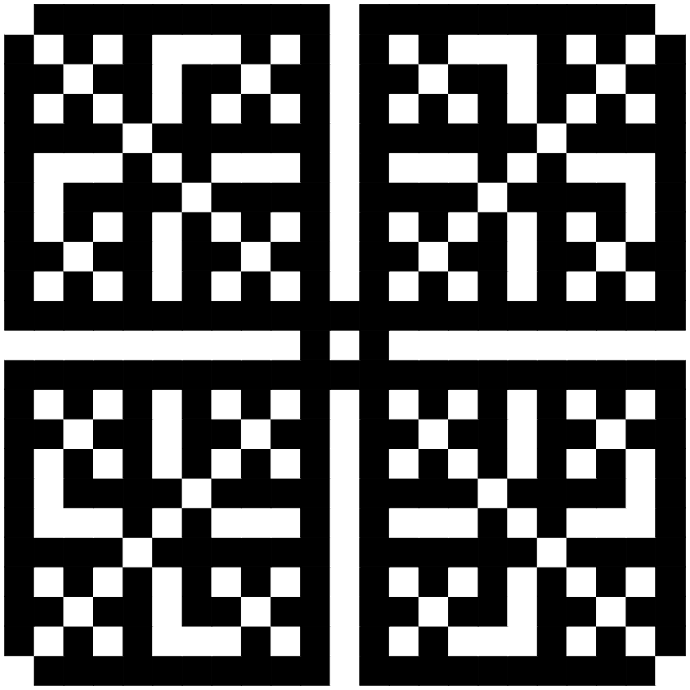
Lukuteoria



Jouni Parkkonen

Luentoja Jyväskylän yliopistossa

talvella 2023 ja keväällä 2024

Sisällys

Johdanto

Tämä teksti on kevään 2024 kurssin Lukuteoria 2 kurssimateriaali, joka sisältää taustamateriaalina talven 2023 kurssin Lukuteoria 1 kurssimateriaalin.

Kurssilla Lukuteoria 1 käsitellään kokonaislukujen jaollisuuteen liittyviä teemoja. Kurssille osallistuminen ei edellytä erityisiä esitietoja.

Luentojen pohjana varsinkin osassa 1 olen käyttänyt Heli Tuomisen luentoja muutaman vuoden takaa. Oheislukemistoksi sopivia lukuteorian kirjoja ovat esimerkiksi [Dud], [HW], [JJ], [LeV] ja monet muut kirjat, joilla on samankaltaisia nimiä.

Tekstissä mainitaan useita matemaatikkoja, jotka ovat panoksellaan edistäneet lukuteorian kehitystä. Olen maininnut jokaisesta ainakin karkeasti, millä aikakaudella he ovat vaikuttaneet. Lisätietoja mainituista henkilöitä ja heidän matematiikastaan voi etsiä matematiikan historiaa käsittelevistä kirjoista ja esimerkiksi arkistosta [Mac]. Kurssin sisältö ei seuraa lukuteorian kehitystä historiallisessa aikajärjestyksessä ja esimerkiksi Gaussin[1] lemma esitetään ennen Eukleideen[2] lemmaa, joka on tämän kurssin kannalta Gaussin lemman seuraus.

[1] Carl Friedrich Gauss (1777-1855).

[2] Eukleides Aleksandrialainen oli kreikkalainen matemaatikko Aleksandriassa, Egyptissä noin 300 eaa.

Merkintöjä ja sopimuksia

Tässä esitellään merkintöjä joilekin käsitteille, jotka saattavat olla tuttuja aiemmilta kursseilta. Jotkut merkinnöistä (esimerkiksi joukkojen erotus) tai valinnoista (onko 0 luonnollinen luku?) poikkeavat eri kursseilla.

- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ on kokonaislukujen joukko
- $\mathbb{N} = \{0, 1, 2, \dots\}$ on luonnollisten lukujen joukko.
- $\mathbb{N}^* = \{1, 2, \dots\}$ on positiivisten luonnollisten lukujen joukko.
- $\max A$ on joukon $A \subset \mathbb{Z}$ suurin alkio, jos sellainen on. Muuten $\max A = \infty$.
- $\#(A) \in \mathbb{N} \cup \{\infty\}$ joukon A alkioiden lukumäärä.
- $A - B = \{a \in A : a \notin B\}$ joukkojen A ja B erotus.
- $A \times B = \{(a, b) : a \in A,\ b \in B\}$ on joukkojen A ja B karteesinen tulo.
- $\log(x)$ on luvun x luonnollinen logaritmi.
- $n! = 1 \cdot 2 \cdot 3 \cdots (n-1)n$ on luvun n kertoma.
- $a \mid b$ tarkoittaa, että a on kokonaisluvun b tekijä, katso luku 1.2.
- $a \nmid b$ tarkoittaa, että a ei ole kokonaisluvun b tekijä, katso luku 1.2.
- $\text{syt}(a, b)$ on kokonaislukujen a ja b suurin yhteinen tekijä, katso luku 2.1.
- $\text{pyj}(a, b)$ on kokonaislukujen a ja b pienin yhteinen jaettava, katso luku 2.6
- $a \equiv b \pmod{m}$ tarkoittaa, että kokonaisluvut a ja b ovat kongruentteja modulo m, katso luku 5.1.
- $a \not\equiv b \pmod{m}$ tarkoittaa, että kokonaisluvut a ja b eivät ole kongruentteja modulo m.
- $\lfloor x \rfloor = \max\{k \in \mathbb{Z} : k \leqslant x\}$. Jos $x > 0$, niin $\lfloor x \rfloor$ on luvun x *kokonaisosa*.

Jos seurauslauseen muotoilun lopussa on todistuksen päättymismerkki $\square$, niin väite seuraa suoraan edellisestä lauseesta eikä sille esitetä täsmällistä perustelua tässä tekstissä.

Uusien käsitteiden *määritelmät* on laatikoitu näin. Niitä ei ole numeroitu.

Tällaisessa laatikossa on jokin huomautus tai sopimus, joka on tärkeä huomata.

Osa I

Luku 1

Jaollisuus

Tässä luvussa tutustumme lyhyesti luonnolisiin lukuihin ja kokonaislukuihin ja määrittelemme jaollisuuden käsitteen. Todistamme Jakoyhtälön,[1] joka on kurssilla tärkeä työkalu ja sovellamme sitä lukujärjestelmien tarkastelussa.

1.1 Kokonaisluvut ja luonnolliset luvut

Tällä kurssilla oletetaan tunnetuiksi *kokonaislukujen joukko*

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

ja sen osajoukko *luonnolliset luvut*[2]

$$\mathbb{N} = \{0, 1, 2, \dots\}.$$

Luonnollisten lukujen ja kokonaislukujen joukoilla on määritelty laskutoimitukset yhteenlasku $+$ ja kertolasku $\cdot$. Luvuilla 0 ja 1 on erityisiä ominaisuuksia: $0 + n = n$, $1 \cdot n = n$ ja $0 \cdot n = 0$ kaikille $n \in \mathbb{Z}$.

Laskutoimituksien lisäksi joukoissa $\mathbb{N}$ ja $\mathbb{Z}$ on *järjestys*, jolle pätee

- $a \leqslant a$,
- $a \leqslant b$ ja $b \leqslant a$, jos $a = b$ ja
- $a \leqslant c$, jos $a \leqslant b$ ja $b \leqslant c$.

Luonnollisten lukujen järjestykselle pätee $a \leqslant b$, jos ja vain jos $b = a + c$ jollain $c \in \mathbb{N}$ ja $a < b$, jos ja vain jos $b = a + c$ jollain $c \in \mathbb{N} - \{0\}$.

Luonnollisilla luvuilla on seuraava tärkeä ominaisuus:

[1] Lause 1.6.

[2] Monilla kursseilla ja monissa kirjoissa 0 ei ole luonnollinen luku. Tämä on syytä ottaa huomioon lähdekirjallisuutta luettaessa. Molemmat valinnat ovat toimivia.

INDUKTIOPERIAATE: Olkoon $Q \subset \mathbb{N}$ joukko, jolle $0 \in Q$ ja kaikille $k \in \mathbb{N}$ ehdosta $1, 2, \ldots, k \in Q$ seuraa, että $k+1 \in Q$,. Tällöin $Q = \mathbb{N}$.

