Tampereen yliopisto

Kalle Korkeamäki

Alkulukukaksosten karakterisoinnista

Informaatioteknologian ja viestinnän tiedekunta
Pro gradu -tutkielma
Toukokuu 2019

TIIVISTELMÄ

Kalle Korkeamäki: Alkulukukaksosten karakterisoinnista
Pro gradu -tutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Toukokuu 2019

Tämä pro gradu -tutkielma käsittelee alkulukukaksosten eli sellaisten alkulukujen, joiden etäisyys toisistaan on 2, karakterisointeja. Aluksi esitellään alkulukukaksosten määritelmä sekä tutustutaan alkulukukaksosten historiaan. Seuraavaksi käydään läpi tarvittavat esitiedot karakterisointien esittämiseksi niin, että ensin esitellään kongruenssituloksia ja sitten multiplikatiivisiin funktioihin liittyviä tuloksia. Multiplikatiivisista funktioista tutustutaan Eulerin phi-funktioon ja tekijäfunktioon. Lopuksi esitellään sekä kongruensseihin että multiplikatiivisiin funktioihin perustuvia karakterisointeja siten, että kongruensseihin perustuvia karakterisointeja esitellään ensin ja niiden jälkeen esitellään multiplikatiivisiin funktioihin perustuvia karakterisointeja.

Avainsanat: alkuluku, alkulukukaksoset, kongruenssi, lukuteoria, multiplikatiivinen funktio

Sisältö

1 Johdanto

Tässä pro gradu -tutkielmassa tarkastellaan alkulukukaksosten eli sellaisten alkulukujen, joiden etäisyys toisistaan on 2, karakterisointeja. Luvussa 2 käsitellään lyhyesti alkulukukaksosten historiaa. Luvussa 3 esitellään tutkielman pääsisältöä varten tarvittavia määritelmiä ja lauseita. Alaluvussa 3.1 esitellään muutamia erityisiä kongruensseja. Alaluvussa 3.2 käsitellään Eulerin phi-funktioon ja tekijäfunktioon liittyviä tuloksia. Luvussa 4 esitellään erilaisia alkulukukaksosten karakterisointeja siten, että alaluvussa 4.1 käsitellään kongruenssirelaatiota hyödyntäviä karakterisointeja ja alaluvussa 4.2 multiplikatiivisten funktioiden ominaisuuksia hyödyntäviä karakterisointeja.

Lukijan oletetaan tuntevan lukuteorian perusteet. Tästä syystä kolmannessa luvussa sivuutetaan Tampereen yliopiston Algebra 1 -kurssilta entuudestaan tutut todistukset ja esittelemättä jätetään muun muassa kongruensseihin, alkulukuihin ja jaollisuuteen liittyvät peruslauseet. Historiaa käsittelevässä luvussa 2 on käytetty lähteinä artikkeleita [11] ja [5]. Multiplikatiivisten funktioiden perustuloksia käsittelevässä alaluvussa 3.2 lähteenä toimii Rosenin oppikirja [12]. Tutkielman luonteesta johtuen kuitenkaan varsinaisia päälähteitä ei voida nimetä, sillä esitellyt karakterisoinnit sekä näihin liittyvät aputulokset ovat peräisin useista lähteistä.

Kaikki tässä tutkielmassa käsiteltävät luvut ovat kokonaislukuja, ellei toisin erikseen mainita. Selvyyden vuoksi tutkielmassa on kuitenkin pyritty ilmoittamaan kunkin luvun yhteydessä, mihin lukujoukkoon luku kuuluu.

2 Alkulukukaksosten määritelmä ja historiaa

Tässä luvussa tutustutaan alkulukukaksosten historiaan. Lähteinä on käytetty katsausartikkelia [11] sekä artikkelia [5].

Määritelmä 2.1. Alkulukuja p_1 ja p_2 kutsutaan *alkulukukaksosiksi*, jos $|p_1 - p_2| = 2$.

Vaikka alkulukukaksosten käsitteen kehittäjänä pidetään 1800- ja 1900-luvun taitteessa elänyttä saksalaista matemaatikkoa Paul Stäckeliä, alkulukukaksosten historia ulottuu huomattavasti niiden nimeämistä kauemmas. Jo antiikin Kreikassa noin vuoden 300 eaa. tietämillä Eukleides otaksui, että on olemassa äärettömästi alkulukukaksosia. Toinen tunnettu alkulukukaksosiin liittyvä otaksuma on Eukleideen otaksumaa yleisempi Alphonse de Polignacin (1826–1863) otaksuma.

Otaksuma 2.1 (Polignacin otaksuma)**.** Jokaista positiivista kokonaislukua k kohden on olemassa äärettömän monta sellaista alkulukua p, että myös $p + 2k$ on alkuluku ja että välillä $[p, p + 2k]$ ei ole muita alkulukuja (eli p ja $p + 2k$ ovat peräkkäisiä alkulukuja).

Kun $k = 1$, saadaan otaksuma alkulukukaksosista. Koska ongelmaa alkulukukaksosten määrän äärettömyydestä tai äärellisyydestä ei ole ratkaistu, myöskään Polignacin otaksumaa ei ole osoitettu oikeaksi eikä vääräksi. Tietoa alkulukukaksosista on kuitenkin onnistuttu saamaan muun muassa tarkastelemalla, minkälaisia välttämättömiä ja riittäviä ehtoja kahden peräkkäisen parittoman kokonaisluvun tulee täyttää ollakseen alkulukukaksosia. Tunnetuin alkulukukaksosten karakterisointi lienee Wilsonin lauseeseen nojautuva Clementin lause vuodelta 1949 (ks. tämän tutkielman lause 4.1). Toinen kirjallisuudessa usein esiintyvä karakterisointi on Leavittin ja Mullinin karakterisointi vuodelta 1981 (ks. tämän tutkielman lause 4.8).

Alkulukukaksosilla on muitakin tunnettuja ominaisuuksia. Vuonna 1919 Viggo Brun osoitti alkulukukaksosten käänteislukujen summan suppenevan kohti lukua, jota kutsutaan Brunin vakioksi. Tulos on yllättävä, sillä kaikkien alkulukujen käänteislukujen summan tiedetään hajaantuvan. Brunin tuloksesta ei kuitenkaan seuraa, ettei voisi olla olemassa äärettömästi alkulukukaksosia. Brun todisti myös, että kaikilla positiivisilla kokonaisluvuilla n pätee, että on olemassa n peräkkäistä alkulukua, jotka eivät ole alkulukukaksosia. Brun tunnetaan myös alkulukuseulojen kehittämisestä.

1970-luvun puolessavälissä Jiang-Run Chen todisti, että on olemassa äärettömästi sellaisia alkulukuja p, että $p+2$ on joko alkuluku tai kahden alkuluvun tulo. Tällaisia alkulukuja p kutsutaan Chenin alkuluvuiksi.

Vuonna 2013 Yitang Zhang todisti kehittämänsä niin sanotun *alkulukukaksosten heikon otaksuman*, jonka mukaan on olemassa äärettömän monta sellaista alkulukuparia, joiden etäisyys on pienempi kuin $7 \cdot 10^7$. Tämän Zhangin läpimurron jälkeen kyseistä alkulukujen etäisyyden ylärajaa on onnistuttu pienentämään huomattavasti. Vain neljä kuukautta myöhemmin Polymath8 project -yhteistyöhanke onnistui

määrittämään tarkemmaksi ylärajaksi luvun 4680. Edelleen saman vuoden aikana Zhangin työstä inspiroitunut James Maynard todisti luvun 600 sopivan ylärajaksi. Vuotta myöhemmin Maynardin ja Polymath8 project -hankkeeseen osallistuneen Terence Taon tekniikoita hyödyntämällä yläraja saatiin laskettua lukuun 246.

3 Esitietoja

3.1 Joitain erityisiä kongruensseja

Tässä alaluvussa tutustutaan muutamiin erityisiin kongruenssituloksiin, joita hyödynnetään neljännen luvun tulosten todistamisessa.

Määritelmä 3.1. Jos a ja b ovat kokonaislukuja ja $n \geq 2$, sanotaan, että *a on kongruentti luvun b kanssa modulo n*, jos $n \mid (a - b)$. Tätä merkitään

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

Jos taas $n \nmid (a - b)$, sanotaan, että *a on epäkongruentti luvun b kanssa modulo n* ja, merkitään

$$a \not\equiv b \pmod{n}.$$

Lause 3.1 (Fermat'n pieni lause)**.** *Olkoon p alkuluku. Tällöin, jos a on positiivinen kokonaisluku siten, että $p \nmid a$, on voimassa $a^{p-1} \equiv 1 \pmod{p}$.*

Todistus (ks. [12, s. 148–149]). Sivuutetaan. □

Lause 3.2 (Wilsonin lause)**.** *Positiivinen kokonaisluku $n \geq 2$ on alkuluku, jos ja vain jos $(n-1)! \equiv -1 \pmod{n}$.*

Todistus (ks. [12, s. 147–148]). Sivuutetaan. □

Lause 3.3 (Leibnizin lause)**.** *Positiivinen kokonaisluku $n \geq 2$ on alkuluku, jos ja vain jos $(n-2)! - 1 \equiv 0 \pmod{n}$.*

Todistus (ks. [13, s. 214]). Sivuutetaan. □

Seurauslause 3.4. *Olkoon n pariton positiivinen lukua 2 suurempi kokonaisluku. Tällöin on voimassa*

$$\left(\left(\frac{n-1}{2}\right)!\right)^2 \equiv \begin{cases} -1 \pmod{n}, & \text{jos ja vain jos } n \text{ on alkuluku muotoa } 4k+1, \\ 1 \pmod{n}, & \text{jos ja vain jos } n \text{ on alkuluku muotoa } 4k+3. \end{cases}$$

Todistus (vrt. [4, s. 129]). Wilsonin lauseen nojalla pätee $(n-1)! \equiv -1 \pmod{n}$, jos ja vain jos n on alkuluku. Koska $(n-1) \equiv -1 \pmod{n}$, myös $(-1)(n-2)! \equiv -1 \pmod{n}$, jos ja vain jos n on alkuluku. Purkamalla edelleen kertomasta tekijöitä saadaan yhtäpitävästi

$$(m-1)!(-1)^{n-1}(n-m)! \equiv -1 \pmod{n},$$

missä $1 \leq m \leq n$. Valitsemalla kokonaisluku $m = (n+1)/2$ saadaan yhtäpitävästi

$$\left(\left(\frac{n-1}{2}\right)!\right)^2 \equiv (-1)^n \pmod{n}.$$

Siis

$$\left(\left(\frac{n-1}{2}\right)!\right)^2 \equiv \begin{cases} -1 \pmod{n}, & \text{jos ja vain jos } n \text{ on alkuluku muotoa } 4k+1, \\ 1 \pmod{n}, & \text{jos ja vain jos } n \text{ on alkuluku muotoa } 4k+3, \end{cases}$$

missä k on positiivinen kokonaisluku. □

Wilsonin lauseesta poiketen seuraava lause perustuu jaottomuuteen.

