Tämän tutkielman lukijalta edellytetään lukuteorian perusteiden ymmärtämistä. Oletetaan mm. että lukija tuntee jaollisuuden ja suurimman yhteisen tekijän määritelmät ja merkinnät sekä ymmärtää niihin liittyviä perustuloksia. Lisäksi lukijan oletetaan tuntevan alkuluvun käsitteen ja jonkin verran alkulukujen ominaisuuksia. Tutkielmassa käytetään myös pariin otteeseen kongruenssia, joten tämän käsitteen tunteminen ja siihen liittyvien perustulosten ymmärtäminen on tarpeellista.

Vaikka täydellisten totienttilukujen tutkiminen alkoi alle sata vuotta sitten, löytyy käsitteen juuret jo antiikin Kreikasta. Erinäisten myyttisten uskojen takia antiikin kreikkalaisia kiinnostivat luvut, jotka olivat yhtä suuria luvun aitojen positiivisten tekijöiden summan kanssa. Tämä johti täydellisten lukujen käsitteeseen, josta myös täydelliset totienttiluvut ovat saaneet nimensä. Täydellisten totienttilukujen tutkiminen alkoi 1900-luvun alkupuolella, kun Perez Cacho julkaisi paperin [6], jossa hän tutki lukuja, jotka ovat yhtä suuria luvusta iteroitujen phi-funktion arvojen summan kanssa. Täydellisten totienttilukujen käsite määriteltiin kuitenkin vasta 1970-luvun puolivälissä. Täydelliset totienttiluvut herättävät vieläkin paljon mielenkiintoa, sillä niihin liittyy yhä paljon avoimia kysymyksiä.

Tutkielman lähteenä on käytetty useita Eulerin phi-funktion iterointiin ja täydellisiin totienttilukuihin liittyviä artikkeleita. Lisäksi alustavien tarkastelujen lähteinä ovat olleet Kenneth H. Rosenin kirja *Elementary Number Theory and Its Applications* ja David M. Burtonin kirja *Elementary Number Theory*.

2 Alustavia tarkasteluja

2.1 Eulerin phi-funktio

Tässä luvussa käsitellään kuuluisan sveitsiläisen matemaatikon Leonhard Eulerin mukaan nimettyä Eulerin phi-funktiota, josta käytetään joskus myös nimitystä Eulerin totienttifunktio. Euler oli yksi kaikkien aikojen tuotteliaimmista matemaatikoista. Elinaikanaan hän kirjoitti yli 700 tieteellistä julkaisua ja vaikutti laajasti matematiikan kehitykseen 1700-luvulla.

Kaikki tässä tutkielmassa esiintyvät muuttujat ovat kokonaislukuja ellei toisin mainita.

Määritelmä 2.1. (Vrt. [2, s. 80]) Lukuja a ja b kutsutaan *suhteellisiksi alkuluvuiksi*, jos niiden suurin yhteinen tekijä on 1.

Määritelmä 2.2 (Eulerin phi-funktio)**.** (Vrt. [1, s. 129]) Olkoon n positiivinen. Eulerin phi-funktiolla $\phi(n)$ tarkoitetaan niiden positiivisten lukujen $k \leq n$ määrää, jotka ovat suhteellisia alkulukuja luvun n kanssa.

Esimerkki 2.1. Nähdään, että $\phi(24) = 8$, sillä on olemassa 8 positiivista lukua, jotka ovat suhteellisia alkulukuja luvun 24 kanssa:

$$1 \quad 5 \quad 7 \quad 9 \quad 11 \quad 13 \quad 17 \quad 19 \quad 23.$$

Taulukossa 1 on esitetty Eulerin phi-funktion $\phi(n)$ arvoja, kun $1 \leq n \leq 15$.

Taulukko 1: Eulerin phi-funktion $\phi(n)$ arvo luvun n arvoilla 1-15

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

Huomataan, että $\phi(1) = 1$, sillä $(1, 1) = 1$. Kuitenkin kun $n > 1$, niin $(n, n) = n \neq 1$ Täten voidaan sanoa, että funktion $\phi(n)$ arvo on lukua n pienempien lukujen, jotka ovat suhteellisia alkulukuja luvun n kanssa, määrä.

Jos n on alkuluku, niin jokainen lukua n pienempi luku on tietenkin suhteellinen alkuluku sen kanssa, joten $\phi(n) = n - 1$. Toisaalta, jos n on yhdistetty luku, niin sillä on olemassa jakaja d siten, että $1 < d < n$. Täten joukossa $\{1, 2, \ldots, n\}$ on ainakin kaksi lukua, jotka eivät ole suhteellisia alkulukuja luvun n kanssa (n ja d). Saadaan siis, että $\phi(n) \leq n - 2$. Ollaan siis todistettu, että

$$\phi(n) = n - 1, \text{ jos ja vain jos } n \text{ on alkuluku.}$$

Pienille luvuille n on helppo saada phi-funktion arvo tarkastelemalla kaikkia lukua n pienempiä lukuja. Luvun n kasvaessa tästä tulee kuitenkin koko ajan työläämpää. Siksi onkin hyvä löytää kaava, jonka avulla arvon $\phi(n)$ laskeminen helpottuu. Aloitetaan johtamalla kaava tilanteessa, missä luku n on alkulukupotenssi. [1, s. 130]

Lause 2.1. *Jos p on alkuluku ja luku k on positiivinen, niin*

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

Todistus. (Vrt. [1, s. 130]) Ne korkeintaan luvun p^k suuruiset luvut, jotka eivät ole suhteellisia alkulukuja sen kanssa, ovat muotoa np, missä $1 \leq n \leq p^{k-1}$, sillä luvun p^k ainoa alkulukutekijä on tietenkin p. Koska tällaisia lukuja on täsmälleen p^{k-1} kappaletta, saadaan Eulerin phi-funktion määritelmästä suoraan, että $\phi\left(p^k\right) = p^k - p^{k-1}$. □

Määritelmä 2.3. (Vrt. [2, s. 222]) *Aritmeettinen funktio* on kuvaus, joka on määritelty positiivisten lukujen joukossa. Aritmeettista funktiota kutsutaan myös joissakin esityksissä *lukuteoreettiseksi funktioksi*.

Määritelmä 2.4. (Vrt. [2, s. 222]) Aritmeettinen funktio f on *multiplikatiivinen*, jos $f(mn) = f(m)f(n)$, kun luvut m ja n ovat suhteellisia alkulukuja eli $(m, n) = 1$.

Eulerin phi-funktio on selvästi aritmeettinen funktio. Todistetaan seuraavaksi, että se on myös multiplikatiivinen. Tätä varten todistetaan ensin seuraava apulause.

Apulause 2.2. *Olkoot a, b, c ja d kokonaislukuja. Tällöin $(a, bc) = 1$, jos ja vain jos $(a, b) = 1$ ja $(a, c) = 1$.*

Todistus. (Vrt. [1, s. 130]) Oletetaan ensin, että $(a, bc) = 1$. Olkoon $d = (a, b)$. Tällöin $d \mid a$ ja $d \mid b$, joten $d \mid a$ ja $d \mid bc$. Mutta tämä tarkoittaa, että luvun d täytyy olla 1. Samanlainen päättely osoittaa myös, että $(a, c) = 1$.

Oletetaan sitten, että $(a, b) = 1$ ja $(a, c) = 1$. Tehdään vastaoletus, että $(a, bc) = d > 1$. Luvulla d täytyy olla alkulukujakaja $p > 1$, joka voi tietenkin olla myös luku d itse. Siis $p \mid a$ ja $p \mid bc$ eli $p \mid b$ tai $p \mid c$. Jos $p \mid b$, niin saadaan, että $(a, b) \geq p > 1$, joka on ristiriita. Samoin päädytään ristiriitaan, jos $p \mid c$. Täten $(a, bc) = 1$ ja lause on todistettu. □

Apulause 2.3. *Jos a, b, c, ja n ovat lukuja, joille pätee, että $n > 0$, $(c, n) = 1$ ja $ac \equiv bc \pmod{n}$, niin $a \equiv b \pmod{n}$.*

Todistus. (Vrt. [2, s. 131]) Jos $ac \equiv bc \pmod{n}$ tiedetään, että $n \mid (ac - bc) = c(a-b)$. Täten on olemassa luku k siten, että $c(a-b) = kn$. Koska $(c, n) = 1$, seuraa, että $n \mid (a - b)$. Siis $a \equiv b \pmod{n}$. □

Lause 2.4. *Funktio ϕ on multiplikatiivinen.*

Todistus. (Vrt. [1, s. 131]) Täytyy siis todistaa, että $\phi(mn) = \phi(m)\phi(n)$, kun luvuilla m ja n ei ole muita yhteisiä tekijöitä kuin 1. Jos $m = 1$, niin $\phi(mn) = \phi(1n) = \phi(n) = 1 \cdot \phi(n) = \phi(1)\phi(n) = \phi(m)\phi(n)$, sillä $\phi(1) = 1$. Samoin saadaan $\phi(mn) = \phi(m)\phi(n)$, jos $n = 1$. Voidaan siis olettaa, että $m, n > 1$. Esitetään kaikki luvut yhdestä mn:ään taulukossa, jossa on m saraketta ja n riviä:

$$\begin{array}{ccccccc}
1 & 2 & \dots & r & \dots & m \\
m+1 & m+2 & \dots & m+r & \dots & 2m \\
2m+1 & 2m+2 & \dots & 2m+r & \dots & 3m \\
\vdots & \vdots & & \vdots & & \vdots \\
(n-1)m+1 & (n-1)m+2 & \dots & (n-1)m+r & \dots & nm.
\end{array}$$

Tässä taulukossa on siis kaikki korkeintaan luvun mn suuruiset luvut. Siis funktion $\phi(mn)$ arvo on niiden tässä taulukossa olevien lukujen, jotka ovat suhteellisia alkulukuja luvun mn kanssa, määrä. Apulauseen 2.2 mukaan tämä on sama kuin niiden lukujen määrä, jotka ovat suhteellisia alkulukuja sekä luvun m että luvun n kanssa.

Tiedetään, että $(r + qm, m) = (r, m)$. Tämän perusteella huomataan, että r:nnellä sarakkeella olevat luvut ovat suhteellisia alkulukuja luvun m

kanssa, jos ja vain jos luku r itse on suhteellinen alkuluku luvun m kanssa. Taulukossa on sarakkeita m kappaletta (eli r saa arvoja yhdestä m:ään), joten $\phi(m)$ sarakkeista sisältää luvun m kanssa suhteellisia alkulukuja ja jokainen kyseisen sarakkeen luku on suhteellinen alkuluku luvun m kanssa. Täytyy nyt siis osoittaa, että jokaisella tällaisella sarakkeella on $\phi(n)$ lukua, jotka ovat suhteellisia alkulukuja luvun n kanssa. Tästä seuraa, että kaiken kaikkiaan taulukossa on $\phi(m)\phi(n)$ lukua, jotka ovat suhteellisia alkulukuja sekä luvun m että luvun n kanssa.

Oletetaan, että $(r, m) = 1$. Tutkitaan r:nnen sarakkeen arvoja:

$$r, m + r, 2m + r, \ldots, (n-1)m + r.$$

Mitkään kaksi tämän sarakkeen lukua eivät kongruentteja modulo n toistensa kanssa. sillä jos

$$km + r \equiv jm + r \pmod{n}$$

missä $0 \leq k < j < n$, pätisi myös $km \equiv jm \pmod{n}$. Koska $(m, n) = 1$, saadaan apulauseen 2.3 avulla selvä ristiriita $k \equiv j \pmod{n}$. Täten r:nnen sarakkeen arvot ovat kaikki kongruentteja modulo n lukujen $0, 1, 2, \ldots, n-1$ kanssa jossakin järjestyksessä. Tämä tarkoittaa, että r:nnellä sarakkeella on yhtä monta luvun n kanssa suhteellista alkulukua kuin niitä on joukossa $\{1, 2, \ldots, n-1\}$. Mutta niitähän on $\phi(n)$ kappaletta Eulerin ϕ-funktion määritelmän mukaan. Täten taulukossa olevien sekä luvun m että luvun n kanssa suhteellisten alkulukujen määrä on $\phi(m)\phi(n)$ eli $\phi(mn) = \phi(m)\phi(n)$. □

Näiden tulosten perusteella voidaan esittää yleinen kaava Eulerin phi-funktion arvon laskemiseksi.

Lause 2.5. *Olkoon $n > 1$ luku, jonka alkulukuhajotelma on $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, missä siis $p_1, p_2, \ldots, p_r$ ovat alkulukuja ja $r, k_1, k_2, \ldots, k_r \in \mathbb{N}$. Tällöin*

$$\begin{aligned}\phi(n) &= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).\end{aligned}$$

Todistus. (Vrt. [1, s. 132]) Todistetaan lause induktiolla luvun r suhteen. Luku r on luvun n alkulukuhajotelman eri alkulukujen määrä. Jos $r = 1$, niin lause on totta lauseen 2.1 perusteella. Oletetaan sitten, että lause pätee,

kun $r = i$ eli $\phi(p_1^{k_1}p_2^{k_2}\cdots p_i^{k_i}) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})\cdots(p_i^{k_i} - p_i^{k_i-1})$. Koska $(p_1^{k_1}p_2^{k_2}\cdots p_i^{k_i}, p_{i+1}^{k_{i+1}}) = 1$, niin ϕ-funktion multiplikatiivisuuden takia saadaan

$$\begin{aligned}\phi((p_1^{k_1}p_2^{k_2}\cdots p_i^{k_i})p_{i+1}^{k_{i+1}}) &= \phi(p_1^{k_1}p_2^{k_2}\cdots p_r^{k_i})\phi(p_{i+1}^{k_{i+1}}) \\ &= \phi(p_1^{k_1}p_2^{k_2}\cdots p_i^{k_i})(p_{i+1}^{k_{i+1}} - p_{i+1}^{k_{i+1}-1}).\end{aligned}$$

Soveltamalla induktio-oletusta saadaan

$$\phi(p_1^{k_1}p_2^{k_2}\cdots p_{i+1}^{k_{i+1}}) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})\cdots(p_{i+1}^{k_{i+1}} - p_{i+1}^{k_{i+1}-1}).$$

Lause on täten todistettu induktiolla. □

Suurien lukujen kohdalla edellisen lauseen käyttäminen on melko työlästä, mutta pienten lukujen kanssa se on hyödyllinen apuväline Eulerin ϕ-funktion arvon laskemiseksi.

Esimerkki 2.2. Luvun 882 alkulukuhajotelma on $882 = 2 \cdot 3^2 \cdot 7^2$. Käyttämällä lausetta 2.5 saadaan

$$\begin{aligned}\phi(882) &= 882\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right) \\ &= 882 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7} = 252.\end{aligned}$$

Usein hyödyllinen tapa esittää phi-funktion arvo on

$$\phi(n) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i - 1),$$

missä $p_1^{a_1}p_1^{a_1}\cdots p_k^{a_k}$ on luvun n alkulukuhajotelma.

