Matti Jutila

Iiro Honkala

Lukuteoria

Syksy 2011

Sisältö

Johdanto

Lukuteoria klassisessa mielessä käsittelee kokonaislukuja koskevia probleemoita. Näiden tutkiminen vaatii usein siirtymistä laajempiin lukuluokkiin kuten algebrallisiin lukuihin (esim. $\sqrt{2}$) tai yleisemmin reaali- ja kompleksilukuihin, missä avautuu itsessäänkin mielenkiintoisia uusia kysymyksiä. Tässä kurssissa pääpaino on kuitenkin kokonaislukujen "alkeellisessa" teoriassa.

Lukuteorian problematiikan valottamiseksi tarkastellaan aluksi joitakin tyypillisiä kysymyksenasetteluita.

a) Multiplikatiiviset probleemat (jaollisuusominaisuudet, alkuluvut jne.).

1) *Alkulukujen jakautuminen.* Merkitään $\pi(x)$:llä niiden alkulukujen lukumäärää, jotka eivät ylitä x:ää. *Alkulukulauseen* mukaan

$$\pi(x) \sim \frac{x}{\ln x}.$$

Tarkempi versio on

$$\pi(x) = \mathrm{li}(x) + R(x),$$

missä

$$\mathrm{li}(x) = \int_0^x \frac{dt}{\ln t}$$

on ns. *logaritminen integraali* ja $R(x)$ on virhetermi. Virhetermin arvio liittyy matematiikan tätä nykyä kuuluisimpaan avoimeen probleemaan, ns. *Riemannin hypoteesiin.* Alun perin se oli analyyttinen väittämä, joka koski ns. *Riemannin zeta-funktion* $\zeta(s)$ nollakohtia, mutta se voidaan lausua myös lukuteoreettisesti esimerkiksi hypoteettisena arviona $R(x) = O(x^{1/2} \ln x)$. Alkulukulause antaa kuvan alkulukujen "globaalisesta" jakautumisesta, mutta alkulukujonon "lokaaliset" ominaisuudet, esimerkiksi peräkkäisten alkulukujen väliset etäisyydet, ovat myös hyvin kiinnostavia. Klassinen avoin probleema koskee *alkulukukaksosia* eli peräkkäisten alkulukujen pareja, joiden erotus on 2 (esimerkiksi (3, 5), (29, 31), (1000000009649, 1000000009651)): onko tällaisia pareja äärettömän monta?

2) *Tekijöihinjako, alkulukutestaus*: Mikä on nopein tapa jakaa luku alkutekijöihin tai testata, onko luku alkuluku? Jälkimmäinen tehtävä on oleellisesti helpompi! Kesällä 2002 esitettiin polynomiajassa toimiva alkulukutestausalgoritmi (Agrawal, Kayal, Saxena).

3) *Tekijöiden lukumäärä*: Mikä on lukujen $n \leq x$ tekijöiden lukumäärän *keskimääräinen* suuruusluokka ? Vastaus: $\ln x$.

b) Additiiviset probleemat.

1) *Waringin probleema* : luvun N esittäminen muodossa

$$N = x_1^k + \cdots + x_s^k.$$

Tämä on mahdollista kun $s = g(k)$ on sopivasti valittu (riittävän suuri). Esim. $g(2) = 4$ (Lagrange), $g(3) = 9$, $g(4) = 19$, $g(5) = 37$, ...

2) *Goldbachin probleema*: luvun esittäminen alkulukujen summana seuraavasti:

$$N = p_1 + p_2 \qquad (N \text{ parillinen}),$$

$$N = p_1 + p_2 + p_3 \qquad (N \text{ pariton}).$$

Jälkimmäisen (ns. ternäärisen) probleeman ratkaisi I. M. Vinogradov v. 1937 riittävän suurille luvun N arvoille, mutta edellinen (ns. binäärinen) probleema on yhä avoin. Chen Jing-run todisti kuitenkin v. 1973, että jokainen riittävän suuri parillinen luku N voidaan esittää muodossa $N = p + P_2$, missä p on alkuluku ja luvulla P_2 on korkeintaan kaksi alkutekijää.

3) *Kahden neliön summa.* P. Fermat todisti (1600-luvulla), että jokainen muotoa $4n+1$ oleva alkuluku p voidaan esittää yksikäsitteisesti muodossa $p = x_1^2 + x_2^2$ (jos ei pidetä erilaisina esityksiä, jotka poikkeavat vain järjestyksen tai merkkien osalta), kun taas millään muotoa $4n-1$ olevalla alkuluvulla ei ole tällaista esitystä. Esimerkiksi $13 = 2^2 + 3^2$, mutta $11 \neq x_1^2 + x_2^2$ (minkä näkee helposti kokeilemalla).

c) Diofantoksen yhtälöt (ts. yhtälöt, joille etsitään kokonaislukuratkaisuja).

1) *Lineaarinen yhtälö* $ax + by + c = 0$. Tämän ratkaisuille on tyhjentävä teoria (sisältyy kurssiin).

2) *Pellin yhtälö* $x^2 - Ny^2 = 1$. Täydellinen teoria on myös olemassa. Esimerkiksi kun $N = 29$, eräs ratkaisu on $(x, y) = (9801, 1820)$. Pellin yhtälön teoria sisältyy lukuteorian jatkokurssiin.

3) *Fermat'n väittämä*: yhtälöllä

$$x^n + y^n = z^n$$

ei ole ratkaisua, jolle $xyz \neq 0$ kun $n \geq 3$. Tämä oli pitkään eräs matematiikan kuuluisimpia avoimia probleemoita, kunnes englantilainen Andrew Wiles todisti sen oikeaksi (todistus julkaistiin v. 1995). Toisaalta yhtälön $x^2 + y^2 = z^2$ ratkaisut (ks. pykälä 4.2) tiesi luultavasti jo Pythagoras.

4) *Catalanin probleema.* Luvut $8 = 2^3$ ja $9 = 3^2$ ovat *peräkkäisiä aitoja potensseja* (siis potensseja, joissa eksponentti on vähintään 2); onko olemassa muita? Catalanin väittämän mukaan muita ei ole, ja P. Mihăilescu todisti äskettäin, että näin on todella asian laita.

d) Diofantoksen approksimaatiot (reaalilukujen approksimointi rationaaliluvuilla). *Dirichlet'n approksimaatiolauseen* mukaan kaikille luvuille $\alpha \in \mathbb{R}$ ja $n \in \mathbb{N} = \{1, 2, 3, \ldots\}$ on olemassa rationaaliluku p/q, jolle

$$0 < q \leq n \quad \text{ja} \quad |p/q - \alpha| \leq \frac{1}{q(n+1)}.$$

Erityisesti siis

$$|p/q - \alpha| < \frac{1}{q^2}.$$

Voidaan osoittaa, että tällä epäyhtälöllä on äärettömän monta ratkaisua p/q tarkalleen silloin kun α on irrationaalinen. Näihin kysymyksiin paneudutaan jatkokurssissa.

Tällä kurssilla $\mathbb{N} = \{1, 2, 3, \ldots\}$.

1 Jaollisuus ja tekijöihinjako

1.1 Jakoalgoritmi ja lukujärjestelmät

Seuraavaan lauseeseen sisältyvä jakoalgoritmi on kokonaislukujen teorian varsinainen kulmakivi. Symbolit $a, b, c, \ldots$ merkitsevät seuraavassa kokonaislukuja eikä tätä aina erikseen toisteta.

Lause 1.1 (Jakoalgoritmi)**.** *Olkoon $b \neq 0$. Silloin jokaisella kokonaisluvulla a on yksikäsitteisesti määrätty esitys*

$$a = qb + r, \quad \textit{missä } 0 \leq r < |b|.$$

Todistus. Joukko $\{qb \mid q \in \mathbb{Z}\}$ sisätää lukusuoran pisteen 0 ja kaikki pisteet siitä lukien $|b|$:n välein kumpaankin suuntaan. Jos kuhunkin näistä luvuista lisätään luvut 0, 1, …, $|b| - 1$, saadaan kaikki lukusuoran pisteet. Em. esitys on selvästi yksikäsitteinen. □

Luonnollisia lukuja on tapana esittää muodossa

$$a = a_0 + a_1 10 + \cdots + a_n 10^n, \quad n \geq 0, \quad 0 \leq a_i < 10, \quad a_n > 0, \tag{1}$$

jolloin $a_0,\ a_1, \ldots,\ a_n$ ovat luvun a "numerot" kymmenjärjestelmässä. Tietokoneissa on luvun 2 potensseihin perustuva binäärijärjestelmä mukavampi. Yleisesti voidaan puhua luvun *a kantaesityksestä kantaluvun k* suhteen (tai luvun a esityksestä *lukujärjestelmässä, jonka kantaluku on k*). Tätä koskee seuraava lause.

Lause 1.2. *Olkoon $k > 1$. Silloin jokainen luonnollinen luku a voidaan esittää yksikäsitteisesti muodossa*

$$a = a_0 + a_1 k + \cdots + a_n k^n, \quad n \geq 0, \quad 0 \leq a_i < k, \quad a_n > 0. \tag{2}$$

Todistus. Osoitetaan induktiolla esityksen *olemassaolo*. Jos $0 < a < k$, niin triviaali esitys $a = a$ käy; tällöin $n = 0$. Jos $a \geq k$, oletetaan esityksen olemassaolo lukua a pienemmille luvuille ja kirjoitetaan jakoalgoritmin mukaan

$$a = qk + r, \quad 0 \leq r < k.$$

Tällöin $q < a$, joten luvulla q on vaadittu esitys, ja sijoitettuna edelle se antaa esityksen luvulle a.

Esityksen *yksikäsitteisyyttä* varten tehdään vastaoletus, että olisi kaksi erilaista esitystä (2). Muodostamalla niiden erotus saadaan yhtälö

$$0 = b_n k^n + b_{n-1} k^{n-1} + \cdots + b_1 k + b_0, \quad |b_i| < k,$$

missä $b_i \neq 0$ ainakin yhdelle indeksille.

Nyt $b_0 = bk$ jollekin $b \in \mathbb{Z}$ ja $|b_0| < k$, joten on oltava $b = 0$ ja siten $b_0 = 0$. Tämän jälkeen päätellään, että $b_1 = 0, b_2 = 0, \ldots, b_n = 0$, mikä on ristiriita. □

Merkintä: $a = (a_n a_{n-1} \cdots a_0)_k$.

Esimerkki 1.3. Esitetään luku 300 lukujärjestelmässä, jonka kantaluku on a) 2, b) 5, c) 10.

a) $300 = 256 + 44 = 2^8 + 32 + 12 = 2^8 + 2^5 + 2^3 + 2^2 = (100101100)_2$.

b) $300 = 5 \cdot 60 = 5(5 \cdot 12) = 5(5(5 \cdot 2 + 2)) = 2 \cdot 5^3 + 2 \cdot 5^2 = (2200)_5$.

c) $300 = 3 \cdot 10^2 = (300)_{10}$.

1.2 Jaollisuus, suurin yhteinen tekijä ja pienin yhteinen jaettava

Määritelmä 1.4. Sanomme, että b on *jaollinen* a:lla (synonyymeja: *a jakaa b:n*, *a on b:n tekijä*), jos $b = ac$ jollakin kokonaisluvulla c. Merkitään $a|b$. Jos a ei jaa b:tä, merkitään $a \nmid b$.

Jaollisuus voidaan karakterisoida jakoalgoritmin avulla seuraavasti (todistus helppo).

Lause 1.5. *Ehto $a|b$ ($a \neq 0$) on ekvivalentti sen kanssa, että lauseen 1.2 esityksessä $b = qa + r$ on $r = 0$.*

Huomautus 1.6. 1) $a|0$.
2) $a|b, \quad b|c \Longrightarrow a|c$.
3) $a|b, \quad c|d \Longrightarrow ac|bd$.
4) $a|b \Longrightarrow a|bc$.
5) $a|b_1, \ldots, a|b_n \Longrightarrow a|c_1b_1 + \cdots + c_nb_n$.
6) $a|b_1, \ldots, a|b_{n-1},\ a \nmid b_n \Longrightarrow a \nmid b_1 + \cdots + b_n$.
7) $a|b,\ b \in \mathbb{N} \Longrightarrow a \leq b$.
8) $a|b,\ b|a,\ a, b \in \mathbb{N} \Longrightarrow a = b$.

Määritelmä 1.7. Lukujen $a_1, \ldots, a_n$, joista ainakin yksi on nollasta eroava, *suurin yhteinen tekijä* (s.y.t.) on suurin kokonaisluku d, joka jakaa jokaisen näistä luvuista. Merkitään $d = (a_1, \ldots, a_n)$. Jos $(a_1, \ldots, a_n) = 1$, sanotaan, että $a_1, \ldots, a_n$ ovat *keskenään jaottomia* (tai *suhteellisia alkulukuja*). Jos $(a_i, a_j) = 1$ aina kun $i \neq j$, sanotaan, että ko. luvut ovat *parittain suhteellisia alkulukuja*.

Esimerkki 1.8 (Fermat'n luvut)**.** Määritellään

$$f_n = 2^{2^n} + 1.$$

Siis $f_0 = 3$, $f_1 = 5$, $f_2 = 17$, $f_3 = 257$, $f_4 = 65537$. Nämä ovat kaikki alkulukuja, ja Pierre de Fermat otaksui, että f_n olisi aina alkuluku. Euler totesi kuitenkin, että $f_5 = 641 \cdot 6700417$,ja nykyään otaksutaankin, että Fermat'n luvut f_n ovat *aina* yhdistettyjä lukuja, kun $n \geq 5$. Tämä on hyvin vaikea kysymys, mutta yksinkertaisempi asia on osoittaa, että

$$(f_m, f_n) = 1, \quad \text{kun } m \neq n.$$

Tätä varten oletetaan, että $n = m + k$, $k \geq 1$, ja merkitään $a = 2^n$, $b = 2^m$, $c = 2^k$. Silloin $a = bc$ ja

$$f_n - 2 = 2^a - 1 = 2^{bc} - 1 = (2^b + 1)(2^{b(c-1)} - 2^{b(c-2)} + \cdots + 2^b - 1).$$

Täten $f_n - 2 = hf_m$, missä $h \in \mathbb{Z}$. Jos siis $d|f_m$ ja $d|f_n$, niin $d|f_n - hf_m = 2$. Näin $(f_m, f_n) = 1$.

Lause 1.9. *Lukujen $a_1, \ldots, a_n$ s.y.t on pienin positiivinen luku, joka on muotoa*

$$x_1a_1 + \cdots + x_na_n. \tag{3}$$

Todistus. Kun luvut x_i käyvät kaikki kokonaisluvut, on lukujen (3) joukossa positiivisia ja siis myös pienin positiivinen luku d. Osoitetaan aluksi, että $d|a_i$. Jakoalgoritmin mukaan

$$a_i = dq_i + r_i, \quad 0 \leq r_i < d.$$

Tässä $r_i = a_i - dq_i$ on muotoa (3), koska d on samaa muotoa, joten luvun d minimaalisuuden nojalla $r_i = 0$ ja siis $d|a_i$. Edelleen on selvä, että jos c on jokin lukujen $a_1, \ldots, a_n$ yhteinen tekijä, niin $c|d$, sillä c jakaa (3):n kaikki termit. Täten $c \leq d$ ja d on tosiaan suurin lukujen a_i yhteisistä tekijöistä. □

Huomautus 1.10. Joukko $M = \{x_1a_1 + \ldots + x_na_n \mid x_1, \ldots, x_n \in \mathbb{Z}\}$ on renkaan $\mathbb{Z}$ ihanne. Luku $d = (a_1, a_2, \ldots, a_n)$ on lauseen 1.9 mukaan pienin positiivinen luku, joka kuuluu ihanteeseen M. Selvästi $M = \langle d \rangle$ (so. alkion d generoima renkaan $\mathbb{Z}$ ihanne).

Huomautus 1.11. Edellisen lauseen nojalla ehto $(a_1, \ldots, a_n) = 1$ on ekvivalentti sen kanssa, että yhtälö $a_1x_1 + \cdots + a_nx_n = 1$ toteutuu joillakin kokonaisluvuilla $x_1, \ldots, x_n$.

Lauseen 1.9 todistus antaa sivutuloksena seuraavan vaihtoehtoisen määritelmän s.y.t:lle.

Lause 1.12. *Lukujen $a_1, \ldots, a_n$ s.y.t. on ainoa positiivinen luku d, joka toteuttaa ehdot*

(a) $d|a_i, \quad i = 1, \ldots, n,$

(b) $c|a_i, \quad i = 1, \ldots, n \Longrightarrow c|d.$

Todistus. Edellä todettiin jo, että d täyttää nämä ehdot ja tällaisia lukuja on siis ainakin olemassa. Jos myös d' täyttää samat ehdot, niin (b):ssä voidaan valita $c = d'$, joten $d'|d$. Symmetrian nojalla $d|d'$ ja täten $d = d'$. □

Lause 1.13. *i) Jos $d > 0$, niin $(a, b) = d \Longleftrightarrow (\frac{a}{d}, \frac{b}{d}) = 1$.*
ii) $(a, b) = (a + kb, b)$.

Todistus. i) Oletetaan, että $(a, b) = d$. Jos $e \in \mathbb{N}$ jakaa kokonaisluvut a/d ja b/d, niin de jakaa luvut a ja b ja siis lauseen 1.12 nojalla luvun d ja näin $e = 1$. Siis $(a/d, b/d) = 1$.