Lause 3.5. *Olkoon n lukua 4 suurempi kokonaisluku olematta kuitenkaan yhtä suuri kuin 6 tai 9. Tällöin n on alkuluku, jos ja vain jos $4\,(n-5)! \not\equiv 0 \pmod{n}$.*

Todistus (vrt. [2, s. 2]). Todistetaan ensin, että jos n on lukua 4 suurempi alkuluku, se ei jaa lukua $4(n-5)!$. Koska kaikki luvun $4(n-5)!$ alkutekijät ovat lukua n pienempiä ja n on alkuluku, luku $4(n-5)!$ ei voi olla jaollinen alkuluvulla n.

Todistetaan sitten, että jos $4\,(n-5)! \not\equiv 0 \pmod{n}$ pätee, on luku n alkuluku. Tämä voidaan todistaa suoraan pienimmille kolmelle luvun n arvolle eli $n = 5$, $n = 7$ ja $n = 8$. Jos $n = 5$, relaatio $4 \cdot 0! \not\equiv 0 \pmod 5$ pätee ja luku 5 on alkuluku. Vastaavasti jos $n = 7$, relaatio $4 \cdot 2! \not\equiv 0 \pmod 7$ on voimassa ja luku 7 on alkuluku. Tapauksessa $n = 8$ relaatio $4 \cdot 3! \not\equiv 0 \pmod 8$ ei ole voimassa, sillä luku 8 jakaa luvun $4 \cdot 3! = 24$ ja luku 8 ei ole alkuluku.

Lukujen $n \geq 10$ tapauksessa hyödynnetään väitteen kontrapositiota, eli näytetään, että mikäli n ei ole alkuluku, kongruenssi $4\,(n-5)! \equiv 0 \pmod{n}$ on voimassa. Jos n ei ole alkuluku, se voidaan esittää kahden lukua 1 suuremman positiivisen tekijänsä avulla muodossa $n = km$. Oletetaan ensin, että n on jonkin alkuluvun neliö eli muotoa $n = p^2$, missä p on lukua 3 suurempi alkuluku. Koska kun $p \geq 5$, luku $\left(p^2\right)!$ sisältää $p+1$ kertaa tekijän p. Siis luku $4\,(n-5)!$ sisältää $p-1$ kertaa tekijän p, joten kongruenssi $4\,(n-5)! \equiv 0 \pmod{n}$ pätee.

Oletetaan sitten, ettei luku n ole alkuluvun neliö, jolloin voidaan valita luvut k ja m siten, että k on luvun n tekijöistä suurempi ja m pienempi. Koska tällöin m on vähintään 2, saadaan selvitettyä luvulle k yläraja $k = n/m \leq n/2$. Koska luvuille $n \geq 10$ pätee $n/m \leq n/2 \leq n-5$, on luvun n tekijöiden k ja m esiinnyttävä lausekkeessa $4\,(n-5)!$, joten kongruenssi $4\,(n-5)! \equiv 0 \pmod{n}$ on voimassa. □

Seuraavaa apulausetta käytetään luvussa 4.1 todistusta sujuvoittamassa.

Apulause 3.6. *Jos $n > 1$ on kokonaisluku ja kongruenssi*

$$12\big((2n-1)! - 1\big) - 5(2n+1) \equiv 0 \pmod{(2n+1)(2n+3)}$$

on voimassa, niin $3 \nmid 2n+1$ ja $3 \nmid 2n+3$.

Todistus (vrt. [7, s. 98]). Oletetaan, että $3 \mid 2n+1$, kun $n > 1$. Koska $3 \mid 2n+1$, pätee $2n+1 = 3k$ jollakin parittomalla kokonaisluvulla $k > 1$. Tällöin kongruenssiksi saadaan

$$12\big((3k-2)! - 1\big) - 5 \cdot 3k \equiv 0 \pmod{3k(3k+2)}.$$

Siis on myös voimassa $12\big((3k-2)!-1\big) \equiv 0 \pmod{3k}$ ja edelleen $(3k-2)!-1 \equiv 0 \pmod{k}$. Koska $k \mid (3k-2)!$, on oltava myös voimassa $k \mid 1$, jolloin $k = \pm 1$, mikä on ristiriidassa oletuksen $k > 1$ kanssa. Siis $3 \nmid 2n+1$.

Oletetaan sitten, että $3 \mid 2n+3$, kun $n > 1$. Tällöin $3 \mid 2n$ eli on voimassa $2n = 3l$ jollakin parillisella kokonaisluvulla $l > 1$. Nyt kongruenssiksi saadaan

$$12\big((3l-1)!-1\big) - 5(3l+1) \equiv 0 \pmod{(3l+1)(3l+3)},$$

jolloin pätee $12\big((3l-1)!-1\big) - 5(3l+1) \equiv 0 \pmod{3}$ ja edelleen myös $-5 \equiv 0 \pmod{3}$, mikä on epätotta. Siis $3 \nmid 2n+3$. □

Koska Lagrangen lausetta tarvitaan tämän luvun lopussa käsiteltävien lauseiden todistamisessa, todistetaan ensin Lagrangen lause. Tätä ennen on kuitenkin syytä esittää seuraava määritelmä.

Määritelmä 3.2. Olkoon $f(x)$ kokonaislukukertoiminen polynomi. Jos $f(c) \equiv 0 \pmod{n}$, sanotaan, että c on *polynomin $f(x)$ juuri modulo m*.

Huomataan, että jos c on polynomin $f(x)$ juuri modulo m, tällöin kaikki luvun c kanssa kongruentit kokonaisluvut ovat myös polynomin $f(x)$ juuria modulo m.

Lause 3.7 (Lagrangen lause)**.** *Olkoon p alkuluku ja olkoon $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ polynomi, jonka aste on n ja jonka johtava kerroin a_n ei ole jaollinen alkuluvulla p. Tällöin polynomilla $f(x)$ on korkeintaan n epäkongruenttia juurta modulo p.*

Todistus (vrt. [12, s. 239]). Todistetaan lause induktiolla. Kun $n = 1$, polynomiksi saadaan $f(x) = a_1 x + a_0$ ja $p \nmid a_1$ on voimassa. Polynomin $f(x)$ juuri on ratkaisu yhden muuttujan lineaariseen kongruenssiin $a_1 x \equiv -a_0 \pmod{p}$. Koska $\operatorname{syt}(a_1, p) = 1$, lineaarisella kongruenssilla on täsmälleen yksi ratkaisu modulo p, joten polynomilla $f(x)$ on täsmälleen yksi juuri modulo p. Siis lauseen väite pätee, kun $n = 1$.

Oletetaan sitten, että lause on voimassa polynomeille, joiden aste on $n-1$. Olkoon $f(x)$ nyt sellainen asteen n polynomi, jolla on voimassa $p \nmid a_n$. Oletetaan, että polynomilla $f(x)$ on $n+1$ epäkongruenttia juurta modulo p. Merkitään näitä juuria $c_0, c_1, \ldots, c_n$, jolloin $f(c_i) \equiv 0 \pmod{p}$, kun $i = 0, 1, \ldots, n$. Nyt voidaan kirjoittaa

$$\begin{aligned}
f(x) - f(c_0) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 - (a_n c_0^n + a_{n-1}c_0^{n-1} + \cdots + a_1 c_0 + a_0) \\
&= a_n(x^n - c_0^n) + a_{n-1}(x^{n-1} - c_0^{n-1}) + \cdots + a_1(x - c_0) \\
&= a_n(x - c_0)(x^{n-1} + x^{n-2}c_0 + \cdots + x c_0^{n-2} + c_0^{n-1}) \\
&\quad + a_{n-1}(x - c_0)(x^{n-2} + x^{n-3}c_0 + \cdots + x c_0^{n-3} + c_0^{n-2}) \\
&\quad + \cdots + a_1(x - c_0) \\
&= (x - c_0)g(x),
\end{aligned}$$

missä $g(x)$ on sellainen polynomi, jonka aste on $n-1$ ja jonka johtava kerroin on a_n.

Osoitetaan seuraavaksi, että $c_1, c_2, \ldots, c_n$ ovat kaikki polynomin $g(x)$ juuria modulo p. Olkoon i kokonaisluku siten, että $1 \leq i \leq n$. Koska on voimassa $f(c_i) \equiv f(c_0) \equiv 0 \pmod{p}$, voidaan kirjoittaa

$$f(c_i) - f(c_0) \equiv (c_i - c_0)g(c_i) \pmod{p}.$$

Koska $c_0, c_1, \ldots c_n$ ovat epäkongruentteja juuria modulo p, on voimassa $c_i - c_0 \not\equiv 0 \pmod{p}$, joten $g(c_i) \equiv 0 \pmod{p}$. Näin ollen c_i on polynomin $g(x)$ juuri modulo p. Tällöin polynomilla $g(x)$, jonka aste on $n-1$ ja jonka johtava kerroin ei ole jaollinen alkuluvulla p, on n kappaletta epäkongruentteja juuria modulo p. Tämä on ristiriidassa oletuksen kanssa, joten polynomilla $f(x)$ ei voi olla n kappaletta enempää epäkongruentteja juuria modulo p. □

Seurauslause 3.8. *Olkoon p alkuluku ja olkoon $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ polynomi, jonka aste on n ja jonka johtava kerroin on a_n. Jos polynomilla $f(x)$ on olemassa $n+1$ epäkongruenttia juurta modulo p, tällöin alkuluku p jakaa johtavan kertoimen a_n ja edelleen myös muut kertoimet a_i, $0 \leq i \leq n-1$.*

Näin saadun seurauslauseen avulla todistetaan apulause.

Apulause 3.9. *Olkoon p on alkuluku ja olkoot $x_1, x_2, \ldots, x_{p-1}$ kokonaislukuja siten, että $p \nmid x_j$, kun $1 \leq j \leq p-1$, ja $p \nmid (x_j - x_i)$, kun $1 \leq j \leq p-1$, $1 \leq i \leq p-1$ ja $x_i \neq x_j$. Tällöin on voimassa*

$$p \mid \left(\prod_{i=j}^{p-1} x_j + (-1)^{p-1} \right).$$

Todistus (vrt. [6, s. 52]). Olkoon $f(x) = \prod_{i=j}^{p-1}(x - x_j) - x^{p-1} + 1$. Tällöin $f(x)$ on polynomi, jonka aste on enintään $p-2$. Lisäksi $p \mid f(x_j)$, kun $1 \leq j \leq p-1$, sillä Fermat'n pienen lauseen 3.1 nojalla $p \mid 1 - x^{p-1}$ ja luonnollisesti $p \mid 0$. Näin ollen seurauslauseen 3.8 perusteella alkuluku p jakaa polynomin $f(x)$ jokaisen termin kertoimen. Siispä alkuluku p jakaa erityisesti myös nollannen asteen kertoimen, eli

$$p \mid \left((-1)^{p-1} \prod_{i=j}^{p-1} x_j + 1 \right).$$

Siis myös

$$p \mid \left(\prod_{i=j}^{p-1} x_j + (-1)^{p-1} \right). \qquad \square$$

Määritellään seuraavaksi jatkossa tarvittava kaksoiskertoma rekursiivisesti.

Määritelmä 3.3. $0!! = 1$, $1!! = 1$ ja $n!! = n\big((n-2)!!\big)$, kun $n \geq 2$.

Esitellään alaluvun lopuksi vielä kaksi myöhemmin tarvittavaa kongruenssitulosta.

