Kongruenssi ja Eulerin lause

Pro gradu -tutkielma
Matematiikka
Iida Huotari
185707
Fysiikan ja matematiikan laitos
Itä-Suomen yliopisto
14. huhtikuuta 2014

Sisältö

1 Johdanto

Vanha nainen on menossa torille myymään kananmunia, mutta kiireinen ratsastaja törmää hevosellaan häneen ja kananmunat rikkoutuvat. Ratsastaja pyytää saada korvata rikkoutuneet kananmunat. Nainen ei muista munien tarkkaa määrää, mutta muistaa niitä kerätessään laskeneensa seuraavasti: "Kun poimin koriini niitä kaksi kerrallaan, jäljelle jäi lopuksi yksi, kun poimin kolme kerrallaan jäi jäljelle yksi, ja samalla tavalla tapahtui myös kun poimin kerrallaan neljä, viisi ja kuusi munaa. Mutta kun poimin kerrallaan seitsemän munaa, ei yhtään jäänyt jäljelle." Mikä siis oli kananmunien pienin mahdollinen määrä? Edellisen kaltaisia jakojäännösongelmia pohdittiin Euroopassa keskiajalla. Ongelmien varhaisin alkuperä vie mahdollisesti Kiinaan ja Intiaan 100-600 -luvuille, jossa niiden alkusysäyksenä toimi kalenterien muodostaminen ja laskeminen. Eurooppaan ongelmat rantautuivat esimerkiksi lorujen ja tarinoiden muodossa keskiajalla. [27]

Saksalainen Carl Friedrich Gauss oli yksi jakojäännösongelmista ja niiden ratkaisumenetelmistä kiinnostuneista. Vuonna 1801 hän julkaisi tunnetuimman teoksensa *Disquisitiones Arithmeticaen*, jossa hän esitteli kongruenssin käsitteen. Työni Luvussa 2 olen esitellyt kongruenssin määritelmän ja tärkeimpien tulosten lisäksi sen taustaa ja sovelluksia.

Luvuissa 3-5 olen esitellyt kolme kuuluisaa kongruenssiin liittyvää tulosta: Fermat'n pienen lauseen, sen yleistyksen Eulerin lauseen ja Wilsonin lauseen. Fermat'n pieni lause helpottaa eksponentteja sisältävien kongruenssien laskemista. Lause osoittaa, että alkuluku p jakaa luvun $a^{p-1} - 1$, kun p ei ole kokonaisluvun a tekijä. Lauseen käyttöä rajoittaa kuitenkin vaatimus luvun p alkulukuominaisuudesta. Myös Eulerin lauseen $a^{\phi(n)} \equiv 1 \pmod{n}$ käyttökelpoisuus perustuu kongruenssilaskujen helpottamiseen, kun niissä on mukana eksponentteja. Eulerin lauseen käyttö ei kuitenkaan vaadi moduloluvun n olevan alkuluku. Wilsonin lauseen nojalla alkuluku p jakaa luvun $(p-1)! + 1$. Lause onkin hyödyllinen kongruenssilaskuissa, joissa on mukana kertomia. Näistä kolmesta lauseesta olen esitellyt erilaisia todistuksia ja kertonut lauseiden taustasta tarkemmin.

Eulerin lauseeseen liittyy läheisesti Eulerin ϕ-funktio ja Lehmerin ja Carmichaelin ratkaisemattomat ongelmat, joita olen käsitellyt Luvuissa 4.1 ja 4.3. Fermat'n pienellä lauseella ja Wilsonin lauseella on myös yhteyksiä alkulukutestaukseen, ja tätä puolta olen tarkastellut työssäni Luvuissa 3.2 ja 5.2.

Lisäksi olen tutustunut ihmisiin näiden käsitteiden ja tulosten taustalla. Olen omistanut omat luvut Carl Friedrich Gaussille, Pierre de Fermat'lle, Leonhard Eulerille ja Edward Waringille, joissa olen kertonut tarkemmin kyseisten ihmisten elämänvaiheista ja saavutuksista matematiikassa.

2 Kongruenssi

2.1 Kongruenssin tausta

Lause 2.1.1. *Olkoon $a, b \in \mathbb{Z}$, $b > 0$. Tällöin on olemassa yksikäsitteiset kokonaisluvut q ja r siten, että*

$$a = qb + r,\ 0 \leq r < b.$$

Lukua r nimitetään jakojäännökseksi jaettaessa a luvulla b.

Todistus. Todistus löytyy kirjasta [6, s. 17]. □

Ikivanhat jakojäännösongelmat ovat lähtöisin Kiinasta ja Intiasta. Kiinassa ne saivat alkunsa kalentereihin liittyvistä laskutoimituksista, joita siellä on laskettu 200-luvulla [19]. 100-400 -lukujen tienoilla kiinalaisessa teoksessa *Sun-Tsŭ Suan Ching* ilmoitettiin runomuodossa sääntö nimeltä *t'ai-yen*, jonka avulla voi selvittää luvun, jolla on jakojäännökset 2, 3 ja 2 jaettaessa luvuilla 3, 5 ja 7. Pienin positiivinen kokonaisluku, joka toteuttaa ehdon, on 23. Ratkaisumenetelmä tunnetaan nimellä kiinalainen jäännöslause, ja kyseinen teos on yksi vanhimmista olemassa olevista jakojäännösongelmia käsittelevistä töistä. Saman ongelman ja ratkaisun esitti myös kreikkalainen Nicomachus ensimmäisen vuosisadan tienoilla.

Ensimmäinen algebran tutkielma oli noin 200-luvulla eläneen kreikkalaismatemaatikko Diofantoksen teos *Arithmetica*. Alun perin 13 kirjasta on säilynyt kuusi, ja ne koostuvat noin 200 ongelmasta, joihin kirjoissa on myös ratkaisut. Diofantoksen yhtälöllä tarkoitetaan yhtälöä, jossa yksi tai useampi tuntematon kokonaisluku tulee ratkaista. Lineaarisella Diofantoksen yhtälöllä, jossa on kaksi tuntematonta, tarkoitetaan muotoa

$$ax + by = c$$

olevaa yhtälöä. Luvut a, b ja c ovat kokonaislukuja, ja a ja b eivät molemmat voi olla nollia. [6, ss. 32-37]

Intiassa noin 400-luvulla elänyt astronomi Aryabhatta osasi ratkaista lineaarisia Diofantoksen yhtälöitä. 600-luvulla intialaisen Brahmaguptan teoksessa

esiintyi sama metodi kuin Aryabhattalla, joka tarkemmilla yksityiskohdilla lisättynä oli Bhaskara II:n teoksessa. Aryabhatta mahdollisesti antoi säännön "jauhimen" (*pulverizer*) löytämiseksi, vaikkakin hämärästi, ja Brahmaguptan teoksesta sääntö löytyy selkeämmässä muodossa. Aryabhattan työtä onkin luettu kommentoijien Bhaskara I:n (600-luku) ja Parameshvaran (1400-luku) sekä seuraajien Brahmaguptan ja Bhaskara II:n antaman lisätiedon valossa. Aryabhattan teos *Aryabhatiya* käsitteli myös astronomiaa. Van der Waerden [33] arvelee intialaisten kiinnostuksen lineaaristen Diofantoksen yhtälöiden ratkaisua kohtaan juontavan juurensa niiden tärkeydestä astronomisissa laskuissa. Myös Kiinassa käsiteltiin lineaarista Diofantoksen yhtälöä teoksessa *Nine Chapters on the Mathematical Art*, joka on kirjoitettu vuoden 206 ennen ajanlaskun alkua ja vuoden 221 välillä. [4, s. 243][11, s. 41] [26][33, s. 114]

Brahmagupta antoi oman sääntönsä sellaisen luvun löytämiseen, jonka jakojäännökset ovat 29 ja 3 jaettaessa luvuilla 30 ja 4. Myöhemmin, 1000-1100 -luvuilla, arabi Ibn al-Haitham ja intialainen Bhaskara II pohtivat ja ratkaisivat samantyyppisiä ongelmia kumpikin tahollaan. Euroopassa Leonardo Pisano mietti sellaista lukua, joka on jaollinen luvulla 7 ja saa jakojäännöksen yksi jaettaessa luvuilla 2, 3, 4, 5 ja 6. Häntä aiemmin saman ongelman oli ratkaissut Ibn al-Haitham. [5, 21][11, ss. 57-59]

Muotoa

$$x + y + z = m \text{ ja } ax + by + cz = n, \tag{2.1}$$

missä $m, n, a, b, c \in \mathbb{Z}_+$, olevien yhtälöiden muodostamat yhtälöryhmät esiintyivät kiinalaisissa käsikirjoituksissa 500-luvulla ja arabien kirjoituksissa 900-luvulla. Esimerkiksi 500-luvulla Chang Ch'iu-chienin teoksessa esiintyy yksi kuuluisimmista muotoa (2.1) olevista ongelmista; sadan linnun ongelma. Pulmassa, johon on useampi ratkaisu, kysytään, kuinka monta kukkoa, kanaa ja kananpoikasta voidaan kutakin ostaa, kun yhteensä niitä tarvitaan sata ja rahaa on sata kolikkoa. Kukon hinta on viisi kolikkoa, kanan kolme ja yhdellä kolikolla saa kolme poikasta. Esimerkkiratkaisuja saadulle kolmen tuntemattoman yhtälöparille

$$x + y + z = 100,\ 5x + 3y + \frac{1}{3}z = 100$$

ovat 4 kukkoa, 18 kanaa ja 78 poikasta, tai 8 kukkoa, 11 kanaa ja 81 poikasta. Euroopassa sadan linnun kaltainen ongelma esiintyy ensimmäisen kerran 800-luvulla Alcuinin teoksessa *Propositions for Sharpening Youths*. Myös Leonardo Pisanon kirjoituksissa 1200-luvulla esiintyy samantyyppisiä laskuja. Yleisinä ratkaisukeinoina yhtälöparille (2.1) olivat *regula coeci* (sokeiden

sääntö) ja *regula virginum* (neitsyiden sääntö). Euroopassa samantyyppinen ongelma on liitetty myös tavernassa käyntiin ja laskun maksamiseen, kun seurueeseen on kuulunut miehiä, naisia ja lapsia. [5, 20][6, s. 37][11, s. vi]

Heeffer on artikkelissaan [19] pohtinut jakojäännösongelmien ja kiinalaisen jäännöslauseen tuloa Eurooppaan. Hän on ottanut huomioon jakojäännöspulmien tarinanomaisuuden tiedon siirrossa ihmiseltä toiselle; suullinen tarinankerronta on mahdollisesti levittänyt ongelmat ja ratkaisukeinot mantereelta toiselle. Euroopassa jakojäännösongelmia onkin käsitelty keskiajalta lähtien. 1600-luvulla suosittuja olivat virkistyskäyttöön tarkoitetut matematiikan kirjat, joissa olennaisena osana oli jakojäännösongelmien ratkaiseminen. Kirjat toimivat kuitenkin lähinnä tiedon välittäjinä, joiden avulla kyseiset ongelmat siirtyivät 1700-luvun ihmisten tietoisuuteen. Systematisointia alkoikin tapahtua 1700-luvulla. Christian Wolff julkaisi vuonna 1710 kirjan *Anfangsgründe aller mathematischen Wissenschaften*, jonka tarkoituksena oli selventää jakojäännösongelmien monia sääntöjä ja todistaa niitä. 1730-luvulla myös Euler julkaisi artikkelin kyseisten pulmien systematisoinnista. Vuonna 1770 julkaistiin Eulerin oppikirja *Algebra* ja 1786 Kästnerin oppikirjan *Anfangsgründe der Mathematik* ensimmäinen lisäosa, jotka molemmat sisälsivät jakojäännösongelmien käsittelyn. Ongelmana oli kuitenkin esimerkiksi ratkaisujen pituus. Myös Carl Friedrich Hindenburg loi oman versionsa jakojäännösongelmista 1700-luvun lopulla. [5]

Saksalainen matemaatikko Carl Friedrich Gauss (1777-1855) tutustui Eulerin, Lagrangen, Lambertin ja Hindenburgin jakojäännösongelmien yleistämistä koskeviin töihin vuodesta 1791 eteenpäin. Gauss oli kiinnostuneena alkanut kirjoittaa omaa teostaan *Disquisitiones Arithmeticae*, ja vasta hänen työnsä selkiytti lukuteoriaa. Gaussin *Disquisitiones Arithmeticaen* takana olevan perusidean voidaan ajatella olevan yleisluontoisemman viitekehyksen luominen jakojäännöspulmien ratkaisemiseen. Bullynck [5] on tutkinut modulaariaritmetiikkaa ennen Gaussin aikaa, ja hänen mukaansa 1700-luvun kiinnostus jakojäännöspulmia kohtaan juonsi juurensa edistyneen matematiikan ja vanhojen perinteiden yhdistämisestä.

Gauss aloitti Collegium Carolinumissa opintonsa vuonna 1792. Niinä neljänä vuotena jotka hän koulussa vietti, Gauss käytti aikansa kielten opiskelun lisäksi myös omien matemaattisten taitojensa syventämiseen tutustumalla muiden matemaatikoiden teoksiin. Alkuluvut kiinnostivat Gaussia, samoin Lagrangen työt lukuterorian parissa. Bühlerin [7, ss. 9-10] mukaan tämä aika oli Gaussille laajaa tiedon keräämisen ja omaksumisen aikaa ja hänen kiinnostuksensa matematiikkaa kohtaan oli universaalia.

Seuraava opiskelupaikka oli Göttingenin yliopisto, jonka yksi valintaperuste oli paikan laaja kirjasto. Täällä Gauss opiskeli omien mielihalujensa mukaan, ja ilmeisesti kerättyään kaiken mahdollisen yliopistosta saatavan tiedon hän jätti sen jo vuonna 1798. Bühler olettaa, että hän oli tähän vuoteen mennessä kerännyt tarvittavat tiedot tulevia julkaisujaan varten, eikä kokenut tarpeelliseksi palata kouluun. Tohtorin väitöskirjansa hän palautti Helmstedtin yliopistoon vuonna 1799. [7, s. 15, 17]

Disquisitiones Arithmeticaen neljä ensimmäistä lukua oli kirjoitettu jo lähes lopulliseen muotoonsa vuonna 1797 ja viides luku oli valmis vuonna 1799. Ensimmäiset luonnokset viidestä ensimmäisestä luvusta ovat viimeistään vuodelta 1796. *Disquisitiones Arithmeticaen* ja Gaussin työn tärkeyttä lukuteorian parissa kommentoi Frobenius vuonna 1893 seuraavasti: "Diofantokselle ja Fermat'lle lukuteoria oli viihdyttävää ajattelun harjoittamista, älypeliä, ja Eulerin, Lagrangen ja Legendren alustavan työn jälkeen Gauss kohotti sen tieteenalojen joukkoon." [7, s. 32][12, s. 347]

2.2 Kongruenssi

Carl Friedrich Gauss julkaisi teoksessaan *Disquisitiones Arithmeticae* (Aritmeettisia tutkimuksia) kongruenssin käsitteen ja merkintätavan ensimmäisen kerran vuonna 1801. Kongruenssin käyttöön liittyvät päätulokset ovat kuitenkin luultavasti olleet joidenkin matemaatikoiden, kuten Eulerin ja Fermat'n, tiedossa jo aiemmin. [18, s. 77]

Kongruenssin Määritelmä 2.2.1 ja Lauseet 2.2.2 ja 2.2.3 ovat kirjasta [6, ss. 63-65].

Määritelmä 2.2.1. Olkoon n positiivinen kokonaisluku ja luvut a ja b ovat kokonaislukuja. Lukujen a ja b sanotaan olevan *kongruentteja modulo* n eli

$$a \equiv b \,(\bmod\ n),$$

jos erotus $a - b$ on jaollinen luvulla n.