Todistetaan vielä muutamia Eulerin phi-funktion ominaisuuksia. Taulukossa 1 kaikki ϕ-funktion arvot ovat parillisia, kun $n > 2$. Tämä pätee myös yleisesti kuten seuraava lause osoittaa.

Lause 2.6. *Olkoon luku $n > 2$. Tällöin funktion $\phi(n)$ arvo on parillinen luku.*

Todistus. (Vrt. [1, s. 132]) Oletetaan aluksi, että luku n on jokin kakkosen potenssi. Merkitään $n = 2^k$, missä $k \geq 2$. Lauseen 2.5 mukaan

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

joka on tietenkin parillinen, kun $k \geq 2$. Jos n on pariton, niin on olemassa jokin pariton alkuluku p, joka jakaa luvun n. Voidaan siis kirjoittaa $n = p^k m$, missä $m \in \mathbb{Z}_+$, $k \geq 1$ ja $(p^k, m) = 1$. Hyödyntämällä phi-funktion multiplikatiivisuutta saadaan

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

Koska p on pariton, täytyy luvun $p-1$ olla parillinen. Täten funktion $\phi(p^k m)$ arvo on myös parillinen. □

Lause 2.7. (Vrt. [4, s. 36]) *Jos luku $m \in \mathbb{Z}_+$ on pariton, niin*

$$\phi(2^i m) = 2^{i-1}\phi(m),$$

missä $i \geq 1$. Erityisesti, jos $n \geq 2$ on parillinen luku, niin $\phi(n) \leq \frac{1}{2}n$.

Todistus. Lauseen ensimmäinen osa seuraa suoraan phi-funktion multiplikatiivisuudesta ja lauseesta 2.1:

$$\phi(2^i m) = \phi(2^i)\phi(m) = \left(2^i\left(1 - \frac{1}{2}\right)\right)\phi(m) = 2^{i-1}\phi(m).$$

Jos n on parillinen luku, niin se on muotoa $n = 2^i m$, missä $i \geq 1$ ja m on pariton luku. Tällöin

$$\phi(n) = \phi(2^i m) = \phi(2^i)\phi(m) = \frac{1}{2}\left(2^i\phi(m)\right),$$

missä $2^i\phi(m) \leq 2^i m$, koska $\phi(m) \leq m$. Täten $\phi(n) \leq \frac{1}{2}n$. □

Lause 2.8. *Olkoon n parillinen luku ja $a > 0$. Tällöin*

$$\phi(2^a n) = 2^a\phi(n).$$

Todistus. Olkoon n parillinen luku ja $a > 0$. Koska n on parillinen, on se muotoa $2^b \cdot x$, missä luku x sisältää kaikki luvun n mahdolliset parittomat tekijät ja $b > 0$. Lausetta 2.7 soveltamalla saadaan

$$\begin{aligned}\phi(2^a n) &= \phi(2^a(2^b x)) = \phi(2^{a+b}x) = 2^{a+b-1}\phi(x) \\ &= 2^a \cdot 2^{b-1}\phi(x) = 2^a\phi(2^b x) = 2^a\phi(n).\end{aligned}$$

□

Lause 2.9. (Vrt. [4, s. 36]) *Jos $i, j > 0$, niin $\phi(2^i 3^j) = 2^i 3^{j-1}$.*

Todistus. Tämä lause seuraa suoraan soveltamalla lausetta 2.5. Sivuutetaan tarkemmat laskut. □

Todistetaan vielä lopuksi Johann Carl Friedrich Gaussin (1777-1855) ensimmäisenä huomaama phi-funktion ominaisuus: Funktion arvojen $\phi(d)$ summa, kun d käy läpi luvun n positiiiviset jakajat, on sama kuin luku n itse.

Lause 2.10. *Jokaiselle positiivisille luvulle n pätee*

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

missä d käy läpi luvun n positiiviset tekijät.

Todistus. (Vrt. [1, s. 140]) Jaetaan luvut väliltä $1-n$ luokkiin S_d seuraavasti:

$$S_d = \{m \mid (m, n) = d; 1 \leq m \leq n\}$$

Siis luku m laitetaan luokkaan S_d, jos $(m, n) = d$. Nyt $(m, n) = d$, jos ja vain jos $(m/d, n/d) = 1$. Täten jokaisessa luokassa S_d olevien lukujen määrä on sama kuin positiivisten lukujen, jotka eivät ylitä lukua n/d ja jotka ovat suhteellisia alkulukuja n/d:n kanssa. Mutta tämähän on sama kuin $\phi(n/d)$. Jokainen luku $1, 2, \ldots, n$ sisältyy vain yhteen luokkaan S_d. Siis

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

Mutta kun luku d käy läpi kaikki luvun n jakajat, samoin tekee n/d. Täten

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

ja lause on näin todistettu. □

Esimerkki 2.3. Esitetään kaikki luokat S_d tapauksessa $n = 8$:

$$S_1 = \{1, 3, 5, 7\}$$
$$S_2 = \{2, 6\}$$
$$S_4 = \{4\}$$
$$S_8 = \{8\}.$$

Eulerin phi-funktion arvot jakajille ovat $\phi(8) = 4$, $\phi(4) = 2$, $\phi(2) = 1$ ja $\phi(1) = 1$, joten

$$\sum_{d|8} \phi(d) = \phi(8) + \phi(4) + \phi(2) + \phi(1) = 4 + 2 + 1 + 1 = 8.$$

2.2 Eulerin lause

Ensimmäinen julkaistu todistus Fermat'n pienelle lauseelle on Eulerin laatima vuonna 1736. Fermat'n pieni lause siis sanoo, että jos p on alkuluku ja a luku, joka ei ole jaollinen luvulla p, niin $a^{p-1} \equiv 1 (\text{mod } p)$. Hieman myöhemmin Euler onnistui yleistämään lauseen mille tahansa positiiviselle luvulle n alkuluvun p sijaan. Tämä *Eulerin lauseeksi* tai *Fermat-Eulerin lauseeksi* kutsuttu tulos sanoo, että jos positiiviselle luvulle n pätee $(a, n) = 1$, niin $a^{\phi(n)} \equiv 1 \pmod{n}$. [1, s.134]

Jotta voitaisiin todistaa Eulerin lause, todistetaan seuraava aputulos.

Apulause 2.11. *Olkoon $n > 1$ ja $(a, n) = 1$. Jos $a_1, a_2, \ldots, a_{\phi(n)}$ ovat lukua n pienemmät ja sen kanssa suhteellisia alkulukuja olevat positiiviset luvut, niin luvut $aa_1, aa_2, \ldots, aa_{\phi(n)}$ ovat kongruentteja modulo n lukujen $a_1, a_2, \ldots, a_{\phi(n)}$ kanssa jossain järjestyksessä.*

Todistus. (Vrt. [1, s. 135]) Aluksi huomataan, että mitkään kaksi lukua aa_i ja aa_j, missä $1 \leq i < j \leq \phi(n)$, eivät ole kongruentteja modulo n keskenään. Jos nimittäin $aa_i \equiv aa_j \pmod{n}$, niin apulauseen 2.3 mukaan saadaan $a_i \equiv a_j \pmod{n}$, joka on tietenkin ristiriidassa oletusten kanssa. Lisäksi, koska $(a_i, n) = 1$ kaikilla $i \in \{1, 2, \ldots, \phi(n)\}$, ja $(a, n) = 1$ niin apulauseen 2.2 mukaan kaikki luvut aa_i ovat suhteellisia alkulukuja luvun n kanssa.

Tutkitaan yhtä lukua aa_i. Nyt on olemassa luku b, missä $0 \leq b < n$, jolle pätee $aa_i \equiv b \pmod{n}$. Koska $(b, n) = (aa_i, n) = 1$, täytyy luvun b olla jokin luvuista $a_1, a_2, \ldots, a_{\phi(n)}$. Siis luvut $aa_1, aa_2, \ldots, aa_{\phi(n)}$ ovat kongruentteja modulo n lukujen $a_1, a_2, \ldots, a_{\phi(n)}$ kanssa jossain järjestyksessä. □

Lause 2.12 (Eulerin lause)**.** *Olkoot a ja n lukuja, joille pätee $n \geq 1$ ja $(a, n) = 1$. Tällöin*

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

Todistus. (Vrt. [1, s. 135]) Jos $n = 1$, niin lause pitää tietenkin paikkansa. Oletetaan siis, että $n > 1$. Olkoot $a_1, a_2, \ldots, a_{\phi(n)}$ lukua n pienemmät ja sen kanssa suhteellisia alkulukuja olevat positiiviset luvut. Koska $(a, n) = 1$, niin apulauseen 2.11 perusteella luvut $aa_1, aa_2, \ldots, aa_{\phi(n)}$ ovat kongruentteja modulo n lukujen $a_1, a_2, \ldots, a_{\phi(n)}$ kanssa jossain järjestyksessä. Siis

$$\begin{aligned} aa_1 &\equiv a_1' \pmod{n} \\ aa_2 &\equiv a_2' \pmod{n} \\ &\vdots \\ aa_{\phi(n)} &\equiv a_{\phi(n)}' \pmod{n}, \end{aligned}$$

missä luvut $a_1', a_2', \ldots, a_{\phi(n)}'$ ovat luvut $a_1, a_2, \ldots, a_{\phi(n)}$ jossain järjestyksessä. Nyt ottamalla tulo näistä kongruensseista puolittain saadaan

$$\begin{aligned} (aa_1)(aa_2)\cdots(aa_{\phi(n)}) &\equiv a_1'a_2'\cdots a_{\phi(n)}' \pmod{n} \\ (aa_1)(aa_2)\cdots(aa_{\phi(n)}) &\equiv a_1a_2\cdots a_{\phi(n)} \pmod{n} \\ a^{\phi(n)}(a_1a_2\cdots a_{\phi(n)}) &\equiv a_1a_2\cdots a_{\phi(n)} \pmod{n}. \end{aligned}$$

Koska $(a_i, n) = 1$ kaikilla $i \in \{1, 2, \ldots, \phi(n)\}$, niin apulauseen 2.2 nojalla $(a_1a_2\cdots a_{\phi(n)}, n) = 1$, joten apulauseen 2.3 mukaan

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

□

Seuraus 2.12.1 (Fermat'n pieni lause)**.** (Vrt. [1, s. 136]) *Olkoon p alkuluku ja a luku, jolle pätee $p \nmid a$. Tällöin $a^{p-1} \equiv 1 \pmod{p}$.*

Todistus. Jos p on alkuluku, niin tiedetään, että $\phi(p) = p - 1$. Lause seuraa täten suoraan Eulerin lauseesta. □

Esimerkki 2.4. Yksi Eulerin lauseen sovelluksista on suurien potenssien tutkiminen modulo n. Jos esimerkiksi haluttaisiin tietää luvun 7^{363} kaksi viimeistä numero, voidaan soveltaa Eulerin lausetta.Viimeisten kahden numeron löytämiseksi tulee etsiä pienin positiivinen luku, joka on kongruentti luvun 7^{363} kanssa modulo 100. Koska $(100, 7) = 1$ ja

$$\phi(100) = \phi(2^2 \cdot 5^2) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40,$$

Eulerin lauseen mukaan

$$7^{40} \equiv 1 \pmod{100}.$$

Jakoalgoritmilla saadaan, että $363 = 9 \cdot 40 + 3$, joten

$$7^{363} \equiv 7^{9 \cdot 40 + 3} \equiv (7^{40})^9 7^3 \equiv 7^3 \pmod{100}$$

Edelleen $7^3 \equiv 343 \equiv 43 \pmod{100}$. Siis luvun 7^{363} viimeiset kaksi numeroa ovat 43.

2.3 Täydelliset luvut ja Fermat'n luvut

Tämän luvun päätteksi esitellään vielä täydelliset luvut, joilta täydelliset totienttiluvut ovat saaneet nimensä ja käydään läpi muutamia muitakin myöhemmin hyödyllisiä käsitteitä.

Määritelmä 2.5. (Vrt. [2, s. 232]) *Tekijöiden summa -funktio* σ määritellään asettamalla funktion $\sigma(n)$ arvoksi luvun n kaikkien positiivisten jakajien summa.

Määritelmä 2.6. (Vrt. [2, s. 239]) Positiivinen luku n on *täydellinen luku*, jos sen positiivisten jakajien summa on kaksi kertaa luku n itse eli

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

Toisin sanottuna luku n on täydellinen, jos sen itseään pienempien (eli aitojen) positiivisten jakajien summa on n.

Esimerkki 2.5. Luvulla 6 on neljä positiivista jakajaa: 1, 2, 3 ja 6. Tällöin $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6$. Luku 6 on siis täydellinen luku.

Määritelmä 2.7. (Vrt. [2, s. 249]) Positiivista lukua n kutsutaan *supertäydelliseksi luvuksi*, jos

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

Esimerkki 2.6. Luvun 16 positiiviset jakajat ovat 1, 2, 4, 8 ja 16. Tällöin $\sigma(16) = 1 + 2 + 4 + 8 + 16 = 31$ ja $\sigma(31) = 1 + 31 = 32$, sillä 31 on alkuluku. Siis $\sigma(\sigma(16)) = 32 = 2 \cdot 16$. Luku 16 on siis supertäydellinen.

Määritelmä 2.8. (Vrt. [1, s. 226]) Olkoon luku $n \geq 0$. Muotoa

$$F_n = 2^{2^n} + 1$$

olevaa lukua kutsutaan *Fermat'n luvuksi*. Jos F_n on alkuluku, kutsutaan sitä *Fermat'n alkuluvuksi*.

Esimerkki 2.7. Fermat'n lukuja tutkittaessa nähdään helposti, että luvut $F_0 = 2^{2^0} + 1 = 3$, $F_1 = 5$ ja $F_2 = 17$ ovat Fermat'n alkulukuja. Hieman tarkemmin tarkastelemalla huomataan, että myös $F_3 = 257$ ja $F_4 = 65537$ ovat alkulukuja. Siis ensimmäiset viisi Fermat'n lukua ovat Fermat'n alkulukuja. Ensimmäinen Fermat'n luku, joka ei ole alkuluku on $F_5 = 2^{2^5} + 1 = 4294967297$. Fermat itse uskoi, että kaikki Fermat'n luvut olisivat alkulukuja ja vasta Euler osoitti vuonna 1732, että F_5 on jaollinen luvulla 641. [1, s. 227]

3 Täydelliset totienttiluvut

3.1 Eulerin phi-funktion iterointi

Olkoon luku $n > 1$. Merkitään

$$\begin{aligned}
\phi_1(n) &= \phi(n) \\
\phi_2(n) &= \phi(\phi_1(n)) = \phi(\phi(n)) \\
\phi_3(n) &= \phi(\phi_2(n)) = \phi(\phi(\phi(n))) \\
&\vdots \\
\phi_{r+1}(n) &= \phi(\phi_r(n)) = \underbrace{\phi(\phi(\phi \ldots \phi}_{r+1 \text{ kpl}}(n)) \ldots).
\end{aligned}$$

Tiedetään, että kaikilla luvuilla $n > 1$ pätee, että $\phi(n) < n$. Täten jossain vaiheessa tässä ketjussa saavutetaan luku 1 ja siitä eteenpäin kaikilla luvuilla $k \in \mathbb{Z}_+$ pätee $\phi_k(1) = 1$.