Lause 3.10. *Positiivinen kokonaisluku $n \geq 2$ on alkuluku, jos ja vain jos*

$$\left((n-2)!!\right)^2 + (-1)^{\left\lfloor \frac{n}{2} \right\rfloor} \equiv 0 \pmod{n}. \tag{3.1}$$

Todistus (vrt. [6, s. 52–53]). Oletetaan ensin, että n on alkuluku. Nyt selvästi kongruenssi (3.1) pätee, kun $n = 2$. Oletetaan sitten, että $n \geq 3$. Nyt asettamalla apulauseen 3.9 luvuiksi $x_1, x_2, \ldots, x_{p-1}$ luvut $-(n-2), -(n-4), \ldots, -1, 1, \ldots, n-4, n-2$, joita alkuluku n ei jaa, voidaan todeta, että kongruenssi on voimassa.

Oletetaan sitten, että kongruenssi (3.1) pätee. Ensinnäkin laskemalla huomataan, että kongruenssi on voimassa, kun $n = 2$. Oletetaan sitten, että $n > 2$. Tällöin luvun n on oltava pariton, jotta kongruenssi voisi olla voimassa. Jos n ei ole alkuluku, se voidaan kirjoittaa kahden lukua 1 suuremman positiivisen tekijänsä avulla $n = ab$. Olkoon tässä a luvun n pienin alkutekijä, jolloin pätee $1 \leq a \leq \left\lfloor \frac{n}{2} \right\rfloor$.

Koska $(n-2)!! = 1 \cdot 3 \cdots (n-2)$ ja a on parittoman luvun n pienin alkutekijä, $n \mid (n-2)!!$, sillä n ei ole alkuluku. Oletuksen nojalla pätee myös $a \mid \left((n-2)!!\right)^2 + (-1)^{\left\lfloor \frac{n}{2} \right\rfloor}$. Täten on oltava myös voimassa $a \mid (-1)^{\left\lfloor \frac{n}{2} \right\rfloor}$, mikä ei ole mahdollista. Näin ollen n on alkuluku. □

Lause 3.11. *Positiivinen kokonaisluku $n \geq 2$ on alkuluku, jos ja vain jos*

$$\left((n-1)!!\right)^2 + (-1)^{\left\lfloor \frac{n}{2} \right\rfloor} \equiv 0 \pmod{n}. \tag{3.2}$$

Todistus (vrt. [6, s. 52–53]). Oletetaan ensin, että n on alkuluku. Kongruenssi (3.2) on selvästi voimassa, kun $n = 2$. Oletetaan sitten, että $n \geq 3$. Asettamalla nyt apulauseen 3.9 luvuiksi $x_1, x_2, \ldots, x_{p-1}$ luvut $-(n-1), -(n-3), \ldots, -2, 2, \ldots, n-3, n-1$, huomataan, että kongruenssi on voimassa.

Oletetaan sitten, että kongruenssi (3.2) pätee. Laskemalla huomataan, että $n = 2$ toteuttaa kongruenssin. Oletetaan sitten, että $n > 2$ ja n on pariton. Jos n ei ole alkuluku, se voidaan esittää muodossa $n = ab$, missä a on luvun n pienin alkutekijä. Tällöin pätee $1 \leq a \leq \left\lfloor \frac{n}{2} \right\rfloor$. Koska $(n-1)!! = 2 \cdot 4 \cdot \ldots \cdot (n-1) = 2^{\frac{k-1}{2}} \left(\frac{k-1}{2}\right)!$ ja n on pariton, on voimassa, että $a \mid \left(\frac{k-1}{2}\right)!$. Täten on oltava voimassa $a \mid (-1)^{\left\lfloor \frac{n}{2} \right\rfloor}$, mikä on ristiriitaista.

Oletetaan sitten, että $n \geq 4$ on parillinen ja toteuttaa kongruenssin (3.2). Tällöin a on joko muotoa

(i) $n = 2^\alpha$, missä $\alpha > 1$, tai

(ii) $n = 2^\beta \cdot c$, missä $\beta \geq 1$ ja $c \geq 3$ on pariton.

Jos $n = 2^\alpha$, missä $\alpha > 1$, kongruenssista (3.2) seuraa, että $2^\alpha \mid \left((2^\alpha - 1)!!\right)^2 + 1$. Tämä on kuitenkin ristiriitaista, sillä $4 \mid 2^\alpha$, mutta $4 \nmid \left((2^\alpha - 1)!!\right)^2 + 1$, sillä $\left((2^\alpha - 1)!!\right)^2 + 1$ voidaan ilmaista muodossa $(2k+1)^2 + 1 = 4k^2 + 4k + 2 = 2(2(k^2 + k) + 1)$, missä k on jokin positiivinen kokonaisluku. Näin ollen (i) ei voi olla voimassa.

Mikäli taas $n = 2^\beta \cdot c$, missä $\beta \geq 1$ ja $c \geq 3$ on pariton, pätee $c \mid (n-1)!!$, mistä seuraa $c \nmid \left((n-1)!!\right)^2 + (-1)^{\left\lfloor \frac{n}{2} \right\rfloor}$. Siis myöskään (ii) ei voi päteä, joten n on alkuluku. □

3.2 Multiplikatiiviset funktiot

Tässä alaluvussa esitellään multiplikatiiviset funktiot Eulerin phi-funktio ja tekijäfunktio sekä niihin liittyviä tuloksia luvun 4.2 karakterisointeja varten. Tämän alaluvun lähteenä on käytetty Rosenin oppikirjaa [12]. Määritellään ensin tarvittavat peruskäsitteet.

Määritelmä 3.4. *Aritmeettinen funktio* on reaali- tai kompleksiarvoinen funktio, joka on määritelty kaikille positiivisille kokonaisluvuille.

Määritelmä 3.5. Aritmeettinen funktio f on *multiplikatiivinen*, jos suhteellisilla alkuluvuilla m ja n on voimassa $f(mn) = f(m)f(n)$.

Multiplikatiivisilla funktioilla on voimassa seuraava ominaisuus.

Lause 3.12. *Jos f on multiplikatiivinen funktio ja $n = p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$ on positiivisen kokonaisluvun n alkulukuhajotelma, tällöin pätee $f(n) = f(p_1^{a_1})f(p_2^{a_2})\cdots f(p_s^{a_s})$.*

Todistus (vrt. [12, s. 166–167]). Koska f on multiplikatiivinen funktio ja $\text{syt}(p_1^{a_1}, p_2^{a_2}\cdots p_s^{a_s}) = 1$, multiplikatiivisen funktion määritelmän nojalla voidaan kirjoittaa

$$f(n) = f(p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}) = f\left(p_1^{a_1}(p_2^{a_2}\cdots p_s^{a_s})\right) = f(p_1^{a_1})f(p_2^{a_2}p_3^{a_3}\cdots p_s^{a_s}).$$

Koska myös $\text{syt}(p_2^{a_2}, p_3^{a_3}\cdots p_s^{a_s}) = 1$, voidaan kirjoittaa

$$f(p_2^{a_2}p_3^{a_3}\cdots p_s^{a_s}) = f(p_2^{a_2})f(p_3^{a_3}\cdots p_s^{a_s}),$$

josta seuraa, että $f(n) = f(p_1^{a_1})f(p_2^{a_2})f(p_3^{a_3}\cdots p_s^{a_s})$. Toistamalla vastaavaa menettelyä saadaan lopulta lauseen väitteen mukainen muoto $f(n) = f(p_1^{a_1})f(p_2^{a_2})\cdots f(p_s^{a_s})$. □

Määritellään sitten Eulerin phi-funktio.

Määritelmä 3.6 (Eulerin phi-funktio)**.** Olkoon n positiivinen kokonaisluku. Tällöin *Eulerin phi-funktiolla* $\phi(n)$ ilmaistaan sellaisten positiivisten kokonaislukujen määrää, jotka eivät ole lukua n suurempia ja ovat luvun n kanssa suhteellisia alkulukuja.

Tarkastellaan seuraavaksi Eulerin phi-funktion arvoja alkuluvuilla.

Lause 3.13. *Jos p on alkuluku, $\phi(p) = p - 1$. Toisaalta, jos p positiivinen kokonaisluku ja $\phi(p) = p - 1$, on p alkuluku.*

Todistus (vrt. [12, s. 167]). Jos p on alkuluku, kaikki lukua p pienemmät positiiviset kokonaisluvut ovat sen kanssa suhteellisia alkulukuja. Koska tällaisia lukuja on $p-1$, pätee $\phi(p) = p - 1$.

Jos taas p ei ole alkuluku, on olemassa sellainen luku $1 < d < p$, joka jakaa luvun p, jolloin p ja d eivät ole suhteellisia alkulukuja. Koska tällöin jokin lukua p pienempi positiivinen kokonaisluku ei ole luvun p kanssa suhteellinen alkuluku, $\phi(p) \leq p - 2$. Näin ollen, jos on voimassa $\phi(p) = p - 1$, on luvun p oltava alkuluku. □

Huomataan edellisen lauseen perusteella, että Eulerin phi-funktiolla on voimassa $\phi(n) \leq n - 1$, missä n on positiivinen kokonaisluku. Seuraavan lauseen perusteella voidaan määrittää Eulerin phi-funktion arvoja alkulukujen potensseille.

Lause 3.14. *Olkoon p alkuluku ja a positiivinen kokonaisluku. Tällöin pätee* $\phi(p^a) = p^a - p^{a-1}$.

Todistus (vrt. [12, s. 167]). Ne kokonaisluvut, jotka eivät ole lukua p^a suurempia ja eivät ole suhteellisia alkulukuja luvun p kanssa, ovat sellaisia lukuja, jotka ovat enintään p^a ja jaollisia luvulla p. Tällaisia lukuja on yhteensä p^{a-1}. Siis on olemassa $p^a - p^{a-1}$ kokonaislukua, jotka eivät ole lukua p^a suurempia ja ovat sen kanssa suhteellisia alkulukuja. □

Seuraavaksi osoitetaan, että Eulerin phi-funktio on multiplikatiivinen.

Lause 3.15. *Olkoot m ja n positiivisia suhteellisia alkulukuja. Tällöin pätee* $\phi(mn) = \phi(m)\phi(n)$.

Todistus (vrt. [12, s. 168–169]). Aloitetaan todistaminen esittämällä seuraavassa taulukossa sellaiset positiiviset kokonaisluvut, jotka eivät ole suurempia kuin tulo mn.

1	$m+1$	$2m+1$	$\dots$	$(n-1)m+1$
2	$m+2$	$2m+2$	$\cdots$	$(n-1)m+2$
3	$m+3$	$2m+3$	$\cdots$	$(n-1)m+3$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
m	$2m$	$3m$	$\cdots$	mn

Oletetaan, että r on positiivinen kokonaisluku, joka ei ole suurempi kuin luku m, ja että $\text{syt}(m, r) = d > 1$. Tällöin yksikään luku rivillä r ei ole suhteellinen alkuluku luvun mn kanssa, sillä jokainen luku tällä rivillä on muotoa $km + r$, missä k on sellainen kokonaisluku, että $1 \leq k \leq n - 1$ pätee. Koska $d \mid m$ ja $d \mid r$, pätee myös, että $d \mid (km + r)$.