Gauss käytti kongruenssille nykyisenkaltaista merkintää $a \equiv b \,(\bmod . a)$ [13, s. 11], ja hänen tavoitteenaan oli luoda sille yhtäsuuruuden käyttöä muistuttava laskukokonaisuus [4, s. 550]. Toinenkin saman ajan matemaatikko, Legendre, oli kiinnostunut kongruenssista, mutta käytti sille hieman erilaista merkintää; $a = b \bmod n$ [9, s. 106]. Teoksessaan *Disquisitiones Arithmeticae* Gauss toteaa yhtäsuuruuden ja kongruenssin välillä olevan yhteyden, mutta

monitulkintaisuuden välttämiseksi käyttää kongruenssille omaa merkintää $\equiv$ Legendren tyylistä poiketen [16, s. 1]. Myös Charles Babbage oli kiinnittänyt huomiota yhtäsuuruusmerkin hämmentävään käyttöön kahdessa eri yhteydessä. Hän viittasi Peter Barlow'n tapaan käyttää kongruenssille merkintää, jossa Legendren yhtäsuuruusmerkin tilalla oli vaakasuorassa kaksi päällekkäistä f-kirjainta. Gaussin *Disquisitiones Arithmeticaesta* tuli kuitenkin tunnettu teos, mikä aiheutti merkinnän $\equiv$ vakiintumisen [4, 550]. Sana modulo tulee latinasta ja liittyy englanninkieliseen sanaan *measure* eli mitta, mitata [13, s. 12]. [8, s. 34(II)]

Lause 2.2.2. *Olkoon n sovittu positiivinen kokonaisluku ja $a, b, c, d \in \mathbb{Z}$. Kongruenssille pätevät seuraavat säännöt:*

1. $a \equiv a \,(\mathrm{mod}\, n)$.
2. *Jos* $a \equiv b \,(\mathrm{mod}\, n)$, *niin* $b \equiv a \,(\mathrm{mod}\, n)$.
3. *Jos* $a \equiv b \,(\mathrm{mod}\, n)$ *ja* $b \equiv c \,(\mathrm{mod}\, n)$, *niin* $a \equiv c \,(\mathrm{mod}\, n)$.
4. *Jos* $a \equiv b \,(\mathrm{mod}\, n)$ *ja* $c \equiv d \,(\mathrm{mod}\, n)$, *niin* $a + c \equiv b + d \,(\mathrm{mod}\, n)$ *ja* $ac \equiv bd \,(\mathrm{mod}\, n)$.
5. *Jos* $a \equiv b \,(\mathrm{mod}\, n)$, *niin* $a + c \equiv b + c \,(\mathrm{mod}\, n)$ *ja* $ac \equiv bc \,(\mathrm{mod}\, n)$.
6. *Jos* $a \equiv b \,(\mathrm{mod}\, n)$, *niin* $a^k \equiv b^k \,(\mathrm{mod}\, n)$ *kaikille* $k \in \mathbb{Z}_+$.

Todistus. Todistus löytyy kirjasta [6, s. 65]. □

Lause 2.2.3. *Olkoon a ja b mielivaltaiset kokonaisluvut. Tällöin pätee*

$$a \equiv b \,(\mathrm{mod}\, n)$$

jos ja vain jos jaettaessa a ja b luvulla n, ne saavat saman ei-negatiivisen jakojäännöksen.

Todistus. Olkoon $a \equiv b \,(\mathrm{mod}\, n)$, jolloin kongruenssin määritelmän nojalla on olemassa $k \in \mathbb{Z}$, jolle pätee

$$a - b = kn. \tag{2.2}$$

Yhtälö (2.2) on yhtäpitävä muodon

$$a = b + kn \tag{2.3}$$

kanssa. Kun luku b jaetaan luvulla n, voidaan se kirjoittaa muodossa

$$b = qn + r,\ 0 \leq r < n,\ q \in \mathbb{Z}. \tag{2.4}$$

Sijoitetaan saatu b:n arvo yhtälöstä (2.4) yhtälöön (2.3)

$$a = b + kn = (qn + r) + kn = (q + k)n + r,$$

jolloin huomataan, että kongruenteilla luvuilla a ja b on sama jakojäännös r jaettaessa luvulla n.

Oletetaan seuraavaksi, että $a = q_1 n + r$ ja $b = q_2 n + r$, $0 \leq r < n$ ja $q_1, q_2 \in \mathbb{Z}$. Tällöin

$$a - b = q_1 n + r - q_2 n - r = (q_1 - q_2)n,$$

joten $n \mid (a - b)$ eli $a \equiv b \,(\bmod n)$. □

Kongruenssin laskusäännöt Lauseessa 2.2.2, seuraavat aputulokset ja varsinkin niiden seuraukset ovat hyödyllisiä lineaariseen kongruenssiin liittyvissä aputuloksissa Luvussa 2.3, Esimerkkien 2.3.10 ja 2.3.11 kongruenssin avulla ratkaistavissa jaollisuusogelmissa, Luvun 3.1 Esimerkeissä 3.1.3 ja 3.1.4 ja Fermat'n pienen lauseen todistuksissa, täydelliseen jäännösluokkasysteemiin ja redusoituun jäännössysteemiin liittyvissä Lauseissa 4.1.3 ja 4.2.4 ja Eulerin lauseen todistuksessa redusoidun jäännössysteemin avulla. [6, s. 21][29, s. 37, 74, 75, 91, 122]

Määritelmä 2.2.4. Olkoon $a, b \in \mathbb{Z}$ joista ainakin toinen on erisuuri kuin nolla. Lukujen a ja b *suurin yhteinen tekijä*, merkitään $\text{syt}(a, b)$, on $d \in \mathbb{Z}$, jolle pätee

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

Määritelmä 2.2.5. Kokonaisluvut a ja b ovat *suhteellisia alkulukuja*, kun niiden suurin yhteinen tekijä on yksi.

Määritelmä 2.2.6. Olkoon $a, b \in \mathbb{Z}$. Lukujen a ja b *lineaarikombinaatio* on muotoa $ma + nb$ oleva summa, jossa m ja n ovat kokonaislukuja.

Lause 2.2.7. *Jos $a, b, m, n \in \mathbb{Z}$ ja $c|a$ ja $c|b$, niin $c|(ma + nb)$.*

Todistus. Koska $c|a$ ja $c|b$, on olemassa kokonaisluvut k ja l siten, että $a = ck$ ja $b = cl$. Nyt voidaan kirjoittaa

$$ma + nb = mck + ncl = c(mk + nl),$$

eli $c|(ma + nb)$. □

Lause 2.2.8. *Olkoon $a, b \in \mathbb{Z}$, jotka molemmat eivät ole nollia. Lukujen a ja b suurin yhteinen tekijä on pienin positiivinen kokonaisluku, joka voidaan esittää lukujen a ja b lineaarikombinaationa.*

Todistus. Todistus löytyy kirjasta [29, ss. 75-76]. □

Lause 2.2.9. *Olkoon $a, b \in \mathbb{Z}$ ja $\text{syt}(a, b) = d$. Tällöin $\text{syt}(a/d, b/d) = 1$.*

Todistus. Olkoon e positiivinen kokonaisluku, jolle on voimassa $e|\frac{a}{d}$ ja $e|\frac{b}{d}$. Tällöin on olemassa $k, l \in \mathbb{Z}$ siten, että $a = dek$ ja $b = del$. Huomataan, että de jakaa molemmat luvuista a ja b. On kuitenkin oletettu, että $\text{syt}(a, b) = d$, jolloin on oltava $de \leq d$. Tämä pätee vain, jos $e = 1$, joten $\text{syt}(a/d, b/d) = 1$. □

Lemma 2.2.10. *Jos $a, b, c \in \mathbb{Z}_+$, $\text{syt}(a, b) = 1$ ja $a \mid (bc)$, niin $a \mid c$.*

Todistus. Koska $\text{syt}(a, b) = 1$, niin Lauseen 2.2.8 nojalla on olemassa kokonaisluvut k ja l, joille

$$ak + bl = 1. \tag{2.5}$$

Kerrotaan yhtälön (2.5) molemmat puolet luvulla c, jolloin se saa muodon

$$akc + blc = c. \tag{2.6}$$

Tiedetään, että $a|a$ ja $a|(bc)$, jolloin Lauseen 2.2.7 nojalla $a|(akc+blc)$. Koska a jakaa yhtälön (2.6) vasemman puolen, jakaa se myös yhtälön oikean puolen, eli $a|c$. □

Kuten kongruenssin laskusääntöjen nojalla tiedetään, kongruenssiyhtälöitä voidaan kertoa puolittain kokonaisluvuilla. Jakaminen puolittain ei kuitenkaan onnistu yhtä suoraviivaisesti ilman lisäehtoja ja moduloluvun muuttumista.

Lause 2.2.11. *Jos $a, b, c, n \in \mathbb{Z}$, $n > 0$, $\text{syt}(c, n) = d$ ja $ac \equiv bc \pmod{n}$, niin $a \equiv b \pmod{n/d}$.*

Todistus. Koska $ac \equiv bc \pmod{n}$, kongruenssin määritelmän nojalla on olemassa $k \in \mathbb{Z}$ siten, että

$$ac - bc = kn. \tag{2.7}$$

Jakamalla yhtälö (2.7) puolittain luvulla d, saadaan

$$\frac{c}{d}(a - b) = k\frac{n}{d}.$$

Koska $\text{syt}(c, n) = d$, Lauseen 2.2.9 nojalla $\text{syt}(\frac{c}{d}, \frac{n}{d}) = 1$. Lisäksi

$$\frac{n}{d} \mid \frac{c}{d}(a - b),$$

jolloin Lemman 2.2.10 nojalla $\frac{n}{d} \mid (a - b)$. On siis olemassa $l \in \mathbb{Z}$ siten, että

$$l\frac{n}{d} = a - b. \tag{2.8}$$

Yhtälö (2.8) voidaan kirjoittaa kongruenssina

$$a \equiv b \left(\bmod \frac{n}{d} \right).$$

□

Mikäli kuitenkin jakaja ja modululoku ovat suhteellisia alkulukuja, voidaan kongruenssiyhtälö jakaa puolittain ja modululoku säilyy ennallaan.

Seuraus 2.2.12. *Jos $a, b, c, n \in \mathbb{Z}$, $n > 0$, $\text{syt}(c, n) = 1$ ja $ac \equiv bc \,(\bmod n)$, niin $a \equiv b \,(\bmod n)$.*

Suurimman yhteisen tekijän lisäksi toinen hyödyllinen käsite on pienin yhteinen monikerta. Siihen liittyviä tuloksia tarvitaan Esimerkissä 3.2.1 ja Eulerin lauseen todistuksessa binomilauseen avulla Luvussa 4.2. [29, s. 93, 100, 124]

Määritelmä 2.2.13. Positiivisten kokonaislukujen a ja b *pienin yhteinen monikerta*, merkitään $\text{pym}(a, b)$, on pienin positiivinen kokonaisluku, joka on jaollinen sekä luvulla a että b.

Useamman kuin kahden positiivisen kokonaisluvun $a_1, a_2, \ldots, a_n$ pienin yhteinen monikerta on vastaavasti pienin positiivinen kokonaisluku, joka on jaollinen kaikilla luvuilla $a_1, a_2, \ldots, a_n$.

Lause 2.2.14. *Olkoon $a, b \in \mathbb{Z}$ ja $n_1, n_2, \ldots, n_k \in \mathbb{Z}_+$. Jos $a \equiv b \,(\bmod n_1)$, $a \equiv b \,(\bmod n_2)$,..., $a \equiv b \,(\bmod n_k)$, niin*

$$a \equiv b \,(\bmod \text{pym}(n_1, n_2, \ldots, n_k)).$$

Todistus. Todistus löytyy kirjasta [29, s. 124]. □

Seuraus 2.2.15. *Olkoon $a, b \in \mathbb{Z}$ ja $n_1, n_2, \ldots, n_k \in \mathbb{Z}_+$. Jos $a \equiv b \,(\bmod n_1)$, $a \equiv b \,(\bmod n_2)$,..., $a \equiv b \,(\bmod n_k)$ ja luvut $n_1, n_2, \ldots, n_k$ ovat pareittain suhteellisia alkulukuja, niin*

$$a \equiv b \,(\bmod n_1 n_2 \cdots n_k).$$

Todistus. Todistus löytyy kirjasta [29, s. 125]. □

2.3 Kongruenssin sovelluksia

Kongruenssin voidaan ajatella olevan yleisluontoisempi versio yhtäsuuruudesta. Kappaleessa on esitelty muutamia kongruenssin sovelluksia, jotka olisi hankala laskea ilman kongruenssia. Määritellään aluksi lineaarisen kongruenssin käsite, kiinalainen jäännöslause ja niihin liittyviä aputuloksia. [6, s. 23, 76-77, 79-80][29, s. 132]

Lineaarisella kongruenssilla tarkoitetaan muotoa $ax \equiv b \,(\mathrm{mod}\, n)$ olevaa yhtälöä, ja sen ratkaisulla kokonaislukua x_0, joka toteuttaa kyseessä olevan yhtälön eli $ax_0 \equiv b \,(\mathrm{mod}\, n)$.

Lause 2.3.1. *Lineaarisella kongruenssilla* $ax \equiv b \,(\mathrm{mod}\, n)$ *on ratkaisu* x *jos ja vain jos* $d|b$, $d = \mathrm{syt}(a, n)$. *Jos* $d|b$, *niin lineaarisella kongruenssilla on* d *keskenään ei-kongruenttia ratkaisua modulo* n.

Todistus. Todistus löytyy kirjasta [6, ss. 76-77]. □

Seuraus 2.3.2. *Jos* $\mathrm{syt}(a, n) = 1$, *niin lineaarisella kongruenssilla*

$$ax \equiv b \,(\mathrm{mod}\, n)$$

on yksikäsitteinen ratkaisu x *modulo* n.

Lauseen 2.3.1 nojalla kongruenssilla $ax \equiv 1 \,(\mathrm{mod}\, n)$ on ratkaisu jos ja vain jos $\mathrm{syt}(a, n) = 1$, ja nämä ratkaisut ovat kongruentteja modulo n.

Määritelmä 2.3.3. Olkoon $a \in \mathbb{Z}$ ja $\mathrm{syt}(a, n) = 1$. Tällöin lineaarisen kongruenssin $ax \equiv 1 \,(\mathrm{mod}\, n)$ ratkaisu $\bar{a}$ on nimeltään a:n *käänteisluku* modulo n.

Lemma 2.3.4. *Olkoot* a, b *ja* c *kokonaislukuja, ja* a *ja* b *eivät molemmat ole nollia. Jos* $a|c$ *ja* $b|c$ *ja* $\mathrm{syt}(a, b) = 1$, *niin* $ab|c$.

Todistus. Koska $a|c$ ja $b|c$, on olemassa kokonaisluvut k ja l, joiden avulla voidaan kirjoittaa $c = ak = bl$. Koska $\mathrm{syt}(a, b) = 1$, Lauseen 2.2.8 nojalla on olemassa kokonaisluvut m ja n, joiden avulla voidaan kirjoittaa lineaarikombinaatio

$$am + bn = 1. \tag{2.9}$$

Kerrotaan yhtälö (2.9) puolittain luvulla c, jolloin se saa muodon

$$cam + cbn = c. \tag{2.10}$$

Sijoitetaan yhtälöön (2.10) $c = ak$ ja $c = bl$, jolloin se voidaan kirjoittaa muodossa

$$(bl)am + (ak)bn = ab(lm + kn) = c,$$

joka on yhtäpitävää sen kanssa, että $ab|c$. □

Lause 2.3.5. ***Kiinalainen jäännöslause.*** *Olkoon positiiviset kokonaisluvut $m_1, m_2, \ldots, m_r$ pareittain suhteellisia alkulukuja. Kongruenssiyhtälöiden ryhmällä*

$$\begin{aligned} x &\equiv a_1 \,(\bmod m_1) \\ x &\equiv a_2 \,(\bmod m_2) \\ &\vdots \\ x &\equiv a_r \,(\bmod m_r) \end{aligned}$$

on tällöin yksikäsitteinen ratkaisu modulo $M = m_1 m_2 \cdot \ldots \cdot m_r$.