Olkoon nyt r pienin luku, jolla

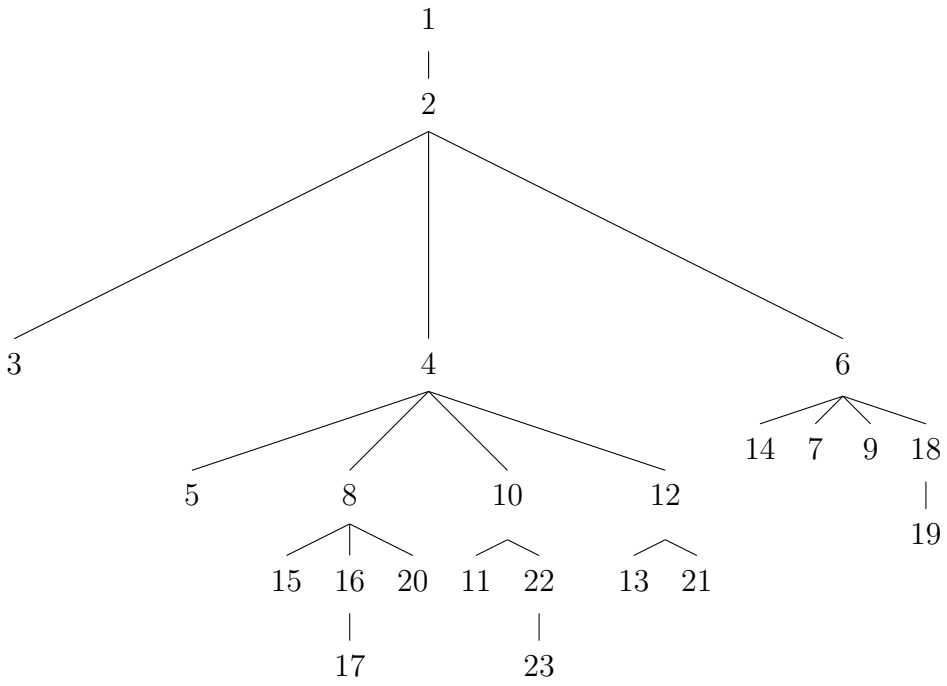
$$\phi_r(n) = 1.$$

Siis jokaiseen lukuun n voidaan liittää luku r, joka kertoo, missä vaiheessa phi-funktion iterointi luvulle n saavuttaa arvon yksi. Merkitään $r = R(n)$. [7, s. 837]

Esimerkki 3.1. Tutkitaan lukua 23. Nyt $\phi(23) = 22$, sillä 23 on alkuluku. Sitten saadaan, että $\phi(22) = 10$, $\phi(10) = 4$, $\phi(4) = 2$ ja $\phi(2) = 1$. Siis $\phi(\phi(\phi(\phi(\phi(23))))) = \phi_5(23) = 1$ eli $R(23) = 5$.

Seuraavassa kuviossa on havainnollistettu phi-funktion arvoja ja sen iterointia. Puun juurena on 1 ja jokaisen solmun vanhempi on kyseisen solmun ϕ-funktion arvo. Funktion $R(n)$ arvo saadaan sen sijaan solmun syvyydestä. Syvyys on solmun esivanhempien lukumäärä eli kuinka monta askelta solmusta on otettava ylöspäin, jotta saavutetaan juurisolmu eli tässä tapauksessa luku 1.

Kuva 1: Puukuvio phi-funktion iteroinnilla saatavista arvoista



Koska $R(2) = 1$ ja $\phi(n)$ on parillinen aina, kun $n > 2$, ei ole aina hyödyllistä tutkia milloin phi-funktion iterointi saavuttaa luvun 1. Usein on käytännöllisempää tutkia pelkästään millon iterointi saavuttaa luvun 2. Olkoon k sellainen luku, että $\phi_k(n) = 2$. Merkitään tällöin $C(n) = k$. Huomataan heti, että $\phi(\phi_k(n)) = \phi(2) = 1$ eli $R(n) = C(n) + 1$. Asetetaan lisäksi, että $C(2) = C(1) = 0$ (kts. [8, s. 18]).

Tutkitaan seuraavaksi funktiota $C(n)$ ja yritetään etsiä sille rajat. Tätä varten todistetaan muutamia funktion $C(n)$ ominaisuuksia.

Apulause 3.1. (Vrt. [8, s. 18]) *Olkoon luku m luvun n monikerta eli $m = kn$, missä luku $k \geq 1$. Tällöin $\phi(mn) = n\phi(m)$.*

Todistus. Oletetaan, että luku n on alkuluku. Tällöin saadaan

$$\phi(mn) = \phi(kn \cdot n) = \phi(kn^2) = \phi(n^{2+x})\phi(k^{'}),$$

missä $k = n^x k^{'}$ $(x \in \mathbb{N})$ ja $k^{'}$ sisältää kaikki luvun k luvusta n eroavat alkulukutekijät. Edelleen

$$\begin{aligned}\phi(n^{2+x})\phi(k^{'}) &= n^{1+x}(n-1)\phi(k^{'}) = n(n^x(n-1)\phi(k^{'})) \\ &= n(\phi(n^{1+x})\phi(k^{'})) = n(\phi(n^x k^{'} n)) \\ &= n\phi(kn) = n\phi(m).\end{aligned}$$

Jos luku n on yhdistetty luku, luvun m täytyy olla myös kaikkien luvun n tekijöiden monikerta. Tällöin luvun n jokaiselle alkulukutekijälle a pätee edeltävän perusteella, että $\phi(an^{'}m) = a\phi(n^{'}m)$, missä $n = an^{'}$. Tällä tavalla jokainen luvun n tekijä saadaan ulos phi-funktiosta ja $\phi(mn) = n\phi(m)$ □

On huomaamisen arvoista, että jos n on alkuluku, niin $\phi(mn) = \phi(m)\phi(n)$ tai $\phi(mn) = n\phi(m)$ ovat ainoat kaksi mahdollisuutta phi-funktion arvoa tutkittaessa.

Lause 3.2. (Vrt. [8, s. 19]) *Jos $n > 1$ on parillinen luku, niin*

$$C(2n) = C(n) + 1.$$

Todistus. Jos $n = 2$, niin $C(2n) = C(4) = 1 = C(2) + 1$. Olkoon $n > 2$ parillinen luku. Lauseen 2.8 perusteella $\phi(2n) = 2\phi(n)$. Koska $\phi(n)$ on aina parillinen, kun $n > 2$, saadaan, että $\phi_2(2n) = \phi(2\phi(n)) = 2\phi_2(n)$. Tätä ketjua jatkamalla saadaan, että $\phi_k(2n) = 2\phi_k(n)$, kun $k \leq C(n)$. Asetetaan $k = C(n)$. Tällöin $\phi_k(2n) = 2\phi_k(n) = 2 \cdot 2 = 4$ ja $\phi(4) = 2$ eli $C(2n) = C(n) + 1$. □

Seuraus 3.2.1. *Olkoon $a \geq 1$. Tällöin*

$$C(2^a) = a - 1.$$

Seuraus 3.2.2. (Vrt. [8, s. 19]) *Olkoon $a \geq 1$. Parillisille luvuille n pätee*

$$C(2^a n) = C(2^a) + C(n) + 1.$$

Todistus. Olkoon n parillinen luku. Tällöin lauseen 3.2 mukaisesti $C(2^a n) = C(2^{a-1} n) + 1$. Tätä toistamalla saadaan $C(2^a n) = C(n) + a$. Seurausta 3.2.1 hyödyntämällä saadaan $C(2^a n) = C(n) + (a-1) + 1 = C(n) + C(2^a) + 1$. □

Lause 3.3. (Vrt. [8, s. 19]) *Jos n on pariton luku, niin*

$$C(2n) = C(n).$$

Todistus. Olkoon n pariton luku. Tällöin phi-funktion multiplikatiivisuuden perusteella $\phi(2n) = \phi(2)\phi(n) = 1 \cdot \phi(n) = \phi(n)$. Siis funktioiden $\phi(2n)$ ja $\phi(n)$ arvot ovat samat kun luku n on pariton. Täten $C(2n) = C(n)$. □

Seuraus 3.3.1. (Vrt. [8, s. 19]) *Parittomille luvuille n pätee $C(2^a n) = C(2^a) + C(n)$.*

Todistus. Todistus onnistuu samalla tavalla kuin seurauksen 3.2.2 kohdalla. Sivuutetaan toiston välttämiseksi yksityiskohdat. □

Huomataan, että nämä lauseet pätevät tietenkin myös funktion $R(n)$ kohdalla, koska $C(n) = R(n) - 1$. Jos n on parillinen luku, niin sijoittamalla $C(x) = R(x) - 1$ lauseeseen 3.2 saadaan

$$\begin{aligned} C(2n) &= C(n) + 1 \\ R(2n) - 1 &= (R(n) - 1) + 1 \\ R(2n) &= R(n) + 1. \end{aligned}$$

ja samoin $R(2n) = R(n)$, jos n on pariton luku.

Lause 3.4. *Kaikille luvuille $n > 1$ pätee*

$$C(3n) = C(n) + C(3).$$

Todistus. (Vrt. [8, s. 19]) Tiedetään, että $C(3) = 1$. Lause voitaisiin siis kirjoittaa muodossa $C(3n) = C(n) + 1$. Oletetaan aluksi, että $n = 2$. Tällöin $C(3n) = C(6) = 1 = C(2) + 1$. Oletetaan sitten, että $n > 2$. Tutkitaan peräkkäisten phi-funktioiden ottamista luvusta $3n$. Jos $(3, n) = 1$, niin phi-funktion

multiplikatiivisuuden nojalla $\phi(3n) = \phi(3)\phi(n) = 2\phi(n)$. Toinen mahdollinen tapaus on, että luku n on luvun 3 monikerta, jolloin apulauseen 3.1 nojalla $\phi(3n) = 3\phi(n)$. Koska luku 3 on alkuluku, nämä ovat ainoat mahdolliset tapaukset. Siis

$$\phi(3n) = 2\phi(n) \quad \text{tai} \quad \phi(3n) = 3\phi(n)$$

ja edelleen

$$\begin{aligned} \phi_2(3n) = \phi(2\phi(n)) \quad &\text{tai} \quad \phi_2(3n) = \phi(3\phi(n)) \\ \phi_2(3n) = 2\phi_2(n) \quad &\text{tai} \quad \phi_2(3n) = 3\phi_2(n), \end{aligned}$$

sillä samoin kuin edellä, jälkimmäisen funktion $\phi(3\phi(n))$ arvo on joko $2\phi_2(n)$ tai $3\phi_2(n)$ riippuen siitä, onko $\phi(n)$ kolmosen monikerta. Tietenkin $\phi(2\phi(n)) = 2\phi_2(n)$, koska $\phi(n)$ on parillinen aina, kun $n > 2$. Jatkamalla phi-funktion ottamista tällä tavalla saadaan, että kun $k \leq C(n)$, niin

$$\phi_k(3n) = 2\phi_k(n) \quad \text{tai} \quad \phi_k(3n) = 3\phi_k(n)$$

ja asettamalla $k = C(n)$

$$\phi_k(3n) = 2\phi_k(n) = 2 \cdot 2 = 4 \quad \text{tai} \quad \phi_k(3n) = 3\phi_k(n) = 3 \cdot 2 = 6.$$

Koska $\phi(4) = \phi(6) = 2$, saadaan, että $C(3n) = k + 1 = C(n) + C(3)$. □

Edellinen lause voidaan yleistää toimimaan mille tahansa parittomalle alkuluvulle.

Lause 3.5. *Olkoon p pariton alkuluku ja luku n positiivinen. Tällöin*

$$C(pn) = C(p) + C(n).$$

Todistus. (Vrt. [8, s. 20]) Todistetaan lause induktiolla alkuluvun p suhteen. Lauseessa 3.4 käytiin jo läpi tapaus $p = 3$. Tehdään sitten induktio-oletus, että lause pätee kaikille alkulukua p pienemmille parittomilla alkuluvuille. Täytyy siis todistaa, että lause pätee alkuluvulle p eli $C(pn) = C(p) + C(n)$. Tiedetään apulauseen 3.1 ja phi-funktion multiplikatiivisuuden perusteella, että

$$\phi(pn) = p\phi(n) \quad \text{tai} \quad \phi(pn) = \phi(p)\phi(n) = (p-1)\phi(n)$$

riippuen siitä onko luku n alkuluvun p monikerta vai ei. Oletetaan ensin, että $\phi(pn) = (p-1)\phi(n)$. Luku $p-1$ voidaan aritmetiikan peruslauseen nojalla esittää muodossa $2^a \prod_{i=1}^{s} q_i^{a_i}$, missä $a > 0$ ja luvut q_i, $i \in \mathbb{Z}_+$, ovat alkulukua p pienempiä alkulukuja. Tällöin

$$\begin{aligned} C((p-1)\phi(n)) &= C((2^a \prod_{i=1}^{s} q_i^{a_i})\phi(n)) \\ &= C((\prod_{i=1}^{s} q_i^{a_i})(2^a\phi(n))). \end{aligned}$$

Nyt voidaan soveltaa induktio-oletusta alkulukuihin q_i ja saadaan

$$\begin{aligned} C((\prod_{i=1}^{s} q_i^{a_i})(2^a\phi(n))) &= \underbrace{C(q_1) + \cdots + C(q_1)}_{a_1 \text{ kpl}} + \underbrace{C(q_2) + \cdots + C(q_2)}_{a_2 \text{ kpl}} \\ &\quad + \cdots + \underbrace{C(q_s) + \cdots + C(q_s)}_{a_s \text{ kpl}} + C(2^a\phi(n)) \\ &= \sum_{i=1}^{s} \sum_{j=1}^{a_i} C(q_i) + C(2^a\phi(n)). \end{aligned}$$

Sitten soveltamalla seurauksia 3.2.2 ja 3.3.1 sekä induktio-oletusta toiseen suuntaan nähdään, että

$$\begin{aligned} C((p-1)\phi(n)) &= \sum_{i=1}^{s} \sum_{j=1}^{a_i} C(q_i) + C(2^a\phi(n)) \\ C(\phi(p)\phi(n)) &= \sum_{i=1}^{s} \sum_{j=1}^{a_i} C(q_i) + C(2^a) + C(\phi(n)) + 1 \\ C(\phi(pn)) &= C(2^a \prod_{i=1}^{s} q_i^{a_i}) + C(\phi(n)) + 1 \\ C(\phi(pn)) &= C(p-1) + C(\phi(n)) + 1 \\ C(\phi(pn)) + 1 &= (C(\phi(p)) + 1) + (C(\phi(n)) + 1) \\ C(pn) &= C(p) + C(n). \end{aligned}$$

Päästään siis haluttuun tulokseen tapauksessa $\phi(pn) = (p-1)\phi(n)$.