Siis jotta voitaisiin löytää ne taulukosta kokonaisluvut, jotka ovat suhteellisia alkulukuja luvun mn kanssa, riittää tarkastella vain sellaisia taulukon rivejä q, joilla pätee $\text{syt}(m, q) = 1$. Jos $\text{syt}(m, q) = 1$ ja $1 \leq q \leq m$ ovat voimassa, on määritettävä, kuinka moni rivin q luvuista on suhteellisia alkulukuja luvun mn kanssa. Tällä rivillä ovat luvut q, $m + q$, $2m + q$, $\dots$, $(n - 1)m + q$. Kaikki rivin luvut ovat suhteellisia alkulukuja luvun m kanssa, sillä $\text{syt}(m, q) = 1$. Toisaalta taas rivillä q olevat n lukua muodostavat täydellisen jäännössysteemin modulo n, joten täsmälleen $\phi(n)$ tällä rivillä olevista luvuista on suhteellisia alkulukuja luvun n kanssa. Koska nämä $\phi(n)$ lukua ovat suhteellisia alkulukuja myös luvun m kanssa ja $\text{syt}(m, n) = 1$, kyseiset luvut ovat myös suhteellisia alkulukuja luvun mn kanssa.

Koska taulukossa on $\phi(m)$ riviä, joissa on $\phi(n)$ kappaletta lukuja, jotka ovat suhteellisia alkulukuja luvun mn kanssa, voidaan todeta, että $\phi(mn) = \phi(m)\phi(n)$ pätee. □

Edellisten lauseiden avulla saadaan johdettua seuraava kaava.

Lause 3.16. *Olkoon $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ positiivisen kokonaisluvun n alkulukuhajotelma. Tällöin pätee*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right).$$

Todistus (vrt. [12, s. 169]). Koska Eulerin phi-funktio on multiplikatiivinen, voidaan lauseen 3.12 perusteella kirjoittaa

$$\phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2})\cdots\phi(p_k^{a_k}).$$

Lisäksi lauseen 3.14 nojalla pätee

$$\phi(p_j^{a_j}) = p_j^{a_j} - p_j^{a_j-1} = p_j^{a_j}\left(1 - \frac{1}{p_j}\right),$$

jossa $j = 1, 2, \ldots, k$. Näin ollen saadaan

$$\begin{aligned}\phi(n) &= p_1^{a_1}\left(1 - \frac{1}{p_1}\right)p_2^{a_2}\left(1 - \frac{1}{p_2}\right)\cdots p_1^{a_k}\left(1 - \frac{1}{p_k}\right)\\ &= p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)\\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).\end{aligned}$$

□

Määritellään sitten tekijäfunktio.

Määritelmä 3.7 (Tekijäfunktio)**.** Olkoon n positiivinen kokonaisluku. Tällöin *tekijäfunktion arvo* $\sigma(n)$ on luvun n positiivisten tekijöiden summa, eli

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

Huomautus. Huomataan, että $\sigma(p) = p + 1$ pätee, jos ja vain jos p on alkuluku, sillä positiivisista luvuista alkuluvun p jakaa vain luku 1 sekä luku itse. Siispä tekijäfunktiolla on voimassa $\sigma(n) \geq n + 1$, missä $n > 1$ on positiivinen kokonaisluku.

Osoitetaan seuraavaksi, että myös tekijäfunktio on multiplikatiivinen. Tätä varten todistetaan ensin seuraava apulause.

Apulause 3.17. *Jos f on multiplikatiivinen funktio, silloin aritmeettinen funktio $F(n) = \sum_{d|n} f(d)$ on myös multiplikatiivinen.*

Todistus (vrt. [12, s. 175–177]). Halutaan todistaa, että suhteellisilla alkuluvuilla m ja n on voimassa $F(mn) = F(m)F(n)$. Olkoot siis m ja n suhteellisia alkulukuja, jolloin

$$F(mn) = \sum_{d|mn} f(d).$$

Koska m ja n ovat suhteellisia alkulukuja, voidaan jokainen luvun mn jakaja esittää lukujen d_1 ja d_2 tulona, jossa d_1 on luvun m jakaja ja d_2 on luvun n jakaja. Voidaan siis kirjoittaa

$$F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2).$$

Koska m ja n ovat suhteellisia alkulukuja, myös lukujen d_1 ja d_2 on oltava suhteellisia alkulukuja. Lisäksi, koska f on multiplikatiivinen, saadaan edelleen

$$F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)f(d_2) = \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) = F(m)F(n). \qquad \square$$

Edellisen apulauseen avulla on helppo osoittaa tekijäfunktion olevan multiplikatiivinen.

Lause 3.18. *Tekijäfunktio on multiplikatiivinen.*

Todistus (vrt. [12, s. 166 & s. 177]). Jotta edellä todistettua apulausetta voidaan hyödyntää, on näytettävä, että identiteettifunktio on multiplikatiivinen. Olkoon siis f identiteettifunktio, eli $f(n) = n$, kun n on positiivinen kokonaisluku, sekä olkoot n_1 ja n_2 positiivisia kokonaislukuja, jotka ovat suhteellisia alkulukuja. Nyt voidaan kirjoittaa $f(n_1 n_2) = n_1 n_2 = f(n_1)f(n_2)$. Koska identiteettifunktio on näin ollen multiplikatiivinen, apulauseesta 3.17 seuraa, että tekijäfunktio on multiplikatiivinen. $\square$

Johdetaan vielä tämän luvun lopuksi seuraavassa luvussa hyödynnettävä kaava. Tähän tarvitaan seuraavaa apulausetta.

Apulause 3.19. *Olkoon p alkuluku ja a positiivinen kokonaisluku. Tällöin on voimassa*

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

Todistus (vrt. [12, s. 177]). Luvun p^a positiiviset jakajat ovat luonnollisesti luvut $1, p, p^2, \ldots, p^a$. Huomataan, että kyseessä on geometrinen summa, joten voidaan kirjoittaa

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

Apulauseen avulla voidaan johtaa seuraavan lauseen kaava.

Lause 3.20. *Olkoon n positiivinen kokonaisluku ja $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ sen alkulukuhajotelma. Tällöin pätee*

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_k^{a_k+1} - 1}{p_k - 1} = \prod_{j=1}^{k} \frac{p_j^{a_j+1} - 1}{p_j - 1}.$$

Todistus (vrt. [12, s. 177 – 178]). Koska tekijäfunktio on multiplikatiivinen, pätee $\sigma(n) = \sigma(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) = \sigma(p_1^{a_1})\sigma(p_2^{a_2}) \cdots \sigma(p_k^{a_k})$. Nyt apulauseen 3.19 nojalla voidaan kirjoittaa

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_k^{a_k+1} - 1}{p_k - 1}. \qquad \square$$

4 Alkulukukaksosten karakterisointeja

4.1 Karakterisointi kongruenssia hyödyntäen

Tässä luvussa käsitellään kongruenssia hyödyntäviä alkulukukaksosten karakterisointeja. Luultavasti tunnetuin kongruenssiin nojautuva alkulukukaksosten karakterisointi on seuraava P. A. Clementin esittelemä Wilsonin lauseen tapainen karakterisointi vuodelta 1949.

Lause 4.1 (Clementin lause)**.** *Positiiviset kokonaisluvut n ja $n+2$ ovat alkulukuja, jos ja vain jos*

$$4\big((n-1)!+1\big)+n \equiv 0 \pmod{n(n+2)}.$$

Todistus (vrt. [3, s. 23–24] ja [8, s. 196–197]). Todistetaan ensin ehdon riittävyys. Oletetaan, että kongruenssi $4\big((n-1)!+1\big)+n \equiv 0 \pmod{n(n+2)}$ pätee, kun n on jokin positiivinen kokonaisluku. Havaitaan, että kongruenssi ei päde, kun $n=2$ tai $n=4$. Nyt, koska n jakaa lausekkeen $4\big((n-1)!+1\big)+n$, täytyy myös päteä, että $n \mid 4\big((n-1)!+1\big)$ ja edelleen, koska $n \neq 2$ ja $n \neq 4$, pätee $n \mid (n-1)!+1$. Siis suoraan Wilsonin lauseen 3.2 nojalla n on alkuluku.

Samaan tapaan havaitaan, että myös luku $n+2$ on alkuluku. Koska $4\big((n-1)!+1\big)+n \equiv 4(n-1)!+(n+2)+2 \equiv 0 \pmod{n+2}$ pätee, voidaan tarkastella kongruenssia

$$4(n-1)!+2 \equiv 0 \pmod{n+2}.$$

Kongruenssi saadaan kertomalla puolittain luvulla $n(n+1)$ muotoon

$$4\big((n+1)!+1\big)+2n^2+2n-4 \equiv 0 \pmod{n+2},$$

josta edelleen saadaan kongruenssi

$$4\big((n+1)!+1\big)+2(n+2)(n-1) \equiv 0 \pmod{n+2}.$$

Siis $n+2 \mid (n+1)!+1$, joten Wilsonin lauseen 3.2 perusteella myös $n+2$ on alkuluku.

Todistetaan sitten ehdon välttämättömyys. Olkoot n ja $n+2$ alkulukuja, jolloin $n \neq 2$. Siis Wilsonin lauseen 3.2 perusteella pätevät kongruenssit

$$(n-1)!+1 \equiv 0 \pmod{n}, \tag{4.1}$$

$$(n+1)!+1 \equiv 0 \pmod{n+2}. \tag{4.2}$$

Kongruenssista (4.2) saadaan $n(n+1)\,((n-1)!)+1 \equiv 0 \pmod{n+2}$ kirjoittamalla kertoman ensimmäiset kaksi tekijää näkyviin. Tämä voidaan edelleen esittää muodossa $2(n-1)!+1 \equiv 0 \pmod{n+2}$, sillä $n(n+1)=(n+2)(n-1)+2$. Näin saatu kongruenssi voidaan esittää yhtälönä

$$2(n-1)! = k(n+2)-1, \tag{4.3}$$

jossa k on jokin kokonaisluku. Toisaalta kongruenssin (4.1) perusteella pätee $2(n-1)! + 1 \equiv (n-1)! \pmod{n}$, eli $kn + 2k - 1 + 1 \equiv (n-1)! \pmod{n}$, josta saadaan edelleen $2k + 1 \equiv 0 \pmod{n}$.

Lisäksi kertomalla yhtälö (4.3) puolittain luvulla 2, saadaan yhtälö $4(n-1)!+2 = 2k(n+2)$, eli toisin muotoiltuna

$$4\big((n-1)! + 1\big) - 2 = 2k(n+2).$$

Edelleen, lisäämällä puolittain $n+2$ yhtälöksi saadaan $4\big((n-1)! + 1\big) + n = (2k+1)(n+2)$, ja koska $2k + 1 \equiv 0 \pmod{n}$, voidaan kirjoittaa

$$4\big((n-1)! + 1\big) + n = rn(n+2),$$

missä r on jokin kokonaisluku. Näin ollen kongruenssi $4\big((n-1)! + 1\big) + n \equiv 0 \pmod{n\,(n+2)}$ pätee. □

Seuraava karakterisointi nojaa Clementin lauseen tapaan Wilsonin lauseeseen seurauslausetta 3.4 hyödyntäen.

Lause 4.2. *Olkoon $n \geq 3$ pariton positiivinen kokonaisluku. Kokonaisluvut n ja $n+2$ ovat alkulukuja ja*

(i) luku n on muotoa $n = 4k + 1$, missä k on jokin positiivinen kokonaisluku, jos ja vain jos kongruenssi

$$2\left(\left(\left(\frac{n-1}{2}\right)!\right)^2 + 1\right) + 5n \equiv 0 \pmod{n\,(n+2)}. \tag{4.4}$$

pätee, tai

(ii) luku n on muotoa $n = 4k - 1$, missä k on jokin positiivinen kokonaisluku, jos ja vain jos kongruenssi

$$2\left(\left(\left(\frac{n-1}{2}\right)!\right)^2 + 1\right) - 5n \equiv 0 \pmod{n\,(n+2)} \tag{4.5}$$

pätee.