Todistus. Muodostetaan tulo $M = m_1 m_2 \cdot \ldots \cdot m_r$. Olkoon $k = 1, 2, \ldots, r$ ja olkoon $M_k = m/m_k = m_1 \cdots m_{k-1} m_{k+1} \cdots m_r$. Kaikki luvut $m_1, m_2, \ldots, m_r$ ovat pareittain suhteellisia alkulukuja, jolloin $\text{syt}(M_k, m_k) = 1$. Muodostetaan lineaarinen kongruenssiyhtälö

$$M_k x \equiv 1 \,(\bmod m_k), \tag{2.11}$$

jolla Seurauksen 2.3.2 nojalla on yksikäsitteinen ratkaisu modulo m_k. Olkoon tämä ratkaisu x_k. Seuraavaksi tulee osoittaa, että

$$\bar{x} = a_1 M_1 x_1 + a_2 M_2 x_2 + \ldots + a_r M_r x_r \tag{2.12}$$

on annetun kongruenssiyhtälöiden ryhmän ratkaisu. Nyt huomataan, että $M_i \equiv 0 \,(\bmod m_k)$, kun $i = 1, 2, \ldots, r$ ja $i \neq k$, eli M_i on jaollinen luvulla m_k. Tällöin yhtälö (2.12) sievenee muotoon

$$\bar{x} = a_1 M_1 x_1 + a_2 M_2 x_2 + \ldots + a_r M_r x_r \equiv a_k M_k x_k \,(\bmod m_k). \tag{2.13}$$

Lisäksi tiedetään yhtälön (2.11) nojalla, että $M_k x \equiv 1 \,(\bmod m_k)$, jolloin yhtälö (2.13) sievenee edelleen muotoon

$$\bar{x} \equiv a_k \,(\bmod m_k).$$

Siis kongruenssiyhtälöiden ryhmälle on olemassa ratkaisu, joka on voimassa kaikilla $k = 1, 2, \ldots, r$.

Osoitetaan seuraavaksi ratkaisun yksikäsitteisyys. Oletetaan, että x' on eräs annetun kongruenssiyhtälöiden ryhmän mikä tahansa toinen ratkaisu. Tällöin voidaan kirjoittaa

$$\bar{x} \equiv a_k \equiv x' \,(\bmod m_k). \tag{2.14}$$

Kongruenssi (2.14) voidaan ilmoittaa yhtäpitävässä muodossa $m_k|(\bar{x} - x')$ kaikilla $k = 1, 2, \ldots, r$. Koska luvut m_i ja m_j, $i, j = 1, 2, \ldots, r$, $i \neq j$, ovat pareittain suhteellisia alkulukuja, saadaan Lemman 2.3.4 nojalla ehto

$$m_1 m_2 \cdots m_r|(\bar{x} - x'), \tag{2.15}$$

joka voidaan kirjoittaa myös muodossa $\bar{x} \equiv x' \,(\bmod M)$. Siis kongruenssiyhtälöiden ryhmällä on ratkaisu ja se on yksikäsitteinen modulo M. □

Luvussa 2.1 mainittu lähes 2000 vuotta vanha ongelma sellaisen luvun etsimisestä, jolla on jakojäännökset 2, 3 ja 2 jaettaessa luvuilla 3, 5 ja 7, voidaan kirjoittaa kongruensseina

$$x \equiv 2 \,(\bmod 3),\ x \equiv 3 \,(\bmod 5),\ x \equiv 2 \,(\bmod 7).$$

Ongelma voidaan ratkaista kiinalaisella jäännöslauseella, sillä 3, 5 ja 7 ovat pareittain suhteellisia alkulukuja. Samantyyppinen ongelma on myös Esimerkissä 2.3.6, jonka on alun perin ratkaissut Frans van Schooten vuonna 1657 [11, s. 60].

Esimerkki 2.3.6. Etsitään kokonaisluku x, joka on jaollinen luvulla 7 ja saa jakojäännöksen 1 jaettaessa luvuilla 2, 3 ja 5.

Ratkaistaan luku x kiinalaisella jäännöslauseella. Luvut 2, 3, 5 ja 7 ovat pareittain suhteellisia alkulukuja. Ongelma voidaan kirjoittaa kongruensseina

$$\begin{aligned} x &\equiv 1 \,(\bmod 2) \\ x &\equiv 1 \,(\bmod 3) \\ x &\equiv 1 \,(\bmod 5) \\ x &\equiv 0 \,(\bmod 7). \end{aligned}$$

Lauseen 2.3.5 nojalla kongruenssiyhtälöiden ryhmällä on yksikäsitteinen ratkaisu modulo $M = 2 \cdot 3 \cdot 5 \cdot 7 = 210$, missä $m_1 = 2$, $m_2 = 3$, $m_3 = 5$ ja $m_4 = 7$. Olkoon $M_i = \frac{M}{m_i}$, $i = 1, 2, 3, 4$. Tällöin $M_1 = \frac{210}{2} = 105$, $M_2 = \frac{210}{3} = 70$, $M_3 = \frac{210}{5} = 42$ ja $M_4 = \frac{210}{7} = 30$. Muodostetaan lineaariset kongruenssit $M_i x_i \equiv 1 \,(\bmod m_i)$, $i = 1, 2, 3, 4$, eli

$$\begin{aligned} 105x_1 &\equiv 1 \,(\bmod 2) \qquad & 70x_2 &\equiv 1 \,(\bmod 3) \\ 42x_3 &\equiv 1 \,(\bmod 5) \qquad & 30x_4 &\equiv 1 \,(\bmod 7), \end{aligned}$$

joiden eräät ratkaisut ovat $x_1 = 1$, $x_2 = 1$, $x_3 = 3$ ja $x_4 = 4$. Alkuperäisen kongruenssiyhtälöiden ryhmän ratkaisu on tällöin

$$\begin{aligned} x &= a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 + a_4M_4x_4 \\ &= 1 \cdot 105 \cdot 1 + 1 \cdot 70 \cdot 1 + 1 \cdot 42 \cdot 3 + 0 \cdot 30 \cdot 4 = 301 \\ &\equiv 91 \,(\bmod 210). \end{aligned}$$

Kongruenssia voidaan käyttää myös arkipäiväisemmissä ongelmissa. Kuten kongruenssin taustasta tiedetään, jakojäännösongelmat saivat Kiinassa alkunsa kalenterilaskennosta. Vuonna 1582 tätä taitoa tarvittiin jälleen, kun paavi Gregorius VIII:n käskystä Euroopan katolisista maista alkaen siirryttiin karkausvuosien käyttöön ja juliaanisesta kalenterista gregoriaaniseen. Law'n esimerkissä [25] esitellään sovellus halutun viikonpäivän löytämiseksi, kun kosinnan jälkeen tulee päättää hääpäivä jollekin kesäkuun lauantaille. Kalenteria ei kuitenkaan ole käytettävissä. Tämä gregoriaanisen kalenterin käyttöön liittyvä kaava (2.16) on kirjasta [6, s. 126]. Esimerkissä 2.3.9 ratkaistaan samantapainen ongelma. Sitä ennen kuitenkin yksi aputulos. [6, s. 117, 122-123]

Määritelmä 2.3.7. Olkoon x mielivaltainen reaaliluku. Merkinnällä $[x]$ tarkoitetaan suurinta kokonaislukua, joka on pienempi tai yhtä suuri kuin x.

Lause 2.3.8. *Päiväyksen, jolle $k =$ päivä kuukaudesta, $m =$ kuukauden järjestysluku ja vuosi $Y = 100C + D$, viikonpäivä f saadaan kaavalla*

$$f \equiv k + [2{,}6m - 0{,}2] + D + \left[\frac{D}{4}\right] + \left[\frac{C}{4}\right] - 2C \,(\bmod 7), \tag{2.16}$$

jossa $C \geq 16$ ja $0 \leq D < 100$. Sunnuntaille $f = 0$, lauantaille $f = 6$ ja maaliskuu on vuoden ensimmäinen kuukausi.

Todistus. Todistus löytyy kirjasta [6, ss. 123-126]. □

Esimerkki 2.3.9. Selvitetään, mitkä päivät ovat toukokuussa 2016 sunnuntaita Lauseen 2.3.8 avulla.

Nyt $f = 0$, $m = 3$, $D = 16$, $C = 20$, ja kaava (2.16) saadaan muotoon

$$-k \equiv -f + [2{,}6m - 0{,}2] + D + \left[\frac{D}{4}\right] + \left[\frac{C}{4}\right] - 2C \,(\bmod 7). \tag{2.17}$$

Kerrotaan yhtälö (2.17) puolittain luvulla -1, jolloin

$$k \equiv f - [2{,}6m - 0{,}2] - D - \left[\frac{D}{4}\right] - \left[\frac{C}{4}\right] + 2C \,(\bmod 7). \tag{2.18}$$

Sijoitetaan tunnetut arvot yhtälöön (2.18) ja ratkaisuksi saadaan

$$\begin{aligned} k &\equiv 0 - [2{,}6 \cdot 3 - 0{,}2] - 16 - \left[\frac{16}{4}\right] - \left[\frac{20}{4}\right] + 2 \cdot 20 \\ &\equiv -7 - 16 - 4 - 5 + 40 = 8 \equiv 1 \,(\bmod 7). \end{aligned}$$

Sunnuntait ovat siis toukokuussa 2016 päivät 1, 8, 15, 22 ja 29.

Myös Esimerkkien 2.3.10 ja 2.3.11 jaollisuusongelmat olisi hankala ratkaista ilman kongruenssia. [6, ss. 67-68]

Esimerkki 2.3.10. Osoitetaan, että $53^{103} + 103^{53}$ on jaollinen luvulla 39, eli $53^{103} + 103^{53} \equiv 0 \,(\bmod 39)$.

Huomataan, että $103^2 \equiv 1 \,(\bmod 39)$ ja $53^2 \equiv 1 \,(\bmod 39)$. Lauseen 2.2.2 kohtien 3 ja 6 mukaan voidaan kirjoittaa

$$103^{53} \equiv 103^{52} \cdot 103 \equiv (103^2)^{26} \cdot 103 \equiv 1^{26} \cdot 103 \equiv 103 \equiv 25 \,(\bmod 39).$$

Samalla periaatteella myös

$$53^{103} \equiv 53^{102} \cdot 53 \equiv (53^2)^{51} \cdot 53 \equiv 1^{51} \cdot 53 \equiv 53 \equiv -25 \,(\bmod 39).$$

Nyt Lauseen 2.2.2 kohdan 4 nojalla

$$103^{53} + 53^{103} \equiv 25 + (-25) \equiv 0 \,(\bmod 39).$$

Esimerkki 2.3.11. Olkoon $n \geq 1$. Osoitetaan kongruenssin laskusääntöjen avulla, että $13 \mid (3^{n+2} + 4^{2n+1})$ eli $3^{n+2} + 4^{2n+1} \equiv 0 \,(\bmod 13)$.

Potenssin laskusääntöjen avulla huomataan, että

$$3^{n+2} \equiv 3^n \cdot 9 \,(\bmod 13) \tag{2.19}$$

ja

$$4^{2n+1} \equiv 4^{2n} \cdot 4 \equiv 16^n \cdot 4 \,(\bmod 13). \tag{2.20}$$

Koska $16 \equiv 3 \,(\bmod 13)$, niin $16^n \equiv 3^n \,(\bmod 13)$, jolloin kongruenssi (2.20) voidaan kirjoittaa muodossa

$$16^n \cdot 4 \equiv 3^n \cdot 4 \,(\bmod 13). \tag{2.21}$$

Yhdistämällä kongruenssit (2.19) ja (2.21) saadaan alkuperäinen yhtälö muotoon

$$3^{n+2} + 4^{2n+1} \equiv 3^n \cdot 9 + 3^n \cdot 4 \equiv 3^n(9 + 4) \equiv 3^n \cdot 13 \equiv 0 \,(\bmod 13).$$

2.4 Carl Friedrich Gauss

Kappaleen tiedot ovat kirjasta [4].

Saksalainen Carl Friedrich Gauss oli yksi 1800-luvun merkittävimmistä matemaatikoista. Lapsena matemaattisilla taidoillaan hämmästyttänyt nero pystyi valitsemaan matematiikan ja kielitieteen välillä vasta 18-vuotiaana onnistuttuaan osoittamaan, että harpilla ja viivoittimella pystyy piirtämään 17-sivuisen säännöllisen monikulmion.

Jo opiskeluaikana Gaussin saavutukset olivat huomattavat, ja hänen vuonna 1799 julkaistun tohtorin väitöskirjansa aiheena oli algebran peruslauseen todistus. Tunnetuimman kirjansa *Disquisitiones Arithmeticaen* hän julkaisi vuonna 1801 vain 24-vuotiaana. Kirja on seitsemän osan kokonaisuus, joka käsittelee lukuteoriaa, Gaussin mielestä "matematiikan kuningatarta". Neljä ensimmäistä osaa käsittelevät tiivistetysti 1700-luvun lukuteorian, kongruenssin ja jäännösluokan ollessa tärkeimmät käsitteet. Myös 17-sivuisen säännöllisen monikulmion konstruktio kuuluu teokseen.

Gaussin taidot ulottuivat lukuteoriasta tähtitieteeseen. Laskettuaan vastalöydetyn asteroidin radan ja näin autettuaan sen uudelleen havaitsemisessa sai Gauss osakseen mainetta ja kunniaa. Tästä seurasi edelleen käytössä oleva taivaan kiertolaisten paikan laskumenetelmä, Göttingenin observatorion johtoasema ja menestyksekäs tähtitieteen tutkielma. Virheteoriassa saavutetut tulokset, maanmittaus ja differentiaaligeometrian perustaminen ovat myös osa hänen ansiolistaansa. Gauss oli hieman vastahakoinen julkaisemaan omia tutkimuksiaan ennen kuin ne olivat tarkasti läpikäytyjä ja loppuun asti hiottuja. Jotkin hänen tutkimustuloksensa jäivät tämän vuoksi pitkiksi aikaa pimentoon, ja myöhemmin muut matemaatikot saivat kunnian niistä omilla julkaisuillaan. Näin kävi esimerkiksi Gaussin tutkiman kompleksimuuttujien teorian ja epäeuklidisen geometrian kohdalla.

3 Fermat'n pieni lause

Rosen listaa kirjassaan [29] kolme erityistä kongruenssia. Ensimmäinen näistä on Fermat'n pieni lause. Kaksi muuta, Eulerin ja Wilsonin lauseet, on esitelty luvuissa 4 ja 5. Koshy [23] kutsuu näitä kolmea lausetta klassikoiksi, sillä niillä on ollut merkittävä rooli kongruenssin ja siihen liittyvän teorian kehityksessä.

3.1 Fermat'n pienen lauseen todistuksia

Fermat'n pienen lauseen historia ulottuu noin 500-luvulle ennen ajanlaskun alkua, jolloin kiinalaiset oletettavasti tiesivät, että $2^p - 2 = 2(2^{p-1} - 1)$ on jaollinen alkuluvulla p. Ranskalainen Pierre de Fermat oli hyvin kiinnostunut lukuteoriasta, ja ilmeisesti tutkiessaan täydellisiä lukuja hän oli kiinnittänyt huomionsa tähän kiinalaisten otaksumaan vuoden 1640 tienoilla. Tarkalleen ottaen 18. päivänä lokakuuta 1640 Fermat lähetti kirjeen Bernhard Frenicle de Bessylle, jossa hän jakoi keksimänsä lauseen. Todistusta kirjeessä ei ollut, sillä hän "olisi kyllä lähettänyt sen, jos se ei olisi liian pitkä". [10, s. 59][23, s. 326]

Seuraavaksi Fermat'n pieni lause ja sen todistus [29, s. 187]. Fermat'n todistusta lauseelle ei ole löydetty, ja vasta vuonna 1736 ensimmäisen todistuksen julkaisi Leonhard Euler. Gottfried Leibniz (1646-1716) todisti lauseen jo ennen Euleria ennen vuotta 1683, mutta todistuksen sisältäneet käsikirjoitukset löytyivät vasta vuonna 1894. [32, s. 371]

Lause 3.1.1. ***Fermat'n pieni lause.*** *Jos a on kokonaisluku, p on alkuluku ja $p \nmid a$, niin*

$$a^{p-1} \equiv 1 \,(\bmod p).$$

Todistus. Aloitetaan listaamalla $p-1$ ensimmäistä a:n monikertaa:

$$a, 2a, 3a, 4a, \ldots, (p-1)a. \tag{3.1}$$

Osoitetaan ensin, että mikään joukon (3.1) luvuista ei ole kongruentti toisen saman joukon luvun kanssa modulo p, ja että mikään joukon (3.1) luvuista ei ole jaollinen luvulla p.

1. Jos olisi $ra \equiv sa \,(\bmod p)$, $1 \leq s < r \leq p-1$, niin Seurauksen 2.2.12 nojalla $r \equiv s \,(\bmod p)$ eli $r - s = kp$, $k \in \mathbb{Z}$. Tämä on mahdotonta, sillä $r, s < p$, jolloin myös $0 < r - s < p$. Ei siis voi olla $k \in \mathbb{Z}$ siten, että $r - s = kp$.