Kääntäen, jos kokonaislukujen a/d ja b/d s.y.t. on 1, niin lauseen 1.9 nojalla on olemassa sellaiset kokonaisluvut x ja y, että $x(a/d) + y(b/d) = 1$ eli $xa + yb = d$. Näin $(a, b) \leq d$. Koska $d|a$ ja $d|b$, niin $(a, b) = d$.

ii) Jos $b = 0$, väite on triviaali. Oletetaan, että $b \neq 0$. Jos $d|b$, niin $d|a$ jos ja vain jos $d|a + kb$. □

Esimerkki 1.14 (Fibonaccin luvut)**.** Määritellään rekursiivisesti $F_1 = F_2 = 1$ ja $F_{n+1} = F_n + F_{n-1}$ kun $n \geq 2$. Näin saadussa Leonardo Fibonaccin (n. 1170–1250) määrittelemässä lukujonossa $1, 1, 2, 3, 5, 8, 13, \ldots$ kaksi peräkkäistä lukua ovat aina suhteellisia alkulukuja, sillä

$$(F_n, F_{n-1}) = (F_n - F_{n-1}, F_{n-1}) = (F_{n-1}, F_{n-2}) = \cdots = (F_2, F_1) = (1, 1) = 1.$$

lauseen 1.13 jälkimmäisen kohdan mukaan.

Eukleideen algoritmi: Kahden luvun a ja b s.y.t. voidaan laskea tutulla Eukleideen algoritmilla. Oletetaan esimerkiksi, että $a \geq b > 0$. (Tapaus, missä $a = 0$ tai $b = 0$ on muutenkin selvä, ja rajoituksetta voidaan olettaa, että a ja b ovat positiivisia, koska (a, b) ei muutu jos a:n tai b:n merkkejä muutetaan). Muodostetaan vähenevä jono positiivisia kokonaislukuja $r_0 \geq r_1 > \cdots > r_n > r_{n+1} = 0$ seuraavalla algoritmilla. Valitaan $r_0 = a,\ r_1 = b$ ja kirjoitetaan yleisesti jakoalgoritmin mukaan

$$r_{j-2} = r_{j-1}q_{j-1} + r_j, \quad 0 \leq r_j < r_{j-1}, j = 2, 3, \ldots, n+1.$$

Ensimmäiset kaksi yhtälöä ovat $a = bq_1 + r_2$, ja $b = r_2q_2 + r_3$. Koska yleisesti on $(a, b) = (a + kb, b)$, kuten lauseessa 1.13 todettiin, niin $d = (a, b) = (a - bq_1, b) = (r_2, b)$, eli $(r_0, r_1) = (r_1, r_2)$. Jatkamalla samoin nähdään, että $d = (r_j, r_{j+1}), \quad j = 0, 1, \ldots, n$. Mutta koska $r_{n+1} = 0$, on $(r_n, r_{n+1}) = r_n$. Täten $d = r_n$, mikä onkin Eukleideen algoritmin varsinainen idea. Lisäksi esitys $d = ax+by$ saadaan käymällä läpi laskelmat lopusta alkuun.

Esimerkki 1.15. Lasketaan (252,198):
$252 = 1 \cdot 198 + 54$
$198 = 3 \cdot 54 + 36$
$54 = 1 \cdot 36 + 18$
$36 = 2 \cdot 18$
Siis $(252, 198) = 18 = 54 - 36 = \ldots = 4 \cdot 252 - 5 \cdot 198$.

Lause 1.16. *Jos kokonaisluvuille a, b ja c on voimassa $a|bc$ ja $(a, b) = 1$, niin $a|c$.*

Todistus. Koska $(a, b) = 1$, niin on olemassa sellaiset kokonaisluvut x ja y, että $ax+by = 1$. Kertomalla puolittain luvulla c saadaan $c = cax+cby$. Koska $a|bc$, niin a jakaa oikean puolen ja siis myös luvun c. □

Useamman kuin kahden luvun s.y.t. voidaan laskea myös Eukleideen algoritmilla käyttäen hyväksi seuraavaa lausetta.

Lause 1.17. *Jos $n \geq 3$ ja $a_n \neq 0$, niin*

$$(a_1, \ldots, a_n) = (a_1, \ldots, a_{n-2}, (a_{n-1}, a_n)).$$

Todistus. Lauseen 1.12 ja huomautuksen 1.6 kohdan 2 nojalla $d|(a_{n-1}, a_n)$ jos ja vain jos d jakaa molemmat luvuista a_{n-1} ja a_n. □

Esimerkki 1.18. Lasketaan $d = (666, 405, 48)$. Eukleideen algoritmia käyttämällä todetaan, että $(405, 48) = 3$, ja koska $3|666$, on $d = (666, 3) = 3$.

Määritelmä 1.19. Nollasta eroavien lukujen $a_1, \ldots, a_n$ *yhteinen jaettava* on jokainen ehdot $a_i|b$ täyttävä luku b, ja

$$h = \min\{\, b \mid \ a_i|b,\ i = 1, \ldots, n,\ b > 0 \,\}$$

on ko. lukujen *pienin yhteinen jaettava*(p.y.j.). Merkitään

$$h = [a_1, \ldots, a_n].$$

Lause 1.20. *Lukujen $a_1, \ldots, a_n$ p.y.j. on se yksikäsitteisesti määrätty luonnollinen luku h, joka täyttää ehdot*

(a) $a_i \mid h, \quad i = 1, \ldots, n,$

(b) $a_i \mid b, \quad i = 1, \ldots, n \Longrightarrow h \mid b.$

Todistus. Oletetaan, että $h = [a_1, \ldots, a_n]$. Silloin $h > 0$ ja (a) pätee. Kohdan (b) osoittamiseksi oletetaan, että $a_i|b$, $i = 1, 2, \ldots, n$. Jakoalgoritmin nojalla on olemassa sellaiset luvut q ja r, että $b = qh + r$ ja $0 \leq r < h$. Nyt $a_i|b - qh = r$. Koska $r < h$, niin $r = 0$. Siis $h|b$.

Oletetaan, että myös $h' \in \mathbb{N}$ toteuttaisi ehdot (a) ja (b). Silloin $h|h'$ (valitaan $b = h'$ lukua h koskevissa ehdoissa (a) ja (b)) ja symmetrian nojalla $h'|h$, eli $h' = h$. □

Seuraavan lauseen (joka on lauseen 1.17 analogia) avulla voidaan askel askeleelta palautua *kahden* luvun p.y.j:n määrittämiseen.

Lause 1.21. *Kun $n \geq 3$, niin*

$$[a_1, \ldots, a_n] = [a_1, \ldots, a_{n-2}, [a_{n-1}, a_n]].$$

Todistus. Edellisen lauseen nojalla $[a_{n-1}, a_n]|b$ jos ja vain jos sekä $a_{n-1}|b$ että $a_n|b$. □

1.3 Alkuluvut ja tekijöihinjako

Määritelmä 1.22. Luonnollinen luku $p > 1$ on *alkuluku*, jos sillä on vain triviaalit tekijät ± 1, $\pm p$. Jos alkuluku p on luvun a tekijä, sanotaan, että p on luvun a *alkutekijä*. Alkulukujen joukolle käytetään merkintää $\mathbb{P}$. Jos $a > 1$ ja a ei ole alkuluku, niin a on *yhdistetty luku*.

Huomautus 1.23. Seuraavassa todistetaan, että jokainen luonnollinen luku voidaan esittää (tietyssä mielessä) yksikäsitteisesti alkulukujen tulona. Tässä yhteydessä on käsite "tulo" ymmärrettävä hieman laajemmin kuin yleensä on tapana. Tulo, jossa ei ole lainkaan tekijöitä, on ns. "tyhjä tulo", ja sen arvoksi sovitaan 1. Tulon, jossa on vain yksi tekijä a, arvo on a. Päälauseen 1.27 todistusta varten tarvitaan kaksi apulausetta.

Lemma 1.24. *Jokainen luonnollinen luku voidaan esittää alkulukujen tulona.*

Todistus. Luku 1 voidaan triviaalisti esittää alkulukujen tulona huomautuksen 1.23 mielessä. Tehdään induktio-oletus, että lukua $n \geq 2$ pienemmät luvut voidaan esittää tällä tavalla. Sama pätee luvulle n, ainakin jos se on alkuluku. Muuten $n = ab$ on yhdistetty luku ja $1 < a, b < n$. Induktio-oletuksen nojalla a ja b voidaan esittää alkulukujen tulona, ja sama pätee silloin luvulle $n = ab$. □

Lemma 1.25. *Jos p on alkuluku, $a, b \in \mathbb{Z}$ ja $p|ab$, niin $p|a$ tai $p|b$.*

Todistus. Riittää osoittaa, että jos $p \nmid a$ niin $p|b$. Luku (a, p) on joko 1 tai p, koska se on luvun p positiivinen tekijä. Mutta jälkimmäinen mahdollisuus ei käy, sillä silloin p olisi luvun a tekijä. Koska nyt $(a, p) = 1$ ja $p|ab$, niin lauseen 1.16 mukaan $p|b$. □

Seuraus 1.26. *Jos p on alkuluku ja $p|a_1 \cdots a_n$, niin p jakaa ainakin yhden luvuista a_i.*

Lause 1.27 (Aritmetiikan peruslause)**.** *Jokainen luonnollinen luku voidaan esittää yksikäsitteisesti (tekijöiden järjestystä lukuunottamatta) alkulukujen tulona.*

Todistus. Lemman 1.24 mukaan jokainen luonnollinen luku voidaan esittää alkulukujen tulona, kenties usealla tavalla. Jos on olemassa luonnollisia lukuja, joilla on oleellisesti erilaisia esityksiä, on niiden joukossa pienin luku n. Olkoot

$$n = p_1 \cdots p_r = q_1 \cdots q_s$$

sen kaksi erilaista alkutekijäesitystä. Lemman 1.25 seurauksen mukaan p_1 jakaa jonkin alkuluvuista q_i, esim. luvun q_1. Koska q_1 on alkuluku, on välttämättä $p_1 = q_1$. Silloin luvulla $p_2 \cdots p_r$, joka on pienempi kuin n, olisi kaksi erilaista esitystä alkutekijöiden tulona, mutta tämä on vastoin luvun n valintaa. Näin on lause todistettu. □

Luvun n esityksessä alkulukujen tulona voi sama alkuluku esiintyä useita kertoja, esim. $72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$. Kokoamalla yhteen useammankertaiset alkutekijät päädytään seuraavan määritelmän mukaiseen standardiesitykseen, joka on lauseen 1.27 mukaan oleellisesti yksikäsitteinen.

Esimerkki 1.28 (Eratostheneen seula)**.** Alkulukujen *luetteloimiseen* on olemassa jo antiikin ajoilta tunnettu yksinkertainen menetelmä, *Eratostheneen seula*. Asetetaan tehtäväksi löytää kaikki alkuluvut lukujen $2, 3, \ldots, n$ joukosta. Kirjoitetaan luettelo näistä luvuista ja pyyhitään aluksi pois kaikki (alku)luvun 2 *aidot* monikerrat eli siis luvut 4, 6, ... Luku 2 jää pyyhkimättä, ja seuraava pyyhkimätön luku on 3. Poistetaan sen aidot monikerrat, ja jatketaan samoin siirtymällä joka vaiheessa seuraavaan pyyhkimättömään lukuun (niin kauan kuin niitä riittää), jonka aidot monikerrat poistetaan. Jäljelle jäävät luvut ovat tarkalleen kaikki alkuluvut, jotka eivät ylitä lukua n, sillä ensinnäkään mikään alkuluku ei tule pyyhityksi, koska sillä ei ole itseään pienempää ei-triviaalia tekijää, ja toiseksi jokaisella yhdistetyllä luvulla on itseään pienempi alkutekijä, jonka aitona monikertana ko. luku poistuu kuvasta. Lisäksi huomataan, että koska jokaisella yhdistetyllä luvulla $m \leq n$ on alkutekijä $p \leq \sqrt{n}$, viimeinen mahdollinen luku, jonka aitoja monikertoja tarvitsee pyyhkiä, on *korkeintaan* $\sqrt{n}$. Siis esimerkiksi haluttaessa luetteloida kaikki miljoonaa pienemmät alkuluvut riittää pyyhkiä pois kaikki tuhatta pienempien alkulukujen aidot monikerrat.

Määritelmä 1.29. Kokonaisluvun $n \neq 0, \pm 1$ esitystä muodossa

$$n = \pm p_1^{a_1} \cdots p_r^{a_r}, \tag{4}$$

missä luvut p_i ovat erisuuria alkulukuja ja luvut a_i luonnollisia lukuja, sanotaan luvun n *kanoniseksi esitykseksi.*

Jos $p \in \mathbb{P}$ ja $n \in \mathbb{Z} \setminus \{0\}$, merkitään

$$\nu_p(n) = \begin{cases} a_i, & \text{jos luvulla } n \text{ on kanoninen esitys (4) ja } p = p_i, \\ 0, & \text{jos } n = \pm 1. \end{cases}$$

Luonnollisille luvuille a ja b ovat selvästi voimassa kaavat

$$\nu_p(ab) = \nu_p(a) + \nu_p(b), \tag{5}$$

$$a|b \quad \Longleftrightarrow \nu_p(a) \leq \nu_p(b) \text{ kaikille } p \in \mathbb{P}, \tag{6}$$

$$\nu_p((a,b)) = \min\{\nu_p(a),\ \nu_p(b)\} \tag{7}$$

ja

$$\nu_p([a,b]) = \max\{\nu_p(a),\ \nu_p(b)\}. \tag{8}$$

Kaavat (7) ja (8) yleistyvät luonnollisella tavalla myös useammalle kuin kahdelle luvulle.

Helposti nähdään, että jos $a_1, \ldots, a_n$ ovat luonnollisia lukuja, niin

$$[a_1, \ldots, a_n] = a_1 \cdots a_n \tag{9}$$

tarkalleen silloin, kun ko. luvut ovat parittain suhteellisia alkulukuja.

Yhtälöistä (5), (7) ja (8) seuraa, että jos a ja b ovat luonnollisia lukuja, niin

$$(a,b)[a,b] = ab,$$

sillä yleisesti $\max\{\alpha,\beta\} + \min\{\alpha,\beta\} = \alpha + \beta$.

Lause 1.30. *Alkulukuja on äärettömän monta.*

Todistus. 1 (Eukleides). Tehdään vastaoletus, että alkulukuja on vain äärellinen määrä: $p_1,\ p_2, \ldots,\ p_n$. Tarkastellaan lukua

$$k = p_1 p_2 \cdots p_n + 1.$$

Koska alkulukuja on joka tapauksessa olemassa, on $k > 1$. Tällöin luvulla k on ainakin yksi alkutekijä, jonka täytyy vastaoletuksen nojalla olla jokin em. alkuluvuista p_i. Mutta jos $p_i|k$, niin $p_i|1$, mikä on mahdotonta. □

Todistus. 2 (Euler). Olkoon p mielivaltainen alkuluku. Silloin

$$\frac{1}{1-p^{-1}} = 1 + p^{-1} + p^{-2} + \cdots$$

Annetaan luvun p käydä tässä kaikki alkuluvut, jotka eivät ylitä jotakin lukua k. Oikealla puolella olevat sarjat suppenevat itseisesti ja voidaan siis kertoa keskenään termeittäin, jolloin saadaan muotoa

$$(p_1^{a_1} \cdots p_n^{a_n})^{-1} = (n^*)^{-1}$$

olevia termejä, missä n^* käy (tarkalleen kerran!) kaikki luonnolliset luvut, joiden alkutekijöistä mikään ei ylitä lukua k. Päättely perustuu aritmetiikan peruslauseeseen. Näin saadaan yhtälö

$$\prod_{p\le k, p\in\mathbb{P}} \frac{1}{1-p^{-1}} = \sum_{n^*} \frac{1}{n^*}. \tag{10}$$

Tässä n^* käy ainakin kaikki luonnolliset luvut, jotka eivät ylitä lukua k, joten

$$\prod_{p\le k, p\in\mathbb{P}} \frac{1}{1-p^{-1}} \ge \sum_{n\le k} \frac{1}{n} \ge \ln k, \tag{11}$$

sillä analyysistä tiedetään, että kaikille $k \in \mathbb{N}$ pätee

$$\frac{1}{2} + \ldots + \frac{1}{k} \le \int_1^k \frac{1}{t}\,dt = \ln k \le \int_1^{k+1} \frac{1}{t}\,dt \le 1 + \frac{1}{2} + \ldots + \frac{1}{k}. \tag{12}$$

Jos alkulukuja olisi vain äärellinen määrä, pysyisi (11):n vasen puoli muuttumattomana kun k ylittää suurimman niistä, mutta toisaalta oikea puoli lähestyisi ääretöntä. Täten alkulukuja on oltava ääretön määrä. □

Todistus. 3. On olemassa luonnollisten lukujen jonoja $\{a_n\}_{n=1}^{\infty}$, joilla on se ominaisuus, että $a_n > 1$ kaikilla indekseillä n ja $(a_m, a_n) = 1$, kun $m \neq n$; eräs esimerkki on Fermat'n lukujen $f_n = 2^{2^n} + 1$ jono (kts. § 1.2). Luvun a_1 alkutekijöinä esiintyvät alkuluvut eivät voi tulla käyttöön myöhempien lukujen a_n tekijöinä. Toistamalla sama päättely lukuihin $a_2, a_3, \ldots$ nähden huomataan, että joka vaiheessa tarvitaan *uusia* alkulukuja, joiden varaston täytyy täten olla ehtymätön. □

Jatkamalla hieman toisen todistuksen tarkasteluja päätellään seuraava lausetta 1.30 kvantitatiivisempi tulos.