Tutkitaan sitten tapausta, että $\phi(pn) = p\phi(n)$. Sovelletaan tähän yhtälöön uudestaan phi-funktiota, jolloin saadaan jälleen kaksi eri mahdollisuutta riippuen siitä onko funktion $\phi(n)$ arvo alkuluvun p monikerta vai ei:

$$\phi(p\phi(n)) = \begin{cases} p\phi(\phi(n)) = p\phi_2(n), & \text{kun } (\phi(n), p) = p \\ \phi(p)\phi(\phi(n)) = (p-1)\phi_2(n), & \text{kun } (\phi(n), p) = 1. \end{cases}$$

Jälkimmäinen tapaus $\phi(p\phi(n)) = (p-1)\phi_2(n)$ johtaa haluttuun tulokseen samalla tavalla kuin edellä. Siis ainoa epäselvä tapaus on taas $\phi(p\phi(n)) = p\phi_2(n)$. Jatkamalla phi-funktion iterointia tähän tapaan huomataan, että kaikilla $k \leq C(n)$ ainoa tapaus, josta tulos ei seuraa välittömästi on

$$\phi_k(pn) = p\phi_k(n).$$

Mutta asettamalla $k = C(n)$ saadaan

$$\phi_k(pn) = p\phi_k(n) = p \cdot 2$$

ja

$$C(pn) = k + C(2p) = C(n) + C(p)$$

lauseen 3.3 perusteella. Ollaan siis jokaisessa tapauksessa päästy haluttuun tulokseen ja lause on täten todistettu. □

Nyt voidaan yhdistää edelliset tulokset seuraavaksi lauseeksi.

Lause 3.6. (Vrt. [8, s. 18]) *Olkoot m ja n positiivisia lukuja. Jos molemmat luvut m ja n ovat parillisia, niin*

$$C(mn) = C(m) + C(n) + 1. \tag{3.1}$$

Muussa tapauksessa

$$C(mn) = C(m) + C(n). \tag{3.2}$$

Todistus. Todistetaan aluksi yhtälö (3.1). Jos luku n on muotoa 2^a, niin tulos pitää paikkansa lauseen 3.2 seurauksen perusteella. Muussa tapauksessa luku n on muotoa $2^a \prod_{i=1}^{s} p_i^{a_i}$, missä $a > 0$ ja luvut p_i, $i \in \mathbb{Z}_+$, ovat alkulukuja. Tällöin voidaan soveltaa lausetta 3.5 sekä seurausta 3.2.2 ja saadaan

$$\begin{aligned}
C(mn) = C(m2^a \prod_{i=1}^{s} p_i^{a_i}) &= C(2^a m) + \sum_{i=1}^{s}\sum_{j=1}^{a_i} C(p_i)) \\
&= C(m) + C(2^a) + 1 + \sum_{i=1}^{s}\sum_{j=1}^{a_i} C(p_i) \\
&= C(m) + C(2^a) + \sum_{i=1}^{s}\sum_{j=1}^{a_i} C(p_i) + 1 \\
&= C(m) + C(2^a \prod_{i=1}^{s} p_i^{a_i}) + 1 \\
&= C(m) + C(n) + 1.
\end{aligned}$$

Todistetaan vielä yhtälö (3.2). Symmetrian perusteella riittää todistaa lause tapauksessa, että luku n on pariton ja luku m on joko pariton tai parillinen. Nyt $n = \prod_{i=1}^{s} p_i^{a_i}$, missä luvut p_i, $i \in \mathbb{Z}_+$, ovat parittomia alkulukuja. Soveltamalla lausetta 3.5 saadaan hieman välivaiheita sivuuttamalla

$$C(mn) = C(m \prod_{i=1}^{s} p_i^{a_i}) = C(m) + C(\prod_{i=1}^{s} p_i^{a_i}) = C(m) + C(n).$$

□

Nyt edellisiä lauseita hyödyntämällä voidaan helposti jakaa luvut luokkiin riippuen niiden funktion C arvosta (kts. [8, s. 18]). Kuten edellä määriteltiin $C(2) = C(1) = 0$, joten luvut 1 ja 2 kuuluvat luokkaan 0. Tiedetään, että $C(3) = 1$, joten luku 3 kuuluu luokkaan 1. Käyttämällä edellistä lausetta nähdään, että $C(4) = C(2 \cdot 2) = C(2) + C(2) + 1 = 1$, joten luku 4 kuuluu myös luokkaan 1. Yleisesti yhdistetyn luvun luokka voidaan laskea sen tekijöiden luokista lauseen 3.6 avulla. Alkuluvun $p > 3$ tapauksessa tiedetään, että $\phi(p) = p - 1$, missä $p - 1$ on yhdistetty luku. Alkuluvun p luokka on siis yhden suurempi kuin luvun $p - 1$ luokka. Näiden tietojen avulla pystytään määrittämään lukujen luokat niitä edeltävien lukujen avulla. Seuraavassa taulukossa on ensimmäisten neljän luokan kaikki luvut (kts. [8, s. 21]).

Taulukko 2: Luokkien 0, 1, 2 ja 3 luvut

Luokka	Luokassa olevat luvut
0	1 2
1	3 4 6
2	5 7 8 9 10 12 14 18
3	11 13 15 16 19 20 21 22 24 26 27 28 30 36 38 42 54

Määritetään nyt luokkien rajat ja sen avulla myös funktion $C(n)$ rajat.

Lause 3.7. *Suurin pariton luku luokassa $k = 0, 1, 2, \ldots$ on 3^k ja suurin parillinen luku on $2 \cdot 3^k$.*

Todistus. (Vrt. [8, s. 21]) Todistetaan lause induktiolla luokan k suhteen. Taulukosta 2 nähdään, että lause pätee luokille 0, 1, 2 ja 3. Oletetaan sitten,

että lause pätee kaikille luokkaa k pienemmille luokille, ja osoitetaan, että se pätee myös luokalle k.

Tiedetään, että kaikille alkuluvuille pätee $\phi(p) = p - 1$. Tällöin, jos alkuluku $p > 2$ kuuluu luokkaan k, eli $C(p) = k$, niin luvun $p - 1$ täytyy kuulua luokkaan $k - 1$. Siis $C(p-1) = k - 1 < k$ ja induktio-oletuksen nojalla tiedetään, että parilliselle luvulle $p - 1$ pätee

$$p - 1 \leq 2 \cdot 3^{k-1}.$$

Koska $2 \cdot 3^{k-1} + 1 \leq 3 \cdot 3^{k-1} = 3^k$, saadaan

$$p \leq 3^k.$$

Lause siis pätee alkuluvuille p.

Olkoon n nyt yhdistetty luku, joka kuuluu luokkaan k eli $C(n) = k$. Luku n voidaan kirjoittaa sen tekijöiden tulona muodossa $2^a \prod_{i=1}^{s} p_i^{a_i}$, missä $a \geq 0$ ja luvut p_i ovat parittomia alkulukuja. Todistuksen alkuosan perusteella tiedetään, että jokaiselle parittomalle alkuluvulle p_i pätee

$$p_i \leq 3^{C(p_i)} \iff \log p_i \leq \log 3^{C(p_i)} \iff C(p_i) \geq \frac{\log p_i}{\log 3}.$$

Oletetaan ensin, että luku n on pariton eli se on parittomien alkulukujen tulo. Tällöin $a = 0$. Lausetta 3.6 soveltamalla saadaan

$$\begin{aligned} C(n) &= C(2^a \prod_{i=1}^{s} p_i^{a_i}) = C(\prod_{i=1}^{s} p_i^{a_i}) \\ C(n) &= \sum_{i=1}^{s} \sum_{j=1}^{a_i} C(p_i) \\ C(n) &\geq \sum_{i=1}^{s} \sum_{j=1}^{a_i} \frac{\log p_i}{\log 3}. \end{aligned}$$

Logaritmien laskusääntöä $\log x + \log y = \log(xy)$ soveltamalla saadaan

$$\begin{aligned} C(n) &\geq \frac{\log(\prod_{i=1}^{s} p_i^{a_i})}{\log 3} \\ C(n) &\geq \frac{\log n}{\log 3} \\ C(n) \log 3 &\geq \log n \\ \log 3^{C(n)} &\geq \log n \\ n &\leq 3^{C(n)} = 3^k. \end{aligned}$$

Lause siis pätee parittomille luvuille. Oletetaan sitten, että luku n on parillinen eli $a \geq 1$. Tällöin saadaan lausetta 3.6 sekä seurauksia 3.2.1 ja 3.3.1 soveltamalla

$$\begin{aligned}
C(n) &= C(2^a \prod_{i=1}^{s} p_i^{a_i}) \\
C(n) &= C(2^a) + C(\prod_{i=1}^{s} p_i^{a_i}) \\
C(n) &= (a-1) + \sum_{i=1}^{s} \sum_{j=1}^{a_i} C(p_i) \\
C(n) &\geq (a-1) + \sum_{i=1}^{s} \sum_{j=1}^{a_i} \frac{\log p_i}{\log 3}.
\end{aligned}$$

Huomataan, että

$$(a-1) = \frac{(a-1)\log 3}{\log 3} \geq \frac{(a-1)\log 2}{\log 3} = \frac{\log 2^{a-1}}{\log 3} = \frac{\log 2^a - \log 2}{\log 3}.$$

Tätä huomiota sekä logaritmien laskusääntöjä soveltamalla saadaan

$$\begin{aligned}
C(n) &\geq \sum_{i=1}^{s} \sum_{j=1}^{a_i} \frac{\log p_i}{\log 3} + (a-1) \\
C(n) &\geq \frac{\log(\prod_{i=1}^{s} p_i^{a_i})}{\log 3} + \frac{\log 2^a - \log 2}{\log 3} \\
C(n) &\geq \frac{\log(2^a \prod_{i=1}^{s} p_i^{a_i})}{\log 3} - \frac{\log 2}{\log 3} \\
C(n) &\geq \frac{\log n - \log 2}{\log 3} \\
C(n)\log 3 &\geq \log\left(\frac{n}{2}\right) \\
\log 3^{C(n)} &\geq \log\left(\frac{n}{2}\right) \\
3^{C(n)} &\geq \frac{n}{2} \\
n &\leq 2 \cdot 3^{C(n)} = 2 \cdot 3^k.
\end{aligned}$$

Lause on täten todistettu. □

Ollaan siis saatu selvitettyä funktion $C(n)$ alaraja.

Seuraus 3.7.1. (Vrt. [8, s. 23]) *Kaikille luvuille n pätee $n \leq 2 \cdot 3^{C(n)}$. Toisin sanoen*

$$C(n) \geq \frac{\log n - \log 2}{\log 3}.$$

Vaihtamalla funktion $C(n)$ tilalle funktio $R(n)$ saadaan vuorostaan

$$R(n) \geq \frac{\log n - \log 2}{\log 3} + 1$$

(kts. [7, s. 840]).

Etsitään seuraavaksi luokkien $k = 0, 1, 2, \ldots$ pienin luku ja sen avulla funktioiden $C(n)$ ja $R(n)$ yläraja.

Lause 3.8. *Pienin pariton luku luokassa $k = 1, 2, 3, \ldots$ on suurempi kuin 2^k ja pienin parillinen luku luokassa $k = 0, 1, 2, \ldots$ on 2^{k+1}.*

Todistus. (Vrt. [8, s. 22]) Todistetaan aluksi induktiolla luokan k suhteen, että pienin parillinen luku luokassa k on 2^{k+1}. Taulukosta 2 nähdään, että väite pätee luvun k arvoilla 0, 1, 2 ja 3. Tehdään sitten induktio-oletus, että väite pätee kaikille luokkaa $k > 3$ pienemmille luokille, ja todistetaan, että lause pitää paikkansa myös luokalle k.

Olkoon parillinen luku n luokassa $k > 3$ eli $C(n) = k$. Luku n voidaan esittää muodossa $2^a s$, missä $s \geq 0$ on pariton luku. Oletetaan aluksi, että $a > 1$, jolloin $n = 2^a s = 2 \cdot 2^{a-1} s$, missä $a - 1 > 0$. Seurausten 3.2.1 ja 3.3.1 perusteella tiedetään, että

$$\begin{aligned} C(2^{a-1}s) &= C(2^{a-1}) + C(s) = a - 2 + C(s) = ((a-1) + C(s)) - 1 \\ &= (C(2^a) + C(s)) - 1 = C(2^a s) - 1 = k - 1. \end{aligned}$$

Siis $C(2^{a-1}s) = k - 1$ ja lukuun $2^{a-1}s$ voidaan soveltaa induktio-oletusta. Saadaan

$$\begin{aligned} 2^{a-1}s &\geq 2^{(k-1)+1} \\ 2 \cdot 2^{a-1}s &\geq 2 \cdot 2^k \\ 2^a s &\geq 2^{k+1} \end{aligned}$$

ja lause on täten todistettu parillisille luvuille $n = 2^a s$, missä $a > 1$. Oletetaan sitten, että $a = 1$ eli $n = 2s$. Pitää siis osoittaa, että $2s \geq 2^{k+1}$. Tehdään vastaoletus, että $2s < 2^{k+1}$. Tällöin $s < 2^k$ ja koska s on pariton luku, niin lauseen 3.3 mukaan $C(n) = C(2s) = C(s) = k$. Tiedetään, että $C(\phi(s)) = C(s) - 1 = k - 1$. Voidaan siis soveltaa lukuun $\phi(s)$ induktio-oletusta ja saadaan, että $\phi(s) \geq 2^{(k-1)+1} = 2^k$. Mutta vastaoletuksesta ja

phi-funktion perusominaisuuksista saadaan, että $\phi(s) \leq s < 2^k$, joka on tietenkin ristiriidassa edellisen tuloksen kanssa. Siis $s \geq 2^k$ ja $2s \geq 2^{k+1}$ ja lause on täten todistettu induktiolla parillisille luvuille.

Todistetaan vielä, että pienin pariton luku luokassa $k > 0$ on suurempi kuin 2^k. Tämä onnistuu helposti tarkastelemalla luokan k pienintä paritonta lukua n. Koska $C(n) = C(2n) = k$, tiedetään lauseen alkuosan perusteella, että $2n \geq 2^{k+1}$, josta saadaan helposti laventamalla, että $n \geq 2^k$. Koska luku n on pariton, yhtäsuuruus ei voi olla voimassa kun $k > 0$, joten $n > 2^k$. □

Seuraus 3.8.1. (Vrt. [8, s. 23]) *Kaikille luvuille $n > 1$ pätee, että $n > 2^{C(n)}$. Toisin sanoen*

$$C(n) < \frac{\log n}{\log 2}.$$

Vaihtamalla funktion $C(n)$ tilalle funktio $R(n)$ saadaan jälleen vuorostaan

$$R(n) < \frac{\log n}{\log 2} + 1$$

(kts. [7, s. 838]).