2. Jos olisi $p \mid ra$, niin koska $\text{syt}(a, p) = 1$, Lemman 2.2.10 nojalla $p \mid r$. Tämä on mahdotonta, sillä $1 \leq r < p$.

Joukossa (3.1) on siis $p-1$ lukua, joilla kaikilla on eri jakojäännökset jaettaessa luvulla p. Luvulla p jaettaessa pienimmät positiiviset jakojäännökset ovat $1, 2, 3, 4, \ldots, (p-1)$, ja niitä on $p-1$ kappaletta. Nyt siis joukon (3.1) kokonaislukujen pienimmät positiiviset jakojäännökset ovat $1, 2, 3, 4, \ldots, (p-1)$

mielivaltaisessa järjestyksessä. Lauseen 2.2.2 kohdan 4 mukaan voidaan kirjoittaa

$$a \cdot 2a \cdot 3a \cdot 4a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-1) \,(\bmod p)$$

eli

$$a^{p-1}(p-1)! \equiv 1 \cdot (p-1)! \,(\bmod p).$$

Tiedetään, että $\text{syt}((p-1)!, p) = 1$, jolloin Seurauksen 2.2.12 nojalla

$$a^{p-1} \equiv 1 \,(\bmod p).$$

□

Fermat ei aikanaan kirjoittanut väitettään varsinaisesti kongruenssina, vaan "Jokainen alkuluku jakaa minkä tahansa luvun potenssin miinus yksi, ja tämä potenssi jakaa aina edellä mainitun alkuluvun vähennettynä yhdellä." Hän ei siis ottanut huomioon sitä, että alkuluvulla p ja kokonaisluvulla a ei ole yhteisiä tekijöitä. [32, s. 366]

Fermat'n pienelle lauseelle on useita todistuksia. Leonhard Euler todisti lauseen useilla eri tavoilla muun muassa induktion ja binomilauseen avulla [32, ss. 371-377]. Seuraavaksi binomilause ja Fermat'n pienen lauseen todistus sen pohjalta. [6, ss. 88-89][9, ss. 110-111]

Lause 3.1.2. ***Binomilause.*** *Olkoon $a, b, n \in \mathbb{Z}_+$. Tällöin on voimassa*

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^j.$$

Todistus. Todistus löytyy kirjasta [29, ss. 31-32]. □

Todistus. **(Fermat'n pieni lause)** Osoitetaan ensin induktiolla, että jos $a \in \mathbb{Z}$ ja p on alkuluku, niin $a^p \equiv a \,(\bmod p)$.

1. Olkoon $a = 1$. Nyt väite saa muodon $1^p \equiv 1 \,(\bmod p)$. Tämä pitää paikkansa, sillä $p \mid 0$, koska $0 = 0 \cdot p$.

2. Induktio-oletus: $a^p \equiv a \,(\bmod p)$.

3. Induktioaskel: tulee osoittaa, että $(a+1)^p \equiv a + 1 \,(\bmod p)$. Binomilauseen nojalla

$$(a+b)^p = \sum_{j=0}^{p} \binom{p}{j} a^{p-j} b^j,$$

missä

$$\binom{p}{j} = \frac{p!}{j!(p-j)!} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-j+1)}{j \cdot \ldots \cdot 2 \cdot 1}. \tag{3.2}$$

Huomataan, että kaavassa (3.2) osoittaja on jaollinen luvulla p, kun $0 < j < p$. Yhtälö (3.2) voidaan kirjoittaa muodossa

$$j!\binom{p}{j} = p \cdot (p-1) \cdot \ldots \cdot (p-j+1) \equiv 0 \,(\mathrm{mod}\, p). \tag{3.3}$$

Koska $j < p$, on voimassa $p \nmid j!$ eli $\mathrm{syt}(p, j!) = 1$. Tällöin Lemman 2.2.10 nojalla täytyy olla $p|\binom{p}{j}$, joka voidaan kirjoittaa yhtäpitävässä muodossa $\binom{p}{j} \equiv 0 \,(\mathrm{mod}\, p)$. Lisäksi tiedetään, että $\binom{p}{0} = \binom{p}{p} = 1$. Tällöin

$$(a+b)^p = \binom{p}{0}a^p b^0 + \binom{p}{1}a^{p-1}b^1 + \ldots + \binom{p}{p}a^0 b^p \equiv a^p + b^p \,(\mathrm{mod}\, p). \tag{3.4}$$

Kun yhtälöön (3.4) sijoitetaan $b = 1$, se saadaan muotoon

$$(a+1)^p \equiv a^p + 1 \,(\mathrm{mod}\, p),$$

joka induktio-oletuksen $a^p \equiv a \,(\mathrm{mod}\, p)$ nojalla sievenee muotoon

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \,(\mathrm{mod}\, p).$$

Siis kaikilla $a \in \mathbb{N}$ pätee $a^p \equiv a \,(\mathrm{mod}\, p)$.

Tarkastellaan vielä tilanteita, joissa $a < 0$ tai $a = 0$.

Jos $a < 0$, niin a^p on myös negatiivinen, kun p on pariton alkuluku. Tällöin kongruenssiyhtälö $a^p \equiv a \,(\mathrm{mod}\, p)$ voidaan jakaa puolittain luvulla -1, sillä $\mathrm{syt}(-1, p) = 1$, ja saadaan $(-a)^p \equiv -a \,(\mathrm{mod}\, p)$. Jos p on parillinen alkuluku eli $p = 2$, niin $a^2 - a \equiv 0 \,(\mathrm{mod}\, 2)$ eli $2|a(a-1)$. Tämä pitää paikkansa, sillä toinen luvuista a ja $a-1$ on pariton ja toinen parillinen, jolloin niiden tulo on parillinen. Mikäli $a = 0$, niin $0^p \equiv 0 \,(\mathrm{mod}\, p)$.

Nyt

$$a^p \equiv a \,(\mathrm{mod}\, p) \tag{3.5}$$

pätee kaikilla $a \in \mathbb{Z}$.

Fermat'n pienen lauseen oletuksena on lisäksi $p \nmid a$. Tällöin Seurauksen 2.2.12 nojalla yhtälö (3.5) voidaan jakaa puolittain luvulla a, jolloin $a^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$, ja Fermat'n pieni lause on todistettu. □

Fermat'n pienen lauseen avulla voidaan selvittää pienin positiivinen jakojäännös. [6, s. 92][29, s. 188, 190]

Esimerkki 3.1.3. Selvitetään luvun $2^{1000000}$ pienin positiivinen jakojäännös modulo 17.

Fermat'n pienen lauseen nojalla tiedetään, että $2^{16} \equiv 1 \pmod{17}$, sillä 17 on alkuluku ja $17 \nmid 2$. Koska $16 \cdot 62500 = 1000000$, niin kongruenssin laskusääntöjen nojalla

$$2^{1000000} \equiv (2^{16})^{62500} \equiv 1^{62500} \equiv 1 \pmod{17}.$$

Siis luvun $2^{1000000}$ pienin positiivinen jakojäännös modulo 17 on 1.

Esimerkki 3.1.4. Osoitetaan Fermat'n pienen lauseen avulla, että

$$13 \mid (11^{12n+6} + 1), \text{ kun } n \geq 0.$$

Tulee siis osoittaa, että $11^{12n+6} \equiv -1 \pmod{13}$. Fermat'n pienen lauseen nojalla tiedetään, että $11^{12} \equiv 1 \pmod{13}$, sillä 13 on alkuluku ja $13 \nmid 11$. Kongruenssin laskusääntöjen nojalla tiedetään, että $11^{12n} \equiv 1^n \pmod{13}$ ja edelleen $11^{12n} \cdot 11^6 \equiv 11^6 \pmod{13}$. Koska $11 \equiv -2 \pmod{13}$, niin

$$11^{12n+6} \equiv 11^6 \equiv (-2)^6 \equiv 64 \equiv 12 \equiv -1 \pmod{13}.$$

3.2 Fermat'n pieni lause alkulukutestauksessa

Vaikka Fermat'n pieni lause helpottaakin kongruensseilla laskemista kuten Esimerkeissä 3.1.3 ja 3.1.4, ei sen avulla voida suoraan todeta moduloluvun olevan alkuluku. Seuraavassa esimerkissä osoitetaan, että vaikka $1105 \nmid 2$ ja $2^{1105-1} \equiv 1 \pmod{1105}$, niin 1105 ei ole alkuluku. [6, s. 89]

Esimerkki 3.2.1. Osoitetaan, että $2^{1105-1} \equiv 1 \pmod{1105}$.

Fermat'n pienen lauseen nojalla tiedetään, että alkuluvuille 5, 13 ja 17 pätee $2^4 \equiv 1 \pmod{5}$, $2^{12} \equiv 1 \pmod{13}$ ja $2^{16} \equiv 1 \pmod{17}$, sillä $5, 13, 17 \nmid 2$. Lisäksi potenssiin sopivasti korottamalla saadaan $2^{1104} \equiv (2^4)^{276} \equiv 1 \pmod{5}$, $2^{1104} \equiv (2^{12})^{92} \equiv 1 \pmod{13}$ ja $2^{1104} \equiv (2^{16})^{69} \equiv 1 \pmod{17}$. Seurauksen 2.2.15 nojalla moduloluvuksi voidaan valita tulo $5 \cdot 13 \cdot 17 = 1105$, jolloin $2^{1104} \equiv 1 \pmod{1105}$. Luku 1105 ei ole kuitenkaan alkuluku, sillä $1105 = 5 \cdot 13 \cdot 17$.

Fermat'n pienen lauseen avulla voidaan kuitenkin joissakin tapauksissa selvittää, onko moduloluku n yhdistetty. Valitaan kokonaisluku $1 < a < n$ ja lasketaan $a^{n-1} \pmod{n}$. Mikäli tulos ei ole kongruentti luvun 1 kanssa modulo n, on luku yhdistetty. Vaikka Fermat'n pientä lausetta ei aivan sellaisenaan voikaan käyttää alkulukujen varmaan löytämiseen, voi sitä käyttää aputuloksena sen selvittämiseen, onko luku n alkuluku. Vuonna 1876 ranskalainen Edouard Lucas esitti Lauseen 3.2.7 [6, s. 367]. Sen todistamiseen tarvitaan seuraavia aputuloksia. [6, s. 131, 147-148][13, s. 51][29, s. 208]

Määritelmä 3.2.2. Kokonaisluvuille $n \geq 1$ merkintä $\phi(n)$ ilmaisee niiden lukua n pienempien kokonaislukujen määrän, jotka ovat suhteellisia alkulukuja luvun n kanssa.

Lause 3.2.3. *Olkoon n positiivinen kokonaisluku. Tällöin $\phi(n) = n - 1$ jos ja vain jos n on alkuluku.*

Todistus. Todistus löytyy kirjasta [29, s. 208]. □

Määritelmä 3.2.4. Olkoon $n > 1$ ja $\text{syt}(a, n) = 1$. Luvun a *kertaluku modulo n* on pienin positiivinen kokonaisluku k, jolle $a^k \equiv 1 \pmod{n}$.

Lause 3.2.5. *Olkoon $a \in \mathbb{Z}$ kertalukua k modulo n. Tällöin $a^h \equiv 1 \pmod{n}$ jos ja vain jos $k \mid h$.*

Todistus. Oletetaan ensin, että $a^h \equiv 1 \pmod{n}$, missä $h \in \mathbb{Z}_+$. Tällöin, koska $k \leq h$, on olemassa $q, r \in \mathbb{Z}$ siten, että $h = qk + r$, $0 \leq r < k$. Voidaan siis kirjoittaa

$$a^h = a^{qk+r} = a^{qk}a^r \equiv 1^q a^r \equiv a^r \equiv 1 \pmod{n}.$$

Tiedetään, että $0 \leq r < k$. Mikäli kuitenkin $r > 0$, päädytään ristiriitaan, sillä k on pienin mahdollinen kokonaisluku, jolla kongruenssi toteutuu. Siis $r = 0$ ja $h = qk$ eli $k \mid h$.
Oletetaan seuraavaksi, että $k \mid h$. Tällöin on olemassa $j \in \mathbb{Z}$, jolle $h = jk$. Voidaan kirjoittaa

$$a^h = (a^k)^j \equiv 1^j \equiv 1 \pmod{n}.$$

□

Seuraus 3.2.6. *Jos $\text{syt}(a, n) = 1$ ja $a, n \in \mathbb{Z}$, $n > 0$ ja luku a on kertalukua k modulo n, niin $k \mid \phi(n)$.*

Todistus. Luvussa 4.2 todistettavan Eulerin lauseen nojalla $a^{\phi(n)} \equiv 1 \pmod{n}$. Lauseen 3.2.5 nojalla $k \mid \phi(n)$. □

Lause 3.2.7. ***Lucasin alkulukutesti.*** *Jos on olemassa kokonaisluku a siten että $a^{n-1} \equiv 1 \pmod{n}$ ja $a^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}$ kaikille luvun $n-1$ alkutekijöille p, niin n on alkuluku.*

Todistus. Olkoon a kertalukua k modulo n, eli Määritelmän 3.2.4 nojalla $\text{syt}(a, n) = 1$ ja k on pienin positiivinen kokonaisluku, jolla $a^k \equiv 1 \pmod{n}$. On siis Lauseen 3.2.5 nojalla oltava $k \mid (n-1)$, eli jollekin $j \in \mathbb{Z}$, $n-1 = kj$. Jos $j > 1$, niin sillä on olemassa alkutekijä q, eli jollekin $h \in \mathbb{Z}$, $j = qh$. Tällöin $n-1 = kqh$. Tästä seuraa, että

$$a^{(n-1)/q} = a^{kh} = (a^k)^h \equiv 1^h \equiv 1 \pmod{n}.$$

Päädyttiin ristiriitaan oletuksen kanssa, sillä $a^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}$. On siis oltava $j = 1$. Tiedetään myös Seurauksen 3.2.6 nojalla, että $k \mid \phi(n)$ eli luvun a kertaluku ei voi olla suurempi kuin $\phi(n)$. Tällöin $n-1 = k \leq \phi(n) \leq n-1$ eli $\phi(n) = n-1$, ja Lauseen 3.2.3 nojalla n on alkuluku. □

Lucasin lauseen heikkous on luvun $n-1$ tekijöihinjaon työläys. Tekijöitä voi olla hyvinkin paljon, ja ehdon $a^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}$ osoittamiseen kaikille alkutekijöille p voi mennä paljon aikaa. Vuonna 1914 Henry Pocklington kehitteli samantyylisen, mutta osittain tehokkaamman menetelmän. [6, s. 368]

Lause 3.2.8. *Olkoon $n-1 = mj$, missä $m = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}$, $m \geq \sqrt{n}$ ja $\text{syt}(m, j) = 1$. Jos jokaiselle alkuluvulle p_i, $1 \leq i \leq s$, on olemassa $a_i \in \mathbb{Z}$, jolle $a_i^{n-1} \equiv 1 \pmod{n}$ ja $\text{syt}(a_i^{(n-1)/p_i} - 1, n) = 1$, niin n on alkuluku.*

Todistus. Olkoon p luvun n mikä tahansa alkutekijä ja olkoon a_i kertalukua h_i modulo p. Kertaluvun määritelmän nojalla on oltava $\text{syt}(a_i, p) = 1$ ja Fermat'n pienen lauseen nojalla $a_i^{p-1} \equiv 1 \pmod{p}$. Siispä Lauseen 3.2.5 nojalla $h_i \mid (p-1)$. Koska $n \mid (a_i^{n-1} - 1)$, on $a_i^{n-1} - 1$ jaollinen myös kaikilla luvun n alkutekijöillä, eli voidaan kirjoittaa $a_i^{n-1} \equiv 1 \pmod{p}$. Tällöin myös $h_i \mid (n-1)$. Koska $\text{syt}(a_i^{(n-1)/p_i} - 1, n) = 1$, niin

$$a_i^{\frac{n-1}{p_i}} \not\equiv 1 \pmod{n} \tag{3.6}$$

ja $a_i^{\frac{n-1}{p_i}} \not\equiv 1 \pmod{p}$. Tästä seuraa, että $h_i \nmid (n-1)/p_i$, sillä jos näin olisi, päädyttäisiin ristiriitaan kohdan (3.6) kanssa.