Lause 1.31. *Sarja* $\sum_{p\in\mathbb{P}} \frac{1}{p}$ *hajaantuu.*

Todistus. Väite seuraa, kun osoitetaan, että on olemassa sellainen vakio C, että kaikilla $k \ge 2$ pätee

$$\sum_{p\le k, p\in\mathbb{P}} \frac{1}{p} \ge \ln\ln k + C. \tag{13}$$

Tämän todistamiseksi otetaan logaritmit (11):sta puolittain. Vasemman puolen logaritmin laskemiseksi otetaan huomioon, että

$$-\ln(1-\frac{1}{p}) \leq \frac{1}{p}+\frac{1}{p^2}$$

(mikä nähdään helposti toteamalla, että funktio $f(x) = \ln(1+x) - x + x^2$ on vähenevä välillä $[-\frac{1}{2}, 0]$) ja että sarja $\sum_p p^{-2}$ suppenee. □

1.4 Lukuteoreettisista funktioista

Kuvauksia $f : \mathbb{N} \to \mathbb{C}$ sanotaan *lukuteoreettisiksi funktioiksi*. Näiden joukossa voidaan määritellä erilaisia binäärisiä operaatioita, mm. *summa* $f+g$ ja *tulo* fg seuraavasti:

$$(f+g)(n) = f(n)+g(n), \qquad (fg)(n) = f(n)g(n).$$

Näiden lisäksi määritellään vielä toisenlainen "kertolasku" seuraavasti.

Määritelmä 1.32. Lukuteoreettisten funktioiden f ja g (Dirichlet'n) *konvoluutio* on funktio

$$(f*g)(n) = \sum_{d|n, d>0} f(d)g(n/d). \tag{14}$$

Sovitaan, että jatkossa edellisen kaltaisessa summassa ehto $d > 0$ voidaan jättää kirjoittamatta ja summaus silti ulotetaan koskemaan vain luvun n positiivisia tekijöitä.

Esimerkki 1.33. Määritellään

$$E(n) = 1 \quad \forall n \in \mathbb{N},$$
$$E_0(n) = \begin{cases} 1, \text{ kun } n = 1, \\ 0, \text{ kun } n > 1. \end{cases}$$

Lasketaan näiden konvoluutiot mielivaltaisen lukuteoreettisen funktion f kanssa. Määritelmän mukaan saadaan

$$(E*f)(n) = \sum_{d|n} f(d),$$
$$(E_0*f)(n) = f(n).$$

Lause 1.34. *Lukuteoreettisten funktioiden joukko on operaatioihin $+$ ja $*$ ("konvoluutiokertolasku") nähden kommutatiivinen rengas, jossa on ykkösalkio E_0.*

Todistus. Lukuteoreettiset funktiot muodostavat selvästi Abelin ryhmän yhteenlaskun suhteen; nolla-alkiona on "nollafunktio" $f_0(n) = 0$.

Kommutatiivilaki $f * g = g * f$ nähdään oikeaksi kirjoittamalla (14) symmetriseen muotoon

$$(f * g)(n) = \sum_{ab=n} f(a)g(b).$$

Distributiivilaki $f * (g + h) = f * g + f * h$ on helppo verifioida suoraan laskemalla.

Assosiatiivilain $f * (g * h) = (f * g) * h$ todistusta varten merkitään $A = g * h$. Silloin

$$\begin{aligned}(f * (g * h))(n) = (f * A)(n) &= \sum_{ad=n} f(a)A(d) \\ &= \sum_{ad=n} f(a) \sum_{bc=d} g(b)h(c) = \sum_{abc=n} f(a)g(b)h(c).\end{aligned}$$

Tämä on symmetrinen f:n, g:n ja h:n suhteen. Soveltamalla tätä kaavaa funktioon $(f*g)*h = h * (f * g)$ saadaan sama tulos vain eri merkinnöin.

Edellisessä esimerkissä todettiin jo, että $E_0 * f = f$, ja kommutatiivilain mukaan on silloin myös $f * E_0 = f$, joten E_0 on ykkösalkio konvoluutiotuloon nähden. □

Huomautus 1.35. Voidaan todistaa, että f:llä on *käänteisalkio* g konvoluutioon nähden, *jos ja vain jos* $f(1) \neq 0$. Tällöin siis $f * g = g * f = E_0$. Voidaan kirjoittaa $g = f^{-1}$, mitä ei tietenkään pidä sekoittaa funktion $1/f(n)$ kanssa. Funktio g määräytyy induktiivisesti yhtälöistä

$$\begin{aligned}g(1) &= \frac{1}{f(1)}, \\ g(n) &= -\frac{1}{f(1)} \sum_{\substack{d|n \\ d<n}} g(d)f(n/d) \quad (n > 1),\end{aligned}$$

kuten nähdään suoraan ehdosta $g * f = E_0$.

Määritellään seuraavaksi eräitä tärkeitä lukuteoreettisten funktioiden luokkia.

Määritelmä 1.36. Lukuteoreettinen funktio f, joka ei ole identtisesti nollafunktio, on *multiplikatiivinen*, jos

$$f(mn) = f(m)f(n) \qquad \text{aina kun } (m, n) = 1. \tag{15}$$

ja *täydellisesti multiplikatiivinen*, jos ehto $f(mn) = f(m)f(n)$ pätee aina. Vastaavasti f (joka saa olla identtisesti nolla) on *additiivinen*, jos

$$f(mn) = f(m) + f(n) \qquad \text{aina kun } (m, n) = 1, \tag{16}$$

ja *täydellisesti additiivinen* jos $f(mn) = f(m) + f(n)$ aina.

Otetaan käyttöön merkintä $\mathcal{M}$ multiplikatiivisten funktioiden joukolle.

Huomautus 1.37. Jos $f \in \mathcal{M}$, niin $f(1) = 1$. Ensiksikin $f(1) \neq 0$, sillä muuten olisi aina $f(n) = f(1 \cdot n) = f(1)f(n) = 0$ vastoin oletusta, että f ei ole identtisesti nolla. Täten yhtälöstä $f(1) = f(1 \cdot 1) = f(1)f(1)$ voidaan päätellä, että $f(1) = 1$.

Esimerkki 1.38. Yksinkertaisia esimerkkejä täydellisesti multiplikatiivisista funktioista ovat E ja E_0. Myös funktio $N_\alpha(n) = n^\alpha$ on täydellisesti multiplikatiivinen. Luvun n *erilaisten* alkutekijöiden lukumäärä $\omega(n)$ on additiivinen ja luvun n *kaikkien* alkutekijöiden lukumäärä $\Omega(n)$ on täydellisesti additiivinen funktio. Jos

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \tag{17}$$

on luvun n kanoninen esitys, niin

$$\omega(n) = r, \qquad \Omega(n) = a_1 + a_2 + \cdots + a_r.$$

Tapauksessa $n = 1$ näiden yhtälöiden tulkinta on $\omega(1) = \Omega(1) = 0$. Funktio $\omega(n)$ ei ole täydellisesti additiivinen, sillä esim. $\omega(12) = 2 \neq \omega(2) + \omega(6) = 3$.

Lause 1.39. *Jos $f \in \mathcal{M}$ ja luvulla n on kanoninen esitys* (17)*, niin*

$$f(n) = \prod_{i=1}^{r} f(p_i^{a_i}). \tag{18}$$

Kääntäen, jos funktiolla f on muotoa (18) *oleva esitys ja $f(1) = 1$, on f multiplikatiivinen.*

Todistus. Multiplikatiivisuuden määritelmän ehdosta (15) seuraa helposti induktiolla yleisempi yhtälö

$$f(n_1 n_2 \cdots n_k) = f(n_1) f(n_2) \cdots f(n_k),$$

jos oletetaan, että luvut n_i ovat parittain suhteellisia alkulukuja. Tästä seuraa välittömästi väite (18). Lauseen käänteisen puolen todistus on ilmeinen suoraan multiplikatiivisuuden määritelmän perusteella. Koska $f(1) = 1$, niin f ei voi olla nollafunktio. □

Lause 1.40. *Jos $f, g \in \mathcal{M}$, niin $f * g \in \mathcal{M}$.*

Todistus. Merkitään $h = f * g$. Olkoon $(m, n) = 1$. Silloin

$$h(mn) = \sum_{d|mn} f(d) g(mn/d).$$

Koska $(m, n) = 1$, luku $d = ab$ käy luvun mn positiiviset tekijät kun a käy luvun m positiiviset tekijät ja b käy luvun n positiiviset tekijät. Lisäksi $(a, b) = 1$ ja $(m/a, n/b) = 1$. Sijoittamalla tämä luvun d esitys edelliseen kaavaan ja käyttämällä hyväksi funktioiden f ja g multiplikatiivisuutta saadaan

$$\begin{aligned} h(mn) &= \sum_{a|m, a>0} \sum_{b|n, b>0} f(ab) g(mn/ab) \\ &= \sum_{a|m} \sum_{b|n} f(a) f(b) g(m/a) g(n/b) \\ &= \Big(\sum_{a|m} f(a) g(m/a)\Big)\Big(\sum_{b|n} f(b) g(n/b)\Big) \\ &= h(m) h(n), \end{aligned}$$

joten $h \in \mathcal{M}$. □

Lause 1.41. $(\mathcal{M}, *)$ *on Abelin ryhmä, jonka ykkösalkio on* E_0.

Todistus. Edellisen lauseen mukaan $\mathcal{M}$ on suljettu konvoluutioon nähden. Konvoluutiokertolaskun kommutatiivisuus ja assosiatiivisuus todettiin jo lauseessa 1.34 samoin kuin funktion E_0 ykkösalkio-ominaisuus. Koska lisäksi $f(1) = 1 \neq 0$, kun $f \in \mathcal{M}$, on käänteisalkio f^{-1} (lukuteoreettisten funktioiden muodostamassa renkaassa) huomautuksen 1.35 mukaan olemassa. Kuitenkaan ei ole heti selvää, että $f^{-1} \in \mathcal{M}$, vaan tämä pitää todistaa. Huomautuksen 1.35 nojalla $f^{-1}(1) = 1$.

Määritellään funktio g ehdoilla $g(1) = 1$, $g(p^a) = f^{-1}(p^a)$, kun $p \in \mathbb{P}$ ja $a \in \mathbb{N}$ ja yleisesti

$$g(p_1^{a_1} p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}) = \prod_{i=1}^{r} g(p_i^{a_i}).$$

Lauseen 1.39 nojalla $g \in \mathcal{M}$. Silloin $f * g \in \mathcal{M}$ ja

$$(f * g)(p^a) = \sum_{d|p^a} f(d) g(p^a/d) = \sum_{d|p^a} f(d) f^{-1}(p^a/d) = (f * f^{-1})(p^a) = E_0(p^a).$$

Koska nyt multiplikatiiviset funktiot $f * g$ ja E_0 ovat samat alkulukupotensseilla, ne ovat samat muutenkin. Täten $f^{-1} = g \in \mathcal{M}$, kuten väitettiin. □

Lause 1.42. *Jos funktio* $f \in \mathcal{M}$ *ja*

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

niin $g \in \mathcal{M}$. *Jos luvulla* n *on kanoninen esitys* (17), *niin*

$$g(n) = \prod_{i=1}^{r} (1 + f(p_i) + \cdots + f(p_i^{a_i})).$$

Todistus. Koska $g = f * E$, missä f ja E ovat multiplikatiivisia, on g lauseen 1.40 mukaan multiplikatiivinen. Funktion $g(n)$ tuloesitys seuraa nyt kaavasta (18), koska $g(p^k) = 1 + f(p) + \cdots + f(p^k)$. □

Lause 1.43. *Funktio*

$$\sigma_\alpha(n) = \sum_{d|n, d>0} d^\alpha$$

on multiplikatiivinen. Erityisesti funktiot

$$d(n) = \sigma_0(n) = \textit{luvun } n \textit{ positiivisten tekijöiden lukumäärä,}$$
$$\sigma(n) = \sigma_1(n) = \textit{luvun } n \textit{ positiivisten tekijöiden summa}$$

ovat multiplikatiivisia. Lisäksi

$$d(n) = (a_1 + 1) \cdots (a_r + 1), \tag{19}$$

jos luvulla n on kanoninen esitys (17)*, ja jos $\alpha \neq 0$, niin*

$$\sigma_\alpha(n) = \prod_{p|n, p\in\mathbb{P}} \frac{(p^\alpha)^{\nu_p(n)+1} - 1}{p^\alpha - 1}. \tag{20}$$

Todistus. Funktion σ_α multiplikatiivisuus nähdään valitsemalla edellisessä lauseessa $f = N_\alpha$. Kaava (19) seuraa kaavasta (18), kun otetaan huomioon, että $d(p^k) = k + 1$; luvun p^k tekijöitähän on $k + 1$ kappaletta, nimittäin $1,\ p, \ldots,\ p^k$. Kaava (20) nähdään samoin kirjoittamalla näiden lukujen α:nsien potenssien summa "suljetussa muodossa". □

Määritelmä 1.44. Luonnollinen luku on *neliövapaa*, jos sen ainoa neliötekijä on 1.

Huomautus 1.45. Toinen karakterisointi luvun $n > 1$ neliövapaudelle on ehto $a_1 = \cdots = a_r = 1$ sen kanonisessa esityksessä (17).

Määritelmä 1.46. *Möbiuksen funktio* on lukuteoreettinen funktio

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} \text{ jos } n \text{ on neliövapaa,} \\ 0 \text{ muulloin,} \end{cases}$$

ja *Liouvillen funktio* on

$$\lambda(n) = (-1)^{\Omega(n)}.$$

Suoraan määritelmien perusteella voidaan helposti verifioida seuraava

Lause 1.47. *Möbiuksen funktio on multiplikatiivinen ja Liouvillen funktio täydellisesti multiplikatiivinen.*

Lause 1.48. *$\mu * E = E_0$, ts.*

$$\sum_{d|n} \mu(d) = \begin{cases} 1,\ \textit{jos } n = 1, \\ 0,\ \textit{jos } n > 1. \end{cases} \tag{21}$$

Edelleen

$$\sum_{d|n} \lambda(d) = \begin{cases} 1,\ \textit{jos } n \textit{ on neliö,} \\ 0,\ \textit{muulloin.} \end{cases} \tag{22}$$

Todistus. Molemmat väitteet ovat selviä, jos $n = 1$. Oletetaan, että $n > 1$ ja että n on kuten kaavassa (17). Lauseen 1.42 nojalla

$$\sum_{d|n} \mu(d) = \prod_{i=1}^{r} (1 + \mu(p_i) + \mu(p_i^2) + \ldots + \mu(p_i^{a_i})) = \prod_{i=1}^{r} (1 - 1) = 0$$

ja

$$\sum_{d|n} \lambda(d) = \prod_{i=1}^{r} (1 + \lambda(p_i) + \lambda(p_i^2) + \ldots + \lambda(p_i^{a_i})) = \prod_{i=1}^{r} (1 - 1 + 1 - \ldots + (-1)^{a_i}),$$

joka on 1 jos ja vain jos kaikki luvut a_i ovat parillisia (eli n on neliö), ja muuten 0. □

Huomautus 1.49. Edellisen mukaan funktiolla μ on konvoluutioon nähden käänteisalkio $E = \mu^{-1}$.

Lause 1.50 (Möbiuksen inversiokaava)**.** *Lukuteoreettisille funktioille f ja g ovat seuraavat relaatiot ekvivalentit:*

$$f(n) = \sum_{d|n} g(d) \text{ kaikilla } n \in \mathbb{N},$$

$$g(n) = \sum_{d|n} f(d)\mu(n/d) \text{ kaikilla } n \in N.$$

Todistus. Huomautuksen 1.49 mukaan on

$$f = g * E \Longleftrightarrow g = f * E^{-1} = f * \mu,$$

mikä todistaa väitteen. □

Määritelmä 1.51. *Eulerin funktio* $\varphi(n)$ merkitsee niiden luonnollisten lukujen $m \leq n$ lukumäärää, joille $(m, n) = 1$.

Lauseen 2.12 nojalla $\varphi \in \mathcal{M}$. Jos $p \in \mathbb{P}$ ja $k \in \mathbb{N}$, niin selvästi $\varphi(p^k) = p^k - p^{k-1}$ ja näin funktiolle φ saadaan kaava

$$\varphi(n) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i}) = \prod_{i=1}^{r} p_i^{a_i - 1}(p_i - 1), \tag{23}$$

jos luvulla n on kanoninen esitys (17).

Koska $\mu \in \mathcal{M}$ ja $N_1 \in \mathcal{M}$, niin $\mu * N_1 \in \mathcal{M}$. Jos $p \in \mathbb{P}$ ja $k \in \mathbb{N}$, niin

$$(\mu * N_1)(p^k) = p^k - p^{k-1} = \varphi(p^k),$$

mikä osoittaa, että

$$\varphi = \mu * N_1.$$

Kertomalla konvoluutiomielessä molemmat puolet funktiolla E saadaan

$$\varphi * E = \mu * N_1 * E = (\mu * E) * N_1 = N_1.$$

Näin on todistettu seuraava lause.

Lause 1.52. $\varphi * E = N_1$ *eli*

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

kaikilla $n \in \mathbb{N}$. □

Tähän yhteyteen sopii vielä kaksi analyyttista tulosta, jotka valaisevat luonnollisten lukujen ominaisuuksia statistiselta kannalta. Tarkastellaan summafunktioiden

$$D(x) = \sum_{n \le x} d(n),$$

$$Q(x) = \sum_{n \le x} \mu^2(n)$$

käyttäytymistä kun $x \to \infty$.

Summan $D(x)$ tutkiminen on geometrisesti katsottuna esimerkki ns. *verkkopisteprobleemoista*. *Verkkopisteeksi* sanotaan tason (tai yleisemmin $\mathbb{R}^n$:n) pistettä, jonka koordinaatit ovat kokonaislukuja. Nyt $d(n)$ on niiden luonnollisten lukujen muodostamien parien (u, v) lukumäärä, joille $uv = n$, joten $D(x)$ merkitsee verkkopisteiden lukumäärää siinä alueessa, jonka koordinaattiakselit ja hyperbeli $uv = x$ rajoittavat uv-tason ensimmäiseen neljännekseen.