Todistus (vrt. [4, s. 129–130]). Todistetaan ensin tapaus *(i)*. Oletetaan aluksi, että n on alkuluku muotoa $n = 4k+1$. Tällöin $n+2 = 4k+3$, missä k on jokin positiivinen kokonaisluku. Nyt seurauslauseen 3.4 perusteella ovat voimassa kongruenssit

$$\left(\left(\frac{n-1}{2}\right)!\right)^2 \equiv -1 \pmod{n},$$
$$\left(\left(\frac{n+1}{2}\right)!\right)^2 \equiv 1 \pmod{n+2}.$$

Näistä jälkimmäinen kongruenssi voidaan kirjoittaa myös muodossa

$$(n+1)^2\left(\left(\frac{n-1}{2}\right)!\right)^2 \equiv 4 \pmod{n+2},$$

laskemalla kertomaa auki ja kertomalla kongruenssi puolittain luvulla 4. Koska toisaalta pätee myös kongruenssi $(n+1)^2 \equiv 1 \pmod{n+2}$, voidaan edelleen kirjoittaa

$$\left(\left(\frac{n-1}{2}\right)!\right)^2 \equiv 4 \pmod{n+2}.$$

Näin ollen on voimassa yhtälö

$$\left(\left(\frac{n-1}{2}\right)!\right)^2 = 4 + r(n+2), \tag{4.6}$$

jossa r on jokin kokonaisluku. Siispä myös kongruenssi $4 + r(n+2) \equiv -1 \pmod{n}$ ja näin ollen myös yhtälö $2r = -5 + sn$, jossa s on jokin kokonaisluku, pätee. Ratkaisemalla yhtälö luvun r suhteen, sijoittamalla näin saatu r yhtälöön (4.6) ja kertomalla yhtälö puolittain kahdella saadaan

$$2\left(\left(\frac{n-1}{2}\right)!\right)^2 = -5n - 2 + sn(n+2),$$

jota vastaa kongruenssi

$$2\left(\left(\left(\frac{n-1}{2}\right)!\right)^2 + 1\right) + 5n \equiv 0 \pmod{n(n+2)}.$$

Oletetaan sitten, että kongruenssi (4.4) pätee. Tällöin pätee, että

$$n \mid 2\left(\left(\left(\frac{n-1}{2}\right)!\right)^2 + 1\right) + 5n,$$

joten myös pätee, että

$$n \mid 2\left(\left(\left(\frac{n-1}{2}\right)!\right)^2 + 1\right).$$

Koska n on pariton, on voimassa

$$n \mid \left(\left(\frac{n-1}{2}\right)!\right)^2 + 1$$

eli

$$\left(\left(\frac{n-1}{2}\right)!\right)^2 \equiv -1 \pmod{n}.$$

Tällöin seurauslauseen 3.4 perusteella, n on alkuluku muotoa $4k+1$, missä k on jokin positiivinen kokonaisluku.

Näytetään vielä luvun $n+2$ olevan alkuluku, jos kongruenssi (4.4) on voimassa. Koska

$$2\left(\left(\left(\frac{n-1}{2}\right)!\right)^2+1\right)+5n \equiv 2\left(\left(\frac{n-1}{2}\right)!\right)^2+4n+(n+2) \equiv 0 \pmod{n+2}$$

pätee, ja myös $n+2$ on pariton, koska n on pariton, saadaan tarkasteltavaksi kongruenssi

$$\left(\left(\frac{n-1}{2}\right)!\right)^2+2n \equiv 0 \pmod{n+2}.$$

Kertomalla tämä puolittain luvulla $4\big((n+1)/2\big)^2$ eli luvulla $(n+1)^2$ saadaan kongruenssi

$$4\left(\frac{n+1}{2}\right)^2\left(\left(\frac{n-1}{2}\right)!\right)^2+2n(n+1)^2 \equiv 0 \pmod{n+2},$$

josta edelleen saadaan

$$4\left(\left(\frac{n+1}{2}\right)!\right)^2-4 \equiv 0 \pmod{n+2},$$

koska $n \equiv -2 \pmod{n+2}$ ja $n+1 \equiv -1 \pmod{n+2}$. Kun näin saatu kongruenssi kerrotaan vielä puolittain luvun 4 käänteisluvulla modulo $n+2$, joka on olemassa, koska $\text{syt}(4, n+2) = 1$, saadaan lopulta

$$\left(\left(\frac{n+1}{2}\right)!\right)^2 \equiv \left(\left(\frac{(n+2)-1}{2}\right)!\right)^2 \equiv 1 \pmod{n+2}.$$

Näin ollen $n+2$ on seurauslauseen 3.4 nojalla alkuluku muotoa $4k+3$, missä k on jokin positiivinen kokonaisluku.

Todistetaan seuraavaksi vastaavalla tavalla tapaus *(ii)*. Oletetaan siis ensin, että n on alkuluku muotoa $n = 4k-1$. Tällöin $n+2 = 4k+1$, missä k on jokin positiivinen kokonaisluku. Tällöin seurauslauseen 3.4 perusteella ovat voimassa kongruenssit

$$\left(\left(\frac{n-1}{2}\right)!\right)^2 \equiv 1 \pmod{n},$$
$$\left(\left(\frac{n+1}{2}\right)!\right)^2 \equiv -1 \pmod{n+2}.$$

Toisaalta edellisistä kongruensseista jälkimmäinen voidaan esittää myös muodossa

$$(n+1)^2\left(\left(\frac{n-1}{2}\right)!\right)^2 \equiv -4 \pmod{n+2},$$

kun lasketaan kertoman kaksi ensimmäistä tuloa ja kerrotaan kongruenssi puolittain luvulla 4. Edelleen voidaan kirjoittaa kongruenssi muotoon

$$\left(\left(\frac{n-1}{2}\right)!\right)^2 \equiv -4 \pmod{n+2},$$

koska on voimassa, että $(n+1)^2 \equiv 1 \pmod{n+2}$. Näin ollen saadaan yhtälö

$$\left(\left(\frac{n-1}{2}\right)!\right)^2 = -4 + r(n+2), \tag{4.7}$$

jossa r on jokin kokonaisluku. Näin ollen pätee myös kongruenssi $-4 + r(n+2) \equiv 1 \pmod{n}$ ja täten myös yhtälö $2r = 5 + sn$, jossa s on jokin kokonaisluku. Ratkaisemalla yhtälöstä luku r, sijoittamalla se yhtälöön (4.7) ja kertomalla lopuksi saatu uusi yhtälö puolittain kahdella saadaan lopulta

$$2\left(\left(\frac{n-1}{2}\right)!\right)^2 = 5n + 2 + sn(n+2),$$

joka kongruenssina esitettynä on

$$2\left(\left(\left(\frac{n-1}{2}\right)!\right)^2 - 1\right) - 5n \equiv 0 \pmod{n(n+2)}.$$

Oletetaan sitten, että kongruenssi (4.5) on voimassa. Koska nyt pätee, että

$$n \mid 2\left(\left(\left(\frac{n-1}{2}\right)!\right)^2 - 1\right) - 5n,$$

on myös voimassa, että

$$n \mid 2\left(\left(\left(\frac{n-1}{2}\right)!\right)^2 - 1\right).$$

Koska n on pariton, pätee

$$n \mid \left(\left(\frac{n-1}{2}\right)!\right)^2 - 1.$$

Nyt seurauslauseen 3.4 perusteella n on alkuluku muotoa $4k+3$, eli toisin sanoen muotoa $4j-1$, missä k on jokin positiivinen kokonaisluku, ja $j = k+1$.

Todistetaan vielä, että myös luku $n+2$ on alkuluku, jos kongruenssi (4.5) pätee. Koska on voimassa

$$2\left(\left(\left(\frac{n-1}{2}\right)!\right)^2 - 1\right) - 5n \equiv 2\left(\left(\frac{n-1}{2}\right)!\right)^2 - 4n - (n+2) \equiv 0 \pmod{n+2}$$

ja $n+2$ on pariton, voidaan edellinen kongruenssi ilmaista muodossa

$$\left(\left(\frac{n-1}{2}\right)!\right)^2 - 2n \equiv 0 \pmod{n+2}.$$

Kun tämä kerrotaan puolittain luvulla $4\big((n+1)/2\big)^2$ eli luvulla $(n+1)^2$, saadaan kongruenssi

$$4\left(\frac{n+1}{2}\right)^2\left(\left(\frac{n-1}{2}\right)!\right)^2 - 2n(n+1)^2 \equiv 0 \pmod{n+2},$$

joka voidaan esittää yksinkertaisemmassa muodossa

$$4\left(\left(\frac{n+1}{2}\right)!\right)^2 + 4 \equiv 0 \pmod{n+2},$$

sillä $n \equiv -2 \pmod{n+2}$ ja $n+1 \equiv -1 \pmod{n+2}$.

Nyt kuten aiemmassakin tapauksessa, koska $\operatorname{syt}(4, n+2) = 1$, voidaan saatu kongruenssi kertoa puolittain luvun 4 käänteisluvulla modulo $n+2$, jolloin saadaan lopulta kongruenssi

$$\left(\left(\frac{n+1}{2}\right)!\right)^2 \equiv \left(\left(\frac{(n+2)-1}{2}\right)!\right)^2 \equiv -1 \pmod{n+2}.$$

Nyt seurauslauseen 3.4 nojalla $n+2$ on alkuluku muotoa $4k+1$, jossa k on jokin positiivinen kokonaisluku. □

Lausetta 4.2 vastaavaan tulokseen on päädytty myös toisenlaisella lähestymistavalla lähteessä [7]. Seuraava karakterisointi perustuu puolestaan Leibnizin lauseeseen 3.3.

Lause 4.3. *Luvut* $2n+1$ *ja* $2n+3$ $(n \geq 1)$ *ovat alkulukuja, jos ja vain jos*

$$12\big((2n-1)!-1\big) - 5(2n+1) \equiv 0 \pmod{(2n+1)(2n+3)}. \tag{4.8}$$

Todistus (vrt. [7, s. 98–99]). Oletetaan, että kongruenssi (4.8) on voimassa. Jos $n = 1$, niin $2n+1$ ja $2n+3$ ovat alkulukuja. Oletetaan sitten, että $n \geq 2$. Tällöin on voimassa myös $12\big((2n-1)!-1\big) - 5(2n+1) \equiv 0 \pmod{2n+1}$ ja edelleen

$$(2n-1)! - 1 \equiv 0 \pmod{2n+1},$$

sillä apulauseen 3.6 nojalla $3 \nmid 2n+1$. Nyt lauseen 3.3 nojalla $2n+1$ on alkuluku. Toisaalta on myös voimassa $12\big((2n-1)!-1\big) - 5(2n+1) \equiv 0 \pmod{2n+3}$ ja ekvivalentisti myös

$$12\big((2n-1)!-1\big) + 10 \equiv 0 \pmod{2n+3}, \tag{4.9}$$

sillä $2n+1 \equiv -2 \pmod{2n+3}$.