Tarkastellaan ehtoja $h_i \mid (n-1)$ ja $h_i \nmid (n-1)/p_i$ tarkemmin. Päättely on lähteestä [24]. Jos luvun $n-1$ yksi alkutekijä p_i poistetaan, ei h_i enää jaa sitä. Siis kaikki luvun $n-1$ tekijät ovat myös h_i:n tekijöitä, jolloin $p_i^{k_i} \mid h_i$. Tästä seuraa, että $p_i^{k_i} \mid (p-1)$ kaikilla i, eli $m \mid (p-1)$. Äskeisen perusteella

$p > m \geq \sqrt{n}$ eli $p^2 > n$. Koska p on luvun n mikä tahansa alkutekijä, ei luvulla n voi täten olla muita tekijöitä kuin p, eli $n = p$ on itsekin alkuluku. □

Alkulukutestaukseen liittyy myös Miller-Rabinin testi. Menetelmä on probabilistinen, sillä se osoittaa luvun olevan yhdistetty, mutta ei todista alkulukuominaisuutta. Mikäli luku ei läpäise testiä, on se varmasti yhdistetty. Jos se taas läpäisee, on syytä epäillä sen olevan alkuluku. 2000-luvulla yksi tärkeimmistä alkulukutestaukseen liittyvistä tuloksista julkaistiin vuonna 2004. Agrawal, Kayal ja Saxena kehittivät testin, joka perustuu Fermat'n pienen lauseen yleistykseen. Heidän algoritminsa avulla voidaan selvittää varmasti, onko luku alkuluku vai ei, eli testi on deterministinen. [2][6, ss. 369-370]

3.3 Pierre de Fermat

Tiedot ovat teoksista [1, 4, 6, 23, 31, 32].

Yksi 1600-luvun merkittävimmistä matemaatikoista oli ranskalainen Pierre de Fermat (1601-1665). Ammatiltaan hän oli lakimies ja valtion virkamies, ja matematiikka oli hänelle pelkkä harrastus. Harrastelijoiden kuninkaaksi nimetty Fermat oli kuitenkin erityisen kiinnostunut Antiikin Kreikan matematiikasta, ja hän harrasti muun muassa tuon ajan kadonneiden teosten sisällön selvittämistä. Kun Claude Gaspard de Bachet vuonna 1621 käänsi Diofantoksen *Arithmetican* latinaksi ja julkaisi sen muistiinpanojen ja kommenttien kera, vetosi teos Fermat'han. Hänestä tuli nykyisen lukuteorian perustaja. Fermat'a kiinnostivat monet lukuteorian ongelmat kuten täydelliset luvut, Pythagoraan kolmikot ja jaollisuus. Juuri täydellisiä lukuja tutkiessaan hän luultavasti pääsi Fermat'n pienen lauseen jäljille. Hänen kynästään on lähtöisin myös Fermat'n suuri lause, jonka ratkaisemiseen kului 350 vuotta. Vuonna 1995 englantilainen Andrew Wiles todisti lauseen uurastettuaan seitsemän vuotta.

Vaikka Fermat oli hyvin kiinnostunut lukuteoriasta, vaikutti hän myös muiden matematiikan alojen kehitykseen. Fermat tutki ja kehitti analyyttistä geometriaa ja hän olikin Descartesin rinnalla toinen analyyttisen geometrian keksijöistä. Lisäksi hän kehitteli derivointia vastaavan menetelmän löytääkseen pisteet, joissa funktio saa maksimi- ja minimiarvonsa. Fermat työskenteli nykyistä integraalilaskentaa vastaavan aiheen parissa, sillä hän keksi käyrien rajoittaman alan teoreeman. Myös todennäköisyyslaskenta kehittyi Fermat'n ansiosta.

Fermat oli hyvin vastahakoinen julkaisemaan omia töitään ja varsinkin teoreemiensa todistuksia. Kirjeissään muille matemaatikoille hän saattoi kyllä kertoa uusimmasta lauseestaan, mutta jätti todistuksen tarkoituksella kertomatta. Elämänsä aikana hän julkaisi vain yhden suuremman teoksen. Useita Fermat'n keksintöjä on kuitenkin pystytty jäljittämään hänen lähettämistään kirjeistä. Fermat'n kuoleman jälkeen hänen poikansa löysi Fermat'n kopion *Arithmeticasta*, jonka marginaalit olivat täynnä omistajansa muistiinpanoja lukuteoriasta. Tilaa kirjoituksille ei ollut kuitenkaan ollut paljon, joten esimerkiksi Fermat'n suureen lauseeseen liittyvä reunamerkintä päättyy sanoihin "Olen keksinyt siihen todella ihmeellisen todistuksen, jolle tämä marginaali ei kuitenkaan riitä."

Fermat'a viehätti lukuteorian esitys kokoelmana ongelmia ja niiden ratkaisuja. Tämä ei kuitenkaan kiinnostanut ajan matemaatikkoja, joille lukuteoria näyttäytyi valikoimana ongelmia, joissa oli Wallisin mukaan "enemmän työtä kuin käyttöä tai vaikeutta". Fermat'n kuoleman jälkeen lukuteoria jäikin pimentoon useiksi vuosikymmeniksi.

4 Eulerin lause

Fermat'n pienen lauseen yleisempi muoto tunnetaan Eulerin lauseena (joissain yhteyksissä myös Eulerin ja Fermat'n lauseena). Euler esitti lauseen todistuksen vuonna 1758, joka oli alun perin Eulerin neljäs todistus Fermat'n pienelle lauseelle. Lauseen esitykseen tarvitaan ϕ-funktion käsite ja muita aputuloksia, joita Luvussa 4.1 käsitellään. [32, s. 377]

4.1 ϕ-funktio

Kuten Luvussa 3.2 määriteltiin, $\phi(n)$-funktiolla tarkoitetaan niiden lukua n pienempien positiivisten kokonaislukujen määrää, jotka ovat suhteellisia alkulukuja luvun n kanssa. Tällaisten lukujen tärkeyden Euler oli huomannut todistaessaan Fermat'n pientä lausetta [32, s. 378]. Kreikkalaisella kirjaimella $\phi(N)$ funktiota merkitsi vasta Gauss *Disquisitiones Arithmeticaessa*. Eulerin käyttämä merkintä funktiolle oli πN. ϕ-funktiosta voidaan käyttää myös nimitystä totientti ja J. J. Sylvesterin merkintää $T(n)$ vuodelta 1883 [8, s. 35(II)]. Sylvester myös määritteli luvun n totitiivit (*totitive*) olevan ne lukua n pienemmät kokonaisluvut, jotka ovat suhteellisia alkulukuja luvun n kanssa. Totienttifunktio siis kertoo totitiivien määrän. [10, s. 113-114, 124]

Luvussa käsiteltävät tulokset ovat kirjoista [6, s. 64, 132] ja [29, s. 121, 123-124, 209-211].

Määritelmä 4.1.1. *Täydellinen jäännösluokkasysteemi modulo n* on sellaisten kokonaislukujen joukko, jossa jokainen kokonaisluku on kongruentti modulo n yhden joukon kokonaisluvun kanssa.

Mitkä tahansa n kokonaislukua muodostavat täydellisen jäännösluokkasysteemin modulo n jos ja vain jos mitkään kaksi joukkoon kuuluvaa lukua eivät ole kongruentit keskenään modulo n.

Esimerkki 4.1.2. Luvut $\{5, -4, 7, -2, -1\}$ muodostavat täydellisen jäännösluokkasysteemin modulo 5, sillä mitkään kaksi tähän joukkoon kuuluvaa lukua eivät ole kongruentit keskenään modulo 5. Ehto huomataan helpommin kirjoittamalla $5 \equiv 0 \,(\mathrm{mod}\, 5)$, $-4 \equiv 1 \,(\mathrm{mod}\, 5)$, $7 \equiv 2 \,(\mathrm{mod}\, 5)$, $-2 \equiv 3 \,(\mathrm{mod}\, 5)$ ja $-1 \equiv 4 \,(\mathrm{mod}\, 5)$.

Lause 4.1.3. *Jos $r_1, r_2, \ldots, r_m$ on täydellinen jäännösluokkasysteemi modulo m ja $\mathrm{syt}(a, m) = 1$, $a \in \mathbb{Z}_+$, niin*

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

on täydellinen jäännösluokkasysteemi modulo m kaikille $b \in \mathbb{Z}$.

Todistus. Osoitetaan ensin, että mitkään kaksi luvuista

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

eivät ole kongruentit keskenään modulo m. Olkoon $1 \leq j, k \leq m$ ja

$$ar_j + b \equiv ar_k + b \,(\mathrm{mod}\, m).$$

Kongruenssin laskusääntöjen ja Seurauksen 2.2.12 nojalla $r_j \equiv r_k \,(\mathrm{mod}\, m)$. Koska $r_1, r_2, \ldots, r_m$ on täydellinen jäännösluokkasysteemi modulo m, on oltava $j = k$. Lisäksi tarkasteltava joukko koostuu m kappaleesta keskenään eikongruentteja kokonaislukuja modulo m, ja tälle moduloluvulle on m kongruenssiluokkaa. Siis $ar_1 + b, ar_2 + b, \ldots, ar_m + b$ on täydellinen jäännösluokkasysteemi modulo m. □

Lause 4.1.4. *Olkoot positiiviset kokonaisluvut m ja n keskenään suhteellisia alkulukuja. Tällöin $\phi(mn) = \phi(m)\phi(n)$.*

Todistus. Ilmoitetaan lukua mn pienemmät positiiviset kokonaisluvut seuraavalla tavalla.

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

Olkoon $r \in \mathbb{Z}$ ja $1 \leq r \leq m$. Oletetaan ensin, että $\text{syt}(m, r) = d > 1$. Koska $d \mid m$ ja $d \mid r$, niin $d \mid km + r$, missä $1 \leq k \leq n-1$, $k \in \mathbb{Z}$. Tällöin yksikään r:nnen rivin luku ei ole suhteellinen alkuluku tulon mn kanssa.

Koska tarkoituksena on löytää ne luvut, jotka ovat suhteellisia alkulukuja luvun mn kanssa, voidaan riviä r tarkastella vain, jos $\text{syt}(m, r) = 1$. Oletetaan siis, että

$$\text{syt}(m, r) = 1. \tag{4.1}$$

Rivin r luvut ovat $r, m+r, 2m+r, \dots, (n-1)m+r$. Oletuksen (4.1) nojalla jokainen näistä luvuista on suhteellinen alkuluku luvun m kanssa. Lauseen 4.1.3 nojalla rivin r luvut muodostavat täydellisen jäännösluokkasysteemin modulo n. Tällöin rivillä on $\phi(n)$ kappaletta lukuja, jotka ovat suhteellisia alkulukuja luvun n kanssa. Nämä luvut ovat luonnollisesti suhteellisia alkulukuja luvun m kanssa, eli myös tulon mn kanssa. Rivejä, joissa luvut ovat suhteellisia alkulukuja luvun m kanssa on $\phi(m)$ kappaletta, ja niissä on $\phi(n)$ lukua, jotka ovat suhteellisia alkulukuja tulon mn kanssa. Siis $\phi(mn) = \phi(m)\phi(n)$ ja ϕ on multiplikatiivinen. □

Lause 4.1.5. *Jos p on alkuluku ja $k > 0$, niin*

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

Todistus. Tiedetään, että $\text{syt}(n, p^k) = 1$ jos ja vain jos $p \nmid n$. Lukujen 1 ja p^k välillä on p^{k-1} kokonaislukua

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

jotka ovat jaollisia alkuluvulla p. Nyt siis joukossa $1, 2, 3, \dots, p^k$ on $p^k - p^{k-1}$ kappaletta kokonaislukuja, jotka ovat suhteellisia alkulukuja luvun p^k kanssa eli $\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$. □

Lause 4.1.6. *Olkoon luku $n > 1$ alkutekijöidensä potenssien avulla ilmoitettu muodossa $n = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$, $k_j > 0$ $\forall j \in \{1, \ldots, r\}$. Tällöin*

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdot \ldots \cdot (1 - \frac{1}{p_r}).$$

Todistus. Koska $\phi(n)$ on multiplikatiivinen ja $\text{syt}(p_i^{k_i}, p_j^{k_j}) = 1$, $1 \leq i, j \leq r$, $i \neq j$, voidaan kirjoittaa

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

Lisäksi Lauseen 4.1.5 nojalla tiedetään, että kun $1 \leq j \leq r$, niin

$$\phi(p_j^{k_j}) = p_j^{k_j} - p_j^{k_j - 1} = p_j^{k_j}(1 - 1/p_j).$$

Tällöin

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

□

4.2 Eulerin lauseen todistuksia

Jotta Eulerin lause voitaisiin todistaa redusoidun jäännössysteemin avulla, tarvitaan seuraavat kolme aputulosta. [6, s. 40, 137][29, ss. 202-204]

Määritelmä 4.2.1. *Redusoitu jäännössysteemi modulo n* on $\phi(n)$ kokonaisluvun joukko, joista jokainen on suhteellinen alkuluku luvun n kanssa ja mitkään kaksi joukon alkiota eivät ole kongruentteja keskenään modulo n.

Esimerkki 4.2.2. Joukko $\{1, 5\}$ muodostaa redusoidun jäännössysteemin modulo 6, sillä joukkoon kuuluu $\phi(6) = 2$ lukua, ne ovat suhteellisia alkulukuja luvun 6 kanssa ja ne eivät ole keskenään kongruentteja modulo 6, koska $1 \not\equiv 5 \,(\bmod 6)$.

Lause 4.2.3. *Olkoon p alkuluku ja $a, b \in \mathbb{Z}$. Jos $p|(ab)$, niin $p|a$ tai $p|b$.*

Todistus. Oletetaan, että $p \nmid a$. Luvun p ainoat positiiviset tekijät ovat 1 ja p. Tällöin $\text{syt}(a, p) = 1$, ja Lemman 2.2.10 nojalla $p|b$. Jos taas $p|a$, niin väite on selvä. □

Lause 4.2.4. *Jos $r_1, r_2, \ldots, r_{\phi(n)}$ on redusoitu jäännössysteemi modulo n, $a \in \mathbb{Z}_+$ ja* $\text{syt}(a, n) = 1$*, niin joukko $ar_1, ar_2, \ldots, ar_{\phi(n)}$ on redusoitu jäännössysteemi modulo n.*

Todistus. Osoitetaan ensin, että kaikki joukon $ar_1, ar_2, \ldots, ar_{\phi(n)}$ alkiot ovat suhteellisia alkulukuja luvun n kanssa. Oletetaan vastoin väitettä, että

$$\text{syt}(ar_j, n) > 1, \text{ missä } 1 \leq j \leq \phi(n).$$

Koska jokainen kokonaisluku voidaan Aritmetiikan peruslauseen nojalla esittää alkulukujen tulona, on olemassa alkuluku p jolle pätee $p \mid \text{syt}(ar_j, n)$. Lauseen 4.2.3 nojalla voidaan kirjoittaa $p \mid a$ tai $p \mid r_j$, koska p on tulon ar_j tekijä. On siis kaksi tapausta: joko $p \mid a$ ja $p \mid n$ tai $p \mid r_j$ ja $p \mid n$. Ensimmäinen tapaus ei pidä paikkaansa, sillä $p \mid a$ ja $p \mid n$ eivät voi olla voimassa, koska $\text{syt}(a, n) = 1$. Myöskään $p \mid r_j$ ja $p \mid n$ eivät voi olla totta, koska r_j kuuluu redusoituun jäännössysteemiin modulo n, jolloin $\text{syt}(r_j, n) = 1$. On siis päädytty ristiriitaan, joten $\text{syt}(ar_j, n) = 1$ kun $1 \leq j \leq \phi(n)$.