Summa $Q(x)$ puolestaan merkitsee niiden neliövapaiden lukujen lukumäärää, jotka eivät ylitä lukua x.

Olkoon $f(x)$ positiiviarvoinen funktio. Kaavoissa esiintyvä merkintä $O(f(x))$ tarkoittaa, että on olemassa sellainen funktio $g(x)$, joka voidaan sijoittaa sen paikalle ja joka toteuttaa ehdon $|g(x)| \le Cf(x)$ kaikille $x \ge x_0$, kun vakiot x_0 ja C on valittu sopivasti.

Lause 1.53. $D(x) = x \ln x + O(x)$.

Todistus. Kun $d(n)$ tulkitaan edellä esitetyllä tavalla ja $x \ge 1$, saadaan kaavan (12) nojalla (missä $\lfloor x \rfloor$ tarkoittaa suurinta kokonaislukua, joka on enintään luvun x suuruinen)

$$D(x) = \sum_{uv \le x} 1 = \sum_{u \le x} \lfloor \frac{x}{u} \rfloor \le \sum_{u \le x} \frac{x}{u} = x \sum_{u \le \lfloor x \rfloor} \frac{1}{u} \le x(1 + \ln \lfloor x \rfloor) \le x \ln x + x,$$

ja toisaalta

$$D(x) \ge \sum_{u \le x} \left(\frac{x}{u} - 1 \right) \ge -x + x \sum_{u \le \lfloor x \rfloor} \frac{1}{u} \ge -x + x \int_1^{\lfloor x \rfloor + 1} \frac{1}{t}\, dt \ge -x + x \int_1^x \frac{1}{t}\, dt = x \ln x - x,$$

joista väite nähdään. □

Kun $s > 1$, määritellään Riemannin zeta-funktio yhtälöllä

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Kun tämä määritelmä laajennetaan kompleksiluvuille, päädytään funktioteoreettiseen Riemannin zeta-funktioon, joka näyttelee keskeistä osaa ns. analyyttisessä lukuteoriassa.

Lause 1.54. $Q(x) = \zeta(2)^{-1} x + O(\sqrt{x})$.

Todistus. Todetaan aluksi, että

$$\mu^2(n) = \sum_{d^2|n} \mu(d). \tag{24}$$

Jos ensinnäkin n on neliövapaa, käy d vain luvun 1, ja yhtälö pätee muodossa $1 = 1$. Muuten $n = hk^2$, missä h on neliövapaa ja $k > 1$, ja d käy nyt luvun k positiiviset tekijät. Tällöin yhtälön (24) oikea puoli on 0 lauseen 1.48 nojalla, ja vasen puoli on myös 0, koska n ei ole neliövapaa.

Yhtälön (24) mukaan

$$Q(x) = \sum_{n\le x}\sum_{d^2|n} \mu(d) = \sum_{d\le\sqrt{x}} \mu(d) \sum_{\substack{n\le x \\ d^2|n}} 1 = \sum_{d\le\sqrt{x}} \mu(d)(\frac{x}{d^2} + O(1)).$$

Tässä merkintä $O(1)$ tarkoittaa, että sen paikalle voidaan kirjoittaa funktio $f(x)$, jolle pätee $|f(x)| \le C$ kaikille $x \ge x_0$ (missä x_0 ja C ovat sopivia vakioita). Edelleen

$$Q(x) = x \sum_{d\le\sqrt{x}} \frac{\mu(d)}{d^2} + O(\sqrt{x}) = x\left(\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O(\frac{1}{\sqrt{x}})\right) + O(\sqrt{x}) = x\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O(\sqrt{x}).$$

Tässä on käytetty hyväksi arviota

$$\left|\sum_{d>\sqrt{x}} \frac{\mu(d)}{d^2}\right| \le \sum_{d>\sqrt{x}} \frac{1}{d^2} \le \frac{1}{x} + \int_{\sqrt{x}}^{\infty} \frac{1}{t^2}\,dt = \frac{1}{x} + \frac{1}{\sqrt{x}} \le \frac{2}{\sqrt{x}} \qquad (x \ge 1).$$

Käyttämällä hyväksi itseisesti suppenevien sarjojen kertomista ja lausetta 1.48 nähdään, että jos $s > 1$, niin

$$\sum_{c=1}^{\infty} \frac{1}{c^s} \sum_{d=1}^{\infty} \frac{\mu(d)}{d^s} = \sum_{n=1}^{\infty} \sum_{cd=n} \frac{\mu(d)}{(cd)^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{d|n} \mu(d) = 1,$$

joten funktiolle $Q(x)$ saadussa viimeisessä lausekkeessa oleva summa on $\zeta(2)^{-1}$. □

Huomautus 1.55. Voidaan osoittaa, että $\zeta(2) = \pi^2/6$. Siis $Q(x) = (6/\pi^2)x + O(\sqrt{x})$. Koska $6/\pi^2 = 0.6079...$, voidaan sanoa, että satunnaisesti valittu luonnollinen luku on neliövapaa noin 61:n prosentin todennäköisyydellä.

2 Jäännösluokkarenkaat ja kongruenssit

2.1 Jäännösluokkarengas $\mathbb{Z}_n$

Määritelmä 2.1. Olkoon $n \in \mathbb{N}$ ja $a,\ b \in \mathbb{Z}$. Sanotaan, että a on *kongruentti b:n kanssa modulo n*, jos $n|a - b$. Tällöin merkitään $a \equiv b \pmod{n}$ tai $a \equiv b\ (n)$, ja sanotaan, että n on ko. kongruenssin *moduli*. Jos $n \nmid a - b$, sanotaan, että a ja b ovat *epäkongruentteja modulo n* ja merkitään $a \not\equiv b \pmod{n}$.

Huomautus 2.2. Kongruenssi on ekvivalenssirelaatio, ts. se toteuttaa ehdot 1) $a \equiv a \pmod{n}$, 2) jos $a \equiv b \pmod{n}$, niin $b \equiv a \pmod{n}$, ja 3) jos $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$, niin $a \equiv c \pmod{n}$.

Huomautus 2.3. Kongruensseja voidaan laskea yhteen ja kertoa puolittain:

$$a \equiv b\ (n),\ c \equiv d\ (n) \Longrightarrow a + c \equiv b + d\ (n),\ ac \equiv bd\ (n).$$

Ensimmäinen väite seuraa suoraan määritelmästä; jälkimmäinen nähdään toteamalla, että $ac \equiv bc \pmod{n}$ ja $bc \equiv bd \pmod{n}$, ja käyttämällä edellisen huomautuksen kohtaa 3).

Lause 2.4. *Olkoon $P(x_1, \ldots, x_k)$ kokonaiskertoiminen polynomi ja $a_i \equiv b_i \pmod{n}$, $i = 1, \ldots, k$. Silloin*

$$P(a_1, \ldots, a_k) \equiv P(b_1, \ldots, b_k) \pmod{n}.$$

Todistus. Sovelletaan toistuvasti edellisen huomautuksen sääntöjä. □

Seuraava yksinkertainen lause on jatkon kannalta avainasemassa.

Lause 2.5. *Jos $(a, n) = 1$, niin on olemassa sellainen $a' \in \mathbb{Z}$, että $aa' \equiv 1 \pmod{n}$.*

Todistus. Lauseen 1.9 nojalla on olemassa sellaiset kokonaisluvut x_1 ja x_2, että $x_1a + x_2n = 1$. Luvuksi a' voidaan valita x_1. □

Huomautus 2.6. Jos myös $aa'' \equiv 1 \pmod{n}$, niin $a' \equiv a'aa'' \equiv a'' \pmod{n}$.

Seuraus 2.7. *Jos $ac \equiv bc \pmod{n}$ ja $(c, n) = 1$, niin $a \equiv b \pmod{n}$.*

Todistus. Edellisen lauseen nojalla on olemassa sellainen c', että $cc' \equiv 1 \pmod{n}$. Väite seuraa, kun oletus kerrotaan puolittain luvulla c'. □

Lause 2.8. *Jos $ac \equiv bc \pmod{n}$ ja $d = (c, n)$, niin $a \equiv b \pmod{n/d}$.*

Todistus. Lauseen oletuksen mukaan on luku $ac - bc = kn$ jollakin kokonaisluvulla k. Kun tämä yhtälö jaetaan puolittain luvulla d, saadaan $(c/d)(a - b) = k(n/d)$. Koska lauseen 1.13 mukaan on $(c/d, n/d) = 1$, tästä seuraa, että $(n/d)|a - b$, mikä merkitsee samaa kuin lauseen väite. □

Luvun a määräämä **jäännösluokka** $\pmod{n}$ on joukko $\{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$, jolle käytetään merkintää $\overline{a}$. Usein luvun a yläpuolinen viiva myös jätetään merkitsemättä. Jokainen kokonaisluku x kuuluu (jakoalgoritmin nojalla) tarkalleen yhteen jäännösluokista $\overline{0}, \overline{1}, \ldots, \overline{n-1}$, ja näiden n eri jäännösluokan muodostama joukko $\mathbb{Z}_n$ on kommutatiivinen rengas, kun yhteenlasku määritellään ehdolla $\overline{a} + \overline{b} = \overline{a + b}$ ja tulo ehdolla $\overline{a}\overline{b} = \overline{ab}$. Nämä operaatiot ovat hyvinmääriteltyjä huomautuksen 2.3 nojalla. Jos kustakin jäännösluokasta valitaan yksi alkio, saadaan jäännösluokkien **edustajisto**. Esimerkiksi luvut $0, 1, \ldots, n-1$ muodostavat jäännöluokkien modulo n edustajiston. Tällaiselle joukolle käytetään usein myös toista nimitystä.

Määritelmä 2.9. Lukujoukko, joka muodostaa jäännösluokkien (mod n) edustajiston, on *täydellinen jäännössysteemi* (t.j.s.) *modulo n.*

Huomautus 2.10. Lukujoukko on selvästi t.j.s. (mod n) silloin ja vain silloin kun seuraavat ehdot ovat voimassa: 1) lukuja on n kappaletta, ja 2) luvut ovat epäkongruentteja (mod n).

Esimerkki 2.11. 1) Edellä nähtiin jo, että joukko $\{0, 1, \ldots, n-1\}$ on t.j.s. (mod n). Nämä luvut ovat ns. **pienimmät ei-negatiiviset jäännökset modulo** n.
2) Jos n on pariton, muodostavat luvut m, joille $|m| < n/2$, t.j.s:n (mod n). Nämä luvut ovat ns. **itseisesti pienimmät jäännökset modulo** n. Jos n on parillinen, pitää ottaa mukaan jompikumpi luvuista $\pm n/2$.
3) {6, 13, 100, -11, 27} on t.j.s. (mod 5).

Annetusta t.j.s:stä voidaan muodostaa uusia seuraavalla tavalla.

Lause 2.12. *Jos $(k, n) = 1$, $h \in \mathbb{Z}$ ja a käy t.j.s:n (mod n), niin samoin käy $h + ka$. Erityisesti lukujoukko*

$$h,\ h+k,\ ,\ h+2k, \ldots,\ h+(n-1)k \tag{25}$$

on t.j.s. (mod n).

Todistus. Jos $h + ka_1 \equiv h + ka_2 \pmod{n}$, missä a_1 ja a_2 kuuluvat annettuun systeemiin, niin $a_1 \equiv a_2 \pmod{n}$ (luvulla k voitiin jakaa, koska $(k, n) = 1$). Täten $a_1 = a_2$, sillä luvut a ovat epäkongruentteja. Nähdään siis, että luvut $h + ka$ ovat epäkongruentteja. Koska niitä on lisäksi yhtä monta kuin lukuja a eli n kpl, ne muodostavat t.j.s:n (mod n) lauseen 2.10 nojalla. Joukko (25) saadaan erikoistapauksena antamalla luvun a käydä luvut 0, 1, ..., $n - 1$. □

Lause 2.13. *Jos $m, n \in \mathbb{N}$ ja $(m, n) = 1$, niin*

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

Todistus. Annetut kaksi kokonaislukua (joista ainakin toisen oletetaan poikkeavan nollasta) ovat suhteellisia alkulukuja tarkalleen silloin, kun niillä ei ole yhtään yhteistä alkutekijää. Näin $(a, mn) = 1$ jos ja vain jos $(a, m) = (a, n) = 1$.

Kirjoitetaan luvut $1, 2, \ldots, mn$ kaavioon

$$\begin{array}{rccccc}
1 & 2 & \ldots & i & \ldots & m \\
m+1 & m+2 & \ldots & m+i & \ldots & 2m \\
2m+1 & 2m+2 & \ldots & 2m+i & \ldots & 3m \\
\vdots & & & \vdots & & \vdots \\
(n-1)m+1 & (n-1)m+2 & \ldots & (n-1)m+i & \ldots & nm.
\end{array}$$

Sarakkeen i luku on suhteellinen alkuluku luvun m kanssa jos ja vain jos $(i, m) = 1$; olkoon i jokin näistä $\varphi(m)$ luvusta. Ko. sarakkeen luvut muodostavat edellisen lauseen nojalla t.j.s:n (mod$n$), joten niiden joukossa on tarkalleen $\varphi(n)$ lukua, jotka ovat suhteellisia alkulukuja myös luvun n kanssa. □

Edellä on tarkasteltu miten kongruensseista tietyn saman modulin suhteen voidaan johtaa uusia kongruensseja. Seuraava lause koskee päinvastaista tilannetta: kongruentit luvut ovat samat mutta modulit erilaisia.

Lause 2.14. *Jos* $a \equiv b \pmod{n_i},\ i = 1, \ldots, m,$ *niin*

$$a \equiv b \pmod{[n_1, \ldots, n_m]}.$$

Todistus. Oletuksen mukaan $n_i | a - b$, joten $a - b$ on lukujen n_i eräs yhteinen jaettava ja siis jaollinen niiden p.y.j:llä. □

Seuraus 2.15. *Jos* $a \equiv b \pmod{n_i},\ i = 1, \ldots, m,$ *missä luvut* n_i *ovat parittain suhteellisia alkulukuja, niin*

$$a \equiv b \pmod{n_1 \cdots n_m}.$$

Todistus. Lukuja n_i koskevasta oletuksesta seuraa, että niiden p.y.j. on yhtä kuin niiden tulo (kaavan (9) nojalla). □

Jaollisuussääntöjä. Kongruenssien avulla voidaan helposti johtaa sääntöjä, joiden avulla voidaan jakolaskua suorittamatta selvittää, onko jokin luku a jaollinen annetulla luvulla n. Oletetaan tunnetuksi a:n esitys jossakin lukujärjestelmässä, esimerkiksi kymmenjärjestelmässä. Siis $a = (a_k a_{k-1} \ldots a_0)_{10}$ eli

$$a = a_0 + a_1 10 + \cdots + a_k 10^k. \tag{26}$$

Johdetaan säännöt tapauksissa $n = 3,\ 9,$ ja 11. Merkitään

$$S_0(a) = \sum_{i=0}^{k} a_i, \qquad S_1(a) = \sum_{i=0}^{k} (-1)^i a_i.$$

Säännöt ovat seuraavat:

(i) $3|a \iff 3|S_0(a)$,

(ii) $9|a \iff 9|S_0(a)$,

(iii) $11|a \iff 11|S_1(a)$.

Esimerkiksi luvulle $a = 4127835$ on $S_0(a) = 30$ ja $S_1(a) = 8$. Siten $3|a,\ 9 \nmid a,\ 11 \nmid a$. Luvulle $a = 723160823$ on $S_1(a) = 22$ ja siis $11|a$.

Sääntöjen (i) - (iii) todistamiseksi sovelletaan (26):ssä kongruensseja

$$10 \equiv 1 \pmod{3},\ 10 \equiv 1 \pmod{9},\ 10 \equiv -1 \pmod{11},$$

jolloin saadaan

$$a \equiv S_0(a) \pmod{3}, \quad a \equiv S_0(a) \pmod{9}, \quad a \equiv S_1(a) \pmod{11}.$$

Väitteet seuraavat helposti näistä kongruensseista. Huomattakoon, että em. jaollisuussääntöjä voidaan myös iteroida, ts. soveltaa samaa sääntöä uudestaan lukuihin

$$S_i(a),\ S_i(S_i(a)), \ldots$$

jotka kaikki ovat kongruentteja a:n kanssa vastaavasti 3:n, 9:n tai 11:n suhteen.

2.2 Alkuluokkaryhmä $\mathbb{Z}_n^*$

Määritelmä 2.16. Jäännösluokka (mod n) on *alkuluokka* (mod n), jos sen sisältämät luvut ovat suhteellisia alkulukuja luvun n kanssa. Alkuluokkien edustajisto on *supistettu jäännössysteemi* (s.j.s.) (mod n).

Koska $(a + kn, n) = (a, n)$, on edellinen määritelmä järkevä.
Eulerin funktio $\varphi(n)$ antaa määritelmän 1.51 mukaisesti alkuluokkien lukumäärän.

Huomautus 2.17. Lukujoukko on selvästikin s.j.s. (mod n) silloin ja vain silloin, kun seuraavat ehdot ovat voimassa: 1) lukuja on $\varphi(n)$ kappaletta, 2) luvut ovat suhteellisia alkulukuja luvun n kanssa, ja 3) luvut ovat epäkongruentteja (mod n).