Apulauseen 3.6 nojalla $3 \nmid 2n+3$, joten luvut $2n$ ja $2n+3$ sekä lisäksi $2n+1$ ja $2n+3$ ovat suhteellisia alkulukuja. Kongruenssi (4.9) voidaan siis kertoa puolittain luvulla $2n(2n+1)$, jolloin saadaan

$$12\big((2n+1)! - 2n(2n+1)\big) + 10(2n)(2n+1) \equiv 0 \pmod{2n+3}.$$

Edelleen laskemalla sekä lisäämällä ja vähentämällä kongruenssin vasemmalle puolelle luku 12 saadaan ekvivalentisti

$$\begin{aligned}
&12(2n+1)! - 4n(2n+1) \\
&\quad\equiv 12(2n+1)! - 12 - 4n(2n+1) + 12 \\
&\quad\equiv 12\big((2n+1)! - 1\big) - 4(2n+3)(n-1) \\
&\quad\equiv 0 \pmod{2n+3}.
\end{aligned}$$

Tämä taas on ekvivalentti kongruenssin

$$(2n+1)! - 1 \equiv 0 \pmod{2n+3}$$

kanssa. Siispä lauseen 3.3 nojalla myös $2n+3$ on alkuluku.

Oletetaan sitten, että luvut $2n+1$ ja $2n+3$ ovat alkulukuja. Siispä kongruenssi $(2n+1)! - 1 \equiv 0 \pmod{2n+3}$ on voimassa. Edelleen apulauseen 3.6 perusteella pätee kongruenssi (4.9). Koska $10 = (-2)(-5)$ ja $-2 \equiv 2n+1 \pmod{2n+3}$,

$$12\big((2n-1)! - 1\big) - 5(2n+1) \equiv 0 \pmod{2n+3}.$$

Toisaalta apulauseen 3.6 nojalla on myös voimassa

$$12\big((2n-1)! - 1\big) - 5(2n+1) \equiv 0 \pmod{2n+1}.$$

Koska $2n+1$ ja $2n+3$ ovat suhteellisia alkulukuja, voidaan kirjoittaa

$$12\big((2n-1)! - 1\big) - 5(2n+1) \equiv 0 \pmod{(2n+1)(2n+3)}. \qquad \square$$

Seuraava lause perustuu luvussa 3.1 esitettyyn lauseeseen 3.5.

Lause 4.4. *Olkoon n positiivinen kokonaisluku siten, että $n > 2$ ja $n \neq 7$. Tällöin kokonaisluvut n ja $n+2$ ovat alkulukuja, jos ja vain jos luku $4\,(n-3)! + n + 2$ on jaollinen luvulla n mutta ei ole jaollinen luvulla $n+2$, eli kongruensseina esitettynä kongruenssit*

$$4\,(n-3)! + n + 2 \equiv 0 \pmod{n}$$

ja

$$4\,(n-3)! + n + 2 \not\equiv 0 \pmod{n+2}$$

ovat voimassa.

Todistus (vrt. [2, s. 3–4]). Todistetaan ensin ehdon välttämättömyys. Oletetaan, että luvut n ja $n+2$ ovat alkulukuja, jolloin $n > 2$. Tällöin Wilsonin lauseen 3.2 nojalla kongruenssi $(n-1)!+1 \equiv 0 \pmod{n}$ pätee. Koska $n > 2$, voidaan kirjoittaa $(n-1)! = (n-1)(n-2)\,((n-3)!)$. Koska lisäksi pätee $(n-1)(n-2) \equiv n(n-3)+2 \equiv 2 \pmod{n}$, on voimassa myös $2(n-3)! + 1 \equiv 0 \pmod{n}$. Kun tämä kerrotaan puolittain luvulla 2, saadaan kongruenssi $4(n-3)! + 2 \equiv 0 \pmod{n}$. Siis pätee myös kongruenssi

$$4(n-3)! + n + 2 \equiv 0 \pmod{n}.$$

Soveltamalla lausetta 3.5 luvulle $n+2$ luku $n+2$ on alkuluku, jos ja vain jos pätee $4(n-3)! \not\equiv 0 \pmod{n+2}$ lukuun ottamatta poikkeuksia $n = 4$ ja $n = 7$. Tosin koska luku 6 ei ole alkuluku, poikkeus $n = 4$ ei ole voimassa tämän lauseen suhteen. Siis koska $n+2$ on oletuksen nojalla alkuluku, pätee myös

$$4(n-3)! \equiv 4(n-3)! + n + 2 \not\equiv 0 \pmod{n+2}.$$

Todistetaan seuraavaksi ehdon riittävyys. Oletetaan siis, että luku $4\,(n-3)!+n+2$ on jaollinen luvulla n, mutta ei ole jaollinen luvulla $n+2$. Siispä on voimassa kongruenssi

$$4\,(n-3)! + n + 2 \equiv 0 \pmod{n}.$$

Aiemmin todistuksessa todetun perusteella pätee

$$2 \cdot 2\,(n-3)! + 2 \equiv 2(n-1)(n-2)\,(n-3)! + 2 \pmod{n},$$

joten tällöin myös on voimassa kongruenssi

$$2(n-1)! + 2 \equiv 0 \pmod{n}. \tag{4.10}$$

Mikäli n on pariton, voidaan kongruenssi (4.10) kertoa puolittain luvun 2 käänteisluvulla modulo n, joka on olemassa, koska $\text{syt}(2, n) = 1$. Tällöin Wilsonin lauseesta 3.2 suoraan seuraa, että luku n on alkuluku. Jos n taas on parillinen, on se muotoa $n = 2q$, jossa q on jokin positiivinen kokonaisluku. Tällöin kongruenssi (4.10) voidaan esittää muodossa $(2q-1)! \equiv -1 \pmod{q}$, josta edelleen seuraa epätosi kongruenssi $0 \equiv -1 \pmod{q}$, joten luku n ei voi olla parillinen. Näin ollen sen on oltava alkuluku.

Lisäksi oletuksen nojalla pätee myös $4\,(n-3)! + n + 2 \not\equiv 0 \pmod{n+2}$, joten on myös voimassa

$$4(n-3)! \not\equiv 0 \pmod{n+2}.$$

Aiemmin todistuksessa uudelleen muotoillun lauseen 3.5 nojalla myös luku $n+2$ on tällöin alkuluku. □

Seuraava karakterisointi nojaa lauseeseen 3.10.

Lause 4.5. *Luvut* $2n+1$ *ja* $2n+3$ $(n \geq 1)$ *ovat alkulukuja, jos ja vain jos*

$$8\Big(\big((2n-1)!!\big)^2 + (-1)^n\Big) + 5(-1)^n(2n+1) \equiv 0 \pmod{(2n+1)(2n+3)}. \tag{4.11}$$

Todistus (vrt. [7, s. 97]). Oletetaan, että kongruenssi (4.11) on voimassa. Tällöin pätee myös kongruenssi $8\Big(\big((2n-1)!!\big)^2 + (-1)^n\Big) \equiv 0 \pmod{2n+1}$ ja edelleen myös $\Big(\big((2n-1)!!\big)^2 + (-1)^n\Big) \equiv 0 \pmod{2n+1}$. Näin ollen lauseen 3.10 nojalla $2n+1$ on alkuluku.

Toisaalta kongruenssin (4.11) voimassaolosta seuraa myös, että

$$8\Big(\big((2n-1)!!\big)^2 + (-1)^n\Big) + 5(-1)^n(2n+1) \equiv 0 \pmod{2n+3}$$

pätee. Näin ollen pätee myös

$$8\Big(\big((2n-1)!!\big)^2 + (-1)^n\Big) - 10(-1)^n \equiv 0 \pmod{2n+3}.$$

Koska luvut $2n+1$ ja $2n+3$ ovat suhteellisia alkulukuja, voidaan kongruenssi kertoa puolittain luvulla $(2n+1)^2$, jolloin saadaan

$$8\Big(\big((2n+1)!!\big)^2 + (2n+1)^2(-1)^n\Big) - 10(-1)^n(2n+1)^2 \equiv 0 \pmod{2n+3}.$$

Edelleen laskemalla saadaan

$$8\big((2n+1)!!\big)^2 + 8(2n+1)^2(-1)^n - 10(-1)^n(2n+1)^2 \equiv 0 \pmod{2n+3}. \tag{4.12}$$

Laskemalla toinen ja kolmas termi yhteen saadaan

$$8\big((2n+1)!!\big)^2 - 2(-1)^n(2n+1)^2 \equiv 0 \pmod{2n+3}.$$

Lisäämällä ja vähentämällä termi $8(-1)^{n+1}$ tulee kongruenssi muotoon

$$8\Big(\big((2n+1)!!\big)^2 + (-1)^{n+1}\Big) - 2(-1)^n(2n+1)^2 - 8(-1)^{n+1} \equiv 0 \pmod{2n+3}.$$

Sillä $-2(-1)^n(2n+1)^2 - 8(-1)^{n+1} = -2(-1)^n(2n+1)^2 + 8(-1)^n = -2(-1)^n\big((2n-1)(2n+3)\big)$, pätee $(2n+3) \mid -2(-1)^n(2n+1)^2 + 8(-1)^n$, joten kongruenssi saadaan edelleen muotoon

$$8\Big(\big((2n+1)!!\big)^2 + (-1)^{n+1}\Big) \equiv 0 \pmod{2n+3}. \tag{4.13}$$

Koska $\operatorname{syt}(8, 2n+3) = 1$, voidaan luku 8 supistaa pois. Siispä lauseen 3.10 nojalla myös $2n+3$ on alkuluku.

Oletetaan sitten, että luvut $2n+1$ ja $2n+3$ ovat alkulukuja. Siispä lauseen 3.10 nojalla on voimassa

$$8\Big(\big((2n+1)!!\big)^2 + (-1)^{n+1}\Big) \equiv 0 \pmod{2n+3}.$$

Kulkemalla kongruenssista (4.13) kongruenssiin (4.12) seuraten aiempaa ekvivalentisti menevää päättelyä saadaan

$$8\Big(\big((2n+1)!!\big)^2 + (2n+1)^2(-1)^n\Big) - 10(-1)^n(2n+1)^2 \equiv 0 \pmod{2n+3}.$$

Tämä voidaan kertoa puolittain luvun $(2n+1)^2$ käänteisluvulla modulo $2n+3$, joka on olemassa, sillä $\operatorname{syt}\big((2n+1)^2, 2n+3\big) = 1$. Silloin saadaan

$$8\Big(\big((2n-1)!!\big)^2 + (-1)^n\Big) - 10(-1)^n \equiv 0 \pmod{2n+3}.$$

Koska $2n+1 \equiv -2 \pmod{2n+3}$, voidaan kirjoittaa edelleen

$$8\Big(\big((2n-1)!!\big)^2 + (-1)^n\Big) + 5(-1)^n(2n+1) \equiv 0 \pmod{2n+3}.$$

Toisaalta lauseen 3.10 nojalla pätee myös

$$8\Big(\big((2n-1)!!\big)^2 + (-1)^n\Big) + 5(-1)^n(2n+1) \equiv 0 \pmod{2n+1}.$$

Lisäksi luvut $2n+1$ ja $2n+3$ ovat suhteellisia alkulukuja. Siis voidaan kirjoittaa

$$8\Big(\big((2n-1)!!\big)^2 + (-1)^n\Big) + 5(-1)^n(2n+1) \equiv 0 \pmod{(2n+1)(2n+3)}. \qquad \square$$

Seuraava tulos perustuu lauseeseen 3.11. Lauseen muotoilussa on korjattu lähteessä [7] esiintynyt virhe. Lähteestä poiketen esitetään myös lauseen todistus.