Seuraavaksi osoitetaan, että mitkään kaksi alkiota ar_j eivät ole kongruentteja keskenään modulo n. Oletetaan jälleen vastoin väitettä, että

$$ar_j \equiv ar_k \,(\bmod n), \text{ missä } 1 \leq j, k \leq \phi(n) \text{ ja } j \neq k. \tag{4.2}$$

Koska $\text{syt}(a, n) = 1$, voidaan Seurauksen 2.2.12 nojalla jakaa yhtälö (4.2) puolittain luvulla a, jolloin se saadaan muotoon $r_j \equiv r_k \,(\bmod n)$. Koska r_j ja r_k kuuluvat redusoituun jäännössysteemiin modulo n, eivät ne voi olla kongruentteja keskenään. Päädyttiin taas ristiriitaan, ja koska molemmat redusoidun jäännössysteemin modulo n ehdot on nyt täytetty, ja joukko $ar_1, ar_2, \ldots, ar_{\phi(n)}$ koostuu $\phi(n)$ luvusta, on alkuperäinen väite todistettu. □

Lause 4.2.5. ***Eulerin lause.*** *Jos $a \in \mathbb{Z}$, $n \geq 1$ ja* $\text{syt}(a, n) = 1$*, niin*

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

Todistus. Olkoon $r_1, r_2, \ldots, r_{\phi(n)}$ positiivisista kokonaisluvuista muodostuva redusoitu jäännössysteemi modulo n, jossa $r_i < n$ kaikilla $i = 1, 2, \ldots, \phi(n)$. Koska $\text{syt}(a, n) = 1$, Lauseen 4.2.4 nojalla myös $ar_1, ar_2, \ldots, ar_{\phi(n)}$ on redusoitu jäännössysteemi modulo n. Edelleen joukon $ar_1, ar_2, \ldots, ar_{\phi(n)}$ pienimmät positiiviset jakojäännökset ovat $r_1, r_2, \ldots, r_{\phi(n)}$ modulo n. Tämä voidaan osoittaa siten, että valitaan kokonaisluku b, $0 \leq b < n$, jolle

$$ar_i \equiv b \,(\bmod n), \tag{4.3}$$

$i = 1, 2, \ldots, \phi(n)$, ja osoitetaan, että $\text{syt}(b, n) = 1$. Tehdään vastaoletus $\text{syt}(b, n) = d > 1$. Tällöin $d|b$ ja $d|n$. Yhtälö (4.3) voidaan kirjoittaa yhtäpitävässä muodossa

$$ar_i = kn + b, k \in \mathbb{Z}. \tag{4.4}$$

Huomataan, että yhtälön (4.4) oikea puoli on jaollinen luvulla d, jolloin myös $d|(ar_i)$. Tällöin luku $d > 1$ jakaa molemmat luvuista ar_i ja n. Tämä on ristiriita, sillä $\text{syt}(ar_i, n) = 1$. Siis $\text{syt}(b, n) = 1$, jolloin luvun b täytyy olla yksi luvuista $r_1, r_2, \ldots, r_{\phi(n)}$.

Kongruenssin laskusäännön (Lause 2.2.2) kohdan 4 nojalla

$$ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\phi(n)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)} \,(\bmod n). \tag{4.5}$$

Yhtälö (4.5) voidaan kirjoittaa yhtäpitävässä muodossa

$$a^{\phi(n)} \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)} \,(\bmod n). \tag{4.6}$$

Koska $\text{syt}(r_j, n) = 1$ kaikilla $j = 1, 2, \ldots, \phi(n)$, Seurauksen 2.2.12 nojalla voidaan yhtälö (4.6) supistaa puolittain tulolla $r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)}$, jolloin

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

□

Kuten Fermat'n pientä lausetta, myös Eulerin lausetta voidaan käyttää apuna pienimmän positiivisen jakojäännöksen laskemisessa. [6, s. 140]

Esimerkki 4.2.6. Osoitetaan Eulerin lauseen avulla, että $51 \mid (10^{32n+9} - 7)$ eli $10^{32n+9} \equiv 7 \,(\bmod 51)$ kun $n \geq 0$.

Lauseen 4.1.6 nojalla tiedetään, että $\phi(51) = 51(1 - \frac{1}{3})(1 - \frac{1}{17}) = 32$, sillä $51 = 3 \cdot 17$. Koska $\text{syt}(10, 51) = 1$, voidaan Eulerin lauseen nojalla kirjoittaa $10^{\phi(51)} \equiv 10^{32} \equiv 1 \,(\bmod 51)$. Siispä

$$10^{32n+9} \equiv 10^9 \equiv (10^2)^4 \cdot 10 \equiv (-2)^4 \cdot 10 \equiv 160 \equiv 7 \,(\bmod 51),$$

sillä $160 - 7 = 153 = 3 \cdot 51$.

Eulerin lause voidaan todistaa myös käyttämällä induktiota ja binomilausetta [6, s. 139].

Todistus. **(Eulerin lause)** Olkoon p alkuluku. Osoitetaan ensin induktiolla, että jos $p \nmid a$, niin $a^{\phi(p^k)} \equiv 1 \,(\bmod p^k)$, $k > 0$.

1. Olkoon $k = 1$. Tällöin väite saa muodon $a^{\phi(p)} = a^{p-1} \equiv 1 \,(\bmod p)$, joka on Fermat'n pieni lause ja pitää siis paikkansa.

2. Induktio-oletus: $a^{\phi(p^k)} \equiv 1 \,(\bmod p^k)$, $k > 0$.

3. Induktioaskel: tulee osoittaa, että $a^{\phi(p^{k+1})} \equiv 1 \,(\bmod p^{k+1})$. Induktio-oletuksen nojalla voidaan kirjoittaa

$$a^{\phi(p^k)} = qp^k + 1, q \in \mathbb{Z}. \tag{4.7}$$

Lisäksi Lauseen 4.1.5 nojalla tiedetään, että

$$\phi(p^{k+1}) = p^{k+1} - p^k = p(p^k - p^{k-1}) = p\phi(p^k). \tag{4.8}$$

Yhtälöiden (4.7), (4.8) ja binomilauseen nojalla

$$\begin{aligned}
a^{\phi(p^{k+1})} &= a^{p\phi(p^k)} = (a^{\phi(p^k)})^p = (qp^k + 1)^p \\
&= \sum_{j=0}^{p} \binom{p}{j} (qp^k)^{p-j} \\
&= \binom{p}{0}(qp^k)^p + \binom{p}{1}(qp^k)^{p-1} + \binom{p}{2}(qp^k)^{p-2} + \dots \\
&\quad + \binom{p}{p-1}(qp^k) + \binom{p}{p}(qp^k)^0 \\
&= (qp^k)^p + p(qp^k)^{p-1} + \binom{p}{2}(qp^k)^{p-2} + \ldots + p(qp^k) + 1 \\
&\equiv 1 \,(\bmod p^{k+1}).
\end{aligned}$$

Kongruenssi pätee, sillä $p \mid \binom{p}{j}$ kun $0 < j < p$, ja lisäksi $p^{k+1} \mid p^{kp}$, sillä $kp \geq k + 1$ kun $k \geq 2$.

Oletetaan seuraavaksi, että $\text{syt}(a, n) = 1$ ja $n = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$. Koska $\text{syt}(a, n) = 1$, myös $\text{syt}(a, p_i) = 1$, $1 \leq i \leq r$, ja edellisen induktiotodistuksen nojalla myös

$$a^{\phi(p_i^{k_i})} \equiv 1 \,(\bmod p_i^{k_i}). \tag{4.9}$$

ϕ-funktion multiplikatiivisuudesta seuraa, että $\phi(n)$ on jaollinen luvulla $\phi(p_i^{k_i})$. Korotetaan yhtälö (4.9) potenssiin $\frac{\phi(n)}{\phi(p_i^{k_i})}$, jolloin

$$a^{\phi(n)} \equiv 1 \,(\bmod p_i^{k_i}).$$

Koska modululuvut $p_i^{k_i}$ ovat keskenään suhteellisia alkulukuja, niin Seurauksen 2.2.15 nojalla $a^{\phi(n)} \equiv 1 \,(\bmod n)$. □

4.3 Ratkaisemattomia ongelmia

Lauseen 3.2.3 nojalla positiivinen kokonaisluku n on alkuluku jos ja vain jos $\phi(n) = n - 1$. Tällöin on voimassa $1 \cdot \phi(n) = n - 1$. Lehmer osoitti vuonna 1932, että yhtälön

$$k\phi(n) = n - 1, \tag{4.10}$$

missä $k \in \mathbb{Z}$, toteuttava kokonaisluku $n > 0$ on joko alkuluku tai pariton, vähintään seitsemän erillisen alkuluvun tulo eikä minkään luvun neliö. Yhtälölle (4.10) ei ole löydetty kokonaislukuratkaisua, joka olisi yhdistetty, kun $k > 1$, mutta ei ole myöskään pystytty osoittamaan, että ratkaisuja ei ole olemassa. Lehmerin saamaa arviota yhdistetylle luvulle n ovat parannelleet muutkin matemaatikot, esimerkiksi Lieuwens osoitti, että luvun n on oltava vähintään 11 erillisen parittoman alkuluvun tulo, ja mikäli $3|n$, niin luvulla n on vähintään 212 alkutekijää ja $n > 5,5 \cdot 10^{570}$. Wall osoitti artikkelissaan [34], että mikäli kaikki luvun n alkutekijät ovat suurempia tai yhtä suuria kuin 7, luvulla n on vähintään 26 alkutekijää. [3]

Toinen Eulerin ϕ-funktioon liittyvä ratkaisematon ongelma on Carmichaelin konjektuuri. Robert Carmichael osoitti vuonna 1907 virheellisesti, että yhtälöllä

$$\phi(x) = n, \tag{4.11}$$

missä n on kokonaisluku, on joko vähintään kaksi tai ei yhtään ratkaisua x. Hänen todistuksessaan oli kuitenkin epäkohta, eikä väitettä ole pystytty todistamaan. Konjektuuri voidaan muotoilla myös niin, että jos $\phi(x) = n$, niin $\phi(y) = n$ jollekin $y \neq x$. [15, 30]

Kokonaisluvun kertaluvulla tarkoitetaan sitä, kuinka monta kertaa luku esiintyy Eulerin funktion arvona. Schlafly ja Wagon ovat artikkelissaan [30] taulukoineet eri kertalukujen arvoja, ja esimerkiksi luvun 2 kertaluku on 3, sillä luku 2 esiintyy kolme kertaa funktion $\phi(x)$ arvona; $\phi(3) = \phi(4) = \phi(6) = 2$. Carmichaelin konjektuuri siis olettaa, että kokonaisluvun kertaluku ei voi olla yksi. Paul Erdös osoitti, että jos kertaluku esiintyy kerran, niin se esiintyy äärettömän monta kertaa. Sierpinskin konjektuurin, jonka mukaan jokainen kokonaisluku, joka on suurempi kuin yksi, esiintyy kertalukuna, todisti Kevin Ford vuonna 1998. [15, 30]

Kuten Lehmerin ongelmallekin, myös Carmichaelin konjektuurin vastaesimerkille n on löydetty suuria alarajoja. Carmichael itse määritti alarajan $n > 10^{37}$, ja Victor Klee paranteli tulosta vuonna 1947 nostaen sen lukuun 10^{400}. Fordin alaraja vastaesimerkille vuodelta 1998 on $n > 10^{10^{10}}$. [15, 22]

4.4 Leonhard Euler

Luvun tiedot ovat kirjoista [1, 4, 32].

1700-luvun merkittävin sveitsiläinen matemaatikko oli Leonhard Euler (1707-1783). Eulerin isä oli toivonut pojastaan pappia, mutta Leonhardin kutsumus oli matematiikka. Hän kuitenkin opiskeli monipuolisesti myös teologiaa, lääketiedettä, tähtitiedettä, fysiikkaa ja itämaisia kieliä. 20-vuotiaana Euler sai kuulla ystäviltään Daniel ja Nicolaus Bernoullilta Pietarin akatemiassa avautuvasta virasta lääketieteellisessä tiedekunnassa. Hän sai viran, ja akatemian jouduttua sekasortoon hallitsija Katariina I kuoltua, pääsi Euler vaivihkaa sujahtamaan matemaattiseen tiedekuntaan. Tiedekunnan vaihto ei kuitenkaan paljastunut, ja hiljaisuudessa elellyt Euler nimitettiin 26-vuotiaana akatemian johtavaksi matemaatikoksi.

Jo Pietarin aikanaan Euler oli hyvin tuottoisa ja akatemian aikakauskirja oli pullollaan hänen tuotantoaan. Eulerista onkin sanottu, että hän laski "samoin kuin ihmiset hengittävät ja kotkat lentävät taivaalla" ja että hän oli "analyysin ruumiillistuma" (Francois Arago).

Vuonna 1741 Euler kutsuttiin Berliinin akatemiaan, jossa hän viipyi 25 vuotta. Saksan hallitsija Frederik Suuri suosi kuitenkin filosofeja matemaatikoiden kustannuksella, eikä Euler viihtynyt Berliinissä. 1766 hän palasi Venäjälle, missä hän vietti lopun elämäänsä. Vuonna 1735 Eulerin toinen silmä oli sokeutunut, ja vuonna 1771 hän menetti näkönsä täysin. Euler pystyi kuitenkin jatkamaan matematiikan parissa työskentelyään, sillä hänen lapsensa toimivat kirjureina Eulerin sanellessa. Leonhard pysyikin tuotteliaana aina kuolemaansa saakka, ja hänen töitään julkaistiin lähes puoli vuosisataa Pietarin akatemian julkaisuissa vielä Eulerin kuoleman jälkeen.

Euler kehitti suuresti matemaattisia merkintöjä. Hänen kynästään ovat lähtöisin luonnollisen logaritmin kantaluvun merkki e, ympyrän kehän ja halkaisijan suhteen merkintä π, imaginaariyksikkö i, summa $\sum$, binomikerroin $\binom{p}{j}$ ja funktion merkintä $f(x)$. Euler myös kehitti differentiaali- ja fluksiolaskentaa kohti nykypäivän analyysiä, jonka peruskäsitteeksi tuli funktio. Jo pelkästään differentiaaliyhtälöiden ratkaiseminen kehittyi hänen ansiostaan. Myös päättymättömien sarjojen käsittely ja todennäköisyyslaskenta kehittyi Eulerin käsissä. Kaiken tuotteliaisuutensa keskellä Euler kirjoitti myös suosittuja oppikirjoja muun muassa algebrasta.

Vaikka Euler vaikutti lukuteorian kehitykseen, ei hän ollut aluksi siitä kiin-

nostunut. Aiheesta innostunut Christian Goldbach sai pitkällisen suostuttelun jälkeen Eulerin ratkaisemaan erään lukuteorian ongelman vuonna 1730. Seuraavana vuonna Euler oli päätynyt Fermat'n pienen lauseen suppeampaan muotoon "Jos p on alkuluku, niin p jakaa luvun $2^{p-1}-1$", ja vuonna 1732 se esiintyi muodossa "Jos n on alkuluku, niin kaikki potenssit, joissa eksponentti on $n-1$ saavat jakojäännöksen 0 tai 1 jaettaessa luvulla n." Hän esitti todistukset omille versioilleen lauseesta vuosina 1736 ja 1742. Vuonna 1755 Euler todisti lauseen tarkalleen siitä muodosta, jota Fermat oli käyttänyt, ja 1758 hän oli jo päätynyt Eulerin lauseeseen. Lukuteorian parissa vietetyt vuodet olivat saaneet hänet uskomaan tämän matematiikan alan tärkeyteen. Vaikka lukuteoria ei 1700-luvulla ollut suuressa suosiossa, sai Eulerin työ aiheen parissa 1700-luvun suuret matemaatikot Joseph Louis Lagrangen (1736-1813) ja Adrien Marie Legendren (1752-1833) kiinnostumaan siitä. Seuraavalla vuosisadalla Carl Friedrich Gauss julkaisi *Disquisitiones Arithmeticaen.*

5 Wilsonin lause

5.1 Wilsonin lauseen todistuksia

Englantilainen Edward Waring julkaisi ensimmäisen kerran Wilsonin lauseen vuonna 1770 teoksessaan *Meditationes algebraicae.* Ilman todistusta ilmoitettu lause on nimetty Waringin oppilaan ja ystävän John Wilsonin mukaan, joka oli päätynyt tulokseen. Ensimmäisen todistuksen julkaisi Lagrange vuotta myöhemmin. On kuitenkin epäilyjä, että Leibniz oli jo vuonna 1682 todennut Wilsonin lauseen kanssa samanlaisen tuloksen. [6, ss. 93-94][10, s. 60]

Seuraavaksi Wilsonin lause ja Lagrangen todistus sille. Samalla menetelmällä voi todistaa myös Fermat'n pienen lauseen, ja todistuksen loppuun onkin lisätty myös tämän lauseen todistus. [10, s. 62][18, ss. 110-111]

Lause 5.1.1. ***Wilsonin lause.*** *Jos p on alkuluku, niin* $(p-1)! \equiv -1 \pmod{p}$.