Propositio 1.1. *Olkoon $A \subset \mathbb{N}$ joukko, jolle $0 \in A$ ja kaikille $k \in \mathbb{N}$ ehdosta $\{1, 2, \ldots, k\} \subset A$ seuraa, että $k+1 \in A$. Tällöin $A = \mathbb{N}$.*

Todistus. Väite seuraa induktioperiaatteesta tarkastelemalla joukkoa

$$B = \{n \in \mathbb{N} : \{0, 1, 2, \ldots, n\} \subset A\}.$$ □

Jos todistuksessa käytetään induktioperiaatetta tai Propositiota 1.1, on tapana sanoa, että *todistuksessa käytetään induktiota* tai *väite todistetaan induktiolla.*

Olkoon $A \subset \mathbb{Z}$. Alkio $a \in A$ on joukon A *pienin alkio*, jos $a \leqslant b$ kaikilla $b \in A$.

Propositio 1.2 (Hyvän järjestyksen periaate)**.** *Jos $C \subset \mathbb{N}$ on epätyhjä joukko, niin joukossa C on pienin alkio.*

Todistus. Olkoon $A \subset \mathbb{N}$ joukko, jolla ei ole pienintä alkiota. Olkoon $B = \mathbb{N} - A$. Osoitamme induktiolla, että $B = \mathbb{N}$, jolloin siis $A = \varnothing$.

Koska joukolla A ei ole pienintä alkiota, niin 0 ei ole sen pienin alkio. Mutta 0 on pienin kokonaisluku, joten $0 \in B$. Oletetaan, että $\{1, 2, \ldots, k\} \subset B$. Jos $k+1 \in A$, niin $k+1$ on joukon A pienin alkio, koska ainoat sitä pienemmät luonnolliset luvut ovat $1, 2, \ldots, k$. Siis $k+1 \in B = \mathbb{N} - A$. Proposition 1.1 nojalla $B = \mathbb{N}$, joten $A = \varnothing$. □

1.2 Kokonaislukujen jaollisuus

Olkoot $n, m \in \mathbb{Z}$. Luku n on *jaollinen* luvulla m jos

$$n = km \quad \text{jollain } k \in \mathbb{Z}.$$

Tällöin m on luvun n *tekijä* tai *jakaja* ja m *jakaa* luvun n.

Jos n on jaollinen luvulla m, niin merkitään $m \mid n$. Jos n ei ole jaollinen luvulla m, niin merkitään $m \nmid n$.

Jos $m \in \mathbb{Z}$ on jaollinen luvulla 2, niin m on *parillinen luku*. Muuten m on *pariton luku*.

Lause 1.3 (Jaollisuuslause)**.** *Olkoot $n, m, d, a, b \in \mathbb{Z}$. Tällöin*

(1) $n \mid n$ (REFLEKSIIVISYYS)

(2) jos $d \mid n$ ja $n \mid m$, niin $d \mid m$ (TRANSITIIVISUUS)

(3) jos $d \mid n$ ja $d \mid m$, niin $d \mid (an + bm)$ (LINEAARISUUS)

(4) jos $d \mid n$, niin $ad \mid an$ (TULO)

(5) jos $ad \mid an$ ja $a \neq 0$, niin $d \mid n$ (SUPISTAMINEN)

(6) $1 \mid n$

(7) $n \mid 0$

(8) jos $0 \mid n$*, niin* $n = 0$

(9) jos $d \mid n$ *ja* $n \neq 0$*, niin* $|d| \leqslant |n|$ *(VERTAILU)*

(10) jos $d \mid n$ *ja* $n \mid d$*, niin* $|d| = |n|$

Todistus. Todistetaan kohdat (5) ja (9), muut kohdat jätetään harjoitustehtäväksi.

(5): Olkoot $k \in \mathbb{Z}$ luku, jolle $an = kad$. Koska $a \neq 0$, niin on $n = kd$ ja siten $d \mid n$.

(9): Koska $d \mid n$, niin on $k \in \mathbb{Z}$, jolle $n = dk$. Koska $n \neq 0$, niin $k \neq 0$. Lisäksi koska $k \in \mathbb{Z}$, niin $|k| \geqslant 1$. Siten

$$|n| = |dk| = |d||k| \geqslant |d|\,. \qquad \square$$

Esimerkki 1.4. (1) Jos $u \mid 1$, niin Lauseen 1.3(9) nojalla $|1| \leqslant 1$, joten $u \in \{-1, 0, 1\}$. Kuitenkin $1 \neq 0$, joten $0 \nmid 1$. Toisaalta $1 = 1 \cdot 1 = (-1)(-1)$, joten luvun 1 tekijät ovat 1 ja -1.

(2) Luvun 6 tekijät ovat $\pm 1, \pm 2, \pm 3$ ja ± 6.

Esimerkki 1.5. Olkoon $k \in \mathbb{Z}$ jaollinen luvulla 3. Osoitetaan, että $3 \mid (k^2 + k + 9)$. Koska $3 \mid 9$, niin Lauseen 1.3 ((3)):n nojalla riittää näyttää, että $3 \mid (k^2 + k)$. Koska $3 \mid k$, niin on $l \in \mathbb{Z}$, jolle $k = 3l$. Nyt

$$k^2 + k = k(k + 1) = 3l(3l + 1) = 3m,$$

missä $m = 3l^2 + l \in \mathbb{Z}$. Siten $3 \mid (k^2 + k)$.

1.3 Jakoyhtälö

Lause 1.6 (Jakoyhtälö)**.** *Olkoot* $a, b \in \mathbb{Z}$ *ja olkoon* $b \neq 0$*. Tällöin on yksikäsitteiset* $q, r \in \mathbb{Z}$*, joille*

$$a = qb + r \quad \textit{ja} \quad 0 \leqslant r < |b|.$$

Jakoyhtälössä a on *jaettava*, b on *jakaja*, q on *(vaillinainen) osamäärä* ja r on *jakojäännös*.

Todistus. Osoitetaan ensin, että jakoyhtälö toteutuu joillain $q, r \in \mathbb{Z}$. Osoitetaan, että joukko

$$S = \{y \geqslant 0 : y = a - qb \text{ jollain } q \in \mathbb{Z}\} \subset \mathbb{N}$$

ei ole tyhjä. Tarkastelu jakautuu kolmeen tapaukseen.

- Jos $a \geqslant 0$, niin $a = a - 0 \cdot b \in S$.
- Jos $a \leqslant 0$ ja $b \geqslant 1$, niin $a - ab = a(1 - b) \geqslant 0$ ja siten $(a - ab) \in S$.
- Jos $a \leqslant 0$ ja $b \leqslant -1$,[3] niin $(1 + b) \leqslant 0$. Nyt $a + ab = a(1 + b) \geqslant 0$ ja siten $(a + ab) \in S$.

[3] Muista, että $b \neq 0$.

Hyvän järjestyksen periaatteen[4] nojalla joukossa S on pienin luku $r \in S$. Joukon S määritelmän mukaan $a = qb + r$ jollain $q \in \mathbb{Z}$.

Näytetään vielä, että $r < |b|$. Oletetaan ensin, että $b > 0$. Jos olisi $r \geqslant b$, niin luku

$$a - (q+1)b = a - qb - b = r - b \geqslant 0$$

kuuluisi joukkoon S. Toisaalta $r - b < r$, mikä on mahdotonta, sillä r on joukon S pienin luku. Siis $0 \leqslant r < b$.

Oletetaan sitten, että $b < 0$. Jos olisi $r \geqslant -b$, niin

$$a - (q-1)b = a - qb + b = r + b \geqslant 0$$

kuuluisi joukkoon S ja $r + b < r$. Siis $r < -b$.

Osoitetaan, että luvut q ja r ovat yksikäsitteisiä. Oletetaan, että joillain luvuilla $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, joille $0 \leqslant r_1, r_2 < |b|$ pätee

$$a = q_1 b + r_1 = q_2 b + r_2.$$

Tällöin $(q_1 - q_2)b = r_2 - r_1$, joten $b \mid (r_2 - r_1)$. Jos $q_1 \neq q_2$, niin $r_2 - r_1 \neq 0$. Lemman 1.3(9) nojalla $|r_2 - r_1| \geqslant |b|$. Tämä on mahdotonta, sillä $0 \leqslant r_1, r_2 \leqslant |b| - 1$. On siis $q_1 = q_2$ ja siten myös $r_1 = r_2$. □

Määritelmän mukaan jokainen kokonaisluku on joko parillinen tai pariton. Jakoyhtälön nojalla jokainen pariton luku on muotoa $2k + 1$ jollain kokonaisluvulla k. Vastaavasti jokaiselle $a \in \mathbb{Z}$ on yksikäsitteiset $q_3 \in \mathbb{Z}$ ja $r_3 \in \{0, 1, 2\}$, joille $a = 3q_3 + r_3$. Siis jokainen kokonaisluku on joko jaollinen luvulla 3 ja niin edelleen.

