

Ville Kaukoranta

NÄENNÄISALKULUVUT

Tiivistelmä

Ville Kaukoranta: Näennäisalkuluvut

Kandidaattitutkielma

Tampereen yliopisto

Matematiikan ja tilastotieteen tutkinto-ohjelma

Maaliskuu 2023

Tämän tutkielman tarkoituksena on esitellä pseudo- eli näennäisalkulukujen erilaisia määritelmiä ja sitä, miten nämä määritelmät liittyvät lukuteorian perustavanlaatuisiin käsitteisiin, kuten jaollisuuteen. Tutkielmassa rajataan laajuussyistä ulos aiheita koskevat käytännön sovellukset. Teoksen lähdeaineistona käytetään kahta oppikirjalähdettä.

Tutkielman toinen luku sisältää aiheen kannalta olennaiset esitiedot. Lukuteorian käsitteistä esitellään jaollisuuden, suurimman yhteisen tekijän, alkuluvun, kongruenssin sekä Diofantoksen yhtälön ratkaisujen määritelmät. Jaollisuuden, kongruenssin sekä Diofantoksen yhtälön ratkaisujen osalta esitellään myöhemmin tarvittavia lauseita todistuksineen. Lukuteorian lisäksi esitiedoissa käsitellään havainnollistavina keinoina myös logiikan perustavanlaatuisia käsitteitä, kuten välttämättömän ehdon (implikaation) sekä välttämättömän ja riittävän ehdon (ekvivalenssin) määritelmät.

Tutkielman kolmannessa luvussa esitellään eräs alkulukuja koskeva välttämätön ja riittävä ehto, Wilsonin lause, sekä todistetaan, että lause on todella yhtäpitävä sen kanssa, että tarkasteltava luku on alkuluku. Wilsonin lauseesta annetaan yksittäinen esimerkki, jota hyödynnetään todistuksen havainnollistamisessa. Tämän jälkeen esitellään eräs alkulukuja koskeva välttämätön ehto, Fermat'n pieni lause, sekä todistetaan, että alkuluvut toteuttavat kyseisen ehdon, mutta ettei lauseen toteutumisesta seuraa, että tarkasteltava luku olisi välttämättä alkuluku. Luvussa todistetaan lisäksi, että Fermat'n pienessä lauseessa tarkoitettu ehto voidaan esittää vaihtoehtoisessa muodossa, jota hyödynnetään esimerkiksi näennäisalkuluvun määritelmässä.

Tutkielman neljännessä ja viimeisessä luvussa käsitellään nimenomaan näennäisalkulukuja. Luvussa esitellään kolme erilaista näennäisalkuluvun tyyppiä: (Fermat'n) näennäisalkuluvut, näennäisalkuluvut kantaluvun a suhteen sekä absoluuttiset näennäisalkuluvut eli Carmichaelin luvut. Kaikista näennäisalkulukutyypeistä

annetaan esimerkit, ja erityisesti absoluuttisten näennäisalkulukujen osalta myös todistetaan, millä ominaisuuksilla tällaiset luvut voidaan löytää.

Avainsanat: Lukuteoria, alkuluvut, näennäisalkuluvut

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck -ohjelmalla.

Sisällys

1	Johdanto	5
2	Valmistelevia esitietoja	6
2.1	Lukuteorian valmistelevat esitiedot	6
2.2	Logiikan valmistelevat esitiedot	8
3	Alkulukujen ehtoja	10
3.1	Alkuluvun riittävät ja välttämättömät ehdot	10
3.2	Alkuluvun välttämättömät ehdot	12
4	Näennäisalkuluvut	14
4.1	Näennäisalkuluvut	14
4.2	Näennäisalkuluvut kantaluvun a suhteen	15
4.3	Carmichaelin luvut	15
	Lähteet	17

1 Johdanto

Tutkielmassa esitellään näennäis- eli pseudoalkulukuja ja niitä koskevia olennaisia määritelmiä ja lauseita sekä lauseiden todistuksia. Määritelmiä ja lauseita havainnollistetaan esimerkein.