Ollaan siis onnistuttu rajaamaan funktioiden $C(n)$ ja $R(n)$ arvot:

$$\begin{aligned} \frac{\log n - \log 2}{\log 3} \leq & C(n) < \frac{\log n}{\log 2} \\ \frac{\log n - \log 2}{\log 3} + 1 \leq & R(n) < \frac{\log n}{\log 2} + 1. \end{aligned}$$

Sivasankaranarayana Pillai päätyy omassa artikkelissaan [7] näihin samoihin tuloksiin kuin Shapiro, mutta hänen todistuksensa jäävät hieman epäselviksi ja puuttellisiksi, joten tässä tutkielmassa todistukset noudattavat Shapiron artikkelia.

3.2 Määritelmä ja perustuloksia

Soveltamalla phi-funktion iterointia voidaan määritellä täydelliset totienttiluvut.

Määritelmä 3.1. (Vrt. [4, s. 36]) Olkoon n positiivinen luku. Lukua n kutsutaan *täydelliseksi totienttiluvuksi* (engl. *perfect totient number* ja lyh. PTN), jos

$$\sum_{i=1}^{R(n)} \phi_i(n) = n.$$

Esimerkki 3.2. Pienten lukujen kohdalla on helppo tutkia, onko kyseessä täydellinen totienttiluku. Esimerkiksi luvulle 20 pätee, että R(20)= 4, joten

$$\begin{aligned}\sum_{i=1}^{R(20)} \phi_i(20) &= \phi(20) + \phi_2(20) + \phi_3(20) + \phi_4(20) \\ &= \phi(20) + \phi(8) + \phi(4) + \phi(2) = 8 + 4 + 2 + 1 = 15 \neq 20.\end{aligned}$$

Luku 20 ei ole täten täydellinen totienttiluku. Toisaalta luvun 39 kohdalla R(39) = 5 ja

$$\begin{aligned}\sum_{i=1}^{R(39)} \phi_i(39) &= \phi(39) + \phi_2(39) + \phi_3(39) + \phi_4(39) + \phi_5(39) \\ &= \phi(39) + \phi(24) + \phi(8) + \phi(4) + \phi(2) = 24 + 8 + 4 + 2 + 1 = 39.\end{aligned}$$

Luku 39 on siis täydellinen totienttiluku.

Merkitään tästä eteenpäin yksinkertaisuuden vuoksi $\sum_{i=1}^{R(n)} \phi_i(n) = \Phi(n)$ ja käydään läpi muutamia funktiota $\Phi(n)$ koskevia aputuloksia, jotka ovat hyödyllisiä jatkossa.

Apulause 3.9. (Vrt. [4, s. 37]) *Kaikille luvuille $n > 1$ pätee*

$$\Phi(n) = \phi(n) + \Phi(\phi(n)).$$

Todistus. Tämä tulos seuraa suoraan Φ-funktion määritelmästä, sillä

$$\Phi(n) = \sum_{i=1}^{R(n)} \phi_i(n) = \phi(n) + \sum_{i=2}^{R(n)} \phi_i(n) = \phi(n) + \Phi(\phi(n)).$$

□

Apulause 3.10. (Vrt. [4, s. 37]) *Kaikille luvuille $i, j > 0$ pätee*

$$\Phi(2^i 3^j) = 2^{i-1}(3^j + 1) - 1.$$

Todistus. Lauseen 2.9 perusteella tiedetään, että $\phi(2^i 3^j) = 2^i 3^{j-1}$. Tällöin

$\phi_j(2^i 3^j) = 2^i$. Lisäksi edellisessä luvussa huomattiin, että $\phi(2^i) = 2^{i-1}$. Siis

$$\begin{aligned}
\Phi(2^i 3^j) &= \sum_{m=0}^{j-1} 2^i 3^m + \sum_{n=0}^{i-1} 2^n \\
&= 2^i \sum_{m=0}^{j-1} 3^m + \sum_{n=0}^{i-1} 2^n \\
&= 2^i \frac{(1-3^j)}{1-3} + \frac{1-2^i}{1-2} \\
&= 2^i \frac{3^j - 1}{2} + \frac{2^i - 1}{1} \\
&= 2^{i-1} 3^j - 2^{i-1} + 2^i - 1 \\
&= 2^{i-1} 3^j - 2^{i-1}(2-1) - 1 \\
&= 2^{i-1} 3^j + 2^{i-1} - 1 \\
&= 2^{i-1}(3^j + 1) - 1.
\end{aligned}$$

□

Lause 3.11. *Olkoon $n > 0$ parillinen luku. Tällöin*

$$\Phi(n) < n.$$

Todistus. (Vrt. [4, s. 37]) Todistetaan lause induktiolla. Jos $n = 2$, niin $\phi(2) = 1$ ja täten $\Phi(n) = 1 < 2$. Tehdään induktio-oletus, että lause pätee kaikilla parillista lukua k pienemmillä parillisilla luvuilla n. Apulauseen 3.9 nojalla $\Phi(k) = \phi(k) + \Phi(\phi(k))$. Toisaalta tiedetään, että phi-funktion $\phi(x)$ arvo on parillinen aina kun $x > 2$. Siis funktion $\phi(k)$ arvo on parillinen ja phi-funktion määritelmän nojalla pienempi kuin k. Täten induktio-oletuksen mukaan $\Phi(\phi(k)) < \phi(k)$ ja

$$\Phi(k) = \phi(k) + \Phi(\phi(k)) < \phi(k) + \phi(k) = 2\phi(k).$$

Koska k on parillinen, tiedetään lauseen 2.7 perusteella, että $\phi(k) \leq \frac{1}{2}k$. Siis $\Phi(k) < k$ ja lause on täten todistettu induktiolla. □

Tämä lause tarkoittaa tietenkin, että jokainen täydellinen totienttiluku on pariton. Tarkemmin tätä tulosta tarkastelemalla huomataan myös toinen ehto koskien täydellisiä totienttilukuja.

Lause 3.12. *Olkoon $n > 1$ pariton luku. Jos $\phi(n) < \frac{1}{2}n$, niin luku n ei ole täydellinen totienttiluku.*

Todistus. Tiedetään, että kaikilla luvuilla $n > 2$ pätee, että $\phi(n)$ on parillinen. Tällöin jos $\phi(n) < \frac{1}{2}n$, niin edellisen lauseen nojalla saadaan

$$\begin{aligned}\Phi(n) &= \phi(n) + \Phi(\phi(n)) \\ &< \phi(n) + \phi(n) < \frac{1}{2}n + \frac{1}{2}n = n\end{aligned}$$

□

Nyt kun käytössämme on muutamia täydellisten totienttilukujen ominaisuuksia, voidaan kirjoittaa lyhyt Mathematica-koodi niiden etsimiseksi. Taulukossa 3 on listattu kaikki lukua 40000 pienemmät täydelliset totienttiluvut, jotka on saatu seuraavalla Mathematica-ohjelmassa käännetyllä koodinpätkällä aikaiseksi (vrt. [4, s. 36]):

```
For[n = 3, n < 40000, n = n + 2, k = 0; t = n;
     If[2*EulerPhi[t] >= t,
        While[(t = EulerPhi[t])! > 1, k = k + t];
        If[k + 1 == n, Print[n]]]]
```

Taulukko 3: Lukua 40000 pienemmät täydelliset totienttiluvut

3	$81 = 3^4$	$327 = 3 \cdot 109$	$2199 = 3 \cdot 733$	$6561 = 3^8$
$9 = 3^2$	$111 = 3 \cdot 37$	$363 = 3 \cdot 11^2$	$3063 = 3 \cdot 1021$	$8751 = 3 \cdot 2917$
$15 = 3 \cdot 5$	$183 = 3 \cdot 61$	$471 = 3 \cdot 157$	$4359 = 3 \cdot 1453$	$15723 = 3^2 \cdot 1747$
$27 = 3^3$	$243 = 3^5$	$729 = 3^6$	$4375 = 5^4 \cdot 7$	$19683 = 3^9$
$39 = 3 \cdot 13$	$255 = 3 \cdot 5 \cdot 17$	$2187 = 3^7$	$5571 = 3^2 \cdot 619$	$36759 = 3 \cdot 12253$

Taulukkoa 3 tarkastelemalla huomataan ainakin yksi ryhmä lukuja, jotka näyttäisivät olevan täydellisiä totienttilukuja.

Lause 3.13. *Jokainen muotoa 3^k, missä $k \in \mathbb{Z}_+$, oleva luku on täydellinen totienttiluku.*

Todistus. (Vrt. [4, s. 37]) Olkoon luku n muotoa 3^k, missä $k \in \mathbb{Z}_+$. Tällöin $\phi(n) = \phi(3^k) = 3^{k-1}(3-1) = 2 \cdot 3^{k-1}$ ja apulauseen 3.10 mukaan $\Phi(2 \cdot 3^{k-1}) = 3^{k-1} + 1 - 1 = 3^{k-1}$. Täten apulausetta 3.9 soveltamalla saadaan

$$\begin{aligned}\Phi(n) = \Phi(3^k) &= \phi(3^k) + \Phi(\phi(3^k)) = 2 \cdot 3^{k-1} + 3^{k-1} \\ &= (2+1)3^{k-1} = 3 \cdot 3^{k-1} = 3^k.\end{aligned}$$

□

Taulukkoa 3 tutkimalla näyttäisi siltä, että mikään muu alkulukupotenssi ei ole täydellinen totienttiluku. Tämä pitääkin paikkansa ja todistetaan se seuraavassa lauseessa.

Lause 3.14. *Olkoon luku n jonkin kolmosesta eroavan alkuluvun potenssi. Siis $n = p^k$, missä luku $p \neq 3$ on alkuluku ja $k > 0$. Tällöin*

$$\Phi(n) \neq n.$$

Todistus. (Vrt. [4, s. 37]) Tutkitaan aluksi kakkosen potensseja. Kaikille luvuille $n = 2^k$ pätee, että $\phi(n) = \phi(2^k) = 2^{k-1}$. Siis

$$\begin{aligned}\Phi(2^k) &= \phi(2^k) + \phi(2^{k-1}) + \cdots + \phi(2) \\ &= 2^{k-1} + 2^{k-2} + \cdots + 2 + 1 = \frac{1-2^k}{1-2} = 2^k - 1 \neq 2^k,\end{aligned}$$

joten kakkosen potenssit eivät ole täydellisiä totienttilukuja millään luvun $k > 0$ arvolla.

Tarkastellaan sitten alkulukupotensseja, joissa kantana on kolmosta suuremmat alkuluvut. Tiedetään, että jos $n > 2$, niin $\Phi(n) \geq \phi(n) + \phi(\phi(n))$, sillä funktiossa $\Phi(n)$ on vähintään kaksi ensimmäistä phi-funktion iteroitua arvoa. Nyt jos $p > 3$, niin

$$\Phi(p) \geq \phi(p) + \phi(\phi(p)) = p - 1 + \phi(p-1) > p,$$

sillä $\phi(p-1) > 1$, kun $p > 3$. Mikään kolmosesta eroava alkuluku ei siis ainakaan ole täydellinen totienttiluku. Tutkitaan seuraavaksi suurempia potensseja. Jos $k \geq 2$, niin lauseen 2.1 mukaan $\phi(p^k) = p^k - p^{k-1}$. Tällöin, koska $(p-1, p^{k-1}) = 1$, saadaan phi-funktion multiplikatiivisuuden avulla

$$\begin{aligned}\phi(\phi(p^k)) &= \phi(p^k - p^{k-1}) = \phi((p-1)p^{k-1}) = \phi(p-1)\phi(p^{k-1}) \\ &= \phi(p-1)(p^{k-1} - p^{k-2}) \geq 2(p^{k-1} - p^{k-2}).\end{aligned}$$

Tällöin

$$\begin{aligned}\Phi(p^k) \geq \phi(p^k) + \phi(\phi(p^k)) &\geq p^k - p^{k-1} + 2(p^{k-1} - p^{k-2}) \\ &= p^k + p^{k-1} - 2p^{k-2}.\end{aligned}$$

Kun $p > 3$, niin $p^{k-1} > 3p^{k-2} > 2p^{k-2}$ ja täten $\Phi(p^k) \geq p^k + p^{k-1} - 2p^{k-2} > p^k + p^{k-1} - p^{k-1} > p^k$. Siis kaikki alkulukupotenssit, joiden kantana on kolmosta suurempi luku, eivät voi olla täydellisiä totienttilukuja ja lause on näin todistettu. □

Seuraus 3.14.1. *Alkulukupotenssi p^k on täydellinen totienttiluku, jos ja vain jos $p = 3$.*

Ollaan siis löydetty yksi ääretön joukko täydellisiä totienttilukuja. Seuraavaksi pyritään etsimään sellaisia täydellisiä totienttilukuja, jotka voidaan johtaa jostakin toisesta täydellisestä totienttiluvusta.

Lause 3.15. *Jos luku n on täydellinen totienttiluku ja $4n + 1$ alkuluku, niin $3(4n + 1)$ on myös täydellinen totienttiluku.*

Todistus. (Vrt. [4, s. 37]) Merkitään $m = 3(4n + 1)$ ja $r = R(n)$. Aloitetaan ottamalla phi-funktion arvo luvusta m. Koska funktio ϕ on multiplikatiivinen ja sekä 3 että $4n + 1$ ovat alkulukuja,

$$\phi(3(4n + 1)) = \phi(3) \cdot \phi(4n + 1) = 2 \cdot 4n = 8n.$$

Ottamalla phi-funktion arvo uudestaan saadaan taas multiplikatiivisuuden avulla $\phi_2(m) = \phi(8n) = \phi(8)\phi(n) = 4\phi(n)$, sillä n on täydellisenä totienttilukuna pariton. Lauseen 2.8 nojalla parilliselle q pätee, että $\phi(4q) = 4\phi(q)$. Hyödyntämällä tätä tietoa huomataan, että $\phi_k(4q) = 4\phi_k(q)$ aina kun $\phi_{k-1}(4q)$ on parillinen.

Koska $r = R(n)$, täytyy olla, että $\phi_{i-2}(n)$ on parillinen kun luvun i arvo on välillä $3 \leq i \leq r + 1$. Käyttämällä tätä tietoa ja tulosta $\phi_2(m) = 4\phi(n)$ saadaan, että

$$\phi_i(m) = \phi_{i-2}(\phi_2(m)) = \phi_{i-2}(4\phi(n)) = 4\phi_{i-2}(\phi(n)) = 4\phi_{i-1}(n) \tag{3.3}$$

Lisäksi huomataan, että $\phi_{r+2}(m) = \phi(\phi_{r+1}(m)) = \phi(4\phi_r(n)) = \phi(4 \cdot 1) = \phi(4) = 2$ ja edelleen $\phi_{r+3}(m) = \phi(\phi_{r+2}(m)) = \phi(2) = 1$ eli $R(m) = r + 3$. Nyt

voidaan näitä kaikkia tietoja hyväksi käyttäen laskea funktion arvo $\Phi(m)$:

$$\Phi(m) = \sum_{i=1}^{r+3} \phi_i(m) = \phi(m) + \sum_{i=2}^{r+1} \phi_i(m) + \phi_{r+2}(m) + \phi_{r+3}(m)$$
$$= 8n + \sum_{i=1}^{r} 4\phi_i(n) + 2 + 1 = 8n + 4\sum_{i=1}^{r} \phi_i(n) + 3.$$

Koska n on täydellinen totienttiluku, niin $\Phi(n) = \sum_{i=1}^{r} \phi_i(n) = n$, joten

$$\Phi(3(4n+1)) = \Phi(m) = 8n + 4n + 3 = 12n + 3 = 3(4n+1)$$

ja $m = 3(4n+1)$ on täten täydellinen totienttiluku. □

Huomataan, että taulukon 3 luku $183 = 3 \cdot 61$ on selitettävissä tämän lauseen avulla, sillä $61 = 4 \cdot 15 + 1$ on alkuluku ja luku 15 on täydellinen totienttiluku. Samoin tämän lauseen avulla selittyvät taulukon 3 luvut 471, 2199, 3063, 4359 ja 36759.