Esimerkki 1.7. Jaettaessa minkä tahansa kokonaisluvun n neliö luvulla 4 saadaan jakojäännökseksi 0 tai 1. Jakoyhtälön 1.6 nojalla $n = 4q + r$ jollain $r \in \{0, 1, 2, 3\}$. Siis

$$n^2 = (4q + r)^2 = 4^2 q^2 + 8qr + r^2 = 4(4q^2 + 2qr) + r^2 = 4N + r^2\,,$$

missä $N = 4q^2 + 2qr \in \mathbb{Z}$. Jos n on jaollinen luvulla 4, niin $r = 0$, joten $4 \mid n^2$. Tämä seuraa myös esimerkiksi Jaollisuuslauseen[5] kohdasta (2). Jos $r = 1$, niin $r^2 = 1$, joten $n^2 = 4N + 1$. Jos $r = 2$, niin $r^2 = 4$, joten $n^2 = 4(N + 1)$ ja erityisesti $4 \mid n^2$. Jos $r = 3$, niin $r^2 = 9 = 2 \cdot 4 + 1$, joten $n = 4(N + 2) + 1$.

1.4 Lukujärjestelmät

Tässä luvussa tarkastelemme tuttua tapaa kokonaislukujen nimeämiseksi ja sen yleistyksiä. Näiden *lukujärjestelmien* toimivuus perustuu seuraavaan tulokseen, joka seuraa jakoyhtälöstä.

Lause 1.8. *Olkoot $n, k \in \mathbb{N} - \{0\}$, $k > 1$. Tällöin on yksikäsitteiset luvut $s \in \mathbb{N}$ ja $a_0, a_1, \ldots a_s \in \mathbb{Z}$, joille $0 \leqslant a_i < k$ kaikilla $i = 0, 1, \ldots, s$, $a_s > 0$ ja*

$$n = a_s k^s + a_{s-1} k^{s-1} + \cdots + a_1 k + a_0\,.$$

[4] Propositio 1.2

[5] Lause 1.3

Todistus. Todistetaan esityksen olemassaolo induktiolla luvun n suhteen. Jos $n = 1$, niin voidaan valita $s = 0$ ja $a_0 = 1$.

Oletetaan, että esitys on olemassa luvuille $1, 2, \ldots, n-1$. Koska $k > 1$, niin Harjoitustehtävän 1.1 nojalla on yksikäsitteinen kokonaisluku $s \geqslant 0$, jolle

$$k^s \leqslant n < k^{s+1}.$$

Jakoyhtälön[6] perusteella on yksikäsitteiset $a_s, r \in \mathbb{Z}$, joille

$$n = a_s k^s + r,$$

missä $0 \leqslant r < k^s$. Lisäksi on $0 < a_s < k$, sillä muuten $n > k^{s+1}$.

Jos $r = 0$, niin $n = a_s k^s$ ja voimme lopettaa. Oletetaan, että $r > 0$. Koska $r \in \mathbb{N}$ ja $r < n$, niin induktio-oletuksen mukaan on kokonaisluvut $t \geqslant 0$ ja $b_0, \ldots, b_t$, joille

$$r = b_t k^t + \cdots b_1 k + b_0,$$

$0 \leqslant b_i < k$ kaikilla $0, 1, \ldots, t$ ja $b_t > 0$. Koska $r < k^s$, niin $t < s$. Siis

$$n = a_s k^s + 0 \cdot k^{s-1} + \cdots + 0 \cdot k^{t+1} + b_t k^t + \cdots b_1 k + b_0\,,$$

joten luvulla n on haluttu esitys. Induktioperiaatteen nojalla esityskaava on voimassa kaikilla $n \in \mathbb{N}$.

Osoitetaan sitten, että esitys on yksikäsitteinen. Olkoon $n \in \mathbb{N}$. Oletetaan, että on kokonaisluvut $s, t \geqslant 0$, $a_0, a_1, \ldots a_s$, $b_0, b_1, \ldots b_t$ joille $0 \leqslant a_i < k$, kaikilla $i = 0, 1, \ldots, s$, $0 \leqslant b_j < k$, kaikilla $j = 0, 1, \ldots, t$, $a_s > 0$, $b_t > 0$ ja

$$n = a_s k^s + \cdots + a_1 k + a_0 = b_t k^t + \cdots + b_1 k + b_0. \tag{1.1}$$

Vähentämällä luvun n esitykset yhtälössä (1.1) saadaan

$$0 = e_m k^m + \cdots + e_1 k + e_0, \tag{1.2}$$

missä $e_i = a_i - b_i$ ja m on suurin kokonaisluku, jolle $a_i \neq b_i$. Tällöin $e_m \neq 0$.

Jos olisi $m = 0$, niin olisi $0 \neq e_m = e_0 = 0$, mikä on ristiriita. On siis oltava $m > 0$. Koska $0 \leqslant a_i < k$ ja $0 \leqslant b_i < k$ kaikilla indekseillä i, niin

$$|e_i| = |a_i - b_i| \leqslant k - 1 \tag{1.3}$$

kaikilla $i = 0, 1, \ldots, m$. Nyt käyttämällä tietoa $e_m \in \mathbb{Z} - \{0\}$, kaavaa (1.2), kolmioepäyhtälöä, arviota (1.3) ja geometrisen summan kaavaa, saadaan

$$\begin{aligned} k^m &\leqslant |e_m k^m| = |e_{m-1} k^{m-1} + \cdots + e_1 k + e_0| \\ &\leqslant |e_{m-1}| k^{m-1} + \cdots + |e_1| k + |e_0| \\ &\leqslant (k-1)(k^{m-1} + \cdots + k + 1) = k^m - 1, \end{aligned}$$

mikä on ristiriita. On siis oltava $s = t$ ja $a_i = b_i$ kaikilla $i = 0, 1, \ldots, s$. Siten luvun n esitys halutulla tavalla on yksikäsitteinen. □

[6] Lause 1.6

Olkoon $b \in \mathbb{N}$, $b \geqslant 2$. Olkoon $n \in \mathbb{Z} - \{0\}$ ja olkoot $0 \leqslant a_0, a_1, \ldots, a_N < b$ luonnollisia lukuja, joille pätee $a_N \neq 0$ ja

$$n = \pm \sum_{j=0}^{N} a_j b^j \, .$$

Tällöin $\pm(a_N a_{N-1} \cdots a_0)_b$ on luvun n *esitys b-järjestelmässä.*
Luku b on b-järjestelmän *kantaluku.*

Luvun esityksessä b-järjestelmässä voidaan jättää sulut merkitsemättä. Esimerkiksi

$$(12341234)_5 = 12341234_5 \, .$$

Kymmenjärjestelmässä kantaluku jätetään yleensä merkitsemättä tälläkin kurssilla. Muutenkin, jos *yhteydestä on selvää*,[7] että laskut tehdään esimerkiksi 2-järjestelmässä, niin kantaluvun ilmoittava alaindeksi voidaan jättää merkitsemättä.

Esimerkki 1.9. Kymmenjärjestelmän luku 1907 tarkoittaa kantaluvun 10 potenssisummaa

$$1907 = 1 \cdot 10^3 + 9 \cdot 10^2 + 0 \cdot 10^1 + 7 \cdot 10^0.$$

Numeromerkit tarvitaan kantalukua 10 pienemmille luonnollisille luvuille.

Esimerkki 1.10. Kahdeksanjärjestelmässä käytetään luvun 8 peräkkäisiä potensseja: 8^0, 8^1, 8^2, ... Kahdeksan potenssien kertoimina voivat esiintyä luvut $0, 1, 2, 3, 4, 5, 6$ ja 7.