Ensin tutkielman esitietoja koskevassa luvussa käsitellään lukuteorian valmistelvat tiedot, joihin sisältyy sekä perustavanlaatuisia määritelmiä että myöhemmissä todistuksissa tarvittavia lauseita. Tutkielman esitietoja koskevassa luvussa käsitellään omana osanaan logiikan valmistelvat tiedot, joita ovat lähinnä implikaation ja ekvivalenssin määritelmät esimerkkeineen.

Toiseksi tutkielmassa tarkastellaan alkulukujen ominaisuuksia. Tarkemmin käsitellään alkulukujen a) välttämättömiä ja riittäviä ehtoja sekä niiden b) välttämättömiä ehtoja. Erityisesti Wilsonin lauseen ja Fermat'n pienen lauseen merkitysten tarkastelussa hyödynnetään logiikan valmistelevia esitietoja.

Lopulta tutkielmassa käsitellään näennäisalkulukujen käsitettä ja eri tyyppisten näennäisalkulukujen määritelmiä.

Lukijan odotetaan tuntevan lukuteorian peruskäsitteitä kuten jakoyhtälön sekä lukujoukkoja, erityisesti kokonaislukujen joukon, ja kombinatoriikan peruskäsitteitä, erityisesti binomilauseen. Esityksen selkeyden nimissä kuitenkin lukuteorian ja logiikan peruskäsitteitä, kuten jaollisuus ja kongruenssi sekä riittävä ehto ja välttämätön ehto, käsitellään valmistelemissä esitiedoissa. Tutkielman lähdeoteksena käytetään Burtonin teosta *Elementary Number Theory* sekä logiikan määritelmien osalta Genslerin teosta *Introduction to Logic*.

2 Valmistelevia esitietoja

2.1 Lukuteorian valmistelevat esitiedot

Luvussa 2 esitellään joitakin pääaiheen käsittelyssä tarpeellisia määritelmiä ja lauseita. Tässä alaluvussa esitellään viisi määritelmää: jaollisuuden, suurimman yhteisen tekijän, alkuluvun, kongruenssin ja Diofantoksen yhtälön määritelmät. Lisäksi luvussa esitellään Diofantoksen yhtälöiden ratkeavuutta ja lineaarisen kongruenssin ratkaisujen määrää koskevat lauseet.

Määritelmä 2.1 ([1, s. 20]). Olkoot a ja b kokonaislukuja. Luvun b sanotaan olevan *jaollinen* luvulla a , jos on olemassa kokonaisluku c siten, että $b = ac$. Tällöin merkitään $a \mid b$. Jos b ei ole jaollinen luvulla a , merkitään $a \nmid b$.

Määritelmä 2.2 ([1, s. 21]). Olkoot a ja b kokonaislukuja, joista vähintään yksi on nollasta poikkeava. Lukujen a ja b *suurin yhteinen tekijä* on positiivinen kokonaisluku d , joka täyttää seuraavat ehdot:

1. $d \mid a$ ja $d \mid b$; ja
2. Jos $c \mid a$ ja $c \mid b$, niin $c \leq d$.

Jos d täyttää ehdot edellä kuvatulla tavalla, niin sitä merkitään $\text{sy}(a, b) = d$.

Lause 2.1. Jos $a \mid b$, niin myös $2^a - 1 \mid 2^b - 1$.

Todistus. Lauseen oletuksesta tunnetaan, että $a \mid b$, siis toisin sanoen $b = ka$ jollakin kokonaisluvulla k . $x^b - 1 = x^{ka} - 1$ voidaan kirjoittaa uudelleen muotoon

$$(x^a - 1)((x^a)^{k-1} + (x^a)^{k-2} + \dots + (x^a)^0).$$

Näin ollen $x^a - 1 \mid x^b - 1$, kun $a \mid b$.

□

Määritelmä 2.3 ([1, s. 40]). Kokonaisluku $p > 1$ on *alkuluku*, jos 1 ja p ovat ainoat positiiviset kokonaisluvut, joilla se on jaollinen. Kokonaislukua, joka on suurempi kuin 1, mutta joka ei ole alkuluku, kutsutaan *yhdistetyksi* luvuksi.