Lause 4.6. *Luvut* $2n+1$ *ja* $2n+3$ $(n \geq 1)$ *ovat alkulukuja, jos ja vain jos*

$$\big((2n)!!\big)^2 + (-1)^n(2n+2) \equiv 0 \pmod{(2n+1)(2n+3)}. \tag{4.14}$$

Todistus. Oletetaan, että kongruenssi (4.14) pätee. Tällöin on voimassa

$$\big((2n)!!\big)^2 + (-1)^n \equiv 0 \pmod{2n+1},$$

sillä $2n+2 \equiv 1 \pmod{2n+1}$. Siispä lauseen 3.11 nojalla $2n+1$ on alkuluku.

Toisaalta kongruenssista (4.14) seuraa myös, että

$$\big((2n)!!\big)^2 + (-1)^n(2n+2) \equiv 0 \pmod{2n+3}$$

pätee. Edelleen on voimassa

$$\big((2n)!!\big)^2 + (-1)^{n+1} \equiv 0 \pmod{2n+3},$$

sillä $2n+2 \equiv -1 \pmod{2n+3}$. Nyt voidaan kirjoittaa

$$\big((2n+2)!!\big)^2 + (-1)^{n+1} \equiv 0 \pmod{2n+3},$$

koska $(2n+2)^2 \equiv 1 \pmod{2n+3}$. Siispä lauseen 3.11 nojalla $2n+3$ on alkuluku.

Oletetaan sitten, että luvut $2n+1$ ja $2n+3$ ovat alkulukuja. Tällöin lauseen 3.11 perusteella pätee

$$\big((2n+2)!!\big)^2 + (-1)^{n+1} \equiv 0 \pmod{2n+3}.$$

Tämä voidaan esittää muodossa

$$\big((2n)!!\big)^2 + (-1)^n(2n+2) \equiv 0 \pmod{2n+3}.$$

Koska toisaalta lauseen 3.11 nojalla pätee myös

$$\big((2n)!!\big)^2 + (-1)^n \equiv 0 \pmod{2n+1}$$

eli

$$\big((2n)!!\big)^2 + (-1)^n(2n+2) \equiv 0 \pmod{2n+1},$$

sekä lisäksi luvut $2n+1$ ja $2n+3$ ovat suhteellisia alkulukuja, voidaan kirjoittaa

$$\big((2n)!!\big)^2 + (-1)^n(2n+2) \equiv 0 \pmod{(2n+1)(2n+3)}. \qquad \square$$

4.2 Karakterisointi multiplikatiivisia funktioita hyödyntäen

Tässä alaluvussa lähestytään alkulukukaksosten karakterisointia erilaisesta näkökulmasta. Luvussa esitellään Eulerin phi-funktiota ja tekijäfunktiota hyödyntäviä alkulukukaksosten karakterisointeja.

Seuraavan lauseen muotoilussa on huomioitu artikkelissa [14] merkille pantu puute. Tässä tutkielmassa esitettävässä todistuksessa poiketaan tästä syystä lähteen [1] todistuksesta niiltä osin, joissa lähteen todistus vaati täydentämistä.

Lause 4.7 (Sergušovin lause)**.**

(a) Positiivinen kokonaisluku n on alkulukukaksosten tulo, jos ja vain jos pätee

$$\sigma(n) = n + 1 + 2\sqrt{n+1} \quad \textit{ja } n \neq 8.$$

(b) Positiivinen kokonaisluku n on alkulukukaksosten tulo, jos ja vain jos pätee

$$\phi(n) = n + 1 - 2\sqrt{n+1}.$$

Todistus (vrt. [10, s. 85–86] ja [1, s. 29–30]). Todistetaan ensin karakterisointi *(a)*. Oletetaan, että n on alkulukukaksosten tulo, eli $n = p(p+2)$, jossa p ja $p+2$ ovat alkulukuja. Tällöin suoraan laskemalla saadaan

$$\begin{aligned}
\sigma(n) &= \sigma\big(p(p+2)\big) = \sigma(p)\sigma(p+2) \\
&= (p+1)(p+3) = p(p+2) + 1 + 2(p+1) \\
&= p(p+2) + 1 + 2\sqrt{(p+1)^2} \\
&= p(p+2) + 1 + 2\sqrt{p(p+2)+1} \\
&= n + 1 + 2\sqrt{n+1}.
\end{aligned}$$

Oletetaan sitten, että $\sigma(n) = n+1+2\sqrt{n+1}$ on voimassa ja $n \neq 8$. Jotta kyseessä olisi kokonaisluku, on oltava $n+1 = m^2$, eli $n = m^2 - 1 = (m-1)(m+1)$, jossa m on jokin luvusta 3 poikkeava positiivinen kokonaisluku. Siispä saadaan

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

Oletetaan nyt ensin, että luvut $m-1$ ja $m+1$ ovat suhteellisia alkulukuja. Tällöin pätee

$$m(m+2) = \sigma\big((m-1)(m+1)\big) = \sigma(m-1)\sigma(m+1).$$

Toisaalta tekijäfunktion ominaisuuksien nojalla pätevät $\sigma(m-1) \geq m$ sekä $\sigma(m+1) \geq m+2$. Siispä $\sigma(m-1) = m$ sekä $\sigma(m+1) = m+2$, joten luvut $m-1$ ja $m+1$ ovat luvussa 3.2 määritelmän 3.7 jälkeen esitetyn huomautuksen perusteella kummatkin alkulukuja.

Oletetaan sitten, etteivät luvut $m-1$ ja $m+1$ ole suhteellisia alkulukuja. Tällöin $\text{syt}(m-1, m+1) = d$, jossa $d > 1$. Toisaalta suurimman yhteisen tekijän ominaisuuksien perusteella pätee myös $d = \text{syt}\big(m+1, m-1-(m+1)\big) = \text{syt}(m+1, -2) =$

syt$(m+1,2)$. Koska $d > 1$, on oltava $d = 2$. Näin ollen m on pariton. Merkitään $m = 2k+1$, jossa k on jokin lukua 1 suurempi positiivinen kokonaisluku, koska $m \neq 3$. Näin saadaan

$$\sigma\big((2k+1-1)(2k+1+1\big) = \sigma\big(4k(k+1)\big) = 4k^2+8k+3.$$

Nyt, jos k on pariton, huomataan, että syt$\big(k, 4(k+1)\big) = 1$. Koska lisäksi $k > 1$, voidaan kirjoittaa

$$4k^2+8k+3 = \sigma\big(k \cdot 4(k+1)\big) = \sigma(k)\sigma\big(4(k+1)\big) \geq (k+1)(4k+5) = 4k^2+9k+5.$$

Saatu epäyhtälö ei päde millään luvun k arvolla, joten luvun k on oltava parillinen. Tällöin taas voimassa on syt$(4k, k+1) = 1$. Näin ollen voidaan kirjoittaa

$$4k^2+8k+3 = \sigma\big(4k(k+1)\big) = \sigma(4k)\sigma(k+1) \geq (4k+1)(k+2) = 4k^2+9k+2.$$

Tämä epäyhtälö ei ole voimassa millään parillisella luvun k arvolla, sillä se pätee vain kun $k = 1$. Siis n on alkulukukaksosten tulo.

Todistetaan sitten karakterisointi *(b)*. Oletetaan, että n on alkulukukaksosten tulo, eli $n = p(p+2)$, jossa p ja $p+2$ ovat alkulukuja. Laskemalla saadaan

$$\begin{aligned}
\phi(n) &= \phi\big(p(p+2)\big) = \phi(p)\phi(p+2) \\
&= (p-1)(p+1) = p(p+2)+1-2(p+1) \\
&= p(p+2)+1-2\sqrt{(p+1)^2} \\
&= p(p+2)+1-2\sqrt{p(p+2)+1} \\
&= n+1-2\sqrt{n+1}.
\end{aligned}$$

Oletetaan sitten, että $\phi(n) = n+1-2\sqrt{n+1}$ on voimassa. Jotta kyseessä olisi kokonaisluku, on oltava voimassa $n = m^2-1 = (m-1)(m+1)$, jossa m on jokin positiivinen kokonaisluku. Näin ollen saadaan

$$\phi\big((m-1)(m+1)\big) = m^2-1+1-2m = m(m-2).$$

Oletetaan seuraavaksi, että luvut $m-1$ ja $m+1$ ovat suhteellisia alkulukuja, jolloin on voimassa

$$m(m-2) = \phi\big((m-1)(m+1)\big) = \phi(m-1)\phi(m+1).$$

Toisaalta $\phi(m-1) \leq m-2$ ja $\phi(m+1) \leq m$. Näin ollen on oltava $\phi(m-1) = m-2$ ja $\phi(m+1) = m$, siis lauseen 3.13 perusteella lukujen $m-1$ ja $m+1$ täytyy olla alkulukuja.

Oletetaan sitten, että luvut $m-1$ ja $m+1$ eivät ole suhteellisia alkulukuja. Aivan kuten tekijäfunktion tapauksessa, nytkin pätee syt$(m-1, m+1) = 2$, joten m on pariton. Merkitään siis $m = 2k+1$, jossa k on jokin positiivinen kokonaisluku. Nyt voidaan kirjoittaa

$$\phi\big((2k+1-1)(2k+1+1)\big) = \phi\big(4k(k+1)\big) = 4k^2-1.$$

Jos nyt luku k on pariton, pätee

$$4k^2 - 1 = \phi\big(k \cdot 4(k+1)\big) = \phi(k)\phi(4k+4) \leq (k-1)(4k+3) = 4k^2 - k - 3,$$

mikä on epätotta luvun k positiivisilla arvoilla.

Toisaalta kun luku k on parillinen, pätee

$$4k^2 - 1 = \phi\big(4k(k+1)\big) = \phi(4k)\phi(k+1) \leq k(4k-1) = 4k^2 - k,$$

mikä pätee ainoastaan, kun $k = 1$. Siis luku n on alkulukukaksosten tulo. □

Sergušovin lauseen tapaukset yhdistämällä W. G. Leavitt ja A. Mullin kehittivät seuraavan lauseen.