(1) Kymmenjärjestelmän luku 103 muunnetaan kahdeksanjärjestelmään (soveltamalla jakoyhtälöä kahteen kertaan ja) esittämällä se kahdeksan potenssien summana

$$103 = \begin{cases} 12 \cdot 8 + 7 = (1 \cdot 8 + 4)8 + 7 = \cdot 8^2 + \cdot 8^1 + 7 \cdot 8^0 = 147_8 \\ 1 \cdot 64 + 39 = 1 \cdot 64 + (4 \cdot 8 + 7) = 1 \cdot 8^2 + 4 \cdot 8^1 + 7 \cdot 8^0 = 147_8. \end{cases}$$

Luku 147_8 luetaan "*yksi-neljä-seitsemän*" eikä "sataneljäkymmentäseitsemän".

(2) Luku 2016_8 muunnetaan kymmenjärjestelmään seuraavasti

$$2007_8 = 2 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0 = 2 \cdot 512 + 1 \cdot 8 + 6 = 1038.$$

Esimerkki 1.11. Tietokoneissa käytetään luvun 2 potensseihin perustuvia lukujärjestelmiä, erityisesti 2- ja 16-järjestelmiä, joita kutsutaan *binaari-* ja *heksadesimaalijärjestelmiksi.* Heksadesimaalijärjestelmässä luvuille $10, 11, 12, 13, 14$ ja 15 käytetään symboleja $\mathtt{A}, \mathtt{B}, \mathtt{C}, \mathtt{D}, \mathtt{E}$ ja $\mathtt{F}$. Tässä tekstissä käytetään heksadesimaalilukujen kirjoittamiseen `mathtt`-fonttia, jota ei käytetä muuhun. Tällöin lukujärjestelmän kantalukua ilmaiseva alaindeksi $_{16}$ voidaan jättää kirjoittamatta, jos jokin näistä symboleista esiintyy luvun esityksessä.

(1) Luku 1234 muunnetaan 16-järjestelmään seuraavasti

$$1234 = 77 \cdot 16 + 2 = (4 \cdot 16 + 13) \cdot 16 + 2 = 4 \cdot 16^2 + 13 \cdot 16^1 + 2 \cdot 16^0 = \mathtt{4D2}_{16} = \mathtt{4D2}.$$

(2) Luku $\mathtt{10B}_{16} = \mathtt{10B}$ muunnetaan 10-järjestelmään seuraavasti

$$\mathtt{10B}_{16} = 1 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0 = 256 + 11 = 267.$$

[7] Suomeksi: *on erikseen kerrottu*

(3) Heksadesimaalijärjestelmän ja binaarijärjestelmän väliset muunnokset ovat helppoja: Luvut $\texttt{0}-\texttt{9}$ esitetään binaarilukuina kuten desimaaliluvut $0-9$ ja lisäksi $\texttt{A}=1010$, $\texttt{B}=1011$, $\texttt{C}=1100$, $\texttt{D}=1101$, $\texttt{E}=1110$ ja $\texttt{C}=1111$. Jos heksadesimaaliluvussa esiintyy jokin numeroista $\texttt{0}-\texttt{9}$ muualla kuin ensimmäisenä, sen esitys täytyy täydentää neljän merkin pituiseksi lisäämällä nollia. Heksadesimaaliluku $\texttt{0}$ tulee tällaisessa tilanteessa esittää binaarilukua muodostettaessa muodossa $\texttt{0000}$. Esimerkiksi $\texttt{10B}=100001011$.

Lukujärjestelmissä, joiden kantaluku on kymmenestä eroava, voidaan laskea *tavalliseen tapaan* muuntamatta lukuja 10-järjestelmään.

Esimerkki 1.12. (1) Laske 357_8+126_8. Huomaa, että $7_8+6_8=15_8$ ja $1_8+5_8+2_8=10_8$. Muistinumerot saadaan kyseisen sarakkeen täysien kahdeksaisten määrästä.

$$\begin{array}{r} 357_8 \\ +\,\underline{126_8} \\ 505_8 \end{array}$$

(2) Laske $111110_2+11001_2$.

$$\begin{array}{r} 111110_2 \\ +\;\underline{11001_2} \\ 1010111_2 \end{array}$$

Esimerkki 1.13. Laaditaan kaksi- ja neljäjärjestelmien kertotaulut.

$\cdot$	1	10_2
1	1	10_2
10_2	10_2	100_2

$\cdot$	1	2	3	10_4
1	1	2	3	10_4
2	2	10_4	12_4	20_4
3	3	12_4	21_4	30_4
10_4	10_4	20_4	30_4	100_4.

1.5 Jaollisuus kymmenjärjestelmässä

Lauseen 1.8 mukaan jokaiselle $n\in\mathbb{N}-\{0\}$ on yksikäsitteiset kokonaisluvut $s\geqslant 0$ ja $a_0,a_1,\ldots,a_s$, joille

$$n=a_s10^s+a_{s-1}10^{s-1}+\cdots+a_110+a_0=a_sa_{a-1}\ldots a_0, \tag{1.4}$$

$0\leqslant a_i\leqslant 9$ kaikilla $i=0,1,\ldots,s$ ja $a_s>0$. Tässä luvussa luvut $a_0,\ldots,a_s$ viittaavat esitykseen (1.4).

Jaollisuus luvuilla $2,5$ ja 10

Koska täysiä kymmeniä sisältävät luvut ovat aina jaollisia luvuilla 2, 5 ja 10, niin jaollisuuden voi päätellä kahdesta viimeisestä numerosta Lauseen 1.3 avulla.

Lause 1.14. *Olkoon $n\in\mathbb{N}$. Luku n on jaollinen*

(1) luvulla 2, jos ja vain jos a_0 on jaollinen luvulla 2 eli jos ja vain jos $a_0\in\{0,2,4,6,8\}$,

(2) luvulla 5 *jos ja vain jos* $a_0 = 0$ *tai* $a_0 = 5$,

(3) luvulla 10 *jos ja vain jos* $a_0 = 0$.

Todistus. Väitteet seuraavat helposti Lauseesta 1.3. □

Esimerkki 1.15. (1) Luku $78445 = 78440 + 5$ on jaollinen luvulla 5 mutta ei luvulla 2 eikä luvulla 10.
(2) Luku $100008 = 100000 + 8$ on jaollinen luvulla 2 mutta ei luvulla 5 eikä luvulla 10.

Lohkaisuperiaate

Samaan tapaan voidaan johtaa muitakin jaollisuussääntöjä. Tutkittaessa luvun $n \in \mathbb{N}$ jaollisuutta luvulla t, esitetään n summana, jonka ensimmäinen yhteenlaskettava on jaollinen luvulla t:

$$n = l + k, \quad \text{missä } l, k \in \mathbb{N} \text{ ja } t \mid l. \tag{1.5}$$

Luku l on *lohkaisutermi* ja luku k on *kriittinen termi*.

Jaollisuuslauseesta 1.3 seuraa, että n on jaollinen luvulla t jos ja vain jos $t \mid k$.

Lohkaisuperiaate (1.5) on käyttökelpoinen, jos jaollisuus voidaan selvittää sen avulla helpommin kuin jaettaessa lukua n luvulla t. Jos kriittinen termi on helposti määrättävissä ja se on pieni lukuun n verrattuna, niin lohkaisuperiaatetta kannattaa käyttää. Sopivan lohkaisutermin valinta ja olemassaolo riippuvat luvuista n ja t. Seuraavissa alakohdissa tarkastelemme jaollisuussääntöjä, jotka saadaan tällä tavalla.

Jaollisuus luvulla 4

Jos jakaja t on jokin kymmenen potenssien $10, 100, 1000, \ldots$ tekijä, niin lohkaisutermiksi valitaan luvun n vastaavia kymmenen potensseja sisältävä osa.

Lause 1.16. *Olkoon* $n \in \mathbb{N}$. *Luku* n *on jaollinen luvulla* 4 *jos ja vain jos luku* a_1a_0 *on jaollinen luvulla* 4.

Todistus. Koska $4 \mid 100$, niin lohkaisutermiksi valitaan luvun n täysiä satoja sisältävä osa $a_s a_{s-1} \ldots a_2 00$. □

Esimerkki 1.17. (1) Luvut 12344 ja 2112 ovat 4:llä jaollisia.
(2) Luvut 11013 ja 2007 eivät ole 4:llä jaollisia.