Määritelmä 2.4 ([1, s. 64]). Olkoon n kiinnitetty positiivinen kokonaisluku. Kokonaislukujen a ja b sanotaan olevan *kongruenteja (modulo n)*, jos $n \mid (a - b)$, tai toisin sanoen jos $a - b = kn$ jollekin kokonaisluvulle k . Tällöin merkitään $a \equiv b \pmod{n}$. Muussa tapauksessa kokonaislukujen a ja b sanotaan olevan *epäkongruenteja (modulo n)*.

Määritelmä 2.5 ([1, s. 33]). Olkoot a , b ja c kiinnitettyjä kokonaislukuja siten, että vähintään a tai b on nolasta poikkeava. Yhtälön, joka on muotoa $ax + by = c$, sanotaan olevan *Diofantoksen yhtälö*, jonka (yksittäinen) ratkaisu on kokonaislukujen x ja y muodostama pari.

Lause 2.2 ([1, s. 34]). *Lineaarisella Diofantoksen yhtälöllä $ax + by = c$ on ratkaisu täsmälleen silloin, kun $d \mid c$, missä $d = \text{syt}(a, b)$. Jos x_0, y_0 on jokin nimenomainen ratkaisu, niin muut ratkaisut löytyvät yhtälöillä*

$$x = x_0 + \frac{b}{d}t$$

$$y = y_0 - \frac{a}{d}t,$$

missä t käy läpi kaikki kokonaisluvut.

Todistus (ks. [1, s. 34-35]). Todistus oletetaan tunnetuksi ja sivuutetaan. □

Lause 2.3 ([1, s. 75]). *Kongruenssilla $ax \equiv b \pmod{n}$ on ratkaisu täsmälleen silloin, kun $d \mid b$, missä $d = \text{syt}(a, n)$. Jos $d \mid b$, niin kongruenssilla on d keskenään epäkongruenttia ratkaisua modulo n .*

Todistus (ks. [1, s. 76]). Todistuksessa oletetaan tunnetuksi lause perusteluineen: Jos $ca \equiv cb \pmod{n}$, niin $a \equiv b \pmod{n}$, missä $d = \text{syt}(c, n)$. [1, s. 67].

Tarkasteltava kongruenssi on ekvivalentti Diofantoksen yhtälön $ax - ny = b$ kanssa. Lauseen 2.2 perusteella tunnetaan, että tällä yhtälöllä on ratkaisu täsmälleen silloin, kun $d \mid b$. Lisäksi jos yhtälö on ratkeava ja jos x_0, y_0 on yksi nimenomainen ratkaisu, niin kaikkien muiden ratkaisujen muoto on

$$x = x_0 + \frac{n}{d}t$$

$$y = y_0 + \frac{a}{d}t,$$

jollakin mielivaltaisella kokonaisluvulla t .

Tarkastellaan nyt ensimmäisen yhtälön osalta sellaisia ratkaisuja, jotka esiintyvät luvun t arvoilla $t = 0, 1, 2, \dots, d - 1$:

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \dots, x_0 + \frac{(d-1)n}{d}$$

Väitämme, että kaikki nämä ratkaisut ovat keskenään epäkongruenteja modulo n ja että jokainen muu ratkaisu on kongruentti täsmälleen yhden edellä mainitun ratkaisun kanssa. Todistetaan ensin ratkaisujen inkongruenssi epäsuorasti osoittamalla, että lauseesta poikkeava oletus johtaa ristiriitaan. Jos olisi niin, että

$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \pmod{n},$$

missä $0 \leq t_1 < t_2 \leq d - 1$, niin saadaan

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2$$

Selvästi $\text{sy}(n/d, n) = n/d$. Tunnetuksi oletetun lauseen perusteella sieventämällä saadaan kongruenssi

$$t_1 \equiv t_2 \pmod{d},$$

eli toisin sanoen $d \mid t_2 - t_1$. Tämä on kuitenkin mahdotonta ottaen huomioon, että tarkastelun alussa valittujen luvun t arvojen valinnan perusteella $0 < t_2 - t_1 < d$.