Lause 2.18. *Jos (k,n) = 1 ja a käy s.j.s:n (mod n), niin samoin käy ka.*

Todistus. Lukujen ka muodostama systeemi täyttää selvästi huomautuksen 2.17 ehdot. □

Lause 2.19. *Alkuluokat (mod n) muodostavat kertolaskuun nähden Abelin ryhmän $\mathbb{Z}_n^*$, jonka kertaluku on $\varphi(n)$.*

Todistus. Kahden alkuluokan tulo on ilmeisesti alkuluokka ja luokka $\overline{1}$ on ykkösalkio. Abelin ryhmän määritelmän ehdoista vaatii enää vain käänteisalkion olemassaolo perustelun. Jos $(a, n) = 1$, niin lauseen 2.5 nojalla on olemassa sellainen a', että $aa' \equiv 1 \pmod{n}$: täten $\overline{a'}$ on alkion $\overline{a}$ käänteisalkio. □

Jos n on alkuluku, niin jokaisella kommutatiivisen renkaan $\mathbb{Z}_n$ nollasta eroavalla alkiolla on siis käänteisalkio kertolaskun suhteen. Tämä todistaa seuraavan lauseen.

Lause 2.20. *Jos p on alkuluku, niin $\mathbb{Z}_p$ on kunta.* □

Lause 2.21 (Eulerin lause)**.** *Jos $(a, n) = 1$, niin*

$$a^{\varphi(n)} \equiv 1 \pmod{n}. \tag{27}$$

Todistus. Olkoon $x_1, \ldots, x_{\varphi(n)}$ jokin s.j.s. (mod n). Koska $(a, n) = 1$, niin lauseen 2.18 nojalla myös $ax_1, \ldots, ax_{\varphi(n)}$ on s.j.s. (mod n). Näin

$$x_1 \cdot \ldots \cdot x_{\varphi(n)} \equiv ax_1 \cdot \ldots \cdot ax_{\varphi(n)} \equiv a^{\varphi(n)} x_1 \cdot \ldots \cdot x_{\varphi(n)} \pmod{n}.$$

Koska $(x_1 x_2 \cdot \ldots x_{\varphi(n)}, n) = 1$, niin väite saadaan seurauslauseesta 2.7. □

Alkion $\overline{a} \in \mathbb{Z}_n^*$ kertaluku ryhmässä $\mathbb{Z}_n^*$ on määritelmän mukaan pienin $k \in \mathbb{N}$, jolle $\overline{a}^k = \overline{1}$. Ryhmäteorian tulosten perusteella alkion kertaluku jakaa ryhmän kertaluvun $\varphi(n)$ ja näin $\overline{a}^{\varphi(n)} = \overline{1}$, mikä todistaa toisella tavalla edellisen lauseen.

Lause 2.22 (Fermat'n pikku lause)**.** *Jos p on alkuluku ja $p \nmid a$, niin*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{28}$$

Kaikille kokonaisluvuille a on voimassa

$$a^p \equiv a \pmod{p}. \tag{29}$$

Todistus. Edellinen väite seuraa siitä, että $\varphi(p) = p - 1$. Jälkimmäinen väite saadaan nyt kertomalla edellinen kongruenssi puolittain luvulla a jos $p \nmid a$, ja muuten väite on triviaali. □

Fermat'n pikku lauseen ehto $a^{n-1} \equiv 1 \pmod{n}$ voi olla voimassa, vaikka n olisikin yhdistetty luku, jopa kaikilla sellaisilla luvuilla $a \in \mathbb{N}$, joilla $(a, n) = 1$.

Määritelmä 2.23. Jos n on yhdistetty luku ja $a^{n-1} \equiv 1 \pmod{n}$ aina kun $a \in \mathbb{N}$ ja $(a, n) = 1$, niin n on **Carmichaelin luku**.

Lause 2.24. *Jos $k \geq 2$ ja $n = p_1 p_2 \cdot \ldots \cdot p_k$, missä luvut p_i ovat erisuuria alkulukuja ja $p_i - 1 | n - 1$ kaikilla indekseillä i, niin n on Carmichaelin luku.*

Todistus. Oletetaan, että $a \in \mathbb{N}$ ja $(a, n) = 1$. Silloin $p_i \nmid a$ ja Fermat'n pikku lauseen nojalla $a^{p_i - 1} \equiv 1 \pmod{p_i}$ ja edelleen

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

Näin $a^{n-1} \equiv 1 \pmod{p_1 p_2 \cdot \ldots \cdot p_k}$ seurauslauseen 2.15 nojalla. □

Esimerkki 2.25. Edellisen lauseen nojalla $561 = 3 \cdot 11 \cdot 17$ on Carmichaelin luku.

Seuraava klassinen lause (peräisin englantilaiselta lakimieheltä Sir John Wilsonilta 1700-luvulta) selvittää periaatteessa täydellisesti, onko annettu luku alkuluku vai ei. Sen merkitys on kuitenkin lähinnä teoreettinen, sillä siinä esiintyvä kertoma on laskennollisesti hankala, jos kriteeriä halutaan soveltaa suuriin lukuihin.

Lause 2.26 (Wilsonin lause)**.** *Luonnollinen luku $p > 1$ on alkuluku silloin ja vain silloin kun*

$$(p-1)! + 1 \equiv 0 \pmod{p}. \tag{30}$$

Todistus. Seuraava todistus on peräisin Gaussilta.

1) Oletetaan aluksi, että p on alkuluku. Olkoon a jokin alkuluokka ja a' kuten lauseessa 2.5. Selvitetään aluksi, milloin $a \equiv a' \ (p)$. Näin on, jos ja vain jos

$$0 \equiv a^2 - 1 \equiv (a-1)(a+1) \pmod{p}.$$

Tästä nähdään oikeaksi seuraava aputulos:

$$a \equiv a' \pmod{p} \Longleftrightarrow a \equiv \pm 1 \pmod{p}.$$

Jos siis supistetusta jäännössysteemistä $\{1, 2, \ldots, p-1\}$ poistetaan 1 ja $p - 1$ ($\equiv -1 \ (p)$), jäljelle jäävät luvut voidaan ryhmitellä pareiksi $a,\ a'$, ja kertomalla kaikki nämä kongruenssit puolittain saadaan

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

Kertomalla tämä puolittain luvulla $p-1$ päädytään kongruenssiin

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

joka on ekvivalentti kongruenssin (30) kanssa.

2) Oletetaan toiseksi, että (30) on voimassa. Jos p ei ole alkuluku, se on muotoa $p = ab$, missä $1 < a < p$. Tällöin sama kongruenssi pätee myös modulo a, ja koska $a|(p-1)!$, päädytään mahdottomaan kongruenssiin $1 \equiv 0\ (a)$. □

2.3 Kongruenssien ratkaisemisesta

Oletetaan, että $a_k, a_{k-1}, \ldots, a_0 \in \mathbb{Z}$ ja että $a_k \not\equiv 0 \pmod{n}$. Tarkastellaan yhtälöä

$$\overline{a_k}\,\overline{x}^k + \overline{a_{k-1}}\,\overline{x}^{k-1} + \ldots + \overline{a_1}\,\overline{x} + \overline{a_0} = \overline{0} \tag{31}$$

renkaassa $\mathbb{Z}_n$, ts. kysytään, moniko renkaan $\mathbb{Z}_n$ alkio $\overline{x}$ on yhtälön (31) **juuri**. Ongelma on selvästi yhtäpitävä sen kanssa, moniko luvuista $x \in \{0, 1, \ldots, n-1\}$ toteuttaa kongruenssin

$$a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0 \equiv 0 \pmod{n}. \tag{32}$$

On luonnollista nimittää kyseistä lukumäärää s **kongruenssin** (32) **epäkongruenttien juurten** (tai **ratkaisujen**) (mod n) **lukumääräksi**: kongruenssilla (32) on silloin kokonaislukuratkaisuja tarkalleen s jäännösluokallista modulo n. Lukua k sanotaan kongruenssin (32) asteeksi.

Kun $k = 1$, kongruenssi (32) voidaan kirjoittaa muotoon

$$ax \equiv b \pmod{n} \qquad (a \not\equiv 0 \pmod{n}), \tag{33}$$

jota sanotaan *lineaariseksi kongruenssiksi.*

Lause 2.27. *Lineaarinen kongruenssi* (33) *on ratkeava silloin ja vain silloin kun $d|b$, missä $d = (a, n)$. Jos $d|b$, epäkongruentteja juuria (mod n) on d kpl.*

Todistus. 1) Todetaan aluksi, että ehto $d|b$ on välttämätön ratkeavuudelle. Jos nimittäin kongruenssi (33) on voimassa, niin se pätee myös modulo d, mistä seuraa, että $d|b$. Seuraavassa voidaan olettaa, että tämä ehto on täytetty.

2) Tarkastellaan aluksi tapausta $d = 1$. Jos x käy jonkin t.j.s:n (mod n), niin samoin käy ax lauseen 2.12 mukaan. Täten tarkalleen yksi luvuista $x \in \{0, 1, \ldots, n-1\}$ toteuttaa kongruenssin (33).

3) Yleisessä tapauksessa todetaan aluksi, että luku x toteuttaa kongruenssin (33) silloin ja vain silloin kun

$$(a/d)x \equiv b/d \pmod{n'}, \tag{34}$$

missä $n' = n/d$. Koska $(a/d, n') = 1$, on tällä kongruenssilla kohdan 2) mukaan yksikäsitteinen ratkaisu (mod n'). Olkoon $x_0 \in \{0, 1, \ldots, n'-1\}$ ko. kongruenssin pienin ei-negatiivinen ratkaisu, jolloin kongruenssin ratkaisuja ovat ne kokonaisluvut, jotka ovat kongruentteja luvun x_0 kanssa modulo n'. Luvuista 0, 1, …, $n-1$ luvun x_0 kanssa kongruentteja modulo n' ovat luvut x_0, $x_0 + n'$, …, $x_0 + (d-1)n'$. □

Huomautus 2.28. Lineaarisen kongruenssin ratkaisemiseksi on erilaisia menetelmiä.

1) *Kokeilemalla* jokin t.j.s. (mod n).

2) *Eulerin lauseen* avulla. Jos $(a, n) = 1$, niin $a^{\varphi(n)} \equiv 1 \ (n)$. Oletetaan, ett„ $\varphi(n) > 1$. Silloin

$$ax \equiv b \pmod{n} \Longrightarrow a^{\varphi(n)-1}ax \equiv a^{\varphi(n)-1}b \pmod{n}$$

ja siis

$$x \equiv a^{\varphi(n)-1}b \pmod{n}$$

on kongruenssin (33) ratkaisu.

3) *Eukleideen algoritmin* avulla. Jos $(a, n) = 1$, etsitään Eukleideen algoritmin avulla sellaiset luvut y ja z, että $ya + zn = 1$. Tällöin

$$yb \cdot a + zb \cdot n = b,$$

mistä nähdään, että $x \equiv yb \pmod{n}$ toteuttaa kongruenssin (33).

Esimerkki 2.29. Ratkaistaan kongruenssi $15x \equiv 7 \pmod{32}$ kolmella eri tavalla. Koska (15,32) = 1, on kongruenssilla tarkalleen yksi epäkongruentti juuri (mod 32).

1) Kokeillaan t.j.s. (mod 32), esim. luvut 0, 1, ..., 31. Näistä luku $x = 9$ "tärppää", sillä $15 \cdot 9 - 7 = 128 = 4 \cdot 32$.

2) $\varphi(32) = 16$, joten $x \equiv 15^{15} \cdot 7 \ (32)$. Nyt on $15^2 = 225 \equiv 1 \ (32)$, joten $15^{14} \equiv 1 \ (32)$ ja $x \equiv 15 \cdot 7 = 105 \equiv 9 \ (32)$.

3) Lukuihin 32 ja 15 sovellettuna Eukleideen algoritmi antaa yhtälöt

$$32 = 2 \cdot 15 + 2, \qquad 15 = 7 \cdot 2 + 1.$$

Näiden avulla saadaan

$$1 = 15 - 7 \cdot 2 = 15 - 7(32 - 2 \cdot 15) = (-7) \cdot 32 + 15 \cdot 15.$$

Täten $x \equiv 15 \cdot 7 = 105 \equiv 9 \ (32)$.

Tarkastellaan vielä erikoistapausta, jossa modulina n on alkuluku p.

Lause 2.30. *Jos $p \in \mathbb{P}$ ja $p \nmid a_k$, niin kongruenssilla*

$$P(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0 \equiv 0 \pmod{p} \tag{35}$$

on korkeintaan k epäkongruenttia juurta (mod p).

Todistus. Tapauksessa $k = 1$ väite on oikea lauseen 2.27 nojalla. Oletetaan nyt, että $k > 1$, ja tehdään induktio-oletus, että väite pätee kongruensseille, joiden aste on pienempi kuin k.

Jos (35):llä ei ole lainkaan juuria, on väite selvä. Jos sillä on juuri a, niin jaetaan $P(x)$ polynomilla $x - a$, jolloin jakojäännös on jokin luku r. Saadaan siis

$$P(x) = Q(x)(x - a) + r, \tag{36}$$

missä $Q(x)$ on astetta $k-1$ oleva polynomi, jonka korkeimman asteen termin kerroin on a_k. Koska $p|P(a)$, seuraa yhtälöstä (36), että $p|r$. Täten (35) on ekvivalentti kongruenssin

$$Q(x)(x-a) \equiv 0 \pmod{p} \tag{37}$$

kanssa. Induktio-oletuksen nojalla on kongruenssilla $Q(x) \equiv 0\ (p)$ korkeintaan $k-1$ epäkongruenttia juurta, joten kongruenssilla (37) on korkeintaan k epäkongruenttia juurta, mikä on induktioväite. □

Esimerkki 2.31. Kongruenssilla $x^{p-1} \equiv 1 \pmod{p}$ (missä $p \in \mathbb{P}$) on Fermat'n pikku lauseen mukaan epäkongruentit juuret $1, 2, \ldots, p-1$, joita on siis $p-1$ kpl eli suurin mahdollinen määrä. Toisaalta kongruenssilla $x^3 + 2 \equiv 0$ (5) on vain yksi epäkongruentti juuri $x = 2$. Kongruenssin juurten lukumäärä voi siis olla pienempi kuin sen aste.

2.4 Kiinalainen jäännöslause

Kiinalaisessa matemaattisessa tekstissä vuodelta 1275 on seuraavanlainen tehtävä: mikä luku antaa jakojäännökseksi ykkösen, jos se jaetaan seitsemällä, kakkosen, jos se jaetaan kahdeksalla, ja kolmosen, jos se jaetaan yhdeksällä? Nämä ehdot voidaan kirjoittaa myös *simultaanisina kongruensseina*

$$x \equiv 1 \quad (7), \qquad x \equiv 2 \quad (8), \qquad x \equiv 3 \quad (9).$$

Seuraava lause koskee tämäntyyppisiä kongruenssiryhmiä.

Lause 2.32 (Kiinalainen jäännöslause)**.** *Olkoot $n_1, \ldots, n_r$ parittain suhteellisia alkulukuja ja $a_1, \ldots, a_r$ mielivaltaisia kokonaislukuja. Silloin kongruenssiryhmällä*

$$x \equiv a_i \pmod{n_i}, \quad i = 1, \ldots, r \tag{38}$$

on yksikäsitteinen ratkaisu modulo $N = n_1 \cdots n_r$.

Todistus. 1) Osoitetaan aluksi ratkaisun olemassaolo. Merkitään

$$N_i = N/n_i = n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_r. \tag{39}$$

Silloin $(N_i, n_i) = 1$, sillä lukujen n_i ja N_i yhteinen alkutekijä olisi luvun n_i ja jonkin muun luvun n_j yhteinen tekijä, mikä on mahdotonta oletuksen mukaan. Olkoon N_i' sellainen kokonaisluku, että

$$N_i N_i' \equiv 1 \pmod{n_i}. \tag{40}$$

Väitetään, että luku

$$x = a_1 N_1 N_1' + \cdots + a_r N_r N_r' \tag{41}$$

on kongruenssien (38) eräs yhteinen ratkaisu. Koska $n_i|N_j$ kun $i \neq j$, ovat oikean puolen yhteenlaskettavista kaikki muut paitsi i:s jaollisia luvulla n_i. Ottamalla vielä huomioon kongruenssi (40) saadaan

$$x \equiv a_i N_i N_i' \equiv a_i \pmod{n_i},$$

kuten väitettiin.

2) Jos toisaalta $x_1 \equiv x \pmod{N}$, niin x_1 on selvästi myös kongruenssiryhmän (38) ratkaisu.

3) Jos x_0 ja x_1 ovat kaksi ratkaisua, niin

$$x_0 \equiv a_i \equiv x_1 \pmod{n_i}, \qquad i = 1, \ldots, r.$$

Lauseen 2.14 seurauksen nojalla $x_0 \equiv x_1 \pmod{N}$. □

Esimerkki 2.33. Ratkaistaan pykälän alussa mainittu tehtävä. Nyt $n_1 = 7$, $n_2 = 8$ ja $n_3 = 9$ ovat parittain suhteellisia alkulukuja, ja luvut (39) ovat $N_1 = 72$, $N_2 = 63$ ja $N_3 = 56$. Lasketaan vielä luvut N_i'. Koska $72 \equiv 2 \pmod{7}$, $63 \equiv -1 \pmod{8}$ ja $56 \equiv 2 \pmod{9}$, nähdään helposti, että luvuiksi N_i' voidaan valita $N_1' = 4$, $N_2' = -1$ ja $N_3' = 5$. Luku (41) on nyt

$$x = 1 \cdot 72 \cdot 4 + 2 \cdot 63 \cdot (-1) + 3 \cdot 56 \cdot 5 = 1002.$$

Lisäksi $N = 504$. Näin ollen kaikki positiiviset luvut x, joille $x \equiv 1002 \equiv 498 \pmod{504}$ ovat tehtävän ratkaisuja. Näistä pienin on 498.

Tarkastellaan seuraavaksi, miten kiinalaisen jäännöslauseen avulla voidaan kongruenssi (mod N) palauttaa kongruensseihin yksinkertaisempien modulien suhteen.