Jaollisuus luvuilla 25, 50 ja 75

Lukujen 100 ja 1000 tekijöille saadaan vastaavasti esimerkiksi jaollisuuslauseet:

Lause 1.18. *Olkoon* $n \in \mathbb{N}$. *Luku* n *on jaollinen luvulla* 50 *jos ja vain jos* $a_1 = 0$ *ja* $a_0 = 0$ *tai* $a_1a_0 = 50$. *Luku* n *on jaollinen luvulla* 25 *jos ja vain jos* $a_1 = 0$ *ja* $a_0 = 0$ *tai* $a_1a_0 \in \{25, 50, 75\}$. □

Esimerkki 1.19. Luvut 10550 ja 2300 ovat jaollisia sekä luvulla 50 että luvulla 25. Luku 1205 ei ole jaollinen luvulla 25 eikä luvulla 50.

Jaollisuus luvulla 8

Lause 1.20. *Olkoon $n \in \mathbb{N}$. Luku n on jaollinen luvulla 8 jos ja vain jos luku $a_2a_1a_0$ on jaollinen luvulla 8.*

Todistus. Harjoitustehtävä 1.16 □

Esimerkki 1.21. (1) Luvut 4032 ja 1160 ovat jaollisia luvulla 8, mutta $8 \nmid 2004$.

(2) Onko lukujen 14105 ja 25055 summa jaollinen luvulla 8? Lauseen 1.20 nojalla riittää tarkastella summan kolmea viimeistä numeroa eli lukua $105+55 = 160$. Koska $160 = 20 \cdot 8$, niin tutkittava summa on jaollinen luvulla 8.

Jaollisuus luvuilla 3 ja 9

Tarkasteltaessa jaollisuutta luvuilla 3 ja 9 sopiva lohkaisutermi saadaan lukujen $9 = 10-1$, $99 = 100-1$, $999 = 1000-1, \ldots$ avulla, sillä nämä luvut ovat jaollisia luvuilla 3 ja 9. Esimerkiksi luvussa

$$\begin{aligned} 2481 &= 2(999+1) + 4(99+1) + 8(9+1) + 1 \\ &= (2 \cdot 999 + 4 \cdot 99 + 8 \cdot 9) + (2 + 4 + 8 + 1) \end{aligned}$$

lohkaisutermi on luvuilla 3 ja 9 jaollisten lukujen summana jaollinen sekä luvulla 3 että luvulla 9, joten kriittinen termi 15 ratkaisee alkuperäisen luvun jaollisuuden. Koska $3 \mid 15$ ja $9 \nmid 15$, niin 2481 on jaollinen luvulla 3 mutta ei luvulla 9.

Huomaa, että yllä kriittinen termi on lohkaisutermin valinnan seurauksena *alkuperäisen luvun numeroiden summa.*

Jos

$$n = a_s a_{s-1} \ldots a_0 \,,$$

niin luku

$$a_s + a_{s-1} + \cdots + a_0 \tag{1.6}$$

on luvun n *numerosumma.*

Jos lohkaisutermiksi valitaan luvuilla 3 ja 9 jaollinen summa

$$a_s(10^s - 1) + \cdots + a_1 9,$$

niin numerosumma (1.6) on kriittinen termi.

Lause 1.22. *Olkoon $n \in \mathbb{N}$. Luku n on jaollinen luvulla 3 (9) jos ja vain jos numerosumma* (1.6) *on jaollinen luvulla 3 (9).* □

Esimerkki 1.23. (1) Luvun 4005 numerosumma on $4 + 5 = 9$, joten 4005 on jaollinen luvuilla 3 ja 9.

(2) Luvun 12345 numerosumma $1 + 2 + 3 + 4 + 5 = 15$ on jaollinen luvulla 3, mutta ei luvulla 9. Siten $3 \mid 12345$ ja $9 \nmid 12345$.

Jaollisuus luvulla 11

Lohkaisutermin määrittämistä varten haetaan luvulla 11 jaollisia lukuja, jotka ovat mahdollisimman lähellä kymmenen potensseja $10, 100, 1000, \ldots$

Luvut $11 = 10+1$, $99 = 100-1$ ja $1001 = 1000-1$ ovat jaollisia luvulla 11 ja yleisesti luvut

$$\begin{aligned} &10^m + 1, \text{ kun } m \text{ on pariton} \\ &10^m - 1, \text{ kun } m \text{ on parillinen} \end{aligned} \tag{1.7}$$

ovat jaollisia luvulla 11. Jaollisuuden tarkastelussa käytetään seuraavaa hyödyllistä aputulosta:

Lemma 1.24. *Olkoot $a, b \in \mathbb{Z}$ ja olkoon $m \in \mathbb{N} - \{0, 1\}$.*

$$a^m - b^m = (a-b)(a^{m-1} + a^{m-2}b + \cdots + ab^{m-2} + b^{m-1})\,. \tag{1.8}$$

Todistus. Harjoitustehtävä 1.2. □

Luku $a-b$ on siis luvun $a^m - b^m$ tekijä. Valitsemalla Lemmassa 1.24 $a = 10$ ja $b = -1$, nähdään, että luku

$$10^m - (-1)^m$$

on jaollinen luvulla 11. Koska $(-1)^m = -1$ parittomilla m ja $(-1)^m = 1$ parillisilla m, niin (1.7) on totta.

Korvataan luvun n summaesityksessä (1.4) 10^m summalla

$$(10^m - (-1)^m) + (-1)^m$$

kaikilla $m = 1, \ldots s$. Lohkaisutermiksi valitaan varmasti luvulla 11 jaollinen osa

$$a_s(10^s - (-1)^s) + \cdots + a_2 99 + a_1 11.$$

Kriittiseksi termiksi jää tällöin

$$a_0 - a_1 + a_2 - \cdots + (-1)^s a_s, \tag{1.9}$$

eli alkuperäisen luvun numerot laskettuna yhteen vaihtuvin etumerkein.

Summa (1.9) on luvun *n vuorotteleva numerosumma.*

Esimerkki 1.25. Onko luku 6479 jaollinen luvulla 11? Nyt

$$\begin{aligned} 6479 &= 6 \cdot (1001 - 1) + 4 \cdot (99 + 1) + 7 \cdot (11 - 1) + 9 \\ &= (6 \cdot 1001 + 4 \cdot 99 + 7 \cdot 11) + (-6 + 4 - 7 + 9) \end{aligned}$$

ja koska vuorotteleva numerosumma (kriittinen termi) $-6 + 4 - 7 + 9 = 0$ on jaollinen luvulla 11, niin $11 \mid 6479$.

Lause 1.26. *Olkoon $n \in \mathbb{N}$. Luku $n \in \mathbb{N}$ on jaollinen luvulla* 11 *jos ja vain jos luku* 11 *jakaa luvun n vuorottelevan numerosumman.* □

Esimerkki 1.27. (1) $11 \nmid 641045$ sillä vuorotteleva numerosumma $5-4+0-1+4-6 = -2$ ei ole jaollinen luvulla 11.

(2) $11 \mid 2020909$ sillä vuorotteleva numerosumma $9-0+9-0+2-0+2 = 22$ on jaollinen luvulla 11. Tämän näkee suoraan mutta halutessaan voi käyttää sitäkin, että luvun 22 vuorotteleva numerosumma on 0.

Jaollisuus luvulla 7

Jaollisuussäännöt eivät aina ole yksinkertaisia. Esimerkiksi luvulla 7 jaollisuudelle ei ole yhtä helppoa sääntöä kuin edellä esitetyt jaollisuuslauseet. Tarkastellaan asiaa esimerkin avulla.

Esimerkki 1.28. Onko luku 485 jaollinen luvulla 7? Lohkaisutermin muodostamista varten kirjoitetaan $10 = 7 + 3$ ja $100 = 98 + 2$, missä 7 ja 98 ovat lukuja 10 ja 100 lähimmät luvulla 7 jaolliset luvut. Nyt

$$\begin{aligned} 485 &= 4(98 + 2) + 8(7 + 3) + 5 \\ &= (4 \cdot 98 + 8 \cdot 7) + (2 \cdot 4 + 3 \cdot 8 + 5), \end{aligned}$$

missä kriittinen termi on $2 \cdot 4 + 3 \cdot 8 + 5 = 37$. Koska $7 \nmid 37$, niin 7 ei ole luvun 485 jakaja.