Nyt voidaan jokaisen täydellisen totienttiluvun n kohdalla yrittää johtaa siitä uutta täydellistä totienttilukua testaamalla, onko $4n + 1$ alkuluku. Toisaalta tiedetään jo, että jokainen kolmosen potenssi on täydellinen totienttiluku. Siispä voimme kirjoittaa seuraavan seurauksen.

Seuraus 3.15.1. *Jos* $4 \cdot 3^i + 1$*, missä* $i \in \mathbb{Z}_+$*, on alkuluku, niin* $4 \cdot 3^{i+1} + 3$ *on täydellinen totienttiluku.*

Esimerkki 3.3. Huomataan heti, että koska $4 \cdot 3^1 + 1 = 13$ on alkuluku, täytyy luvun $4 \cdot 3^2 + 3 = 39$ olla täydellinen totienttiluku. Voimme kirjoittaa lyhyen Mathematica-koodin, joka etsii täydellisiä totienttilukuja luvun i arvon vaihdellessa

```
For[i = 0, i < 20, i++, If[PrimeQ[4*3^i + 1],
                           Print[3*(4*3^i + 1)]]]
```

Tämä antaa meille täydelliset totienttiluvut 15, 39, 111, 327, 8751, 57395631 ja 172186887. Ensimmäiset viisi näistä löytyy jo taulukosta 3, mutta luvut 57395631 ja 172186887 ovat lauseen avulla löydettyjä.

Lauseessa 3.15 ollaan siis määritelty muotoa $3p$, missä p on pariton alkuluku, oleva täydellinen totienttiluku. Pyritään seuraavaksi tutkimaan tarkemmin tätä muotoa olevia täydellisiä totienttilukuja. Aloitetaan todistamalla lauseen 3.15 käänteinen tulos.

Lause 3.16. *Olkoon $n > 0$ pariton luku ja $4n+1$ alkuluku. Jos $3(4n+1)$ on täydellinen totienttiluku, niin samoin on luku n.*

Todistus. (Vrt. [6, s. 49]) Olkoon $3(4n+1)$ täydellinen totienttiluku. Siis $\Phi(3(4n+1)) = 3(4n+1)$. Samoin kuin lauseen 3.15 yhteydessä, saadaan tässäkin, että $\phi(3(4n+1)) = 8n$ ja $\phi_2(3(4n+1)) = 4\phi(n) = 2^2\phi(n)$ Koska $\phi(n)$ on parillinen luku, kun $n > 2$, lauseen 2.8 avulla saadaan $\phi_3(3(4n+1)) = \phi(2^2\phi(n)) = 2^2\phi_2(n)$. Samoin $\phi_{r+1}(3(4n+1)) = 2^2\phi_r(n)$, kun $r \leq R(n)$. Asetetaan $r = R(n)$, jolloin saadaan

$$\begin{aligned}
3(4n+1) &= \Phi(3(4n+1)) \\
12n+3 &= 8n + 2^2\phi(n) + 2^2\phi_2(n) + \cdots + 2^2\phi_r(n) + \phi(2^2) + \phi(2) \\
4n + (8n+3) &= 8n + 2^2(\phi(n) + \phi_2(n) + \cdots + \phi_r(n)) + 3 \\
4n &= 4(\phi(n) + \phi_2(n) + \cdots + \phi_r(n)) \\
n &= \Phi(n).
\end{aligned}$$

Siis n on täydellinen totienttiluku. □

Seuraavaksi todistetaan milloin muotoa $3p$ olevat luvut eivät ole täydellisiä totienttilukuja.

Lause 3.17. *Luku $3p$ ei ole täydellinen totienttiluku, jos luku p on muotoa $4n+3$ $(n > 0)$ oleva alkuluku.*

Todistus. (Vrt. [5, s. 101]) Olkoon $x = 3p$, missä $p = 4n+3$, $n > 0$, on alkuluku. Tällöin $\phi(x) = \phi(3p) = \phi(3)\phi(4n+3)$ ja koska $(3, 4n+3) = 1$, niin $\phi(3)\phi(4n+3) = 2(4n+2) = 2^2(2n+1)$. Toisen phi-funktion arvo saadaan samoin multiplikatiivisuuden avulla: $\phi_2(x) = \phi(2^2(2n+1)) = \phi(2^2)\phi(2n+1) = 2\phi(2n+1)$. Koska $\phi(2n+1)$ on phi-funktion arvona parillinen, voidaan jälleen käyttää lausetta 2.8 ja saadaan $\phi_3(x) = \phi(2\phi(2n+1)) = 2\phi_2(2n+1)$. Olkoon $r = R(2n+1)$. Tällöin

$$\begin{aligned}
\Phi(3p) &= 2^2(2n+1) + 2\phi(2n+1) + 2\phi_2(2n+1) + \cdots 2\phi_r(2n+1) + \phi(2) \\
&= 2^2(2n+1) + 2\Phi(2n+1) + 1.
\end{aligned}$$

Tehdään nyt vastaoletus, että luku $3p = 3(4n+3) = 12n+9$ on täydellinen totienttiluku. Tällöin $\Phi(3p) = 12n+9$ ja

$$\begin{aligned} 12n+9 &= 2^2(2n+1) + 2\Phi(2n+1) + 1 \\ (8n+5) + (4n+4) &= 8n+5+2\Phi(2n+1) \\ 2n+2 &= \Phi(2n+1). \end{aligned} \tag{3.4}$$

Mutta tiedetään, että funktion $\Phi(a)$ arvo on pariton kaikilla luvun a arvoilla. Toisaalta $2n+2$ on aina parillinen, joten yhtälö (3.4) ei voi pitää paikkaansa. Ollaan siis päädytty ristiriitaan eli $3p$ ei ole täydellinen totienttiluku, kun luku p on muotoa $4n+3$ oleva alkuluku. □

Lause 3.17 voitaisiin myös ilmaista seuraavassa muodossa: Luku $3p$ ei ole täydellinen totienttiluku, jos $p > 3$ on alkuluku, jolle pätee $p \equiv 3 \pmod 4$ (kts. [3, s. 2]). Toisaalta lauseessa 3.15 todistettiin, että $3p$ on täydellinen totienttiluku, jos $p = 4n+1$, missä n on myös täydellinen totienttiluku. Tällöin $p \equiv 1 \pmod 4$. Ollaan siis onnistuttu täydellisesti karakterisoimaan muotoa $3p$, missä p on pariton alkuluku, olevat täydelliset totienttiluvut seuraavasti: Olkoon $p > 3$ pariton alkuluku. Tällöin

$$\begin{cases} 3p \text{ ei ole täydellinen totienttiluku, jos } p \equiv 3 \pmod 4 \\ 3p \text{ on täydellinen totienttiluku,} & \text{jos ja vain jos } p = 4n+1, \text{ missä } n \text{ on} \\ & \text{täydellinen totienttiluku.} \end{cases}$$

3.3 Fermat'n alkulukuihin liittyvät täydelliset totienttiluvut

Tutkitaan seuraavaksi täydellisiä totienttilukuja, jotka voidaan löytää hyödyntämällä Fermat'n alkulukuja.

Lause 3.18. (Vrt. [4, s. 38]) *Olkoon luku k positiivinen. Jos $2^k - 1$ on täydellinen totienttiluku ja $2^k + 1$ (Fermat'n) alkuluku, niin*

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

on myös täydellinen totienttiluku.

Todistus. Jos $k = 1$, niin $2^{2\cdot 1} - 1 = 3$ on täydellinen totienttiluku. Oletetaan sitten, että $k > 1$. Tällöin jos $2^k + 1$ on alkuluku, niin $(2^k + 1, 2^k - 1) = 1$ ja

$$\phi((2^k - 1)(2^k + 1)) = \phi(2^k - 1)\phi(2^k + 1) = \phi(2^k - 1) \cdot 2^k.$$

Koska phi-funktion arvo $\phi(n)$ on parillinen aina, kun $n > 2$, voidaan soveltaa apulausetta 2.8 ja saadaan

$$\begin{aligned}\phi_2((2^k - 1)(2^k + 1)) &= \phi(\phi(2^k - 1) \cdot 2^k) = 2^k\phi(\phi(2^k - 1)) \\ &= 2^k\phi_2(2^k - 1)\end{aligned}$$

Näin jatkamalla huomataan, että $\phi_r((2^k-1)(2^k+1)) = \phi_r(2^k-1)\cdot 2^k$ kaikilla $r \leq R(2^k - 1)$. Asetetaan sitten $r = R(2^k - 1)$, jolloin

$$\phi_r((2^k - 1)(2^k + 1)) = 2^k\phi_r(2^k - 1) = 2^k \cdot 1 = 2^k.$$

Täten saadaan

$$\begin{aligned}\Phi((2^k - 1)(2^k + 1)) &= 2^k\phi(2^k - 1) + 2^k\phi_2(2^k - 1) + \cdots + 2^k\phi_r(2^k - 1) + \Phi(2^k) \\ &= 2^k(\phi(2^k - 1) + \phi_2(2^k - 1) + \cdots + \phi_r(2^k - 1)) + \Phi(2^k) \\ &= 2^k\Phi(2^k - 1) + \Phi(2^k).\end{aligned}$$

Lauseen 3.14 todistuksessa huomattiin, että $\Phi(2^k) = 2^k - 1$. Tätä huomiota ja sitä, että $2^k - 1$ on täydellinen totienttiluku, käyttämällä saadaan

$$\begin{aligned}\Phi((2^k - 1)(2^k + 1)) &= 2^k\Phi(2^k - 1) + \Phi(2^k) = 2^k(2^k - 1) + 2^k - 1 \\ &= 2^{2k} - 2^k + 2^k - 1 = 2^{2k} - 1.\end{aligned}$$

Siis $\Phi(2^{2k}-1) = \Phi((2^k-1)(2^k+1)) = 2^{2k}-1$ ja lause on täten todistettu. □

Lauseen 3.18 yhteydessä huomattiin jo, että $2^{2^{2^0}} - 1 = 3$ on täydellinen totienttiluku, mikä huomattiin myös lauseen 3.13 yhteydessä. Lauseen 3.18 avulla selittyvät myös taulukossa 3 olevat täydelliset totienttiluvut $15 = 2^4-1$ ja $255 = 2^8-1$. Koska $2^8+1 = 257$ on alkuluku, niin $(2^8+1)(2^8-1) = 2^{16}-1 = 65535$ on lauseen mukaan täydellinen totienttiluku. Myös ketjussa seuraava luku $2^{32} - 1 = 4294967295$ on täydellinen totienttiluku, koska $2^{16} + 1 = 65537$ on alkuluku. Tiedetään kuitenkin, että $2^{32} + 1 = 4294967297$ ei ole alkuluku, joten ketju päättyy ja tällä tavalla ei löydetä enää muita täydellisiä totienttilukuja.

Lause 3.19. *Olkoon $F_n = 2^{2^n}+1$ Fermat'n alkuluku ja $p = 2^a m+1$ alkuluku, missä m on täydellinen totienttiluku ja $a \geq 1$. Tällöin $F_n \cdot p$ on täydellinen totienttiluku, jos ja vain jos joko $n = 0$ ja $a = 2$ tai $a = m = n = 1$.*

Todistus. (Vrt. [5, s. 101]) Huomataan ensin, että F_n ja p ovat eri lukuja, sillä m on täydellisenä totienttilukuna pariton, joten se ei tietenkään voi olla mikään kakkosen potenssi ja $F_n = 2^{2^n} + 1 \neq 2^a m + 1 = p$.

Olkoon $x = F_n \cdot p$. Luvun x ensimmäisen phi-funktion arvo saadaan helposti, koska F_n ja p ovat eri alkulukuja:

$$\begin{aligned}\phi(x) &= \phi((2^{2^n}+1)(2^a m+1)) = \phi(2^{2^n}+1)\phi(2^a m+1) = 2^{2^n} \cdot 2^a m \\ &= 2^{2^n+a} m.\end{aligned}$$

Olkoon $R(m) = t$. Toisen phi-funktion arvo saadaan hyödyntämällä luvun m parittomuutta. Siitä eteenpäin iteroitujen phi-funktioiden arvot saadaan lauseen 2.8 ja tuloksen $\phi(2^y) = 2^{y-1}$ avulla:

$$\begin{aligned}\phi_2(x) &= \phi(2^{2^n+a} m) = \phi(2^{2^n+a})\phi(m) = 2^{2^n+a-1}\phi(m) \\ \phi_3(x) &= \phi(2^{2^n+a-1}\phi(m)) = 2^{2^n+a-1}\phi(\phi(m)) = 2^{2^n+a-1}\phi_2(m) \\ &\vdots \\ \phi_{t+1}(x) &= 2^{2^n+a-1}\phi_t(m) = 2^{2^n+a-1} \\ \phi_{t+2}(x) &= 2^{2^n+a-2} \\ \phi_{t+3}(x) &= 2^{2^n+a-3} \\ &\vdots \\ \phi_{R(x)} &= 2^0 = 1.\end{aligned}$$

Oletetaan nyt, että luku $x = F_n \cdot p$ on täydellinen totienttiluku. Tällöin summakaavaa $\sum_{i=0}^{i=2^n+a-2} 2^i = 2^{2^n+a-1} - 1$ ja tietoa, että luku m on täydellinen totienttiluku (eli $\Phi(m) = m$) käyttäen saadaan

$$\begin{aligned}x &= \Phi(x) \\ F_n \cdot p &= \Phi(x) \\ (2^{2^n}+1)(2^a m+1) &= 2^{2^n+a} m + 2^{2^n+a-1}\phi(m) + \cdots + 2^{2^n+a-1}\phi_t(m) \\ &\quad + 2^{2^n+a-2} + \cdots + 1\end{aligned}$$

$$2^{2^n+a}m + 2^{2^n} + 2^a m + 1 = 2^{2^n+a}m + 2^{2^n+a-1}\Phi(m) + 2^{2^n+a-1} - 1$$
$$2^{2^n+a}m + 2^{2^n} + 2^a m + 1 = 2^{2^n+a}m + 2^{2^n+a-1}m + 2^{2^n+a-1} - 1$$
$$2^{2^n} + 2^a m + 2 = 2^{2^n+a-1}(m+1)$$
$$2^{2^n-1} + 2^{a-1}m + 1 = 2^{2^n+a-2}(m+1). \tag{3.5}$$

Jos $a = 1$, niin yhtälöstä (3.5) saadaan

$$2^{2^n-1} + 2^0 m + 1 = 2^{2^n-1}(m+1)$$
$$1 = (2^{2^n-1} - 1)m,$$

joka pitää paikkansa vain, kun $m = n = 1$.