Oletetaan, että luvut $n_1, n_2, \ldots, n_r \in \mathbb{N}$ ovat parittain suhteellisia alkulukuja ja $N = n_1 n_2 \cdots n_r$. Määritellään kuvaus

$$\psi : \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_r} \longrightarrow \mathbb{Z}_N$$

ehdolla

$$\psi((\overline{a_1}, \overline{a_2}, \ldots, \overline{a_r})) = \overline{a},$$

missä a toteuttaa kongruenssit

$$a \equiv a_i \pmod{n_i} \text{ kaikilla } i = 1, 2, \ldots, r.$$

Silloin kiinalaisen jäännöslauseen nojalla kuvaus ψ on hyvinmääritelty. Koska $\psi((\overline{a}, \ldots \overline{a})) = \overline{a}$, on ψ surjektio ja näin bijektio (koska määrittelyjoukossa ja kuvajoukossa on sama määrä alkioita). On helppoa nähdä, että ψ on rengashomomorfismi ja näin rengasisomorfismi.

Lause 2.34. *Olkoon $P(x)$ kokonaiskertoiminen polynomi, $n_1, \ldots, n_r$ parittain suhteellisia alkulukuja ja $N = n_1 \cdots n_r$. Kongruenssi*

$$P(x) \equiv 0 \pmod{N} \tag{42}$$

on ratkeava silloin ja vain silloin kun kaikki kongruenssit

$$P(x) \equiv 0 \pmod{n_i} \qquad (i = 1, \ldots, r) \tag{43}$$

ovat ratkeavia. Jos $\nu(N)$ on kongruenssin (42) epäkongruenttien juurten (mod N) lukumäärä ja ja $\nu(n_i)$ merkitsee kongruenssin (43) epäkongruenttien ratkaisujen (mod n_i) lukumäärää, niin $\nu(N) = \nu(n_1) \cdots \nu(n_r)$.

Todistus. Määritellään

$$S = \{(\overline{a_1}, \ldots, \overline{a_r}) \in \mathbb{Z}_{n_1} \times \ldots \mathbb{Z}_{n_r} \mid P(a_i) \equiv 0 \pmod{n_i} \text{ kaikilla } i = 1, 2, \ldots, r\}$$

ja

$$T = \{\overline{a} \in \mathbb{Z}_N \mid P(a) \equiv 0 \pmod{N}\}.$$

Silloin $|S| = \nu(n_1)\nu(n_2)\ldots\nu(n_r)$ ja $|T| = \nu(N)$ ja lauseen todistamiseksi riittää osoittaa, että $|S| = |T|$.

Olkoon $(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_r}) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_r}$ mielivaltainen ja $\overline{a} = \psi(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_r}) \in \mathbb{Z}_N$.

Jos $(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_r}) \in S$, niin $P(a) \equiv P(a_i) \equiv 0 \pmod{n_i}$ kaikilla indekseillä i, ja näin $P(a) \equiv 0 \pmod{N}$ seurauksen 2.15 nojalla, eli $\overline{a} \in T$. Päättely toimii myös käänteiseen suuntaan, joten $|S| = |T|$, koska ψ on bijektio. □

2.5 Luvun kertaluku (mod n)

Määritelmä 2.35. Olkoon $(a, n) = 1$ ja $n \geq 1$. Luvun a *kertaluku* (mod n) on pienin luonnollinen luku k, jolle

$$a^k \equiv 1 \pmod{n}, \tag{44}$$

eli alkion $\overline{a}$ kertaluku ryhmässä $\mathbb{Z}_n^*$. Merkitään $k = \mathrm{ord}_n(a)$. Sanotaan myös, että a *kuuluu eksponenttiin* k (mod n).

Lause 2.36. *Olkoon $n \geq 1$, $(a, n) = 1$ ja $k = ord_n(a)$ ja olkoot r, s ja m ei-negatiivisia kokonaislukuja. Silloin*

1) $k|\varphi(n)$,
2) $a^r \equiv a^s \pmod{n} \iff r \equiv s \pmod{k}$,
3) $a^r \equiv 1 \pmod{n} \iff r \equiv 0 \pmod{k}$,
4) $1, a, a^2, \ldots, a^{k-1}$ *ovat epäkongruentteja* (mod n),
5) $ord_n(a^m) = k/(k, m)$.

Todistus. Jos 4) ei olisi voimassa, niin $a^i \equiv a^j \pmod{n}$ joillakin $0 \leq i < j < k$. Kertomalla kongruenssi puolittain i kertaa lauseen 2.5 luvulla a' saataisiin $a^{j-i} \equiv 1\ (n)$, mikä on vastoin luvun k valintaa.

Potenssista k lähtien samat jäännösluokat alkavat toistua:

$$a^k \equiv 1\ (n), \qquad a^{k+1} \equiv a\ (n), \quad \ldots, \qquad a^{2k-1} \equiv a^{k-1}\ (n), \qquad a^{2k} \equiv 1\ (n), \quad \ldots.$$

Näin 2) ja 3) ovat selvästi voimassa.

Eulerin lauseen nojalla $a^{\varphi(n)} \equiv 1 \pmod{n}$, joten kohdasta 3) seuraa kohta 1).

Kohdan 3) nojalla $(a^m)^i \equiv 1 \pmod{n}$ (missä $i \in \mathbb{N}$), jos ja vain jos $k|mi$. Jos merkitään $d = (k, m)$, $k = k'd$ ja $m = m'd$, niin tämä on edelleen yhtäpitävä ehdon $k'd|m'di$ eli $k'|m'i$ kanssa. Koska $(k', m') = 1$, niin lauseen 1.16 nojalla näin on, jos ja vain jos $k'|i$. Siis $\mathrm{ord}_n(a^m) = k' = k/(k, m)$, mikä todistaa kohdan 5). □

Esimerkki 2.37. Etsittäessä luvun kertalukua (mod n) riittää edellisen lauseen kohdan 1) nojalla käydä läpi luvun $\varphi(n)$ positiiviset tekijät. Esimerkiksi $\mathrm{ord}_{14}(5) = 1$, 2, 3, tai 6, jotka ovat luvun $\varphi(14) = (2-1)(7-1) = 6$ positiiviset tekijät. Nyt on

$$5 \not\equiv 1 \ (14), \quad 5^2 \not\equiv 1 \ (14), \quad 5^3 \equiv -1 \ (14), \quad 5^6 \equiv 1 \ (14),$$

mistä seuraa, että $\mathrm{ord}_{14}(5) = 6$.

Määritelmä 2.38. Jos $\mathrm{ord}_n(a) = \varphi(n)$ (eli $\mathbb{Z}_n^*$ on alkion $\overline{a}$ generoima syklinen ryhmä), niin luku a on *primitiivinen juuri* (mod n).

Lause 2.39. *Ryhmä $\mathbb{Z}_n^*$ on syklinen, jos on olemassa primitiivinen juuri (mod n). Jos a on jokin primitiivinen juuri, niin a^m, missä $1 \le m \le \varphi(n)$, on primitiivinen juuri (mod n) jos ja vain jos $(m, \varphi(n)) = 1$. Jos on olemassa primitiivinen juuri* (mod n)*, niin epäkongruentteja primitiivisiä juuria* (mod n) *on $\varphi(\varphi(n))$ kappaletta.*

Todistus. Tämä seuraa suoraan edellisestä määritelmästä ja edellisen lauseen kohdasta 5). □

2.6 Primitiiviset juuret ja indeksit (mod p)

Olkoon p alkuluku. Tässä pykälässä osoitamme, että on olemassa primitiivisiä juuria (mod p). Itse asiassa selvitämme yleisesti kysymyksen, miten monta (epäkongruenttia) lukua kuuluu annettuun eksponenttiin k. Koska $\varphi(p) = p-1$, voidaan olettaa, että $k|(p-1)$. Jos a kuuluu eksponenttiin k (mod p), niin a on *binomikongruenssin*

$$x^k \equiv 1 \pmod{p} \tag{45}$$

juuri. Seuraava lause koskee tämän kongruenssin ratkaisuja.

Lause 2.40. *Jos $ord_p(a) = k$, niin binomikongruenssin* (45) *epäkongruenttien juurten lukumäärä on k. Luvut*

$$1, \ a, \ a^2, \ldots, a^{k-1} \tag{46}$$

ovat ko. kongruenssin epäkongruentteja juuria.

Todistus. 1) Luvut (46) toteuttavat kongruenssin (45) sillä $(a^s)^k \equiv (a^k)^s \equiv 1 \quad (p)$.

2) Luvut ovat epäkongruentteja (mod p) (vrt. lause 2.36 (4)).

3) Kongruenssilla (45) on lauseen 2.30 mukaan korkeintaan k epäkongruenttia juurta. □

Lause 2.41. *i) Jos $k|(p-1)$, niin on olemassa tarkalleen $\varphi(k)$ epäkongruenttia lukua, jotka kuuluvat eksponenttiin k* (mod p)*. Jos a on yksi näistä, niin ne $\varphi(k)$ lukua* (46)*, joiden eksponentti on suhteellinen alkuluku luvun k kanssa, ovat epäkongruentteja ja kuuluvat eksponenttiin k.*

ii) Erityisesti on siis olemassa $\varphi(p-1)$ epäkongruenttia primitiivistä juurta (mod p). Jos a on jokin primitiivinen juuri, niin ne $\varphi(p-1)$ lukua a^m, missä $1 \leq m \leq p-1$ ja $(m, p-1) = 1$, ovat epäkongruentteja primitiivisiä juuria.

Todistus. Luvuista $1,\ 2, \ldots, p-1$ jokainen kuuluu *johonkin* eksponenttiin (mod p). Jos em. luvuista eksponenttiin k kuuluu $f(k)$ lukua, niin

$$\sum_{k|p-1} f(k) = p - 1. \tag{47}$$

Väitetään, että $f(k) = \varphi(k)$.

Osoitetaan aluksi, että $f(k) \leq \varphi(k)$. Tämä on selvä jos $f(k) = 0$ eli eksponenttiin k ei kuulu yhtään lukua. Jos taas jokin luku a kuuluu eksponenttiin k, niin jokainen kongruenssin (45) ratkaisu — ja siis erityisesti jokainen eksponenttiin k kuuluva luku — on kongruentti jonkin luvuista (46) kanssa (mod p). Lauseen 2.36 kohdan (5) mukaan tarkalleen ne potenssit, joiden eksponentti on suhteellinen alkuluku luvun k kanssa, kuuluvat eksponenttiin k. Näin tässä tapauksessa $f(k) = \varphi(k)$.

Lauseen 1.52 mukaan on

$$\sum_{k|p-1} \varphi(k) = p - 1.$$

Tästä ja yhtälöstä (47) seuraa, että

$$\sum_{k|p-1} (\varphi(k) - f(k)) = 0.$$

Edellisen mukaan on tässä jokainen termi ei-negatiivinen. Summa voi olla nolla vain jos kaikki termit ovat nollia. Täten $f(k) = \varphi(k)$ aina kun $k|p-1$. Lause on näin todistettu. □

Esimerkki 2.42. Primitiivisiä juuria (mod 17) on $\varphi(16) = 8$ kpl. Etsitään niistä pienin positiivinen luku. Luku 2 ei ole primitiivinen juuri, sillä $2^4 \equiv -1 \pmod{17}$ ja siis $2^8 \equiv 1 \pmod{17}$. Sen sijaan 3 on primitiivinen juuri, sillä $3^2 \equiv 9 \pmod{17}$, $3^4 \equiv -4 \pmod{17}$ ja $3^8 \equiv -1 \pmod{17}$. Muut primitiiviset juuret ovat 3^m, missä m käy parittomat luvut väliltä $3 \leq m \leq 15$. Niiden pienimmät positiiviset jäännökset (mod 17) ovat 5, 6, 7, 10, 11, 12, ja 14.

Huomautus 2.43. Laskuissa on mukavinta valita primitiivinen juuri itseisarvoltaan mahdollisimman pieneksi. Tiedetään, että pienin primitiivinen juuri (mod p) on suuruusluokkaa $O(p^{1/4+\epsilon})$ (D. A. Burgess 1962). Otaksutaan, että vieläpä arvio $O(p^\epsilon)$ pitäisi paikkansa.

Huomautus 2.44. Lukuteorian jatkokurssilla todistetaan, että *primitiivinen juuri (mod n) on olemassa silloin ja vain silloin kun $n = 1, 2, 4, p^t$, tai $2p^t$*, missä p on pariton alkuluku ja t luonnollinen luku.

Edellistä lausetta käyttäen saadaan seuraava välttämätön ja riittävä ehto sille, että luku n on alkuluku.

Lause 2.45. *Luonnollinen luku $n > 1$ on alkuluku, jos ja vain jos on olemassa kokonaisluku x, joka täyttää ehdot*

$$x^{n-1} \equiv 1 \pmod{n}, \tag{48}$$

$$x^{(n-1)/q} \not\equiv 1 \pmod{n} \text{ kaikille luvun } n-1 \text{ alkutekijöille } q. \tag{49}$$

Todistus. Jos n on alkuluku, valitaan luvuksi x primitiivinen juuri (mod n).

Tarkastellaan sitten käänteistä väitettä. Ehdosta (48) seuraa lauseen 2.36 kohdan (3) nojalla, että $\mathrm{ord}_n(x)|(n-1)$. Osoitetaan, että $\mathrm{ord}_n(x) = n-1$. Tehdään vastaoletus, että $\mathrm{ord}_n(x) \neq n-1$. Silloin on edellisen mukaan $n-1 = k\ \mathrm{ord}_n(x)$, missä $k > 1$. Olkoon q jokin luvun k alkutekijä. Silloin

$$x^{(n-1)/q} = (x^{\mathrm{ord}_n(x)})^{(k/q)} \equiv 1 \pmod{n},$$

mikä on kuitenkin ristiriidassa oletuksen (49) kanssa. Näin $\mathrm{ord}_n(x) = n-1$. Tästä päätellään, että $\varphi(n) = n-1$, sillä yleisesti on $\mathrm{ord}_n(x) \leq \varphi(n) \leq n-1$, kun $n > 1$. Mutta ehdon $\varphi(n) = n-1$ täyttävä luku n on välttämättä alkuluku, mikä nähdään esimerkiksi seuraavasti. Jos n ei ole alkuluku, sillä on triviaalien tekijöiden 1 ja n lisäksi jokin muu positiivinen tekijä a. Siis välillä $1 \leq m \leq n$ olevista luvuista m ainakin kaksi (nim. a ja n) on sellaista, että ehto $(m, n) = 1$ Eulerin funktion määritelmässä ei täyty. Silloin $\varphi(n) \leq n-2$. □

Huomautus 2.46. Testin soveltaminen vaatii luvun $n-1$ alkutekijöiden tuntemista. Näiden etsiminen on yleisesti ottaen hankala tehtävä. Jos kuitenkin on tarkoituksena *tuottaa* alkulukuja esimerkiksi kryptografisiin tarkoituksiin, voidaan suorittaa kokeiluja sellaisen alkuluvun n löytämiseksi, jolle luvun $n-1$ alkutekijät ovat suhteellisen pieniä. Koska tällaiset luvut eivät ole mitenkään harvinaisia ja pienin primitiivinen juuri on myös yleensä melko pieni, on odotettavissa, että kokeilu ennen pitkää johtaa alkuluvun löytymiseen.

Oletetaan edelleen, että p on alkuluku. Valitaan jokin primitiivinen juuri r (mod p), joka on seuraavassa tarkastelussa kiinteä. Silloin r:n potenssit $r^0 = 1,\ r, \ldots, r^{p-2}$ muodostavat s.j.s:n (mod p) eli käyvät luvut 1, 2, ..., $p-1$ (mod p) jossakin järjestyksessä. Jokaista luvulla p jaotonta lukua kohti määräytyy siis tietty eksponentti, jolla on lukuteoriassa sama rooli kuin analyysissa luvun logaritmilla.

Määritelmä 2.47. Olkoon p alkuluku, r primitiivinen juuri (mod p) ja a luvulla p jaoton luku. Lukua i, joka täyttää ehdot

$$r^i \equiv a \pmod{p}, \qquad 0 \leq i \leq p-2, \tag{50}$$

sanotaan *luvun a indeksiksi* (mod p) *kantaluvun r* suhteen. Merkitään $i = \mathrm{ind}_r a$.

Lause 2.48. *Olkoon r primitiivinen juuri* $\pmod p$ *ja* $p \nmid a$, $p \nmid b$. *Silloin*

$$ind_r(ab) \equiv ind_r a + ind_r b \pmod{p-1}, \tag{51}$$

ja

$$ind_r a^n \equiv n \cdot ind_r a \pmod{p-1} \qquad (n = 1, 2, \dots). \tag{52}$$

Todistus. Indeksin määritelmän mukaan on

$$r^{\mathrm{ind}_r(ab)} \equiv ab \pmod p$$

ja samoin

$$r^{\mathrm{ind}_r a} \equiv a \pmod p,$$
$$r^{\mathrm{ind}_r b} \equiv b \pmod p.$$

Kertomalla jälkimmäiset kongruenssit keskenään ja vertaamalla tulosta ensimmäiseen nähdään, että

$$r^{\mathrm{ind}_r(ab)} \equiv r^{\mathrm{ind}_r a + \mathrm{ind}_r b} \pmod p.$$

Tästä seuraa väite (51) lauseen 2.36 (2) nojalla.

Induktiolla voidaan (51) yleistää tapaukseen, jossa tulon tekijöitä on useampia kuin kaksi. Silloin (52) on tämän yleisemmän kaavan erikoistapaus. □

3 Neliönjäännökset

3.1 Neliönjäännökset ja Legendren symboli

Potenssinjäännöksiin $\pmod n$ päädytään kysymällä, mistä alkuluokkaryhmän $\mathbb{Z}_n^*$ alkioista voidaan ottaa m:s juuri. Annetun luokan $\overline{a} \in \mathbb{Z}_n^*$ mahdollinen m:s juuri on luokka $\overline{x} \in \mathbb{Z}_n^*$, jolle $\overline{x}^m = \overline{a}$. Kongruenssimuodossa tämä ehto kuuluu $x^m \equiv a \pmod n$. Sanotaan, että a on *m:nnen potenssin jäännös* $\pmod n$, jos $(a, n) = 1$ ja tämä kongruenssi on ratkeava. Seuraavassa rajoitutaan tapaukseen $m = 2$.