Yleisesti, jos

$$n = a_2a_1a_0 = a_2 10^2 + a_1 10 + a_0$$

on korkeintaan *kolminumeroinen* luku, niin

$$n = (a_2 98 + a_1 7) + (a_2 2 + a_1 3 + a_0).$$

Kriittistä termiä $a_2 2 + a_1 3 + a_0$ sanotaan *ensimmäiseksi jaksotermiksi*. Korkeintaan kolminumeroinen luku on siis jaollinen luvulla 7 täsmälleen silloin, kun ensimmäinen jaksotermi on jaollinen luvulla 7.

Oletetaan seuraavaksi, että $n \in \mathbb{N}$ on korkeintaan kuusinumeroinen. Seitsemällä jaollisen luvun $1001 = 7 \cdot 143$ avulla voidaan lohkaista luvusta n täysiä tuhansia sisältävä, luvulla 7 jaollinen osa. Jäljelle jäävää korkeintaan kolminumeroista lukua käsitellään kuten edellä.

Esimerkki 1.29. Onko 648532 jaollinen luvulla 7? Nyt

$$\begin{aligned} 648532 &= 648(1001 - 1) + 5(98 + 2) + 3(7 + 3) + 2 \\ &= \underbrace{(648 \cdot 1001 + 5 \cdot 98 + 3 \cdot 7)}_{\text{1. lohkaisu}} - 648 + \underbrace{(2 \cdot 5 + 3 \cdot 3 + 2)}_{\text{1. jaksotermi}} \end{aligned}$$

ja luvulle -648 saadaan[8]

$$\begin{aligned} -648 &= -[6(98 + 2) + 4(7 + 3) + 8] \\ &= \underbrace{-(6 \cdot 98 + 4 \cdot 7)}_{\text{2. lohkaisu}} \underbrace{-(2 \cdot 6 + 3 \cdot 4 + 8)}_{\text{2. jaksotermi}} . \end{aligned}$$

Luvun 648532 kriittinen termi on 1. ja 2. jaksotermin summa

$$(2 \cdot 5 + 3 \cdot 3 + 2) - (2 \cdot 6 + 3 \cdot 4 + 8) = 21 - 32 = -11,$$

joka ei ole jaollinen luvulla 7. Siten $7 \nmid 648532$.

Huomautus 1.30. Numeroryhmää -648 vastaava kriittisen termin osa, *toinen jaksotermi*, muodostettiin merkkiä vaille samalla tavalla kuin 1. jaksotermi.

[8] huomaa etumerkki!

Yleisesti: Tutkittaessa luvun $n \in \mathbb{N}$ jaollisuutta luvulla 7, luku n jaetaan oikealta alkaen kolmen numeron ryhmiin $a_2a_1a_0$, $a_5a_4a_3$, ..., (viimeisessä ryhmässä on 1-3 numeroa). Kunkin ryhmän jaksotermi saadaan laskemalla yhteen 2·(vasemmanpuoleinen numero), 3·(keskimmäinen numero) ja oikeanpuolimmainen numero. Tähän summaan liitetään etumerkki $(-1)^{i+1}$, missä i on ryhmän *järjestysnumero oikealta*. Kriittinen termi saadaan laskemalla nämä etumerkilliset jaksotermit yhteen. (Tarkka perustelu induktiolla)

Esimerkki 1.31. Luvun 63 104 333 kriittinen termi on

$$(2 \cdot 3 + 3 \cdot 3 + 3) - (2 \cdot 1 + 3 \cdot 0 + 4) + (3 \cdot 6 + 3). = 18 - 6 + 21 = 33$$

Koska $7 \nmid 33$, niin $7 \nmid 63104333$.

Samaan tapaan voidaan johtaa jaollisuussääntöjä muissa lukujärjestelmissä, katso esimerkiksi [Nev]. Kuten kymmenjärjestelmässäkin, on helpointa löytää jaollisuussäännöt kantaluvun k potenssien tekijöille.

Harjoitustehtäviä

1.1. Olkoon $a \in \mathbb{N} - \{0, 1\}$ ja olkoon $b \in \mathbb{N} - \{0\}$. Osoita induktiolla, että on $k \in \mathbb{N} - \{0\}$ siten, että $a^{k-1} \leqslant b < a^k$.

1.2. Todista Lemma 1.24.[9]

1.3. Todista Lauseen 1.3 kohdat (3), (4) ja (7).

1.4. Todista Lauseen 1.3 kohdat (8) ja (10).

1.5. Olkoot $a, b, c, d \in \mathbb{Z}$. Ovatko seuraavat väitteet totta? Todista tai keksi vastaesimerkki.

(1) Jos $a \mid b$ ja $c \mid d$, niin $(a + c) \mid (b + d)$.

(2) Jos $a \mid b$ ja $c \mid d$, niin $ac \mid bd$.

1.6. Mille kokonaisluvuille $u, v \in \mathbb{Z}$ pätee $u \mid v$ ja $v \mid u$?

1.7. Olkoon $n \in \mathbb{Z}$. Osoita, että $4 \nmid n^2 + 1$.

1.8. Olkoot a ja b parittomia lukuja. Osoita, että $a + b$ ja $a - b$ ovat parillisia ja että ab on pariton.

1.9. Olkoon $n \in \mathbb{Z}$ kokonaisluku.

(1) Osoita, että $n^2 - n$ on parillinen.

(2) Osoita, että $n^2 + n$ on parillinen.

1.10. Olkoon n pariton kokonaisluku. Osoita, että $8 \mid n^2 - 1$.

1.11. Olkoot $a, b \in \mathbb{Z}$. Osoita, että $3 \mid a^3b - b^3a$.

1.12. Olkoon $m \in \mathbb{Z} - \{0\}$ ja olkoon $n \in \mathbb{N}$, $n \geqslant 2$. Olkoot $a_i, c_i \in \mathbb{Z}$ kaikilla $i = 1, 2, \ldots n$.

(1) Oletetaan, että $m \mid a_i$ kaikilla $i = 1, 2, \ldots, n$. Osoita, että [10]

$$m \mid (c_1a_1 + c_2a_2 + \cdots + c_na_n).$$

[9] Todista väite induktiolla luvun m suhteen.

[10] Tämä on Lauseen 1.3 (3) yleistys. Todista induktiolla.

(2) Oletetaan, että $m \mid a_i$ kaikilla $i = 1, 2 \ldots n-1$ ja $m \nmid a_n$. Osoita, että

$$m \nmid (a_1 + a_2 + \cdots + a_n).$$

1.13. Olkoon $k \in \mathbb{Z}$. Osoita, että $9 \mid k^3 + (k+1)^3 + (k+2)^3$. [11]

1.14. Muunna binaariluku 1011101 10-järjestelmän ja 7-järjestelmän luvuiksi.
Muunna 10-järjestelmän luku 175 binaariluvuksi ja 3-järjestelmän luvuksi.

1.15. Muunna heksadesimaaliluku `ABC` binaariluvuksi ja desimaaliluvuksi.[12]
Muunna binaariluku 111000111 heksadesimaaliluvuksi.

1.16. Todista Lause 1.20.

1.17. Muunna binaariluku 10111 10-järjestelmän ja 3-järjestelmän luvuiksi.
Muunna 10-järjestelmän luku 19 binaariluvuksi.

1.18. Tutki luvun 1.5 jaollisuussääntöjen avulla, onko luku 158015 jaollinen luvuilla 2, 3, 4, 5, 9, 10 tai 11.

1.19. Tutki luvun 1.5 jaollisuussääntöjen avulla, onko luku 873255789 jaollinen luvuilla 2, 3, 4, 5, 9, 10 tai 11.

1.20. Tutki luvun 1.5 jaollisuussääntöjen avulla, onko luku 3581721 jaollinen luvuilla 2, 3, 4, 5, 9, 10 tai 11.

1.21. Osoita, että 7-järjestelmän luku $dcba_7$ on jaollinen luvulla 6, jos ja vain jos

$$6 \mid (a + b + c + d)\,.$$

[11] Tämän voi todistaa induktiolla luonnollisille luvuille ja negatiivisille kokonaisluvuille.
[12] Katso Esimerkki 1.11.

Luku 2

Kokonaislukujen suurin yhteinen tekijä

Tässä luvussa määrittelemme kokonaislukujen suurimman yhteisen tekijän. Osoitamme, että kokonaislukujen a ja b suurin yhteinen tekijä on pienin positiivinen kokonaisluku, joka voidaan esittää lineaarisella kokonaislukukertoimisella lausekkeella lukujen a ja b avulla. Sovellamme tätä Bézout'n[1] yhtälöä suurimman yhteisen tekijän tarkasteluun. Luvussa 2.5 tutustumme Eukleideen algoritmiin, jolla suurin yhteinen tekijä voidaan laskea.