Osoitetaan sitten, että mikä tahansa muu ratkaisu $x_0 + (n/d)t$ on kongruentti (modulo n) yhden edellä mainituista d kokonaisluvusta kanssa. Jakoyhtälön avulla t voidaan kirjoittaa muotoon $t = qd + r$, missä $0 \leq r \leq d - 1$. Näin ollen

$$\begin{aligned} x_0 + \frac{n}{d}t &= x_0 + \frac{n}{d}(qd + r) \\ &= x_0 + nq + \frac{n}{d}r \\ &\equiv x_0 + \frac{n}{d}r \pmod{n}, \end{aligned}$$

missä $x_0 + (n/d)r$ on yksi valituista d ratkaisusta. □

2.2 Logiikan valmistelevat esitiedot

Seuraavaksi esitellään riittävän ehdon, välttämättömän ehdon ja riittävän ja välttämättömän ehdon käsitteet ja niiden määritelmät.

Lauseen 1 riittävällä ehdolla tarkoitetaan sellaista lausetta 2, jonka toteutumisesta voidaan päätellä lauseen 1 toteutuminen. Välttämättä kuitenkaan lauseen 1 toteutumisesta ei voida päätellä lauseen 2 toteutumista, eli päättely ei ole yhtäpitävä toisin päin.

Määritelmä 2.6 (vrt. [2, s. 140]). Olkoot p ja n lauseita. Jos n on tosi tai jos n ja p ovat molemmat epätosia, niin $p:n$ (totuuden) sanotaan olevan *riittävä ehto* n :lle ($n:n$ totuudelle). Tällöin merkitään

$$p \Rightarrow n$$

Lauseen 1 välttämättömällä ehdolla tarkoitetaan sellaista lausetta 2, jonka on toteuduttava vähintään silloin, kun lause 1 toteutuu. Kuitenkaan lauseen 2 toteutumisesta ei voida päätellä lauseen 1 toteutumista, eli päättely ei ole yhdenpitävä toisin päin.

Määritelmä 2.7 (vrt. [2, s. 140]). Olkoot p ja n lauseita. Jos p on tosi tai jos n ja p ovat molemmat epätosia, niin $p:n$ (totuuden) sanotaan olevan *välttämätön ehto* n :lle ($n:n$ totuudelle). Tällöin merkitään

$$p \Leftarrow n$$

Lauseen 1 riittävällä ja välttämättömällä ehdolla tarkoitetaan sellaista lausetta 2, joka toteutuu täsmälleen silloin, kun lause 1 toteutuu. Näin ollen lauseen 2 toteutumisesta voidaan päätellä lauseen 1 toteutuminen ja päinvastoin.

Määritelmä 2.8 (vrt. [2, s. 140]). Olkoot p ja n lauseita. Jos p on tosi vain silloin, kun n on tosi ja n on tosi vain silloin, kun p on tosi, niin $n:n$ (totuuden) sanotaan olevan *riittävä ja välttämätön ehto* p :lle ($p:n$ totuudelle) ja toisin päin. Tällöin merkitään

$$n \Leftrightarrow p$$

3 Alkulukujen ehtoja

3.1 Alkuluvun riittävät ja välttämättömät ehdot

Kokonaisluku voidaan tunnistaa alkuluvuksi edellä kuvatun määritelmän 2.3 perusteella. Jaollisuuden tutkimisen lisäksi myös määritelmän 2.3 kanssa yhtäpitävän, riittävän ja välttämättömän ehdon toteutumisen osoittaminen on myös keino tunnistaa luku alkuluvuksi. Tällaiseksi riittäväksi ja välttämättömäksi ehdoksi voidaan osoittaa Lagrangen vuonna 1771 todistamassa Wilsonin lauseessa esitetty kongruenssi [1, s. 98].

Lause 3.1. *Luku p on alkuluku täsmälleen silloin, kun $(p - 1)! \equiv -1 \pmod{p}$.*

Todistetaan ensin ehdon välttämättömyys, eli jos p on alkuluku, niin lauseessa 3.1 esitetty kongruenssi on tosi.

Todistus (ks. [1, s. 98]). Tapauksissa $p = 2$ ja $p = 3$ voidaan helposti havaita, että kongruenssi on tosi: $(2 - 1)! = 1 \equiv -1 \pmod{2} \equiv 1 \pmod{2}$ ja $(3 - 1)! = 2 \equiv -1 \pmod{3} \equiv 2 \pmod{3}$.