Lause 4.8. *Positiivinen kokonaisluku n on alkulukukaksosten tulo, jos ja vain jos*

$$(n-1)^2 - \sigma(n)\phi(n) = 4. \tag{4.15}$$

Todistus (vrt. [9, s. 581]) ja [8, s. 198–201]. Oletetaan ensin, että yhtälö (4.15) on voimassa. Olkoon n jokin positiivinen kokonaisluku ja $n = \prod_{i=1}^{k} p_i^{a_i}$ sen alkulukuhajotelma, jossa $p_1 < p_2 < \cdots < p_k$. Nyt yhtälö (4.15) voidaan kirjoittaa lauseita 3.16 ja 3.20 hyödyntäen muotoon

$$\begin{aligned}
4 &= (n-1)^2 - \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1} \left(n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)\right) \\
&= (n-1)^2 - \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1} \prod_{i=1}^{k} p_i^{a_i} \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \\
&= (n-1)^2 - \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1} \prod_{i=1}^{k} p_i^{a_i-1} (p_i - 1) \\
&= (n-1)^2 - \prod_{i=1}^{k} \left(p_i^{a_i+1} - 1\right) p_i^{a_i-1} \\
&= n^2 - 2n + 1 - \prod_{i=1}^{k} \left(p_i^{2a_i} - p_i^{a_i-1}\right) \\
&= \prod_{i=1}^{k} p_i^{2a_i} - 2\prod_{i=1}^{k} p_i^{a_i} + 1 - \prod_{i=1}^{k} \left(p_i^{2a_i} - p_i^{a_i-1}\right).
\end{aligned}$$

Järjestelemällä yhtälön termit toisin saadaan yhtälö

$$2\prod_{i=1}^{k} p_i^{a_i} + 3 = \prod_{i=1}^{k} p_i^{2a_i} - \prod_{i=1}^{k} \left(p_i^{2a_i} - p_i^{a_i-1}\right). \tag{4.16}$$

Koska tapauksessa $k = 1$ yhtälö (4.16) redusoituisi epätoteen muotoon $2p^{a_1} + 3 = p^{a_1-1}$, on oltava voimassa $k \geq 2$. Toisin sanottuna kokonaisluvulla n on näin ollen oltava ainakin kaksi eri alkutekijää.

Tarkastellaan sitten tilannetta, jossa $p_1 = 2$. Tällöinhän yhtälön (4.16) vasen puoli on pariton, kun taas oikea puoli on parillinen. Voidaan näin ollen todeta, että on oltava $p_1 \geq 3$.

On selvää, että jokainen alkuluku p_i jakaa luvun $\prod_{i=1}^{k} p_i^{a_i}$. Näin ollen alkuluku p_i jakaa myös yhtälön (4.16) oikean puolen ensimmäisen termin lisäksi jälkimmäisen termin tekijän $\left(p_i^{2a_i} - p_i^{a_i-1}\right)$, kunhan $a_i > 1$. Tällaisessa tapauksessa alkuluku p_i jakaa yhtälön (4.16) koko oikean puolen ja näin ollen sen pitäisi voida myös jakaa yhtälön vasen puoli $2\prod_{i=1}^{k} p_i^{a_i} + 3$. Kuitenkin ainoa alkuluku p_i, joka jakaa yhtälön vasemman puolen, on 3. Siispä jos $a_i > 1$, on voimassa $p_i = 3$ ja muiden alkulukujen kohdalla on oltava voimassa $a_i = 1$.

Havaitaan seuraavaksi, että jos $p_1 = 3$, pätee $a_1 \leq 2$, sillä jos pätisi $a_1 \geq 3$, yhtälön (4.16) oikean puolen jälkimmäisen termin tekijä $3^{2a_1} - 3^{a_1-1}$ olisi jaollinen luvulla 3^2. Lisäksi luku 3^2 jakaisi selvästi myös yhtälön oikean sekä vasemman puolen ensimmäisen termin, muttei vasemman puolen toista termiä 3. Siis jos $p_1 = 3$, pätee $a_1 \leq 2$.

Tähän mennessä on siis onnistuttu rajaamaan jäljelle kaksi erilaista mahdollista tapausta luvun n alkulukuhajotelmaksi. Joko

$$n = p_1 p_2 \dots p_k, \tag{4.17}$$

jossa $p_1 \geq 3$, tai

$$n = 3^2 p_2 \dots p_k, \tag{4.18}$$

jossa $p_2 \geq 5$.

On jo osoitettu, että pätee $k \geq 2$. Osoitetaan nyt mahdollisten tapausten avulla, että tarkemmin on oltava voimassa $k = 2$. Tehdään vastaoletus, että $k \geq 3$. Tarkastellaan ensin tapausta (4.17). Tällöin tarkastelemalla yhtälön (4.16) oikeaa puolta, saadaan auki kirjoittamalla ja alaspäin arvioimalla

$$\begin{aligned}
\prod_{i=1}^{k} p_i^{2a_i} - \prod_{i=1}^{k} \left(p_i^{2a_i} - p_i^{a_i-1}\right) &= p_1^2 p_2^2 \cdots p_k^2 - (p_1^2 - 1)(p_2^2 - 1) \cdots (p_k^2 - 1) \\
&> p_1^2 p_2^2 \cdots p_k^2 - (p_1^2 - 1) p_2^2 p_3^2 \cdots p_k^2 \\
&= p_2^2 p_3^2 \cdots p_k^2 \\
&= \frac{p_2 p_3 \cdots p_k}{p_1} \cdot p_1 p_2 \cdots p_k \\
&> \frac{p_2 p_3 \cdots p_k}{p_2} \cdot p_1 p_2 \cdots p_k \\
&= p_3 p_4 \cdots p_k \cdot \prod_{i=1}^{k} p_i \\
&\geq p_3 \cdot \prod_{i=1}^{k} p_i
\end{aligned}$$

$$\geq 7 \prod_{i=1}^{k} p_i \quad (p_3 \geq 7, \text{ koska } p_1 \geq 3)$$
$$> 2 \prod_{i=1}^{k} p_i + 3.$$

Tarkastellaan sitten tapausta (4.18) samaan tapaan vastaoletuksen vallitessa. Siis jälleen auki kirjoittamalla ja alaspäin arvioimalla saadaan

$$\begin{aligned}
\prod_{i=1}^{k} p_i^{2a_i} - \prod_{i=1}^{k} \left(p_i^{2a_i} - p_i^{a_i - 1} \right) &= 3^{2\cdot 2} p_2^2 \cdots p_k^2 - (3^{2\cdot 2} - 3)(p_2^2 - 1) \cdots (p_k^2 - 1) \\
&= 81 p_2^2 \cdots p_k^2 - 78(p_2^2 - 1) \cdots (p_k^2 - 1) \\
&> 81 p_2^2 \cdots p_k^2 - 78 p_2^2 p_3^2 \cdots p_k^2 \\
&= 3 p_2^2 p_3^2 \cdots p_k^2 \\
&= p_1 p_2^2 p_3^2 \cdots p_k^2 \\
&= p_2 p_3 \cdots p_k \cdot \prod_{i=1}^{k} p_i \\
&\geq 35 \prod_{i=1}^{k} p_i \quad \text{(vastaoletuksen nojalla } k \geq 3) \\
&> 2 \cdot 3^2 \prod_{i=2}^{k} p_i + 3.
\end{aligned}$$

Siis yhtälö (4.16) ei voi olla voimassa, kun $k \geq 3$, joten $k = 2$. Tästä seuraa, että mahdolliset tapaukset luvun n alkulukuhajotelmaksi ovat näin ollen joko

$$n = p_1 p_2, \tag{4.19}$$

jossa $p_1 \geq 3$, tai

$$n = 3^2 p_2, \tag{4.20}$$

jossa $p_2 \geq 5$.

Osoitetaan seuraavaksi, että tapaus (4.20) ei ole mahdollinen. Jos se olisi voimassa, yhtälö (4.16) saataisiin muotoon

$$2(3^2 p_2) + 3 = 81 p_2^2 - (81 - 3)(p_2^2 - 1)$$

eli

$$18 p_2^2 + 3 = 3 p_2^2 + 78,$$

joka toisen asteen yhtälön normaalimuotoon kirjoitettuna on $3p_2^2 - 6p_2 + 25 = 0$. Koska tällä yhtälöllä ei ole reaalisia ratkaisuja, jäljelle jää vain tapaus (4.19).

Tarkastellaan siis vielä lopuksi tapausta (4.19). Nyt yhtälöstä (4.16) saadaan

$$2p_1 p_2 + 3 = p_1^2 p_2^2 - (p_1^2 - 1)(p_2^2 - 1) = p_1^2 + p_2^2 - 1,$$

josta edelleen järjestelemällä saadaan

$$4 = p_1^2 - 2p_1p_2 + p_2^2 = (p_1 - p_2)^2.$$

Näin ollen $|p_1 - p_2| = 2$, joten alkulukukaksosten määritelmän nojalla p_1 ja p_2 ovat alkulukukaksosia ja täten n on alkulukukaksosten tulo.

Todistetaan sitten ekvivalenssin toinen suunta. Oletetaan, että n on alkulukukaksosten tulo, eli $n = p(p+2)$, missä p ja $p+2$ ovat alkulukuja. Tällöin lauseen 3.13 nojalla $\phi(n) = (p-1)(p+1)$ ja toisaalta määritelmän 3.7 jälkeen esitetyn huomautuksen perusteella $\sigma(n) = (p+1)(p+2)$. Näin ollen pätee $\phi(n)\sigma(n) = (p-1)(p+1)^2(p+3)$. Toisaalta taas on voimassa

$$(n-1)^2-4 = n^2-2n-3 = (n-3)(n+1) = (p^2+2p-3)(p^2+2p-1) = (p+3)(p-1)(p+1)^2.$$

Siispä $(n-1)^2 - \sigma(n)\phi(n) = 4$ pätee. □

Lähteet

[1] T. Buchert, *On the twin prime conjecture*. Adam Mickiewicz University: Poznań, 2011.

[2] M. Chaves, *Twin primes and a primality test by indivisibility*. Escuela de Fisica, Universidad de Costa Rica, eprint arXiv:math/0211034. 2009.

[3] P. A. Clement, *Congruences for sets of primes*. The American Mathematical Monthly. 56(1):23–25, 1949.

[4] J. B. Dence & T. P. Dence, *A necessary and sufficent condition for twin primes*. Missouri Journal of Mathematical Sciences. 7(3):129–131, 1995.

[5] W. Dunham, *A note on the origin of the twin prime conjecture*. ICCM Notices. Notices of the International Congress of Chinese Mathematicians. 1(1):63–65, 2013.

[6] J. Górowski & A. Łomnicki, *Around the Wilson's theorem*. Annales Universitatis Paedagogicae Cracoviensis Studia ad Didacticam Mathematicae Pertinentia. 5:51–56, 2013.

[7] J. Górowski & A. Łomnicki, *Congruences characterizing twin primes*. Annales Universitatis Paedagogicae Cracoviensis Studia Mathematica. 11:95–100, 2012.

[8] R. Honsberger, *Mathematical delights*. Dolciani Mathematical Expositions. 28, 2004.

[9] W. G. Leavitt & A. A. Mullin, *Primes differing by a fixed integer*. Mathematics of Computation. 37(156):581–585, 1981.

[10] S. A. Sergušov, к проблеме о простых числах-близнецах (engl. *On the problem of prime-twins*). Jaroslavskiĭ Gosudarstvennyĭ Pedagogičeskiĭ Institut im. K. D. Ušinskogo. Učenye Zapiski. 82:85–86, 1971.

[11] H. Rezgui, *Conjecture of twin primes (Still unsolved problem in number theory). An expository essay*. Surveys in Mathematics and its Applications. 12:229–252, 2017.

[12] K. Rosen, *Elementary number theory and its applications*. Addison-Wesley Publishing Company: Reading, Massachusetts, 1986.

[13] W. Sierpiński, *Elementary theory of numbers*. North-Holland Mathematical Library, 31, North-Holland Publishing Co., Amsterdam; PWN–Polish Scientific Publishers: Warsaw, 1988.

[14] A. Tripathi, *A note on products of primes that differ by a fixed integer*. The Fibonacci Quarterly. The Official Journal of the Fibonacci Association. 48(2):144–149, 2010.