Määritelmä 3.1. Olkoon $n \geq 1$ ja $(a, n) = 1$. Sanotaan, että a on *neliönjäännös* (nj) *modulo n* jos kongruenssi

$$x^2 \equiv a \pmod n \tag{53}$$

on ratkeava; muuten a on *neliönepäjäännös* (nej) *modulo n*.

Esimerkki 3.2. Kun $n = 9$ ja $(x, 9) = 1$, niin x on kongruentti jonkin luvuista ± 1, ± 2, ± 4 kanssa (mod 9). Tällöin $x^2 \equiv 1$, 4 tai 7 (mod 9). Täten luvut 1, 4 ja 7 ovat nj:iä (mod 9) ja 2, 5 ja 8 ovat nej:iä (mod 9).

Seuraavassa rajoitutaan tapaukseen $n = p =$ pariton alkuluku. Koska $\mathbb{Z}_p^*$ on syklinen ryhmä, jonka generaattoriksi käy mikä tahansa primitiivinen juuri (mod p), on tässä tapauksessa helppo karakterisoida neliönjäännökset ja -epäjäännökset.

Lause 3.3. *Olkoon $p > 2$ alkuluku ja r jokin primitiivinen juuri (mod p). Luku a, jolle $p \nmid a$, on*

$$nj \pmod p \iff ind_r a \text{ on parillinen,}$$

$$nej \pmod p \iff ind_r a \text{ on pariton.}$$

Neliönjäännöksiä ja -epäjäännöksiä on siis kumpiakin $(p-1)/2$ jäännösluokallista.

Todistus. Riittää todistaa nj:iä koskeva väite. Jos a on nj (mod p), niin kongruenssi

$$x^2 \equiv a \pmod p \tag{54}$$

on ratkeava. Tällöin $\mathrm{ind}_r a \equiv 2\mathrm{ind}_r x \pmod{p-1}$. Koska $p-1$ on parillinen, tämä kongruenssi pätee (mod 2), mikä osoittaa, että $\mathrm{ind}_r a$ on parillinen. Jos toisaalta oletetaan, että $\mathrm{ind}_r a$ on parillinen, sanotaan $\mathrm{ind}_r a = 2\nu$, niin $x = r^\nu$ on kongruenssin (54) ratkaisu ja a on siis nj. □

Huomautus 3.4. Neliönjäännösten (mod p) edustajistoksi voidaan valita myös $1^2, 2^2, \ldots, ((p-1)/2)^2$, sillä nämä luvut ovat nj:iä, epäkongruentteja (mod p) ja niitä on $(p-1)/2$ kpl. Yleisesti neliönjäännösten (mod n) (missä $n \geq 2$) edustajat löytyvät lukujen m^2 joukosta, missä $1 \leq m \leq n/2$ ja $(m,n) = 1$. Tämä joukko ei kuitenkaan ole yleensä neliönjäännösten *edustajisto*, sillä sama luokka voi esiintyä useammin kuin kerran. Esimerkiksi tapauksessa $n = 15$ luvut $1^2, 2^2, 4^2, 7^2$ edustavat luokkia 1 ja 4 (mod 15), joten nämä muodostavat neliönjäännösten (mod 15) edustajiston. Neliönepäjäännöksiä on tässä tapauksessa *enemmän*, nimittäin 6 kpl.

Määritelmä 3.5. Olkoon $p > 2$ alkuluku ja a mielivaltainen kokonaisluku. *Legendren symboli* $(\frac{a}{p})$ määritellään seuraavasti: $(\frac{a}{p}) = 1$, jos a on nj (mod p), $(\frac{a}{p}) = -1$, jos a on nej (mod p) ja $(\frac{a}{p}) = 0$ jos $p|a$.

Huomautus 3.6. Legendren symbolin määritelmästä seuraa välittömästi, että $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ jos $a \equiv b \pmod p$. Toinen perusominaisuus on *täydellinen multiplikatiivisuus* "osoittajan" suhteen, mikä todetaan seuraavassa lauseessa.

Lause 3.7. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Todistus. Väite on selvä jos $p|a$ tai $p|b$. Jos $p \nmid ab$, niin sovelletaan lausetta 3.3, jonka sisältö voidaan kiteyttää seuraavasti:

$$\left(\frac{a}{p}\right) = (-1)^{\mathrm{ind}_r a}.$$

Täten

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (-1)^{\mathrm{ind}_r a + \mathrm{ind}_r b}. \tag{55}$$

Mutta $\mathrm{ind}_r a + \mathrm{ind}_r b \equiv \mathrm{ind}_r(ab) \pmod{p-1}$ lauseen 2.48 mukaan. Koska $p-1$ on parillinen, tämä pätee myös (mod 2), mistä seuraa, että (55):n oikea puoli on $(-1)^{\mathrm{ind}_r(ab)} = (\frac{ab}{p})$. □

Seuraus 3.8.

$$\left(\frac{a_1 a_2 \cdots a_k}{p}\right) = \left(\frac{a_1}{p}\right) \cdots \left(\frac{a_k}{p}\right).$$

Todistus. Induktiolla lauseesta 3.7. □

Esimerkki 3.9. Jos $p = 11$, niin primitiiviseksi juureksi voidaan valita $r = 2$. Tällöin neliönjäännösten (mod 11) edustajisto on 1, 2^2, 2^4, 2^6, 2^8 eli 1, 4, 5, 9, 3. Samat luokat saadaan myös luvuista 1^2, 2^2, 3^2, 4^2, 5^2. Neliönepäjäännökset (mod 11) ovat 2, 6, 7, 8, 10. Nähdään esimerkiksi, että $\left(\frac{10}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{5}{11}\right) = (-1)(+1) = -1$. Siis $\left(\frac{-1}{11}\right) = -1$, mikä tulos selittyy lauseesta 3.11.

3.2 Eulerin kriteeri ja Gaussin lemma

Olkoon $p > 2$ alkuluku ja $p \nmid a$. Fermat'n pikku lauseen mukaan on

$$a^{p-1} - 1 = (a^{(p-1)/2)} - 1)(a^{(p-1)/2} + 1) \equiv 0 \pmod{p}.$$

Tästä seuraa, että joko

$$a^{(p-1)/2} \equiv 1 \pmod{p} \tag{56}$$

tai

$$a^{(p-1)/2} \equiv -1 \pmod{p}. \tag{57}$$

Kumpi tapaus toteutuu, selviää seuraavasta lauseesta.

Lause 3.10 (Eulerin kriteeri)**.** *Jos $p > 2$ on alkuluku, niin*

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}. \tag{58}$$

Todistus. Tapaus $p|a$ on selvä, joten voidaan olettaa, että $p \nmid a$. Jos a on nj (mod p), niin $x^2 \equiv a\ (p)$ jollakin x:llä, jolle $p \nmid x$. Tällöin (58) pätee, sillä

$$a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Kaikki neliönjäännökset ($(p-1)/2$ kpl) toteuttavat siis kongruenssin (56), jolla ei lauseen 2.30 mukaan voi olla enää muita juuria. Näin ollen s.j.s:n (mod p) muut luvut eli neliönepäjäännökset toteuttavat välttämättä kongruenssin (57). Täten (58) pätee tässäkin tapauksessa. □

Lause 3.11 (Resiprookkilain ensimmäinen täydennyslause)**.**

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1, & jos\ p = 4n+1, \\ -1, & jos\ p = 4n-1. \end{cases}$$

Todistus. Kun $a = -1$, saa (58) muodon $(-1)^{(p-1)/2} \equiv \left(\frac{-1}{p}\right) \pmod p$. Koska tämän kongruenssin kumpikin puoli on ± 1, on myös vastaava yhtälö voimassa. □

Lause 3.12 (Gaussin lemma)**.** *Olkoon $p > 2$ alkuluku, $a \in \mathbb{Z}$ ja $p \nmid a$. Olkoon lukujen*

$$a,\ 2a, \ldots,\ ((p-1)/2)a \tag{59}$$

itseisarvoltaan pienimmistä jäännöksistä (mod p) s negatiivista. Silloin $\left(\frac{a}{p}\right) = (-1)^s$.

Todistus. Kullekin luvuista (59) voidaan valita yksikäsitteisesti tietty jäännös (mod p), jonka itseisarvo on pienempi kuin $p/2$. Luvulla ka $(1 \le k \le (p-1)/2)$ on siis jäännös $\epsilon_k r_k$, missä $\epsilon_k = \pm 1$ ja $0 < r_k < p/2$, eli

$$ka \equiv \epsilon_k r_k \pmod p. \tag{60}$$

Luvut r_k ovat erisuuria, sillä jos esimerkiksi $r_h = r_k$, niin $\epsilon_h ha \equiv \epsilon_k ka \pmod p$, mistä seuraa, että $\epsilon_h h \equiv \epsilon_k k \pmod p$ ja edelleen $\epsilon_h h = \epsilon_k k$ ja siis $\epsilon_h = \epsilon_k$ ja $h = k$, sillä $0 < h, k < p/2$. Täten luvut r_k käyvät jossakin järjestyksessä luvut 1, 2, ..., $(p-1)/2$. Kertomalla kongruenssit (60) keskenään saadaan

$$((p-1)/2)!a^{(p-1)/2} \equiv ((p-1)/2)!(-1)^s \pmod p, \tag{61}$$

missä s merkitsee niiden lukujen k lukumäärää, joille $\epsilon_k = -1$. Supistamalla kertomat pois ja soveltamalla Eulerin kriteeriä saadaan lauseen väite. □

Esivalmisteluna seuraavassa pykälässä esitettävän resiprookkilain todistusta varten lausutaan Gaussin lemman sisältö analyyttisemmassa muodossa.

Lause 3.13. *Olkoon $p > 2$ alkuluku, $P = (p-1)/2$, $a \in \mathbb{Z}$, $(a, p) = 1$ ja*

$$T = \sum_{x=1}^{P} \left\lfloor \frac{2ax}{p} \right\rfloor.$$

Silloin

$$\left(\frac{a}{p}\right) = (-1)^T. \tag{62}$$

Todistus. Kongruenssi (60) merkitsee sitä, että

$$ka = np + \epsilon_k r_k,$$

missä n on kokonaisluku. Täten $2ka = 2np + 2\epsilon_k r_k$, missä $0 < 2r_k < p$. Näin ollen

$$\lfloor \frac{2ka}{p} \rfloor = \begin{cases} 2n & \text{jos } \epsilon_k = 1, \\ 2n-1 & \text{jos } \epsilon_k = -1, \end{cases}$$

ja edelleen

$$\epsilon_k = (-1)^{\lfloor 2ka/p \rfloor}.$$

Annetaan luvun k käydä läpi arvot 1, 2, ..., P ja kerrotaan saadut P yhtälöä puolittain, jolloin saadaan

$$\epsilon_1 \cdots \epsilon_P = (-1)^T.$$

Tästä seuraa väite (62), sillä vasen puoli on Gaussin lemman mukaan yhtä kuin $\left(\frac{a}{p}\right)$. □

Esimerkki 3.14. Lasketaan $\left(\frac{3}{29}\right)$. Lukujen 3, 6, ..., $14 \cdot 3$ itseisesti pienimmät jäännökset (mod 29) ovat 3, 6, 9, 12, -14, -11, -8, -5, -2, 1, 4, 7, 10 ja 13. Näistä on 5 kpl negatiivisia. Siis $\left(\frac{3}{29}\right) = -1$. Sama tulos saadaan Eulerin kriteeristä: $3^{14} \equiv -1 \pmod{29}$ (totea !).

3.3 Neliönjäännösten resiprookkilaki

Kuuluisa resiprookkilaki sitoo toisiinsa symbolit $\left(\frac{p}{q}\right)$ ja $\left(\frac{q}{p}\right)$, missä p ja q ovat parittomia alkulukuja. Gauss todisti tämän v. 1796 (19-vuotiaana) ja löysi myöhemmin seitsemän muuta todistusta. Nykyään erilaisia todistuksia tunnettaneen satakunta.

Esitämme resiprookkilaille todistuksen, joka tuottaa sivutuloksena kaavan symbolille $\left(\frac{2}{p}\right)$. Todistusta varten tarvitaan seuraava aputulos.

Lause 3.15. *Olkoon $p > 2$ alkuluku, $a \in \mathbb{Z}$ ja $(a, 2p) = 1$. Merkitään $P = (p-1)/2$ ja*

$$S = \sum_{x=1}^{P} \lfloor \frac{ax}{p} \rfloor.$$

Silloin

$$\left(\frac{2a}{p}\right) = (-1)^{S+(p^2-1)/8}. \tag{63}$$

Todistus. Koska a on pariton, voidaan tutkittava symboli muokata seuraavasti :

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4((a+p)/2)}{p}\right) = \left(\frac{(a+p)/2}{p}\right).$$

Siksi lauseen 3.13 mukaan on $\left(\frac{2a}{p}\right) = (-1)^T$, missä

$$T = \sum_{x=1}^{P} \lfloor \frac{(a+p)x}{p} \rfloor = \sum_{x=1}^{P} \lfloor \frac{ax}{p} \rfloor + \sum_{x=1}^{P} x = S + (p^2-1)/8.$$

Viime vaiheessa käytettiin yhtälöä $1 + 2 + \cdots + N = N(N+1)/2$. □

Lause 3.16 (Resiprookkilain toinen täydennyslause)**.**

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & jos\ p = 8n \pm 1 \\ -1, & jos\ p = 8n \pm 3. \end{cases}$$

Todistus. Valitaan (63):ssä $a = 1$, jolloin $S = 0$. □

Huomautus 3.17. Lauseista 3.15 ja 3.16 seuraa, että $(\frac{a}{p}) = (-1)^S$, jos $(a, 2p) = 1$. Tätä tulosta tarvitaan kohta resiprookkilain todistuksessa.

Lause 3.18 (Neliönjäännösten resiprookkilaki)**.** *Olkoot p ja q erisuuria parittomia alkulukuja. Silloin*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{((p-1)/2)((q-1)/2)}. \tag{64}$$

Todistus. Merkitään $P = (p-1)/2$, $Q = (q-1)/2$. Tarkastellaan lukupareja (x, y), joissa

$$x = 1, 2, \ldots, P, \quad y = 1, 2, \ldots, Q.$$

Näitä pareja on PQ kpl. Luvut qx ja py ovat selvästi erisuuria, joten mikään pari (x, y) ei ole origon kautta kulkevalla suoralla L, jonka kulmakerroin on q/p. Pareista (x, y) suoran L yläpuolella ovat ne, joille

$$qx < py$$

ja alapuolella ne, joille

$$py < qx$$

Kun y on annettu, edellinen epäyhtälö toteutuu $\lfloor py/q \rfloor$ arvolla x. (Koska $y \leq q/2$, niin $py/q \leq p/2$ ja siis $\lfloor py/q \rfloor \leq P$.) Näin suoran L yläpuolella olevien parien (x, y) lukumäärä on

$$S_1 = \sum_{y=1}^{Q} \lfloor \frac{py}{q} \rfloor$$

ja vastaavasti suoran L alapuolella olevien parien (x, y) lukumäärä on

$$S_2 = \sum_{x=1}^{P} \lfloor \frac{qx}{p} \rfloor.$$

Mutta edellä tehdyn huomautuksen mukaan on

$$\left(\frac{p}{q}\right) = (-1)^{S_1}, \quad \left(\frac{q}{p}\right) = (-1)^{S_2},$$

joten

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S_1+S_2}.$$

Tässä $S_1 + S_2$ kaikkien parien (x, y) lukumäärä eli PQ. Näin on (64) todistettu. □

Esimerkki 3.19. Onko kongruenssi $x^2 \equiv 363 \pmod{271}$ ratkeava? Tätä varten lasketaan symboli $\left(\frac{363}{271}\right)$ ottaen huomioon, että 271 on alkuluku. Aluksi saadaan

$$\left(\frac{363}{271}\right) = \left(\frac{92}{271}\right) = \left(\frac{2^2 \cdot 23}{271}\right) = \left(\frac{23}{271}\right).$$

Sovelletaan nyt resiprookkilakia ja sen toista täydennyslausetta:

$$\left(\frac{23}{271}\right) = (-1)^{11 \cdot 135}\left(\frac{271}{23}\right) = -\left(\frac{18}{23}\right) = -\left(\frac{2 \cdot 3^2}{23}\right) = -\left(\frac{2}{23}\right) = -1.$$

Kongruenssi ei siis ole ratkeava.

Esimerkki 3.20. Resiprookkilain avulla voidaan selvittää, mille alkuluvuille annettu luku on neliönjäännös. Milloin esimerkiksi on $\left(\frac{5}{p}\right) = 1$? Resiprookkilain mukaan

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right),$$

kun $p \neq 5$, joten

$$\left(\frac{5}{p}\right) = 1 \Longleftrightarrow \left(\frac{p}{5}\right) = 1 \Longleftrightarrow p \equiv 1, 4 \pmod{5}.$$

Siis p on muotoa $5k + 1$ tai $5k + 4$. Koska p on pariton, pitää luvun k olla edellisessä tapauksessa parillinen ja jälkimmäisessä pariton. Lopullinen tulos on, että p on muotoa $10n + 1$ tai $10n + 9$. Tällaisia alkulukuja ovat $11, 19, 29, 31, \ldots$

3.4 Toisen asteen kongruenssit

Tarkastellaan kongruenssia

$$ax^2 + bx + c \equiv 0 \pmod{p}, \qquad (p \nmid a) \tag{65}$$

missä p on pariton alkuluku. Kertomalla tämä puolittain luvulla $4a$ saadaan kongruenssi

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p},$$

joka on ekvivalentti kongruenssin (65) kanssa, sillä $(4a, p) = 1$. Neliöksi täydentämällä saadaan edelleen

$$(2ax + b)^2 \equiv D \pmod{p}, \tag{66}$$

missä

$$D = b^2 - 4ac.$$

Lukuun D nähden erotetaan nyt kolme tapausta sen mukaan, onko D nj, nej vai $\equiv 0 \pmod{p}$.