Tarkastellaan sitten tapauksia, joissa $p > 3$. Oletetaan, että a on kokonaisluku joukossa $\{1, 2, 3, \dots, p - 1\}$. Tarkastellaan sitten kongruenssia $ax \equiv 1 \pmod{p}$. Nyt $\text{syta}(a, p) = 1$. Lauseen 2.3 mukaisesti kongruenssissa on yksikäsitteinen ratkaisu modulo p , ja näin ollen on olemassa yksikäsitteinen a' siten, että $1 \leq a' \leq p - 1$, ja $aa' \equiv 1 \pmod{p}$. Koska p on alkuluku, $a = a'$, jos ja vain jos $a = 1$ tai $a = p - 1$. Tämän todistamiseksi todetaan, että kongruenssi $a^2 \equiv 1 \pmod{p}$ on ekvivalentti yhtälön $(a - 1) \cdot (a + 1) \equiv 0 \pmod{p}$. Näin ollen on oltava, että joko $a - 1 \equiv 0 \pmod{p}$, jolloin $a = 1$, tai että $a + 1 \equiv 0 \pmod{p}$, jolloin $a = p - 1$.

Edellä osoitetulla tavalla muut kokonaisluvut a ja a' (kuin 1 ja $p - 1$) ovat toisiinsa nähden erisuuria. Nämä muut kokonaisluvut $\{2, 3, \dots, p - 2\}$ voidaan esittää pareittain siten, että niiden tulo $aa' \equiv 1 \pmod{p}$. Näitä parien a ja a' perusteella muodostettuja kongruensseja on yhteensä $(p - 3)/2$ kappaletta, sillä joukon alkioden määrä oli alun perinkin $p - 1$, ja tästä joukosta on edelleen poistettu alkiot 1 ja $p - 1$. Siten alkioita on $p - 3$ kappaletta, jotka muodostavat $(p - 3)/2$ paria. Kun nämä kongruenssit kerrotaan keskenään ja kertoimet esitetään suuruusjärjestyksessä, saadaan

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

tai toisin ilmaistuna

$$(p - 2)! \equiv 1 \pmod{p}$$

Kun tämä kerrotaan puolittain luvulla $p - 1$, saadaan kongruenssi

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

□

Esimerkki 3.1 (vrt. [1, s. 99]). Esitetään asian havainnollistamiseksi käytännön esimerkki Wilsonin lauseen ensin todistetusta implikaatiosta, eli että kongruenssi $(p-1)! \equiv -1 \pmod{p}$ pätee, kun p on alkuluku. Olkoon $p = 17$. Luku p on alkuluku, sillä se ei ole jaollinen millään muilla positiivisilla kokonaisluvuilla kuin luvuilla 1 ja 17. Jaetaan nyt kokonaisluvut $2, 3, \dots, 16$ ($(p - 3)/2 = 7$ pariaksi seuraavasti siten, että jokaisen parin tulo on kongruentti luvun 1 kanssa (modulo $p = 17$):

$$2 \cdot 9 = 18 = (17 + 1) \equiv 1 \pmod{17}$$

$$3 \cdot 6 = 18 = (17 + 1) \equiv 1 \pmod{17}$$

$$4 \cdot 13 = 52 = (3 \cdot 17 + 1) \equiv 1 \pmod{17}$$

$$5 \cdot 7 = 35 = (2 \cdot 17 + 1) \equiv 1 \pmod{17}$$

$$8 \cdot 15 = 120 = (7 \cdot 17 + 1) \equiv 1 \pmod{17}$$

$$10 \cdot 12 = 120 = (7 \cdot 17 + 1) \equiv 1 \pmod{17}$$

$$11 \cdot 14 = 154 = (9 \cdot 17 + 1) \equiv 1 \pmod{17}.$$

Näiden kongruenssien tulo voidaan esittää muodossa

$$15! = (2 \cdot 9)(3 \cdot 6)(4 \cdot 13)(5 \cdot 7)(8 \cdot 15)(10 \cdot 12)(11 \cdot 14) \equiv 1 \pmod{17}$$

ja näin ollen

$$16! \equiv 16 \equiv -1 \pmod{17}$$

Todistetaan seuraavaksi kuvatun ehdon riittävyys eli lauseen 3.1. implikaation voimassaolo myös toiseen suuntaan. Toisin sanoen, jos lauseessa 3.1 esitetty kongruenssi on tosi, niin p on alkuluku.