Oletetaan sitten, että $a \geq 2$. Jos $n \geq 1$, niin yhtälön (3.5) vasen puoli $2^{2^n-1} + 2^{a-1}m + 1 = 2(2^{2^n-2} + 2^{a-2}m) + 1$ on pariton, mutta oikea puoli $2^{2^n+a-2}(m+1) = 2(2^{2^n+a-3}(m+1))$ on parillinen, mikä on tietenkin mahdontonta. Siis $n = 0$. Mutta jos $n = 0$, niin yhtälöstä (3.5) seuraa, että

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

eli $a = 2$.

Käänteinen implikaatio saadaan helposti sijoittamalla annetut arvot. Jos $n = 0$ ja $a = 2$, saadaan $F_n \cdot p = 3(4m+1)$, joka todistettiin lauseessa 3.15 täydelliseksi totienttiluvuksi. Jos taas $a = m = n = 1$, niin $F_n \cdot p = 5 \cdot 3 = 15$, joka on jo aiemmin useaan otteeseen huomattu täydelliseksi totienttiluvuksi. □

Edellisen lauseen parametreissä myös luku 1 laskettiin täydelliseksi totienttiluvuksi ($m = 1$), mutta yleensä määritellään, että $R(1) = 0$, jolloin $\Phi(1) = 0$ ja luku 1 ei ole täydellinen totienttiluku (kts. [4, s. 36]).

Lause 3.20. *Olkoon $F_n = 2^{2^n}+1$ Fermat'n alkuluku ja $p = 2^a \cdot F_n + 1$ alkuluku. Tällöin $(F_{n+1})^4 \cdot p$ on täydellinen totienttiluku, jos ja vain jos $n = 0$ ja $a = 1$.*

Todistus. (Vrt. [5, s. 102]) Olkoon $x = (F_{n+1})^4 \cdot p$. Tutkitaan aluksi luvusta x sen phi-funktiota iteroimalla saatavia arvoja. Koska $(F_{n+1}, p) = 1$, saadaan multiplikatiivisuuden nojalla

$$\phi(x) = \phi((F_{n+1})^4 \cdot p) = \phi((F_{n+1})^4) \cdot \phi(p).$$

Koska F_{n+1} on alkuluku, kun $n < 4$, voidaan sen phi-funktion arvo laskea helposti ja

$$\begin{aligned}\phi((F_{n+1})^4) \cdot \phi(p) &= ((F_{n+1})^3 \cdot (F_{n+1} - 1)) \cdot 2^a F_n \\ &= ((F_{n+1})^3 \cdot (2^{2^{n+1}})) \cdot 2^a F_n \\ &= 2^{2 \cdot 2^n + a} (F_{n+1})^3 F_n.\end{aligned}$$

Nyt koska 2, F_{n+1} ja F_n ovat kaikki eri alkulukuja, voidaan jälleen soveltaa phi-funktion multiplikatiivisuutta seuraavien phi-funktioiden arvojen etsinnässä:

$$\begin{aligned}\phi_2(x) &= \phi(2^{2 \cdot 2^n + a} (F_{n+1})^3 F_n) = \phi(2^{2 \cdot 2^n + a}) \phi((F_{n+1})^3) \phi(F_n) \\ &= 2^{2 \cdot 2^n + a - 1} (F_{n+1})^2 (F_{n+1} - 1)(F_n - 1) \\ &= 2^{2 \cdot 2^n + a - 1} (F_{n+1})^2 2^{2^{n+1}} \cdot 2^{2^n} = 2^{5 \cdot 2^n + a - 1} (F_{n+1})^2 \\ \phi_3(x) &= 2^{5 \cdot 2^n + a - 2} F_{n+1} (F_{n+1} - 1) = 2^{7 \cdot 2^n + a - 2} F_{n+1} \\ \phi_4(x) &= 2^{9 \cdot 2^n + a - 3}.\end{aligned}$$

Tämän jälkeen phi-funktion ottaminen seuraavista luvuista vähentää luvun kaksi potenssia kunnes saavutetaan luku yksi. Olettamalla nyt, että x on täydellinen totienttiluku saadaan

$$\begin{aligned} x &= \Phi(x) \\ (F_{n+1})^4 \cdot p &= 2^{2 \cdot 2^n + a} (F_{n+1})^3 F_n + 2^{5 \cdot 2^n + a - 1} (F_{n+1})^2 \\ &\quad + 2^{7 \cdot 2^n + a - 2} F_{n+1} + 2^{9 \cdot 2^n + a - 3} + \cdots + 1 \\ 2^a (F_{n+1})^4 F_n + (F_{n+1})^4 &= 2^{2 \cdot 2^n + a} (F_{n+1})^3 F_n + 2^{5 \cdot 2^n + a - 1} (F_{n+1})^2 \\ &\quad + 2^{7 \cdot 2^n + a - 2} F_{n+1} + 2^{9 \cdot 2^n + a - 2} - 1. \end{aligned} \tag{3.6}$$

Huomataan, että $F_n = 2^{2^n} + 1 \equiv 1 \pmod{2^{2^n}}$ ja samoin myös $F_{n+1} = (2^{2^n \cdot 2} + 1) \equiv 1 \pmod{2^{2^n}}$. Tällöin nähdään, että yhtälön (3.6) vasen puoli on kongruentti luvun $2^a + 1$ ja oikea puoli luvun -1 kanssa modulo 2^{2^n}. Kongruenssin laskusääntöjä soveltamalla saadaan

$$\begin{aligned} 2^a + 1 &\equiv -1 \pmod{2^{2^n}} \\ 2^a + 2 &\equiv 0 \pmod{2^{2^n}} \\ 2(2^{a-1} + 1) &\equiv 0 \pmod{2^{2^n}}. \end{aligned}$$

Siis 2^{2^n} jakaa luvun 2, mikä on mahdollista vain, kun $n = 0$. Sijoittamalla $n = 0$ yhtälöön (3.6) saadaan

$$2^a 5^4 \cdot 3 + 5^4 = 2^{2+a} 5^3 \cdot 3 + 2^{4+a} 5^2 + 2^{5+a} 5 + 2^{7+a} - 1,$$

josta päästään sieventämällä lopputulokseen $2^a = 2$ eli $a = 1$. Siis jos $(F_{n+1})^4 \cdot p$ on täydellinen totienttiluku, niin $n = 0$ ja $a = 1$. Käänteinen implikaatio seuraa triviaalisti sijoittamalla. □

Lauseen 3.20 avulla saadaan täydellinen totienttiluku $(F_{0+1})^4 \cdot (2F_0 + 1) = 5^4 \cdot 7 = 4375$, joka on taulukon 3 ainoa luvulla kolme jaoton täydellinen totienttiluku.

Lause 3.21. *Olkoon $F_n = 2^{2^n} + 1$ Fermat'n alkuluku ja $p = 2^a F_{n+1} + 1$ alkuluku. Tällöin $F_n \cdot p^2$ on täydellinen totienttiluku, jos ja vain jos $n = 0$ ja $a = 1$.*

Todistus. (Vrt. [5, s. 103]) Olkoon $x = F_n \cdot p^2$. Tutkitaan taas aluksi luvusta x phi-funktiota iteroimalla saatavia arvoja. Koska $(F_n, p) = 1$, voidaan jälleen soveltaa phi-funktion multiplikatiivisuutta ensimmäisen phi-funktion arvon laskemiseksi:

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

Nyt nähdään, että $(2, F_{n+1}, (2^a F_{n+1} + 1)) = 1$, joten seuraavat phi-funktion arvot saadaan myösi multiplikatiivisuuden avulla:

$$\begin{aligned}\phi_2(x) &= \phi(2^{2^n+a} F_{n+1}(2^a F_{n+1} + 1)) = \phi(2^{2^n+a})\phi(F_{n+1})\phi(2^a F_{n+1} + 1) \\ &= 2^{2^n+a-1} 2^{2^{n+1}} 2^a F_{n+1} = 2^{3 \cdot 2^n + 2a - 1} F_{n+1} \\ \phi_3(x) &= \phi(2^{3 \cdot 2^n + 2a - 1})\phi(F_{n+1}) = 2^{3 \cdot 2^n + 2a - 2} \cdot 2^{2^{n+1}} = 2^{5 \cdot 2^n + 2a - 2}.\end{aligned}$$

Jälleen tästä eteenpäin phi-funktion ottamien pienentää kakkosen potenssia yhdellä kunnes saavutetaan $2^0 = 1$. Oletetaan nyt, että x on täydellinen

totienttiluku, jolloin summakaavaa soveltamalla saadaan

$$\begin{aligned} x &= \Phi(x) \\ F_n \cdot p^2 &= 2^{2^n+a} F_{n+1}(2^a F_{n+1} + 1) + 2^{3\cdot 2^n + 2a - 1} F_{n+1} + 2^{5\cdot 2^n + 2a - 2} \\ &\quad + \cdots + 1 \end{aligned}$$

(3.7)
$$F_n(2^a F_{n+1} + 1)^2 = 2^{2^n+a} F_{n+1}(2^a F_{n+1} + 1) + 2^{3\cdot 2^n + 2a - 1} F_{n+1} + 2^{5\cdot 2^n + 2a - 1} - 1.$$

Lauseessa 3.20 huomattiin, että $F_n \equiv F_{n+1} \equiv 1 \pmod{2^{2^n}}$. Tätä faktaa soveltamalla nähdään, että yhtälön (3.7) vasen puoli on kongruentti luvun $2^{2a} + 2^{a+1} + 1$ ja oikea puoli luvun -1 kanssa modulo 2^{2^n}. Saadaan siis, että $2(2^{2a-1} + 2^a + 1) \equiv 0 \pmod{2^{2^n}}$ eli luku 2 on jaollinen luvulla 2^{2^n}. Siis $n = 0$. Sijoittamalla tämä yhtälöön (3.7) saadaan

$$3 \cdot (2^a \cdot 5 + 1)^2 = 2^{1+a} \cdot 5(2^a \cdot 5 + 1) + 2^{2+2a} \cdot 5 + 2^{4+2a} - 1,$$

joka sievenee toisen asteen yhtälöksi luvun 2^a suhteen:

$$11 \cdot (2^a)^2 - 20 \cdot 2^a - 4 = 0.$$

Tämän yhtälön ainoa kokonaislukuratkaisu on $2^a = 2$ eli $a = 1$. Ollaan siis todistettu, että jos $x = F_n \cdot p^2$ on täydellinen totienttiluku, niin $n = 0$ ja $a = 1$.

Oletetaan sitten kääntäen, että $n = 0$ ja $a = 1$. Tällöin saadaan $F_0 \cdot p^2 = F_0(2F_{0+1} + 1)^2 = 3 \cdot 11^2 = 363$, jonka tiedetään olevan täydellinen totienttiluku. □

3.4 Muotoa $3^k p$ olevat täydelliset totienttiluvut

Edellisessä luvussa huomattiin, että jokainen kolmosen potenssi on täydellinen totienttiluku. Lisäksi lauseessa 3.15 osoitettiin. että muotoa $3p$, oleva luku on täydellinen totienttiluku, jos luku $p = 4n + 1$, missä n on täydellinen totienttiluku. Tässä alaluvussa yritetään etsiä täydellisiä totienttilukuja, jotka ovat muotoa $3^k p$, missä p on alkuluku ja $k \geq 2$.

Käydään läpi muutamia riittäviä ehtoja sille, että luku $3^k p$ on täydellinen totienttiluku.

Lause 3.22. *Jos luku* $p = 2 \cdot 3^2 q + 1$ *on alkuluku siten, että* $q = 2^5 3^n + 1$ *on myös alkuluku, niin* $3^2 p$ *on täydellinen totienttiluku.*

Todistus. (Vrt. [5, s. 103]) Olkoon $x = 3^2 p = 3^2 \cdot (2 \cdot 3^2 (2^5 3^n + 1) + 1)$, missä luvut $p = 2 \cdot 3^2 (2^5 3^n + 1) + 1$ ja $q = 2^5 3^n + 1$ ovat alkulukuja. Koska $(3^2, p) = 1$, voidaan soveltaa phi-funktion multiplikatiivisuutta ensimmäisen ϕ-funktion arvon saamiseksi:

$$\begin{aligned} \phi(x) &= \phi(3^2 p) = \phi(3^2)\phi(p) = 2 \cdot 3(2 \cdot 3^2 (2^5 3^n + 1)) \\ &= 2^2 3^3 (2^5 3^n + 1). \end{aligned}$$

Nyt koska $2^5 \cdot 3^n + 1$ on alkuluku, niin $(2^2 3^3, 2^5 \cdot 3^n + 1) = 1$, joten apulauseen 2.9 ja multiplikatiivisuuden avulla saadaan

$$\phi_2(x) = \phi(2^2 3^3)\phi(2^5 \cdot 3^n + 1) = 2^2 3^2 (2^5 \cdot 3^n) = 2^7 \cdot 3^{n+2}.$$

Muiden phi-funktion iteroitujen arvojen laskeminen onnistuu nyt helposti soveltamalla apulausetta 3.10:

$$\Phi(2^7 3^{n+2}) = 2^6 (3^{n+2} + 1) - 1 = 2^6 3^{n+2} + 2^6 - 1.$$

Nyt laskemalla saadut arvot yhteen saadaan luvun x Φ-funktion arvo:

$$\begin{aligned} \Phi(x) &= 2^2 3^3 (2^5 3^n + 1) + 2^7 3^{n+2} + 2^6 3^{n+2} + 2^6 - 1 \\ &= 2^7 3^{n+3} + 2^2 3^3 + (2^7 + 2^6) 3^{n+2} + 2^6 - 1 \\ &= 2^7 3^{n+3} + (3 \cdot 2^6) 3^{n+2} + 2^2 3^3 + 3^2 \cdot 7 \\ &= 2^7 3^{n+3} + 2^6 3^{n+3} + 2^2 3^3 + 3^2 \cdot 7 \\ &= (2^7 + 2^6) 3^{n+3} + (2^2 \cdot 3 + 7) 3^2 \\ &= (3 \cdot 2^6) 3^{n+3} + (2 \cdot 3^2 + 1) 3^2 \\ &= 2^6 3^{n+4} + 2 \cdot 3^4 + 3^2 \\ &= 3^2 (2^6 3^{n+2} + 2 \cdot 3^2 + 1) \\ &= 3^2 (2 \cdot 3^2 (2^5 3^n + 1) + 1) \\ &= x. \end{aligned}$$

Siis x on täydellinen totienttiluku ja lause on täten todistettu. □

Asettamalla luvun n arvoksi 1 saadaan edellisessä lauseessa aikaiseksi alkuluvut $q = 2^5 \cdot 3^1 + 1 = 97$ ja $p = 2 \cdot 3^2 \cdot 97 + 1 = 1747$, jolloin $3^2 \cdot 1747 = 15723$ on täydellinen totienttiluku.