Todistus. Olkoon

$$(x+1)(x+2)\cdot\ldots\cdot(x+p-1) = x^{p-1} + A_1 x^{p-2} + \ldots + A_{p-1}, \qquad (5.1)$$

missä kertoimet A_r, $r = 1, 2, \ldots, p-1$ ovat lukujen $1, 2, 3, \ldots, p-1$ tulojen summa, jossa kerrotaan r kappaletta luvuista kerrallaan. Muokataan yhtälöä (5.1) korvaamalla x luvulla $(x+1)$

$$(x+2)(x+3)\cdot\ldots\cdot(x+p) = (x+1)^{p-1} + A_1(x+1)^{p-2} + \ldots + A_{p-1}, \quad (5.2)$$

ja kerrotaan yhtälö (5.2) puolittain luvulla $x+1$ saaden se muotoon

$$(x+1)(x+2)\cdot\ldots\cdot(x+p) = (x+1)^p + A_1(x+1)^{p-1} + A_2(x+1)^{p-2} + \ldots + (x+1)A_{p-1}.$$

Kun alkuperäinen yhtälö (5.1) kerrotaan luvulla $x+p$, saadaan yhtäsuuruus

$$\begin{aligned}&(x+p)(x^{p-1} + A_1x^{p-2} + \ldots + A_{p-1})\\ &= (x+1)^p + A_1(x+1)^{p-1} + A_2(x+1)^{p-2} + \ldots + (x+1)A_{p-1}.\end{aligned} \tag{5.3}$$

Käytetään binomilausetta ja ratkaistaan kertoimet A_r. Yhtälön (5.3) vasen puoli sievenee muotoon

$$\begin{aligned}&x^p + A_1x^{p-1} + A_2x^{p-2} + \ldots + xA_{p-1} + px^{p-1} + A_1px^{p-2} + \ldots + pA_{p-1}\\ &= x^p + (A_1+p)x^{p-1} + (A_2 + A_1p)x^{p-2} + (A_3 + A_2p)x^{p-3} + \ldots + pA_{p-1}.\end{aligned} \tag{5.4}$$

Käyttämällä binomilausetta yhtälön (5.3) oikea puoli saadaan muotoon

$$\begin{aligned}&(x+1)^p + A_1(x+1)^{p-1} + A_2(x+1)^{p-2} + \ldots + (x+1)A_{p-1}\\ &= x^p + px^{p-1} + \binom{p}{2}x^{p-2} + \ldots + 1 + A_1x^{p-1} + A_1(p-1)x^{p-2}\\ &\quad + A_1\binom{p-1}{2}x^{p-3} + \ldots + A_1 + A_2x^{p-2} + A_2(p-2)x^{p-3} + \ldots + 1\\ &\quad + A_3x^{p-3} + \ldots.\end{aligned} \tag{5.5}$$

Luvun x samojen potenssien kertoimet tulee olla samat yhtälön oikealla ja vasemmalla puolella. Yhtälöiden (5.4) ja (5.5) kertoimista saadaan seuraavat yhtälöt

$$A_1 + p = p + A_1, A_2 + A_1p = \binom{p}{2} + A_1(p-1) + A_2,$$
$$A_3 + A_2p = \binom{p}{3} + A_1\binom{p-1}{2} + A_2(p-2) + A_3, \ldots,$$

joiden ratkaisut ovat

$$A_1 = \binom{p}{2}, 2A_2 = \binom{p}{3} + A_1\binom{p-1}{2},$$
$$3A_3 = \binom{p}{4} + A_1\binom{p-1}{3} + A_2\binom{p-2}{2}, \ldots.$$

Olkoon nyt p alkuluku. Kun $0 < k < p$, niin $\binom{p}{k}$ on jaollinen luvulla p. Tämän nojalla myös $p \mid A_1, p \mid 2A_2, p \mid 3A_3, \ldots, p \mid (p-2)A_{p-2}$. Koska $p \nmid 2, 3, \ldots, p-2$, niin $p \mid A_1, A_2, \ldots, A_{p-2}$. Lisäksi

$$\begin{aligned}(p-1)A_{p-1} =& \binom{p}{p} + A_1\binom{p-1}{p-1} + A_2\binom{p-2}{p-2} + \ldots \\ =& 1 + A_1 + A_2 + \ldots + A_{p-2}. \end{aligned} \tag{5.6}$$

Koska $(p-1)A_{p-1} = pA_{p-1} - A_{p-1}$, voidaan yhtälöä (5.6) muokata yhtäpitävään muotoon

$$1 + A_{p-1} = pA_{p-1} - A_1 - A_2 - \ldots - A_{p-2}. \tag{5.7}$$

Yhtälön (5.7) oikea puoli on jaollinen luvulla p, jolloin myös $p \mid (1 + A_{p-1})$, eli $1 + A_{p-1} \equiv 0 \,(\mathrm{mod}\, p)$. Kertoimien A_r määritelmän nojalla $A_{p-1} = (p-1)!$, jolloin saadaan $(p-1)! \equiv -1 \,(\mathrm{mod}\, p)$, ja Wilsonin lause on todistettu. □

Todistetaan lisäksi Fermat'n pieni lause. Kun $x \in \mathbb{Z}$, tiedetään yhtälöstä (5.1), että

$$x^{p-1} - 1 - (x+1)(x+2)\cdot\ldots\cdot(x+p-1) \equiv A_1x^{p-2} + \ldots + A_{p-2}x \equiv 0 \,(\mathrm{mod}\, p).$$

Jos $p \nmid x$, niin jokin luvuista $x+1$, $x+2$,..., $x+p-1$ on jaollinen luvulla p, eli $(x+1)(x+2)\cdot\ldots\cdot(x+p-1) \equiv 0 \,(\mathrm{mod}\, p)$. Siis kun $p \nmid x$, niin $x^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$, ja Fermat'n pieni lause on todistettu.

Wilsonin lauseen voi todistaa myös käyttämällä lineaarista kongruenssia ja siihen liittyviä aputuloksia Luvusta 2.3 sekä Lausetta 5.1.2. [6, s. 94][29, s. 186].

Lause 5.1.2. *Olkoon p alkuluku. Positiivinen kokonaisluku a on itsensä käänteisluku modulo p jos ja vain jos $a \equiv 1 \,(\mathrm{mod}\, p)$ tai $a \equiv -1 \,(\mathrm{mod}\, p)$.*

Todistus. Todistus löytyy kirjasta [29, s. 133]. □

Todistus. **(Wilsonin lause)** Väite pitää paikkansa alkuluvuille $p = 2$ ja $p = 3$, sillä

$$(2-1)! = 1 \equiv -1 \,(\mathrm{mod}\, 2) \text{ ja } (3-1)! = 2 \equiv -1 \,(\mathrm{mod}\, 3).$$

Tarkastellaan siis tilannetta, jossa $p > 3$.

Luetellaan seuraavaksi $p-1$ positiivista kokonaislukua $1, 2, 3, \ldots, p-1$, ja olkoon a mikä tahansa niistä. Nyt voidaan kirjoittaa lineaarinen kongruenssi

$$ax \equiv 1 \,(\mathrm{mod}\, p). \tag{5.8}$$

Koska syt$(a, p) = 1$, Seurauksen 2.3.2 nojalla kongruenssiyhtälöllä (5.8) on yksikäsitteinen ratkaisu modulo p. Olkoon tämä ratkaisu kokonaisluku a', $1 \leq a' \leq p-1$, eli $aa' \equiv 1 \,(\bmod p)$.
Lauseen 5.1.2 nojalla ainoat positiiviset kokonaisluvut jotka ovat pienempiä kuin p ja jotka ovat itsensä käänteislukuja ovat $a = 1$ ja $a = p-1$. Poistetaan nämä kaksi lukua joukosta $1, 2, 3, \ldots, p-1$ ja jaotellaan jäljelle jääneet luvut pareiksi a ja a', $a \neq a'$, joiden tulo on kongruentti luvun 1 kanssa modulo p. Näin voidaan tehdä, sillä lineaarisella kongruenssilla on yksikäsitteinen ratkaisu a' kaikilla $a \in \{2, 3, \ldots, (p-2)\}$, ja $1 < a' < p-1$. Kun nämä $\frac{p-3}{2}$ paria kerrotaan keskenään ja järjestellään, saadaan yhtälö

$$2 \cdot 3 \cdot 4 \cdots (p-2) = (p-2)! \equiv 1 \,(\bmod p). \tag{5.9}$$

Lopuksi yhtälö (5.9) kerrotaan puolittain luvulla $p-1$ saaden se muotoon

$$(p-1)! \equiv p-1 \equiv -1 \,(\bmod p),$$

ja Wilsonin lause on todistettu. □

Lagrange todisti Wilsonin lauseen myös käyttämällä binomilausetta, Eulerin kaavaa ja Fermat'n pientä lausetta. [10, s. 63][23, s. 330][28]

Lause 5.1.3. ***Eulerin kaava.*** *Olkoon kokonaisluku $x \geq 0$ ja a mikä tahansa reaaliluku. Tällöin*

$$\sum_{i=0}^{x} (-1)^i \binom{x}{i} (a-i)^x = x!.$$

Todistus. Todistus löytyy artikkelista [28]. □

Todistus. **(Wilsonin lause)** Eulerin kaava voidaan kirjoittaa muodossa

$$\begin{aligned} x! = \sum_{i=0}^{x} (-1)^i \binom{x}{i} (a-i)^x =& a^x - x(a-1)^x + \binom{x}{2}(a-2)^x \\ & - \binom{x}{3}(a-3)^x + \ldots + (-1)^x \binom{x}{x}(a-x)^x. \end{aligned} \tag{5.10}$$

Sijoitetaan kaavaan (5.10) $x = p-1$ ja $a = p$. Tällöin

$$\begin{aligned} (p-1)! =& p^{p-1} - (p-1)(p-1)^{p-1} + \binom{p-1}{2}(p-2)^{p-1} \\ & - \binom{p-1}{3}(p-3)^{p-1} + \ldots - \binom{p-1}{p-2}(p-(p-2))^{p-1} \\ & + (-1)^{p-1}\binom{p-1}{p-1}(p-(p-1))^{p-1}. \end{aligned} \tag{5.11}$$

Fermat'n pienen lauseen nojalla

$$(p-1)^{p-1} \equiv 1 \,(\bmod p), (p-2)^{p-1} \equiv 1 \,(\bmod p), \ldots, 2^{p-1} \equiv 1 \,(\bmod p).$$

Nyt käyttämällä Fermat'n pientä lausetta ja ottamalla kongruenssi modulo p saadusta Eulerin kaavasta (5.11), saadaan

$$(p-1)! \equiv 0-(p-1)+\binom{p-1}{2}-\binom{p-1}{3}+\ldots-\binom{p-1}{p-2}+(-1)^{p-1} \,(\bmod p).$$

Binomilausetta käyttämällä huomataan

$$\begin{aligned}
(1-1)^{p-1} &= \sum_{j=0}^{p-1} \binom{p-1}{j} 1^{p-1-j}(-1)^j \\
&= \binom{p-1}{0}1^{p-1}(-1)^0 + \binom{p-1}{1}1^{p-2}(-1)^1 + \binom{p-1}{2}1^{p-3}(-1)^2 \\
&\quad + \ldots + \binom{p-1}{p-2}1^1(-1)^{p-2} + \binom{p-1}{p-1}1^0(-1)^{p-1} \\
&= 1-(p-1)+\binom{p-1}{2}-\binom{p-1}{3}+\ldots-\binom{p-1}{p-2}+(-1)^{p-1} \\
&= 0.
\end{aligned}$$

Nyt siis

$$(p-1)!+1 \equiv (1-1)^{p-1} \equiv 0 \,(\bmod p),$$

ja Wilsonin lause on todistettu. □

5.2 Wilsonin lauseen yleistyksiä

Luvussa 3.2 käytiin läpi Fermat'n pienen lauseen ja alkulukutestauksen välistä yhteyttä. Wilsonin lause on alkulukutesti, sillä mikäli jokin positiivinen kokonaisluku n toteuttaa sen, on se alkuluku. Varsinaista käytännön merkitystä lauseella ei tässä suhteessa kuitenkaan ole, sillä laskuista tulee hankalia suurilla tutkittavilla luvuilla. Seuraavaksi kuitenkin lauseen käänteinen versio. [6, s. 95][29, s. 186]

Lause 5.2.1. *Jos $n \in \mathbb{N}$ ja $(n-1)! \equiv -1 \,(\bmod n)$, niin n on alkuluku.*

Todistus. Tehdään antiteesi: n on yhdistetty, eli sillä on tekijä d, $1 < d < n$. Tällöin $d|(n-1)!$. Koska $(n-1)!+1 \equiv 0 \,(\bmod n)$, niin $n|((n-1)!+1)$. Koska $d|n$, niin myös $d|((n-1)!+1)$. Lauseen 2.2.7 nojalla d jakaa lukujen

$(n-1)!$ ja $(n-1)!+1$ lineaarikombinaation eli $d|((n-1)!+1-(n-1)!) = 1$. Päädyttiin ristiriitaan, sillä $d > 1$. □

Wilsonin lauseelle on kuitenkin olemassa yleisempi muoto, jota voidaan käyttää alkulukutestinä. Version on esitellyt Fred Elston vuonna 1957. Tämä Wilsonin lauseen yleistys on jaettu kolmeen osaan: algoritmin määritykseen, alkulukutestiin ja tarkasteluun, jossa käytettävä alkuluku on parillinen. [14, 17]

Algoritmin määritys. Olkoon p alkuluku. Tällöin Wilsonin lauseen nojalla $(p-1)! \equiv -1 \pmod{p}$, joka on yhtäpitävä yhtälön

$$0!(p-1)! + 1 \equiv 0 \pmod{p} \tag{5.12}$$

kanssa. Järjestellään yhtälön (5.12) termit uudelleen, jolloin

$$(p-1)! + 1 = (p-1)(p-2)! + 1 = p(p-2)! - ((p-2)! - 1). \tag{5.13}$$

Tiedetään, että $0!(p-1)! + 1 \equiv 0 \pmod{p}$ ja $p(p-2)! \equiv 0 \pmod{p}$. Tällöin yhtälön (5.13) nojalla myös $(p-2)! - 1 \equiv 0 \pmod{p}$, eli

$$1!(p-2)! - 1 \equiv 0 \pmod{p}. \tag{5.14}$$

Järjestellään yhtälön (5.14) termit uudelleen muotoon

$$(p-2)! - 1 = (p-2)(p-3)! - 1 = p(p-3)! - (2(p-3)! + 1).$$

Kuten edellisten yhtälöiden (5.12) ja (5.14) kohdalla, voidaan päätellä, että $2(p-3)! + 1 \equiv 0 \pmod{p}$, eli

$$2!(p-3)! + 1 \equiv 0 \pmod{p}. \tag{5.15}$$

Jatketaan yhtälön (5.15) muokkausta muotoon

$$2(p-3)! + 1 = 2(p-3)(p-4)! + 1 = 2p(p-4)! - (6(p-4)! - 1).$$

Jaollisuus alkuluvulla p päätellään kuten kohdissa (5.12) ja (5.14), jolloin $6(p-4)! - 1 \equiv 0 \pmod{p}$, joka on yhtäpitävää yhtälön

$$3!(p-4)! - 1 \equiv 0 \pmod{p} \tag{5.16}$$

kanssa. Nyt on saatu malli neljästä kongruenssista:

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

Jos yhtälöiden (5.12), (5.14), (5.15) ja (5.16) kaltaisten kongruenssiyhtälöiden muodostamista jatketaan, vaikuttaa siltä, että päädytään tilanteeseen, jossa luku r, josta ensimmäinen kertoma lasketaan, on yhtä suuri kuin $p-(r+1)$. Tällöin $r = p-(r+1)$, joka on yhtäpitävää sen kanssa, että $r = \frac{p-1}{2}$. Tällöin

$$\Big(\frac{p-1}{2}\Big)!\Big(\frac{p-1}{2}\Big)! \pm 1 \equiv 0 \,(\bmod p).$$

Riippuen siitä, onko $r = \frac{p-1}{2}$ parillinen vai pariton, voidaan kirjoittaa

$$(r!)^2 + 1 \equiv 0 \,(\bmod p), \text{ jos } r \text{ on parillinen} \tag{5.17}$$

$$(r!)^2 - 1 \equiv 0 \,(\bmod p), \text{ jos } r \text{ on pariton.} \tag{5.18}$$

Lause 5.2.2. *Olkoon p alkuluku ja r ei-negatiivinen kokonaisluku. Tällöin*

$$r!(p-(r+1))! + (-1)^r \equiv 0 \,(\bmod p). \tag{5.19}$$

Todistus. Todistetaan väite induktiolla.