Todistus (ks. [1, s. 99]). Todistetaan väite epäsuorasti osoittamalla, että oletuksesta " p on yhdistetty luku" seuraa ristiriita. Jos p on yhdistetty luku, niin se on jaollinen luvulla d siten, että $1 < d < p$. Edelleen koska $d \leq p - 1$, niin d esiintyy myös luvun $(p - 1)!$ kertoimena, eli $d \mid (p - 1)!$. Oletuksen mukaan $p \mid (p - 1)! + 1$, ja siten myös $d \mid (p - 1)! + 1$. Näin ollen $d \mid 1$, mikä on ristiriidassa sen kanssa, että $1 < d < p$. Näin ollen päinvastaisen oletuksen on oltava tosi. □

3.2 Alkuluvun välttämättömät ehdot

Alkulukujen välttämättömistä ja riittävistä ehdoista on aiheellista erottaa vain välttämättömät ehdot. Alkuluvun välttämätön ehto on ehto, joka on tosi kaikille alkuluville, mutta jonka totuudesta ei seuraa, että luku olisi alkuluku. Tällaiseksi ehdoksi voidaan osoittaa Fermat'n pienessä lauseessa esitetty kongruenssi [1, s. 92].

Lause 3.2. *Olkoon a kokonaisluku ja olkoon p alkuluku siten, että $p \nmid a$. Tällöin $a^{p-1} \equiv 1 \pmod{p}$.*

Todistus (ks. [1, s. 92]). Aloitetaan todistus tarkastelemalla luvun a ensimmäisiä $(p - 1)$ monikertaa, eli kokonaislukuja

$$a, 2a, 3a, \dots, (p - 1)a$$

Koska $p \nmid a$, niin mikään yllä mainituista luvuista ei ole toisen kanssa kongruentti modulo p eikä toisaalta kongruentti luvun 0 kanssa modulo p . Jos olisi niin, että

$$ra \equiv sa \pmod{p}, 1 \leq r < s \leq p - 1$$

niin a voitaisiin supistaa, koska $\text{syt}(a, p) = 1$ ja saada $r \equiv s \pmod{p}$, mikä on yllä mainituin rajoituksin mahdotonta. Näin ollen kokonaislukujen $a, 2a, 3a, \dots, p - 1$ on oltava kongruentteja modulo p lukujen $1, 2, 3, \dots, p - 1$ kanssa (jossakin järjestyksessä.) Kun näistä kongruensseista otetaan tulo, havaitaan että

$$a \cdot 2a \cdot 3a \dots (p - 1)a \equiv 1 \cdot 2 \cdot 3 \dots (p - 1) \pmod{p}$$

joka voidaan kirjoittaa uudelleen

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

Kun $(p - 1)!$ supistetaan molemmilta puolilta (mikä on sallittua, sillä $p \nmid (p - 1)!$); erillinen todistus sivuutetaan) niin havaitaan, että $a^{p-1} \equiv 1 \pmod{p}$. \square

Edellä on todistettu, että jos p on alkuluku, niin Fermat'n pieni lause pätee. Kuitenkin vastaesimerkillä voidaan osoittaa, että Fermat'n pienen lauseen pätemisestä ei seuraa, että p olisi alkuluku.

Esimerkki 3.2. Olkoon $a = 2$ ja olkoon $p = 341$. Nyt $2^{340} \equiv 1 \pmod{p}$. Kuitenkin $11 \mid 341$, eli p ei ole alkuluku. Jaollisuus voidaan ilmaista myös muodossa $341 \mid 2^{341} - 2$.

Lause 3.3. *Olkoon p kokonaisluku siten, että $p \nmid 2$. Nyt $2^{p-1} \equiv 1 \pmod{p}$ eli $p \mid 2^{p-1} - 1$, jos (ja vain jos) $p \mid 2^p - 2$.*

Todistus. Osoitetaan ensin implikaatio vasemmalta oikealle, eli että oletuksesta seuraa lauseessa esitetty johtopäätös. Lauseke $2^p - 2$ voidaan kirjoittaa uudelleen muodossa $2 \cdot (2^{p-1} - 1)$. Oletuksen mukaan $2^{p-1} - 1$ on jaollinen luvulla p , joten selvästi myös $2 \cdot (2^{p-1} - 1)$ on jaollinen luvulla p .