Luvussa 2.6 tutustumme kokonaislukujen pienimpään yhteiseen jaettavaan, joka on tavallaan suurimman yhteisen tekijän vastapari.

2.1 Suurin yhteinen tekijä

Olkoot $a, b, d \in \mathbb{Z}$. Jos $d \mid a$ ja $d \mid b$, niin d on lukujen a ja b *yhteinen tekijä*. Jos $a \neq 0$ tai $b \neq 0$, niin luku

$$\operatorname{syt}(a, b) = \max\big\{d \in \mathbb{N} : d \mid a \text{ ja } d \mid b\big\}$$

on lukujen a ja b *suurin yhteinen tekijä*.

Lause 2.1. *Olkoot $a, b \in \mathbb{Z}$ siten, että $(a, b) \neq 0$. Tällöin luvuilla a ja b on suurin yhteinen tekijä.*

Todistus. Olkoon

$$D = \big\{d \in \mathbb{N} : d \mid a \text{ ja } d \mid b\big\}.$$

Lauseen 1.3 ((6)) perusteella $1 \in D$.

Toisaalta, jos $d \in D$ ja $a \neq 0$, niin Lauseen 1.3 ((9)) nojalla $d \leqslant |a|$. Vastaavasti, jos $b \neq 0$, niin $d \leqslant |b|$. Siten jokaisella $d \in D$ pätee

$$d \leqslant \max\{|a|, |b|\}.$$

[1] Étienne Bézout (1730-1783).

Joukossa D on ainakin yksi alkio ja korkeintaan $\max\{|a|, |b|\}$ alkiota, joten siinä on suurin alkio, joka on määritelmän mukaan $\text{syt}(a, b)$. □

Huomautus 2.2. (1) Jos $a = b = 0$, niin Lauseen 1.3 ((7)) nojalla Lauseen 2.1 todistuksessa käytetty joukko joukko D olisi $\mathbb{N}$, jossa ei ole suurinta alkiota.

(2) Kaikille $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$ pätee selvästi

$$\text{syt}(a, b) = \text{syt}(-a, b) = \text{syt}(a, -b) = \text{syt}(-a, -b)\,.$$

Tämän havainnon perusteella voimme joissain jaollisuustarkasteluissa olettaa, että tarkasteltavat luvut ovat luonnollisia lukuja ja päätellä tuloksia negatiivisillekin luvuille.

Tästä lähtien, kun kirjoitaan $\text{syt}(a, b)$, niin oletetaan, että $(a, b) \neq (0, 0)$.

Esimerkki 2.3. (1) Luvun 14 positiiviset tekijät ovat 1, 2, 7, ja 14 ja luvun 35 positiiviset tekijät ovat 1, 5, 7 ja 35. Siis lukujen 14 ja 35 yhteiset tekijät ovat ± 1 ja ± 7 ja $\text{syt}(14, 35) = 7$.

(2) Olkoon $d \in \mathbb{N}$ lukujen n ja $(n + 1)$ jakaja. Lauseen 1.3 ((3)) perusteella d jakaa luvun

$$(n + 1) + (-1)\, n = 1\,.$$

Siten Lauseen 1.3 ((9)) perusteella on oltava $d = 1$. Luvuilla n ja $n + 1$ ei siis ole muita positiivisia yhteisiä tekijöitä kuin 1, joten kaikilla $n \in \mathbb{N}$ pätee

$$\text{syt}(n, n + 1) = 1\,.$$

Suurin yhteinen tekijä voidaan määritellä myös kolmelle tai useammalle kokonaisluvulle, joista ainakin yksi on nollasta poikkeava.

Olkoot $a_1, a_2, \ldots, a_N \in \mathbb{Z}$ siten, että $a_i \neq 0$ jollain $1 \leqslant i \leqslant N$. Lukujen $a_1, a_2, \ldots, a_N$ *suurin yhteinen tekijä* on

$$\text{syt}(a_1, a_2, \ldots, a_N) = \max\left\{d \in \mathbb{N} : d \mid a_i \text{ kaikilla } 1 \leqslant i \leqslant N\right\}.$$

2.2 Bézout'n yhtälö

Esimerkissä 2.3(2) määritimme lukujen n ja $n+1$ suurimman yhteisen tekijän kirjoittamalla luvun 1 niiden erotuksena ja käyttämällä jaollisuuden perusominaisuuksia. Tässä luvussa tarkastelemme tämän esimerkin yleistystä.

Lause 2.4. *Kokonaislukujen $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$, suurin yhteinen tekijä on joukon*

$$J = \{xa + yb : x, y \in \mathbb{Z}\} \cap (\mathbb{N} - \{0\})$$

pienin alkio.

Todistus. Ainakin yksi luvuista $\pm a, \pm b$ on joukossa J, joten joukossa J on hyvän järjestyksen periaatteen[2] nojalla pienin alkio g. Osoitetaan, että g on luvun a jakaja. Jos g ei jaa lukua a, niin jakoyhtälön nojalla on kokonaisluvut $q \in \mathbb{Z}$ ja $0 < r < g$, joille $a = qg + r$. Määritelmänsä nojalla

$$g = x_0 a + y_0 b \tag{2.1}$$

joillain $x_0, y_0 \in \mathbb{Z}$, joten

$$r = a - qg = a - q(x_0 a + y_0 b) = (1 - qx_0)a - qy_0 b \in J\,.$$

Tämä on ristiriita, koska nyt r olisi joukossa J ja se on pienempi kuin joukon J pienin alkio. Samaan tapaan osoitetaan, että $g \mid b$.

Jos d on lukujen a ja b yhteinen jakaja, niin yhtälön (2.1) ja jaollisuuslauseen 1.3(3) nojalla $d \mid g$. Jaollisuuslauseen 1.3(9) nojalla $d \leqslant g$, joten $g = \operatorname{syt}(a, b)$. □

Seuraus 2.5 (Bézout'n yhtälö)**.** *Olkoot $a, b \in \mathbb{Z}$, $a \neq 0$. Tällöin*

$$\operatorname{syt}(a, b) = xa + yb$$

joillain $x, y \in \mathbb{Z}$. □

Huomaa, että Bézout'n yhtälön kertoimet x ja y eivät ole yksikäsitteisiä: Esimerkiksi lukujen 3 ja 2 suurin yhteinen tekijä 1 saadaan muodoissa

$$1 = 1 \cdot 3 - 1 \cdot 2 = -1 \cdot 3 + 2 \cdot 2\,.$$

Seuraus 2.6. *Olkoot $a, b, c \in \mathbb{Z}$ ja $a \neq 0$. Tällöin $c \mid a$ ja $c \mid b$ jos ja vain jos $c \mid \operatorname{syt}(a, b)$.*

Todistus. Olkoon c lukujen a ja b yhteinen jakaja. Tällöin $a = k_1 c$ ja $b = k_2 c$. Bézout'n yhtälön nojalla on luvut $x, y \in \mathbb{Z}$, joille pätee

$$\operatorname{syt}(a, b) = xa + yb = (xk_1 + yk_2)c\,.$$

Siis $c \mid \operatorname{syt}(a, b)$.

Jos taas $c \mid \operatorname{syt}(a, b)$, niin jaollisuuden transitiivisuuden[3] nojalla $c \mid a$ ja $c \mid b$. □

Bézout'n yhtälön mukaan lukujen a ja b suurin yhteinen tekijä voidaan esittää kokonaislukukertoimisella lineaarisella lausekkeella luvuista a ja b. Seuraava lause kertoo, että täsmälleen luvut, jotka ovat muotoa $k \operatorname{syt}(a, b)$ jollain $k \in \mathbb{Z}$, voidaan esittää tällaisena summana.

Lause 2.7. *Olkoot $a, b, c \in \mathbb{Z}$, $a \neq 0$. Tällöin*

$$c = ka + lb \quad \textit{jollain } k, l \in \mathbb{Z}$$

jos ja vain jos $\operatorname{syt}(a, b) \mid c$.

[2] Propositio 1.2
[3] Lause 1.3(2)

Todistus. Olkoon $d = \operatorname{syt}(a,b)$. Oletaan ensin, että on $k,l \in \mathbb{Z}$, joille $c = ka + lb$. Koska $d \mid a$ ja $d \mid b$, niin Lauseen 1.3 ((3)) mukaan $d \mid c$.