Lause 3.23. *Jos luku $p = 2^2 q + 1$ on alkuluku siten, että $q = 2^4 3^n + 1$ on myös alkuluku, niin $3^3 p$ on täydellinen totienttiluku.*

Todistus. (Vrt. [5, s. 104]) Olkoon $x = 3^3 p = 3^3(2^2(2^4 3^n + 1) + 1)$, missä luvut $p = 2^2(2^4\ 3^n + 1) + 1$ ja $q = 2^4 3^n + 1$ ovat alkulukuja. Koska $(3^3, p) = 1$, voidaan ensimmäinen luvun x phi-funktion arvo selvittää multiplikatiivisuuden avulla:

$$\begin{aligned}\phi(x) &= \phi(3^3 p) = \phi(3^3)\phi(p) = \phi(3^3)\phi(2^2(2^4 3^n + 1) + 1) \\ &= 2 \cdot 3^2(2^2(2^4 3^n + 1)) = 2^3 3^2(2^4 3^n + 1).\end{aligned}$$

Koska $q = 2^4 3^n + 1$ on alkuluku, voidaan seuraavaan phi-funktion arvo laskea käyttämällä lausetta 2.9 ja multiplikatiivisuutta:

$$\begin{aligned}\phi_2(x) &= \phi(2^3 3^2(2^4 3^n + 1)) = \phi(2^3 3^2)\phi(2^4 3^n + 1) \\ &= 2^3 \cdot 3(2^4 3^n) = 2^7 3^{n+1}.\end{aligned}$$

Loput phi-funktioiden arvot saadaan käyttämällä apulausetta 3.10:

$$\Phi(2^7 3^{n+1}) = 2^6(3^{n+1} + 1) - 1 = 2^6 3^{n+1} + 2^6 - 1.$$

Tällöin funktion $\Phi(x)$ arvoksi saadaan

$$\begin{aligned}\Phi(x) &= 2^3 3^2(2^4 3^n + 1) + 2^7 3^{n+1} + 2^6 3^{n+1} + 2^6 - 1 \\ &= 2^7 3^{n+2} + 2^3 3^2 + (2^7 + 2^6)3^{n+1} + 2^6 - 1 \\ &= 2^7 3^{n+2} + 2^6 3^{n+2} + 2^3 3^2 + 3^2 \cdot 7 \\ &= (2^7 + 2^6)3^{n+2} + (2^3 + 7)3^2 \\ &= 2^6 3^{n+3} + (2^2 \cdot 3 + 3)3^2 \\ &= 2^6 3^{n+3} + 2^2 3^3 + 3^3 \\ &= 3^3(2^2(2^4 3^n + 1) + 1) \\ &= x.\end{aligned}$$

Koska $\Phi(x) = x$, luku x on täydellinen totienttiluku ja lause on täten todistettu. □

Sijoittamalla $n = 3$ lauseen 3.23 parametreihin saadaan alkuluvut $q = 2^4 \cdot 3^3 + 1 = 433$ ja $p = 2^2 \cdot 433 + 1 = 1733$, joten luku $3^3 \cdot 1733 = 46791$ on täydellinen totienttiluku. Samoin jos $n = 4$ huomataan, että luvut $q = 2^4 \cdot 3^4 + 1 = 1297$ ja $p = 2^2 \cdot 1297 + 1 = 5189$ ovat alkulukuja, joten $3^3 \cdot 5189 = 140103$ on täydellinen totienttiluku.

Lause 3.24. *Olkoon luku n ei-negatiivinen. Jos r, q ja p, kuten alla, ovat alkulukuja, niin 3^2p on täydellinen totienttiluku:*

1. *$r = 2^4 3^n + 1$, $q = 2 \cdot 3r + 1$ ja $p = 2 \cdot 3q + 1$;*
2. *$r = 2 \cdot 3^n + 1$, $q = 2^3 r + 1$ ja $p = 2q + 1$;*
3. *$r = 2^2 3^n + 1$, $q = 2^3 \cdot 3r + 1$ ja $p = 2q + 1$.*

Todistus. (Vrt. [3, s. 3]) (Osa 1) Sijoittamalla saadaan

$$\begin{aligned}
3^2p &= 3^2(2 \cdot 3q + 1) = 2 \cdot 3^3 q + 3^2 \\
&= 2 \cdot 3^3(2 \cdot 3r + 1) + 3^2 = 2^2 3^4 r + 3^2(2 \cdot 3 + 1) \\
&= 2^2 3^4(2^4 3^n + 1) + 3^2(2 \cdot 3 + 1) = 2^6 3^{n+4} + 2^2 3^4 + 3^2(2 \cdot 3 + 1) \\
&= 2^6 3^{n+4} + 3^2(2^2 3^2 + 2 \cdot 3 + 1) = 2^6 3^{n+4} + 9(36 + 6 + 1) \\
&= 2^6 3^{n+4} + 387.
\end{aligned}$$

Oletetaan, että p, q ja r ovat kaikki (kolmosta suurempia) alkulukuja, jolloin saadaan multiplikatiivisuuden ja lauseen 2.9 avulla, että

$$\begin{aligned}
\phi(3^2p) &= \phi(3^2)\phi(p) = 2 \cdot 3(p-1) = 2 \cdot 3(2 \cdot 3q) = 2^2 3^2 q \\
\phi_2(3^2p) &= \phi(2^2 3^2 q) = \phi(2^2 3^2)\phi(q) = 2^2 3(q-1) = 2^3 3^2 r \\
\phi_3(3^2p) &= \phi(2^3 3^2 r) = \phi(2^3 3^2)\phi(r) = 2^3 3(r-1) = 2^7 3^{n+1}.
\end{aligned}$$

Lausetta 2.9 ja ominaisuutta $\phi(2^a) = 2^{a-1}$ soveltamalla saadaan loput phi-funktion arvot laskettaessa funktion $\Phi(3^2p)$ arvoa. Siis

$$\begin{aligned}
\Phi(3^2p) &= 2^2 3^2 q + 2^3 3^2 r + 2^7 3^{n+1} + 2^7 3^n + 2^7 3^{n-1} + \cdots + 2^7 3 + 2^7 + 2^6 + \cdots + 1 \\
&= 2^2 3^2(2 \cdot 3r + 1) + 2^3 3^2(2^4 3^n + 1) + 2^7(3^{n+1} + \cdots + 3 + 1) + 2^7 - 1 \\
&= 2^3 3^3(2^4 3^n + 1) + 2^7 3^{n+2} + 2^7(3^{n+1} + \cdots + 3 + 1) + 127 + 2^2 3^2 + 2^3 3^2 \\
&= 2^7 3^{n+3} + 2^7 3^{n+2} + 2^7(3^{n+1} + \cdots + 3 + 1) + 235 + 2^3 3^3 \\
&= 2^7(3^{n+3} + 3^{n+2} + \cdots + 3 + 1) + 451.
\end{aligned}$$

Nyt voidaan hyödyntää summakaavaa $\sum_{i=0}^{n+3} 3^i = \frac{3^{n+4}-1}{3-1}$, jolloin saadaan

$$\begin{aligned}\Phi(3^2p) &= 2^7\frac{3^{n+4}-1}{3-1} + 451\\ &= 2^6 3^{n+4} + 387\\ &= 3^2p\end{aligned}$$

eli 3^2p on täydellinen totienttiluku. Osien 2 ja 3 todistukset saadaan lähes täysin samalla tavalla ja sen takia ne sivuutetaan tässä. □

Asettamalla $n = 0$ edellisen lauseen osan 1 parametreihin saadaan luvut $r = 2^4 3^0 + 1 = 17$, $q = 2 \cdot 3 \cdot 17 + 1 = 103$ ja $p = 2 \cdot 3 \cdot 103 + 1 = 619$, jotka ovat kaikki alkulukuja. Tällä tavoin löydetään täydellinen totienttiluku $3^2 \cdot 619 = 5571$. Tietokoneen avulla pystytään helposti tutkimaan löytyykö lisää täydellisiä totienttilukuja, kun luvun n arvo kasvaa. Huomataan, että lukua 3000 pienemmillä luvun n arvoilla ei löydy enempää täydellisiä totienttilukuja. Samoin tietokonehaulla tutkimalla selviää, että lauseen 3.24 osien 2 ja 3 avulla ei löydy täydellisiä totienttilukuja, kun $n \leq 3000$. [3, s. 3]

Esitetään vielä yksi riittävä ehto sille, että luku 3^2p on täydellinen totienttiluku ja kaksi riittävää ehtoa sille, että luku 3^3p on täydellinen totienttiluku. Seuraavien lauseiden todistukset ovat hyvin samankaltaisia kuin jo esitettyjen lauseiden, joten ne sivuutetaan tässä.

Lause 3.25. (Vrt. [3, s. 3]) *Olkoon $n \geq 0$. Jos $q = 2^3 3^n + 1$ ja $p = 2q + 1$ ovat molemmat alkulukuja, niin 3^2p on täydellinen totienttiluku.*

Lause 3.26. (Vrt. [3, s. 3]) *Olkoon $n \geq 0$. Jos $r = 2^2 3^n + 1$, $q = 2^4 r + 1$ ja $p = 2^2 q + 1$ ovat kaikki alkulukuja, niin 3^3p on täydellinen totienttiluku.*

Lause 3.27. (Vrt. [3, s. 4]) *Olkoon $n \geq 0$. Jos $s = 2^5 3^n + 1$, $r = 2 \cdot 3^2 s + 1$, $q = 2^4 3r + 1$ ja $p = 2^2 q + 1$ ovat kaikki alkulukuja, niin 3^3p on täydellinen totienttiluku.*

Lauseiden 3.25 ja 3.26 avulla ei löydy täydellisiä totienttilukuja, kun $n \leq 3000$. Jos $n = 1$ lauseessa 3.27, saadaan luvut $s = 2^5 3 + 1 = 97$, $r = 2 \cdot 3^2 \cdot 97 + 1 = 1747$, $q = 2^4 3 \cdot 1747 + 1 = 83857$ ja $p = 2^2 \cdot 83857 + 1 = 335429$, jotka ovat kaikki alkulukuja. Tällöin $3^3 \cdot 335429 = 9056583$ on täydellinen totienttiluku. Muita täydellisiä totienttilukuja lauseella 3.27 ei löydy, kun $n \leq 2000$. [3, s.4]

3.5 Yhteenveto ja supertäydelliset totienttiluvut

Kootaan vielä lopuksi tässä tutkielmassa esitetyt täydelliset totienttiluvut taulukkoon, josta näkyy, miten kukin täydellinen totienttiluku on löydetty.

Taulukko 4: Yhteenveto täydellisistä totienttiluvuista

Täydelliset totienttiluvut	Selitys
3^k	Lause 3.13
$183, 471, 2199, 3063, 4359, 36759$	Lause 3.15
$15, 39, 111, 327, 8751, 57395631, 172186887$	Seuraus 3.15.1
$15, 255, 65535, 4294967295$	Lause 3.18
4375	Lause 3.20
363	Lause 3.21
15723	Lause 3.22
$46791, 140103$	Lause 3.23
5571	Lause 3.24(1.)

Taulukosta 4 nähdään, että ollaan onnistuttu selittämään kaikki taulukossa 3 esitetyt lukua 40000 pienemmät täydelliset totienttiluvut jollakin lauseella. Lisäksi on löydetty useita lukua 40000 suurempia täydellisiä totienttilukuja.

Määritellään vielä tämän tutkielman lopuksi täydellisistä totienttiluvuista johdettavissa oleva supertäydellisten totienttilukujen käsite.

Määritelmä 3.2. (Vrt. [5, s. 104]) Olkoon n positiivinen luku. Lukua n kutsutaan *supertäydelliseksi totienttiluvuksi* (engl. *super perfect totient number*, lyh. SPTN), jos kaikki sen jakajat ovat täydellisiä totienttilukuja.

Supertäydelliset totienttiluvut ovat helposti karakteroitavissa seuraavan lauseen avulla.

Lause 3.28. *Luku n on supertäydellinen totienttiluku, jos ja vain jos se on kolmosen potenssi eli $n = 3^k$ jollakin luvun $k > 0$ arvolla.*

Todistus. (Vrt. [5, s. 104]) Oletetaan aluksi, että luku n on muotoa 3^k, $k > 0$. Tällöin tietysti luvun n kaikki jakajat ovat myös kolmosen potensseja.

Lauseen 3.13 mukaan kaikki kolmosen potenssit ovat täydellisiä totienttilukuja, joten luku n on supertäydellinen totienttiluku.

Oletetaan sitten kääntäen, että luku n on supertäydellinen totienttiluku. Koska kaikki täydelliset totienttiluvut ovat parittomia ja luku n on täydellisten totienttilukujen tulo, täytyy luvun n olla myös pariton. Tällöin luku n on muotoa $p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \cdots \cdot p_r^{a_r}$, missä luvut p_i, $i = 1, 2, \ldots, r$, ovat parittomia alkulukuja. Voidaan olettaa, että $p_1 < p_2 < \cdots < p_r$. Jos $r \geq 2$, tiedetään, että $p_2 \geq 5$. Koska $p_2^{a_2}$ on luvun n jakaja, täytyy sen olla täydellinen totienttiluku. Mutta lauseessa 3.14 osoitettiin, että mikään kolmosesta eroava alkulukupotenssi ei voi olla täydellinen totienttiluku. Ollaan siis päädytty ristiriitaan ja täten $r = 1$. Nyt, koska $n = p_1^{a_1}$, täytyy seurauksen 3.14.1 mukaan luvun p_1 olla 3. Siis luku n on luvun kolme potenssi ja lause on täten todistettu. □

Viitteet

[1] Burton, David M. *Elementary Number Theory - Fifth Edition*. McGraw-Hill. New York. 2005.

[2] Rosen, Kenneth H. *Elementary Number Theory and Its Applications - Fourth Edition*. Pearson/Addison-Wesley. United States. 2000.

[3] Iannucci, Douglas E.; Moujie, Deng & Cohen, Graeme L. *On Perfect Totient Numbers*. J. Integer Seq. Vol. 6, 2003. s. 1-6.

[4] Loomis, Paul; Plytage, Michael & Polhill, John. *Summing Up the Euler ϕ Function*. College Math. J. Vol. 39, 2008. s. 34-42.

[5] Mohan, A. L. & Suryanarayana D. *Perfect totient numbers*. Number theory (Mysore, 1981), Lecture Notes in Math., 938, Springer, Berlin-New York, 1982. s.101-105.

[6] Pérez Cacho, L. *Sobre la Suma de Indicadores de Ordenes Sucesivos*. Revista Matematica Hispano-Americana Vol. 1, 1939. s. 45-50.

[7] Pillai, S. Sivasankaranarayana. *On a function connected with $\phi(n)$*. Bull. Amer. Math. Soc. Vol. 35, 1929. s. 837-841.

[8] Shapiro, Harold. *An Arithmetic Function Arising From the ϕ Function*. Amer. Math. Monthly. Vol. 50, 1943. s. 18-30.