Osoitetaan sitten, että lauseen mukaisesta johtopäätöksestä seuraa, että $p \mid 2^{p-1} - 1$. Jos $p \mid 2 \cdot (2^{p-1} - 1)$, niin joko

1. $p \mid 2$; tai
2. $p \mid 2^{p-1} - 1$

Implikaation ulkopuolisen oletuksen mukaan 2 ei ole kuitenkaan jaollinen luvulla p , joten jälkimmäisen ehdon on oltava voimassa. Siten myös implikaation toinen suunta on todistettu. \square

Lause 3.4. *Olko p ja a kokonaislukuja Fermat'n pienessä lauseessa kuvatulla tavalla. Luvulle a pätee, että $p \mid a^{p-1} - 1$, jos (ja vain jos) $p \mid a^p - a$.*

Todistus. Lauseke $a^p - a$ voidaan kirjoittaa lauseen 3.3 todistuksessa vastaavalla tavalla uudelleen $a \cdot (a^{p-1} - 1)$. Myös nyt todistettavassa tapauksessa oletuksesta $p \mid a^{p-1} - 1$ seuraa, että $p \mid a \cdot (a^{p-1} - 1)$. Implikaation toinen suunta pätee täysin vastaavasti. \square

Lauseessa 3.3 ja sen yleistyksenä toimivassa lauseessa 3.4 osoitetulla tavalla Fermat'n pienessä lauseessa kuvattu ehto voidaan esittää yhtäpitävällä tavalla uudelleen.

4 Näennäisalkuluvut

4.1 Näennäisalkuluvut

Näennäisalkuluvulla tarkoitetaan sellaista yhdistettyä lukua, joka toteuttaa alkuluvulle välttämättömän ehdon, kuten Fermat'n pienen lauseen tai sen kanssa yhdenpitävän ehdon. Vastaavia välttämättömiä ehtoja on muitakin, mutta ilman eri mainintaa yleensä tarkoitetaan nimenomaan Fermat'n pienessä lauseessa tarkoitettua ehtoa [1, s. 94].

Edellä lauseissa 3.3 ja 3.4 kuvatulla tavalla Fermat'n pienen lauseen mukainen välttämätön, mutta kuitenkin riittämätön ehto alkuluvuille voidaan kirjoittaa muodossa $p \mid a^p - a$. Siten myös jäljempänä määritelmissä 4.1, 4.2 ja 4.3 esitetty jaollisuutta koskeva ehto on yhtäpitävä juuri Fermat'n pienen lauseen ehdon kanssa. Määritelmissä käsitellään ensin tapaus $a = 2$, ja sen jälkeen ehdon yleistetty muoto.

Määritelmä 4.1. Yhdistettyä lukua p sanotaan (*Fermat'n*) *näennäisalkuluvuksi*, jos $p \mid 2^p - 2$.

Esimerkki 4.1. Olkoon $p = 561$. Selvästi $p \nmid 2$. Nyt $561 \mid 2^{561} - 2 (= 2 \cdot (2^{560} - 1))$. Kuitenkin $561 = 11 \cdot 51$, eli 561 on yhdistetty luku ja siten näennäisalkuluku. Ks. myös esimerkki 3.2.

Näennäisalkulukuja voidaan osoittaa olevan ääretön määrä. Tarkastellaan asiaa sitä havainnollistavan lauseen ja sen todistuksen perusteella [1, s. 94].