1) Jos D on nj $\pmod p$, niin kongruenssi

$$y^2 \equiv D \pmod p \tag{67}$$

on ratkeava. Jos y_0 on sen jokin ratkaisu, niin myös $-y_0$ on ratkaisu, ja luvut $\pm y_0$ ovat epäkongruentteja $\pmod p$, sillä $p \neq 2$. Kongruenssit

$$2ax + b \equiv \pm y_0 \pmod p \tag{68}$$

ovat ratkeavia, koska $(p, 2a) = 1$. Oletetaan, että $2ax_1 + b \equiv y_0 \pmod p$ ja $2ax_2 + b \equiv -y_0 \pmod p$. Silloin x_1 ja x_2 ovat epäkongruentteja $\pmod p$, sillä y_0 ja $-y_0$ olivat epäkongruentteja. Nyt x_1 ja x_2 toteuttavat kongruenssin (66) ja siis myös kongruenssin (65). Kongruenssilla (65) on siis kaksi epäkongruenttia juurta $\pmod p$, eikä sillä lauseen 2.30 nojalla voi olla enempää.

2) Jos D on nej $\pmod p$, niin (67) on ratkeamaton ja alkuperäinen kongruenssi (65) on myös ratkeamaton.

3) Jos $D \equiv 0 \pmod p$, niin (66) on ekvivalentti kongruenssin

$$2ax + b \equiv 0 \pmod p$$

kanssa, joten tässä tapauksessa kongruenssilla on tarkalleen yksi epäkongruentti juuri.

Esimerkki 3.21. 1) Ratkaistaan kongruenssi $5x^2+x-8 \equiv 0 \pmod 7$. Kongruenssin vasen puoli voidaan korvata polynomilla $-2x^2 + x - 1$. Tällöin $D = 1 - 8 = -7 \equiv 0\ (7)$, joten kongruenssilla on tarkalleen yksi ratkaisu. Se toteuttaa kongruenssin $-4x+1 \equiv 0\ (7)$, jonka ratkaisu on $x \equiv 2\ (7)$.

2) $x^2+x+1 \equiv 0 \pmod 5$. Nyt $D = -3 \equiv 2\ (5)$. Koska 5 on muotoa $8n-3$, on $\left(\frac{2}{5}\right) = -1$ lauseen (3.16) nojalla. Siis kongruenssi on ratkeamaton.

3) $3x^2+2x+5 \equiv 0 \pmod{71}$. Nyt $D = -56 \equiv 15 \pmod{71}$. Lasketaan $\left(\frac{15}{71}\right) = \left(\frac{3}{71}\right)\left(\frac{5}{71}\right)$. Resiprookkilain ja sen ensimmäisen täydennyslauseen mukaan on

$$\left(\frac{3}{71}\right) = -\left(\frac{71}{3}\right) = -\left(\frac{-1}{3}\right) = 1,$$

ja samoin

$$\left(\frac{5}{71}\right) = \left(\frac{71}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Siis D on nj (mod 71) ja kongruenssilla on kaksi ratkaisua. Kongruenssin $y^2 \equiv 15\ (71)$ ratkaisut ovat $y = \pm 21$. On vielä ratkaistava kongruenssit $6x + 2 \equiv \pm 21\ (71)$ eli

$$\begin{aligned} 6x &\equiv 19 \pmod{71}, \\ 6x &\equiv -23 \pmod{71}. \end{aligned}$$

Koska $12 \cdot 6 \equiv 1\ (71)$, näiden ratkaisut ovat $x_1 \equiv 19 \cdot 12 = 228 \equiv 15\ (71)$ ja $x_2 \equiv -23 \cdot 12 = -276 \equiv 8\ (71)$.

4 Diofantoksen yhtälöistä

4.1 Lineaarisista Diofantoksen yhtälöistä

Tarkastellaan lineaarisen Diofantoksen yhtälön

$$ax + by + c = 0 \qquad (a,\ b \neq 0) \tag{69}$$

ratkeavuutta ja ratkaisuja. Merkitään $d = (a, b)$. Jaollisuussyistä on selvää, että jos $d \nmid c$, niin yhtälöllä (69) ei voi olla yhtään ratkaisua. Toisaalta, jos $d|c$, niin jakamalla yhtälö alun perin luvulla d voidaan rajoituksetta olettaa, että $d = 1$, kuten seuraavassa lauseessa tehdään.

Lause 4.1. *Diofantoksen yhtälö* (69) *on ratkeava silloin ja vain silloin kun* $(a, b)|c$. *Jos* $(a, b) = 1$ *ja* (x_0, y_0) *on jokin yhtälön* (69) *ratkaisu, niin sen kaikki ratkaisut ovat*

$$\begin{cases} x = x_0 + kb \\ y = y_0 - ka \end{cases} \qquad (k \in \mathbb{Z}). \tag{70}$$

Todistus. Edellisen mukaan riittää osoittaa, että jos $(a, b) = 1$, niin yhtälö on ratkeava ja että (70) antaa sen kaikki ratkaisut.

Koska $(a, b) = 1$, niin lauseen 1.9 nojalla on olemassa sellaiset kokonaisluvut u ja v, että $au + bv = 1$. Kertomalla puolittain luvulla $-c$ saadaan yhtälö

$$a(-cu) + b(-cv) + c = 0,$$

mistä nähdään, että $(x_0, y_0) = (-cu, -cv)$ on yhtälön (69) ratkaisu.

Jos myös (x, y) on ratkaisu, niin vähentämällä puolittain yhtälöt $ax_0 + by_0 + c = 0$ ja $ax + by + c = 0$ saadaan yhtälö

$$a(x - x_0) + b(y - y_0) = 0. \tag{71}$$

Erityisesti siis $b|a(x - x_0)$. Koska $(a, b) = 1$, niin lauseen 1.16 nojalla $b|x - x_0$ eli $x = x_0 + kb$ jollakin $k \in \mathbb{Z}$ ja silloin yhtälön (71) nojalla $y = y_0 - ka$. Selvästi kaikki löydetyt parit (70) ovat ratkaisuja. □

Esimerkki 4.2. Yhtälöllä $16x - 28y + 5 = 0$ ei ole ratkaisua, sillä (16,28) $= 4$ ja $4 \nmid 5$.

Esimerkki 4.3. Etsitään Diofantoksen yhtälön $16x - 28y + 4 = 0$ ratkaisut. Jakamalla luvulla $(16, 28) = 4$ saadaan yhtälö $4x - 7y + 1 = 0$. Soveltamalla Eukleideen algoritmia saadaan yhtälöt

$$7 = 1 \cdot 4 + 3, \qquad 4 = 1 \cdot 3 + 1 \qquad 3 = 3 \cdot 1$$

ja

$$1 = 4 - 1 \cdot 3 = 4 - 1(7 - 1 \cdot 4) = 2 \cdot 4 - 1 \cdot 7,$$

eli $2 \cdot 4 - 1 \cdot 7 - 1 = 0$. Kertomalla luvulla -1 saadaan $4 \cdot (-2) - 7 \cdot (-1) = -1$. Näin $(x_0, y_0) = (-2, -1)$ on ko. Diofantoksen yhtälön yksi ratkaisu. Edellisen lauseen nojalla sen kaikki ratkaisut ovat parit $(-2 - 7k, -1 - 4k)$, $k \in \mathbb{Z}$.

Huomautus 4.4. Rajoituksetta voidaan olettaa, että Diofantoksen yhtälössä (69) on voimassa $b > 0$. Jos on olemassa pari $(x, *)$, joka toteuttaa em. yhtälön niin x toteuttaa kongruenssin $ax \equiv -c \pmod{b}$, ja kääntäen. Koska em. yhtälöstä y heti määräytyy yksikäsitteisesti, jos x tunnetaan, on ko. Diofantoksen yhtälön ratkaiseminen olennaisesti sama ongelma kuin em. kongruenssin ratkaiseminen.

4.2 Pythagoraan luvuista

Tutkitaan Diofantoksen yhtälön

$$x^2 + y^2 = z^2 \tag{72}$$

positiivisia kokonaislukuratkaisuja eli *Pythagoraan lukuja* (tai *Pythagoraan kolmikoita*) (x, y, z). Nimitys juontuu siitä että tällaiset luvut ovat kosinilauseen mukaan erään suorakulmaisen kolmion sivujen pituudet.

Tutkittaessa yhtälöä (72) voidaan rajoittua *primitiivisiin* ratkaisuihin, joissa $(x, y, z) = 1$, sillä mikä tahansa ratkaisu (x', y', z') on jonkin primitiivisen ratkaisun (x, y, z) monikerta eli $(x', y', z') = (kx, ky, kz)$ jollakin $k \in \mathbb{N}$.

Primitiivisyysehdosta seuraa, että $(x, y) = (y, z) = (z, x) = 1$, sillä jos luvuista x, y ja z joillakin kahdella on jokin luonnollinen luku yhteisenä tekijänä, se jakaa myös kolmannen ja siis luvun $(x, y, z) = 1$.

Helposti nähdään, että luvuista x ja y on toinen parillinen ja toinen pariton, sillä ne eivät ensinnäkään voi olla molemmat parillisia (koska z olisi silloin myös parillinen vastoin primitiivisyyttä), ja toiseksi ne eivät voi olla myöskään molemmat parittomia, sillä silloin olisi $z^2 \equiv 2 \pmod{4}$, mikä on mahdotonta, sillä jokainen neliö on kongruentti nollan tai ykkösen kanssa (mod 4). Koska x ja y ovat täysin samassa asemassa, riittää etsiä vain sellaiset ratkaisut, missä $2|x$ ja $2 \nmid y$.

Lause 4.5. *Kolmikot*

$$(2ab, a^2 - b^2, a^2 + b^2), \quad \textit{missä } (a, b) = 1,\ a > b > 0,\ 2 \nmid (a - b), \tag{73}$$

käyvät läpi tarkalleen kaikki primitiiviset Pythagoraan kolmikot (x, y, z), *missä* $2|x$.

Todistus. Oletetaan, että (x, y, z) on primitiivinen Pythagoraan kolmikko ja $2|x$. Koska $2|x$, niin $2 \nmid y$ ja $2 \nmid z$. Näin ollen $(z + y)/2 \in \mathbb{N}$ ja $(z - y)/2 \in \mathbb{N}$ ja niiden s.y.t. on 1 (jos nimittäin p jakaisi ne molemmat, niin p jakaisi niiden summan z ja erotuksen y, vaikka $(y, z) = 1$) ja

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right).$$

Koska oikealla puolella tulon tekijät ovat suhteellisia alkulukuja ja niiden tulo on neliö, on molempien oltava neliöitä, ts. $(z + y)/2 = a^2$ ja $(z - y)/2 = b^2$ joillakin kokonaisluvuilla $a > 0$ ja $b > 0$, jotka toteuttavat ehdot $a > b$ ja $(a, b) = 1$. Koska

$$a - b \equiv a^2 - b^2 = y \equiv 1 \pmod{2},$$

niin (x, y, z) on muotoa (73).

Oletetaan kääntäen, että luvut a ja b toteuttavat ehdot $a > b > 0$, $(a, b) = 1$ ja $2 \nmid a - b$ (eli luvuilla a ja b on eri pariteetti). Silloin luvuille $x = 2ab$, $y = a^2 - b^2$ ja $z = a^2 + b^2$ pätevät ehdot $x > 0$, $y > 0$, $z > 0$, $2|x$ ja

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2.$$

Osoitetaan vielä, että $(x, y, z) = 1$. Jos $(y, z) = d$, niin

$$d|y = a^2 - b^2 \qquad d|z = a^2 + b^2,$$

joten $d|2a^2$ ja $d|2b^2$. Koska $(a, b) = 1$, niin $d = 1$ tai $d = 2$. Koska $2 \nmid y$, niin $d = 1$. □

Esimerkki 4.6. Etsitään kaikki primitiiviset Pythagoraan kolmikot (x, y, z), joissa $0 < z < 30$ ja $2|x$. Lauseen 4.5 mukaan nämä ovat muotoa

$$x = 2ab,\ y = a^2 - b^2,\ z = a^2 + b^2 < 30, \quad (a, b) = 1,\ a > b > 0,\ 2 \nmid a - b.$$

Kolmikot saadaan taulukosta

b	a	x	y	z
1	2	3	4	5
1	4	15	8	17
2	3	5	12	13
2	5	21	20	29
3	4	7	24	25 .

5 Lukuteorian sovellus: RSA-salakirjoitusjärjestelmä

Tässä pykälässä käsitellään modernia RSA-salakirjoitusjärjestelmää. Se on julkinen seuraavassa mielessä: henkilö X julkistaa (esim. sanomalehdessä), miten hänelle tulevat viestit tulee *kryptata*, ts. kirjoittaa salakirjoitettuun muotoon. Tällöin kuka tahansa voi suorittaa kryptauksen ja lähettää salaisia viestejä henkilölle X, mutta siitä huolimatta, että kryptausmenetelmä on tiedossa, nykytietämyksen valossa vain henkilö X pystyy kohtuullisessa ajassa *dekryptaamaan*, ts. purkamaan salakirjoituksen.

Henkilö X valitsee kaksi suurta (esim. 300-numeroista) alkulukua p ja q ja muodostaa tulon $n = pq$. Edelleen hän valitsee jonkin positiivisen kokonaisluvun $e \neq 1$, jonka suurin yhteinen tekijä luvun $(p - 1)(q - 1)$ kanssa on 1, ja etsii sellaiset kokonaisluvut $d > 0$ ja $d'' < 0$, joille

$$1 = de + d''(p - 1)(q - 1),$$

mikä on mahdollista lauseen 4.1 mukaan. Merkitään $d' = -d'' > 0$. Tällöin

$$1 = de - d'(p - 1)(q - 1).$$

Tämän jälkeen henkilö X julkistaa luvut n ja e, mutta pitää luvut p, q ja d omana tietonaan. Nyt kuka tahansa voi lähettää salaisen viestin henkilölle X seuraavalla tavalla. Ensiksi viesti koodataan jollakin ennalta sovitulla tavalla kokonaislukujonoksi

$$M_1, M_2, \ldots,$$

missä kullakin indeksin i arvolla $1 < M_i < n$. Viestin lähettäjä suorittaa nyt kryptauksen eli etsii ehdot

$$M_i^e \equiv m_i \pmod{n}, \qquad 0 \leq m_i < n$$

toteuttavan luvun m_i, ts. korottaa luvun M_i kryptauseksponentin e ilmoittamaan potenssiin ja laskee saadun luvun pienimmän ei-negatiivisen jäännöksen modulo n. Laskujen nopeuttamiseksi e voidaan kirjoittaa luvun 2 potenssien summana (siis 2-kantaisessa järjestelmässä) ja käyttää hyväksi kaavaa $M_i^{2^{i+1}} = (M_i^{2^i})^2$. Salakirjoitettu viesti, ns. *kryptoteksti*, on jono

$$m_1, m_2, \ldots.$$

Seuraava lause kertoo, miten henkilö X — joka ainoana tuntee luvun d — voi suorittaa *dekryptauksen* eli selvittää, mikä oli alkuperäinen selväkielinen viesti.

Lause 5.1. $m_i^d \equiv M_i \pmod{n}$.

Todistus. Jos p ei jaa lukua M_i, niin Fermat'n pienen lauseen nojalla

$$m_i^d \equiv M_i^{ed} = M_i^{1+d'(p-1)(q-1)} = (M_i^{p-1})^{d'(q-1)} M_i \equiv M_i \pmod{p}.$$

Jos $p \mid M_i$, niin myös tällöin

$$m_i^d \equiv M_i^{ed} \equiv M_i \pmod{p}.$$

Samoin tietysti $m_i^d \equiv M_i \pmod{q}$. Väite saadaan nyt seurauksesta 2.15. □

Kryptosysteemin ideana on, että vaikka *periaatteessa* kuka tahansa pystyy pelkästään luvun n perusteella laskemaan luvut p ja q, on tekijöihinjako parhaillakin tunnetuilla algoritmeilla niin työlästä, että kun X valitsee riittävän suuret luvut p ja q, niin se ei onnistu missään kohtuullisessa ajassa.

Kirjallisuutta

[1] R. Allenby, E. Redfern: *Introduction to Number Theory with Computing.* Edward Arnold, Lontoo, 1989.

[2] H. Davenport: *The Higher Arithmetic.* Hutchinson, Lontoo, 1952.

[3] G. H. Hardy, E. M. Wright: *Introduction to the theory of numbers.* Oxford University Press, Lontoo, 1938.

[4] L. K. Hua: *Introduction to Number Theory.* Springer, Berliini, 1982.

[5] W. LeVeque: *Topics in Number Theory I-II.* Addison-Wesley, Reading, 1956.

[6] R. A. Mollin, *Fundamental Number Theory with Applications.* CRC Press, Boca Raton, 1998.

[7] P. Ribenboim: *The Book of Prime Number Records.* Springer, New York, 1988.

[8] K. H. Rosen: *Elementary Number Theory and Its Applications.* Addison-Wesley, Reading, 1988.

[9] K. Väisälä: *Lukuteorian ja korkeamman algebran alkeet.* Otava, Helsinki, 1961.