1. Olkoon $r = 0$. Tällöin väite saa muodon

   $$0!(p-(0+1))! + (-1)^0 = (p-1)! + 1 \equiv 0 \,(\bmod p),$$

   sillä kyseessä on Wilsonin lause.

2. Induktio-oletus: $r!(p-(r+1))! + (-1)^r \equiv 0 \,(\bmod p)$.

3. Induktioaskeleella tulee osoittaa, että

   $$(r+1)!(p-(r+1+1))! + (-1)^{r+1} \equiv 0 \,(\bmod p).$$

   Muokataan induktio-oletuksen vasenta puolta muotoon

   $$\begin{aligned} r!(p-(r+1))! + (-1)^r &= r!(p-(r+1))(p-(r+2))! + (-1)^r \\ &= r!p(p-(r+2))! - ((r+1)!(p-(r+2))! - (-1)^r). \end{aligned} \tag{5.20}$$

   Koska $-(-1)^r = (-1)^{r+1}$, voidaan yhtälö (5.20) kirjoittaa muodossa

   $$((r+1)!(p-(r+2))! + (-1)^{r+1}) = r!p(p-(r+2))! - \big(r!(p-(r+1))! + (-1)^r\big).$$

   Induktio-oletuksen ja huomion $r!p(p-(r+2))! \equiv 0 \,(\bmod p)$ nojalla

   $$\begin{aligned} &(r+1)!(p-(r+2))! + (-1)^{r+1} \\ &= r!p(p-(r+2))! - \big(r!(p-(r+1))! + (-1)^r\big) \\ &\equiv 0 - 0 \equiv 0 \,(\bmod p). \end{aligned}$$

   Induktioperiaatteen nojalla väite pätee kaikilla ei-negatiivisilla kokonaisluvuilla r.

□

Alkulukutesti. Olkoon $n = p - 1$ ja $r \in \mathbb{Z}$, $r < n$. Jos p on pariton alkuluku, niin n on parillinen. Nyt $n - r$ ja r ovat joko molemmat parillisia tai molemmat parittomia. Lauseen 5.2.2 nojalla voidaan kirjoittaa yhtälöt (5.21) ja (5.22). Jos $n - r$ ja r molemmat ovat parillisia, niin

$$r!(n-r)! + 1 \equiv 0 \,(\bmod p). \tag{5.21}$$

Jos taas molemmat ovat parittomia, niin

$$r!(n-r)! - 1 \equiv 0 \,(\bmod p). \tag{5.22}$$

Lause 5.2.3. *Olkoon kokonaisluku $p > 5$, $n = p - 1$, $r \in \mathbb{Z}$ ja $r < n$. Jos*

$$r!(n-r)! \pm 1 \equiv 0 \,(\bmod p),$$

niin p on alkuluku.

Todistus. Tarkastellaan ensin tapausta $r!(n-r)! + 1 \equiv 0 \,(\bmod p)$. Muodostetaan antiteesi: p on yhdistetty eli sillä on tekijä d_1, $1 < d_1 < p$. Tällöin luvulla p on myös toinen tekijä d siten, että $1 < d \leq \sqrt{p}$. Mikäli olisi $d_1 > \sqrt{p}$ ja $d > \sqrt{p}$, päädyttäisiin ristiriitaan $p \geq d_1 d > p$. Siispä tekijän d tulee olla $1 < d \leq \sqrt{p}$.

Osoitetaan seuraavaksi, että joko $d|r!$ tai $d|(n-r)!$. Kokonaisluvun r on oltava joko $r \geq \sqrt{p}$ tai $r < \sqrt{p}$. Mikäli $r \geq \sqrt{p}$, on $d \leq r$, sillä $1 < d \leq \sqrt{p}$. Tällöin $d|r!$. Toisaalta, mikäli $r < \sqrt{p}$, niin

$$n - r > n - \sqrt{p} = p - 1 - \sqrt{p} \geq \sqrt{p} \geq d.$$

Epäyhtälö $p - 1 - \sqrt{p} \geq \sqrt{p}$ pitää paikkansa, kun $p \geq 6$. Nyt siis $n - r > d$, jolloin $d|(n-r)!$. Koska $d|r!$ tai $d|(n-r)!$, niin $d|(r!(n-r)!)$. Oletuksen nojalla tiedetään, että $p|(r!(n-r)! + 1)$, ja koska $d|p$, myös $d|(r!(n-r)! + 1)$. Lauseen 2.2.7 nojalla $d|(r!(n-r)! + 1 - r!(n-r)!) = 1$, mikä on ristiriita, sillä $d > 1$.

Tapaus $r!(n-r)! - 1 \equiv 0 \,(\bmod p)$ käsitellään vastaavalla tavalla ja päädytään ristiriitaan $d|(-1)$. Siis p on alkuluku, ja väite on todistettu. □

Esimerkki 5.2.4. Osoitetaan, että 11 on alkuluku. Nyt siis $p = 11$, $n = 10$

ja $r = 0, 1, 2, 3, 4, 5$. Käytetään yhtälöitä (5.21) ja (5.22).

$$\begin{aligned}
0!(10!) + 1 &= 11 \cdot 329891 \\
1!(9!) - 1 &= 11 \cdot 32989 \\
2!(8!) + 1 &= 11 \cdot 7331 \\
3!(7!) - 1 &= 11 \cdot 2749 \\
4!(6!) + 1 &= 11 \cdot 1571 \\
5!(5!) - 1 &= 11 \cdot 1309
\end{aligned}$$

Kun $r = 0$, kyseessä on Wilsonin lause. Jokainen luvun $r = 0, 1, 2, 3, 4, 5$ arvo osoittaa luvun 11 olevan alkuluku Lauseen 5.2.3 nojalla. Erityisesti viimeinen yhtälö $5!(5!) - 1 = (5!)^2 - 1 \equiv 0 \pmod{11}$ todistaa alkulukuominaisuuden. Wilsonin lause voidaan siis korvata yhtälöillä (5.17) ja (5.18).

Kaavaa (5.18) (tapaus, jossa r on pariton) voidaan lisäksi muokata muotoon

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

Eli jos p on alkuluku, niin p jakaa jommankumman luvuista $(\frac{n}{2})! + 1$ tai $(\frac{n}{2})! - 1$.

Esimerkki 5.2.5. Olkoon $p = 19$. Tällöin $n/2 = 9$, eli $n/2$ on pariton. Nyt $9! = 362880$, ja $362880 + 1 = 19 \cdot 19099$. Siis 19 on alkuluku.

Alkuluku p on parillinen. Alkuluku p on parillinen kun $p = 2$, ja tällöin $n = 2 - 1 = 1$. Nyt ei siis saada tapausta, jossa $n - r$ ja r olisivat samanmerkkiset. Lauseen 5.2.2 nojalla voidaan kirjoittaa

$$0!1! \pm 1 \equiv 0 \pmod{2}.$$

Haley on artikkelissaan [17] luetellut Wilsonin lauseen sovelluksia liittyen esimerkiksi täydelliseen jäännösluokkasysteemiin ja Eulerin lukuihin. Seuraavaksi Fleckin yleistys Wilsonin lauseesta vuodelta 1915.

Lause 5.2.6. *Olkoon $n, a \in \mathbb{Z}$, $a \geq 1$, ja luvulla n ei ole alkutekijöitä, jotka ovat pienempiä tai yhtä suuria kuin a. Tällöin n on alkuluku jos ja vain jos*

$$\binom{a}{a}\binom{a+1}{a}\binom{a+2}{a}\cdots\binom{n-1}{a} \equiv (-1)^{\binom{a+1}{2}}\binom{a}{1}\binom{a}{2}\cdots\binom{a}{a-1} \pmod{p}.$$

Todistus. Todistus löytyy artikkelista [17]. □

Lause on Wilsonin lause tapauksessa $a = 1$. Gauss yleisti Wilsonin lauseen *Disquisitiones Arithmeticaessa*, mutta ei varsinaisesti antanut todistusta, vaan totesi kirjan edellisten kappaleiden tietojen riittävän todistukseksi. F. Minding kuitenkin julkaisi todistuksen vuonna 1832.

Lause 5.2.7. *Kaikille kokonaisluvuille $n \geq 2$ pätee*

$$(n-1)_n! \equiv \begin{cases} -1 \,(\bmod n) & \textit{kun } n = 2, 4, p^\alpha, 2p^\alpha \\ 1 \,(\bmod n) & \textit{muulloin,} \end{cases}$$

missä p on pariton alkuluku ja α on positiivinen kokonaisluku.

Todistus. Todistus löytyy artikkelista [17]. □

Merkinnällä $(n-1)_n!$ tarkoitetaan niiden positiivisten kokonaislukujen tuloa, jotka ovat suhteellisia alkulukuja luvun n kanssa ja jotka ovat pienempiä tai yhtä suuria kuin $n-1$. Wilsonin lause saadaan, kun edellisessä lauseessa $n = p$. [17][18, s. 132]

5.3 Edward Waring

Luvun tiedot ovat kirjoista [4, 12, 23].

26-vuotiaana professorin virkaan Cambridgen yliopistoon valitun matemaatikko Edward Waringin (1734-1798) tärkein teos oli *Meditationes algebraicae*, joka sisälsi useita tärkeitä tuloksia. Hän kirjoitti yhteensä kuusi tutkielmaa. Teoksia ei kuitenkaan tunnettu kovin laajasti ja ne olivat melko huonosti kirjoitettuja, jonka vuoksi esimerkiksi ensin Waringin keksimä suppenevuustesti tunnetaan Cauchyn nimellä.

Waringin tunnetuin teos sisälsi Wilsonin lauseen lisäksi Goldbachin konjektuurin ensiesiintymisen (jokainen kahta suurempi parillinen kokonaisluku on kahden alkuluvun summa), oletuksen, että jokainen pariton kokonaisluku on alkuluku tai kolmen alkuluvun summa ja Waringin ongelman. Waring oletti yhä todistamatta olevassa ongelmassaan, että jokainen positiivinen kokonaisluku on korkeintaan yhdeksän kuution summa, korkeintaan yhdeksäntoista neljättä potenssia olevan luvun summa, ja niin edelleen. Tiedetään, että Gauss lainasi *Meditationes algebraicaen* vuonna 1797 Göttingenin yliopiston kirjastosta monien muiden kirjojen lisäksi, neljä vuotta ennen *Disquisitiones Arithmeticaen* julkaisua.

Viitteet

[1] Aczel, A.D. *Fermat'n teoreema*. Werner Söderström Osakeyhtiö, Helsinki. 1997

[2] Agrawal, M., Kayal, N., Saxena, N. *PRIMES is in P*. 2004 http://annals.math.princeton.edu/wp-content/uploads/annals-v160-n2-p12.pdf [Luettu 17.10.2013]

[3] Alter, R. *Can $\phi(n)$ Properly Divide $n-1$?* The American Mathematical Monthly Vol. 80, No. 2 (Feb., 1973), ss. 192-193.

[4] Boyer, C.B. *A History of Mathematics*. Princeton University Press, New Jersey. 1985

[5] Bullynck, M. *Modular Arithmetic before C. F. Gauss. Systematisations and discussions on remainder problems in 18th century Germany*. 2008 http://www.kuttaka.org/Gauss_Modular.pdf [Luettu 28.10.2013]

[6] Burton, D.M. *Elementary Number Theory*. Mcgraw-Hill, Singapore. 2011

[7] Bühler, W.K. *Gauss: A Biographical Study*. Springer-Verlag, USA. 1981

[8] Cajori, F. *A History of Mathematical Notations. Two Volumes Bound As One*. Dover Publications, New York. 1993

[9] Coppel, W.A. *Number Theory. An Introduction to Mathematics. Second Edition*. Springer Science+Business Media, Milton Keynes. 2009

[10] Dickson, L.E. *History of The Theory of Numbers. Volume 1. Divisibility and Primality*. Chelsea Publishing Company, New York. 1971

[11] Dickson, L.E. *History of The Theory of Numbers. Volume 2. Diophantine Analysis*. Chelsea Publishing Company, New York. 1971

[12] Dunnington, Q.W. *Carl Friedrich Gauss: Titan of Science*. The Mathematical Association of America, USA. 2004

[13] Edwards, H.M. *Higher Arithmetic: An Algorithmic Introduction to Number Theory*. American Mathematical Society, USA. 2008

[14] Elston, F.G. *A Generalization of Wilson's Theorem*. Mathematics Magazine, Vol. 30, No. 30 (Jan.-Feb., 1957), ss. 159-162.

[15] Ford, K. *The Distribution of Totients.* Electronic Research Announcements of The American Mathematical Society, Vol. 4 (April 27, 1998), ss. 27-34.

[16] Gauss, C.F. *Disquisitiones Arithmeticae.* Yale University Press, Virginia. 1986

[17] Haley, C. *Generalizations and Extensions of Wilson's Theorem.* 2008 http://www.academia.edu/2552757/Wilsons_theorem_-_an_undergraduate_honors_project [Luettu 12.11.2013]

[18] Hardy, G.H., Wright, E.M. *An Introduction to the Theory of Numbers.* Oxford University Press Inc., Iso-Britannia. 2008

[19] Heeffer, A. *Regiomontanus and Chinese Mathematics.* 2008 http://www.academia.edu/4208226/Regiomontanus_and_Chinese_ mathematics [Luettu 30.12.2013]

[20] Heeffer, A. *The Tacit Appropriation of Hindu Algebra in Renaissance Practical Arithmetic.* 2007 http://www.academia.edu/1889614/The_Tacit_Appropriation_of _Hindu_Algebra_in_Renaissance_Practical_Arithmetic [Luettu 30.12.2013]

[21] Kangsheng, S. *Historical Development of the Chinese Remainder Theorem.* 1987 http://www.math.harvard.edu/ knill/crt/lib/ Kangsheng.pdf [Luettu 19.12.2013]

[22] Klee, V.L.Jr. *On a Conjecture of Carmichael.* Bulletin of the American Mathematical Society, Vol. 53, No. 12 (1947), ss. 1183-1186.

[23] Koshy, T. *Elementary Number Theory with Applications (2nd Edition).* Academic Press, Burlington. 2007

[24] Kraiem, F. http://blog.fkraiem.org/2013/04/08/primality-testing-part-2-the-pocklington-lehmer-primality-test/ [Luettu 21.12.2013]

[25] Law, C. *Arithmetical Congruences with Practical Applications.* Mathematics Magazine, Vol. 31, No. 4 (Mar. - Apr., 1958) ss. 221-227.

[26] Lehtinen, M. *Matematiikan historian luentoja.* 2001 http://math.tut.fi/ eturunen/historia_02.pdf [Luettu 31.12.2013]

[27] Ore, O. *Number Theory and Its History.* McGraw-Hill Book Company, Inc., USA. 1948

[28] LaRoche Turnage, C. *Selected Proofs of Fermat's Little Theorem and Wilson's Theorem.* 2008 http://www.math.wfu.edu/publications/Student/Caroline%20LaRoche%20Turnage%20-%20Thesis.pdf [Luettu 13.11.2013]

[29] Rosen, K. H. *Elementary Number Theory and Its Applications.* Addison-Wesley Publishing Company, New Jersey. 1993

[30] Schlafly, A., Wagon, S. *Carmichael's Conjecture on the Euler Function is Valid Below* $10^{10,000,000}$. Mathematics of Computation, Vol. 63, No. 207 (Jul., 1994), ss. 415-419.

[31] Singh, S. *Fermat'n viimeinen teoreema: Kertomus ongelmasta, joka piinasi maailman parhaita matemaatikoita 358 vuoden ajan.* Kustannusosakeyhtiö Tammi, Jyväskylä. 1998

[32] Suzuki, J. *Euler and Number Theory: A Study in Mathematical Invention*, 363-383, Leonhard Euler: Life, Work and Legacy, Elsevier, Hollanti. 2007

[33] van der Waerden, B.L. *Geometry and Algebra in Ancient Civilizations.* Springer-Verlag, Saksa. 1983

[34] Wall, D.W. *Conditions for* $\phi(N)$ *to Properly Divide* $N - 1$. 1980 http://www.fq.math.ca/Books/Collection/wall.pdf [Luettu 1.1.2014]