Lause 4.1. *Jos p on pariton näennäisalkuluku, niin $M_p = 2^p - 1$ on lukua p suurempi pariton näennäisalkuluku.*

Todistus. Koska p on yhdistetty luku, niin se voidaan kirjoittaa muotoon $p = rs$, missä $1 < r \leq s < p$. Lauseesta 2.1 ja sen todistuksesta seuraa, että koska $r \mid p$, niin myös $2^r - 1 \mid 2^p - 1$. Toisin sanoen $2^r - 1 \mid M_p$, eli M_p on yhdistetty luku. Lauseessa esitetyn oletuksen mukaan $2^p \equiv 2 \pmod{p}$, ja näin ollen $2^p - 2 = kp$ jollekin kokonaisluvulle k . Tästä seuraa, että

$$2^{M_p-1} = 2^{2^p-2} = 2^{kp}$$

Edelleen tästä seuraa, että

$$\begin{aligned}
2^{M_p-1} - 1 &= 2^{kp} - 1 \\
&= (2^p - 1)(2^{p(k-1)} + 2^{p(k-2)} + \dots + 2^p + 1) \\
&= M_p(2^{p(k-1)} + 2^{p(k-2)} + \dots + 2^p + 1) \\
&\equiv 0 \pmod{M_p}
\end{aligned}$$

Edellä luvaton perusteella havaitaan, että $2^{M_p} - 2 \equiv 0 \pmod{M_p}$, eli M_p on näennäisalkuluku. \square

4.2 Näennäisalkuluvut kantluvun a suhteen

Näennäisalkuluvun määritelmässä käytetään aiemmin kuvatulla tavalla kantlukua 2. Luku voi kuitenkin periaatteessa olla myös jokin muu kokonaisluku, joka ei ole jaollinen kokonaisluvulla p . Tällöin on kuitenkin yksilöitävä, minkä kantluvun suhteen p on näennäisalkuluku.

Määritelmä 4.2 ([1, s. 95]). Yhdistettyä lukua n sanotaan (*Fermat'n*) *näennäisalkuluvuksi kantluvun a suhteen*, jos $n \mid a^n - a$.

Esimerkki 4.2. Olkoot $a = 3$ ja $p = 91$. Selvästi $p \nmid a$. Nyt $91 \mid 3^{91} - 3 (= 3 \cdot (3^{90} - 1))$. Kuitenkin $91 = 7 \cdot 13$, eli 91 on yhdistetty luku ja siten näennäisalkuluku kantluvun 3 suhteen.

4.3 Carmichaelin luvut

Määritelmä 4.3 ([1, s. 95]). Yhdistettyä lukua n sanotaan *absoluuttiseksi näennäisalkuluvuksi* tai *Carmichaelin luvuksi*, jos $n \mid a^n - a$ kaikilla kokonaisluvuilla a eli jos $a^n \equiv a \pmod{n}$ kaikilla kokonaisluvulla a .

Carmichaelin lukua koskevan esimerkin antaminen edellyttää keinoa osoittaa, että jokin luku on todellakin näennäisalkuluku kaikkien kantlukujen suhteen.

Lause 4.2. *Olkoon n yhdistetty, neliötön kokonaisluku muotoa $p_1 p_2 \dots p_r$, jossa jokainen luku p_i on toisistaan poikkeava alkuluku. Jos $p_i - 1 \mid n - 1$ kaikille $i = 1, 2, \dots, r$, niin n on absoluuttinen näennäisalkuluku.*

Todistus (ks. [1, s. 96]). Oletetaan, että a on kokonaisluku, jolle $\text{sy}(a, n) = 1$. Näin ollen $\text{sy}(a, p_i) = 1$ jokaiselle kokonaisluvulle i . Fermat'n pienestä lauseesta seuraa,

että $p_i \mid a^{p_i-1} - 1$. Lauseen oletuksesta $p_i - 1 \mid n - 1$ seuraa, että $p_i \mid a^{n-1} - 1$, ja siten $p_i \mid a^n - a$ kaikilla a :n ja $i = 1, 2, \dots, r$ arvoilla. \square

Esimerkki 4.3. Olkoon $p = 1729 = 7 \cdot 13 \cdot 19$. Nyt p on yhdistetty luku, joka koostuu kolmesta alkuluvusta edellä todistetussa lauseessa 4.2 kuvatulla tavalla. Näin ollen 1729 on absoluuttinen näennäisalkuluku.

Lähteet

- [1] Burton, D. *Elementary Number Theory, fifth edition*. McGraw-Hill, 2005.
- [2] Gensler, H. *Introduction to Logic, second edition*. Taylor & Francis Group, 2010.