Jos taas $d \mid c$, niin $c = md$ jollain $m \in \mathbb{Z}$. Bézout'n yhtälön nojalla on $x,y \in \mathbb{Z}$, joille $d = xa + yb$. Siis

$$c = md = mxa + myb\,. \qquad \square$$

Esimerkki 2.8. (1) Jos $\operatorname{syt}(a,b) = 1$, niin jokainen $c \in \mathbb{Z}$ voidaan esittää summana $c = ka + lb$, $k,l \in \mathbb{Z}$.

(2) Koska $\operatorname{syt}(18,64) = 2$, niin kaikki parilliset luvut voidaan esittää muodossa $18l + 64k$, $k,l \in \mathbb{Z}$.

Lause 2.9. *Olkoot $a,b \in \mathbb{Z}$, $(a,b) \neq (0,0)$, $c \in \mathbb{N} - \{0\}$. Tällöin*

$$\operatorname{syt}(ca,cb) = c\operatorname{syt}(a,b)\,.$$

Todistus. Jos $d \mid a$ ja $d \mid b$, niin Lauseen 1.3(4) nojalla $cd \mid ca$ ja $cd \mid cb$. Siis cd on lukujen ca ja cb yhteinen tekijä, joten

$$\operatorname{syt}(ca,cb) \geqslant c\operatorname{syt}(a,b)\,. \tag{2.2}$$

Toisaalta joillekin $z,w \in \mathbb{Z}$ pätee

$$c\operatorname{syt}(a,b) = c(za + wb) = z(ca) + w(cb)\,.$$

Lauseen 2.7 nojalla $\operatorname{syt}(ca,cb) \mid c\operatorname{syt}(a,b)$. Lauseen 1.3(9) nojalla

$$\operatorname{syt}(ca,cb) \leqslant c\operatorname{syt}(a,b)\,. \tag{2.3}$$

Väite seuraa yhdistämällä epäyhtälöt (2.2) ja (2.3). $\square$

Seuraus 2.10. *Olkoot $a,b \in \mathbb{Z}$, $(a,b) \neq (0,0)$ ja olkoon $d \in \mathbb{N} - \{0\}$ lukujen a ja b yhteinen jakaja. Tällöin*

$$\operatorname{syt}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\operatorname{syt}(a,b)}{d}\,.$$

Erityisesti

$$\operatorname{syt}\left(\frac{a}{\operatorname{syt}(a,b)}, \frac{b}{\operatorname{syt}(a,b)}\right) = 1\,.$$

Todistus. Harjoitustehtävä 2.6 $\square$

2.3 Lineaarinen Diofantoksen yhtälö

Bézout'n yhtälö on erikoistapaus lukuteoriassa merkittävistä *Diofantoksen*[4] *yhtälöistä.*

Olkoot $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$ ja $c \in \mathbb{Z}$. Yhtälö $ax + by = c$ on *(kahden muuttujan) lineaarinen Diofantoksen yhtälö.*

Lineaarisen Diofantoksen yhtälön *ratkaisu* on kokonaislukupari $(u,v) \in \mathbb{Z}^2$, jolle pätee $au + bv = c$.

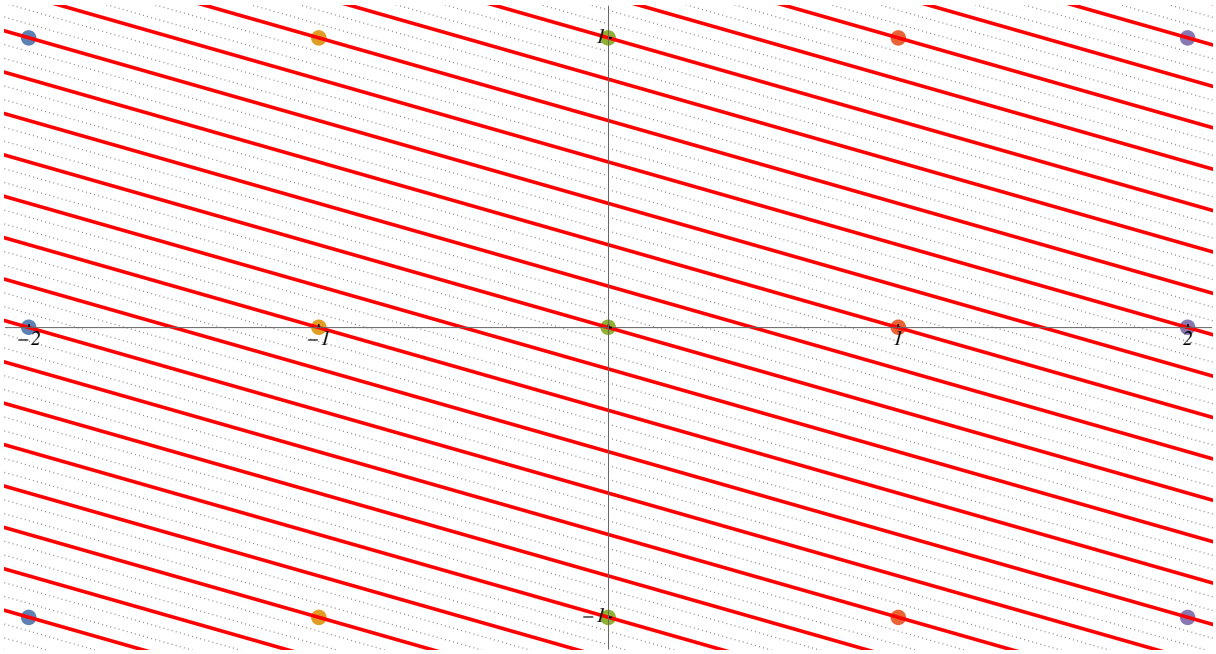
[4] Diofantos Aleksandrialainen oli kreikkalainen matemaatikko 200-luvulla Egyptissä.

Määritelmän mukaan lineaarisen Diofantoksen yhtälön ratkaisuksi hyväksytään ainoastaan kokonaislukupareja.

Seuraus 2.11. *Olkoot* $(a, b) \in \mathbb{Z}^2 - \{(0, 0)\}$ *ja* $c \in \mathbb{Z}$. *Lineaarisella Diofantoksen yhtälöllä* $ax + by = c$ *on ratkaisu* $(x, y) \in \mathbb{Z}^2$, *jos ja vain jos* $\text{syt}(a, b) \mid c$.

Todistus. Väite seuraa suoraan Lauseesta 2.7. □

Esimerkki 2.12. $\text{syt}(6, 21) = 3$, joten lineaarisella Diofantoksen yhtälöllä $6x + 21y = c$ on ratkaisu $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ jos ja vain jos $3 \mid c$.



Kuva 2.1 — Lineaarisen Diofantoksen yhtälön $6x + 21y = c$ ratkaisujen geometrinen tulkinta luvun c eri arvoilla. Punaiset affiinit suorat vastaavat vakion c luvulla 3 jaollisia arvoja. Seurauksen 2.11 nojalla yhtälöllä on ratkaisuja täsmälleen näillä luvun c arvoilla.

Palaamme lineaaristen Diofantoksen yhtälöiden pariin luvussa 6.1, jossa löydämme niiden kaikki ratkaisut. Lukuteoriassa tarkastellaan myös korkeamman asteen Diofantoksen yhtälöitä. Esimerkiksi yhtälöllä

$$x^2 + y^2 = z^2 \tag{2.4}$$

on äärettömän monta ratkaisua $(x, y, z) \in \mathbb{Z}^3$, joita kutsutaan *Pythagoraan*[5] *kolmikoiksi*, koska Pythagoraan lauseen nojalla yhtälön 2.4 ratkaisut ovat jonkin suorakulmaisen kolmion sivujen pituudet. On helppo tarkastaa, että esimerkiksi $(3, 4, 5)$ on Pythagoraan kolmikko. Pythagoraan kolmikoita tarkastellaan osassa II luvussa 9.1.

Fermat[6] kirjoitti 1600-luvulla Diofantoksen Arithmetica-kirjan marginaaliin löytäneensä todistuksen sille, että $(0, 0, 0)$ on Diofantoksen yhtälön

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

[5]Pythagoras Samoslainen oli kreikkalainen filosofi, joka eli noin 570-490 eaa.
[6]Pierre de Fermat (1601-1665).

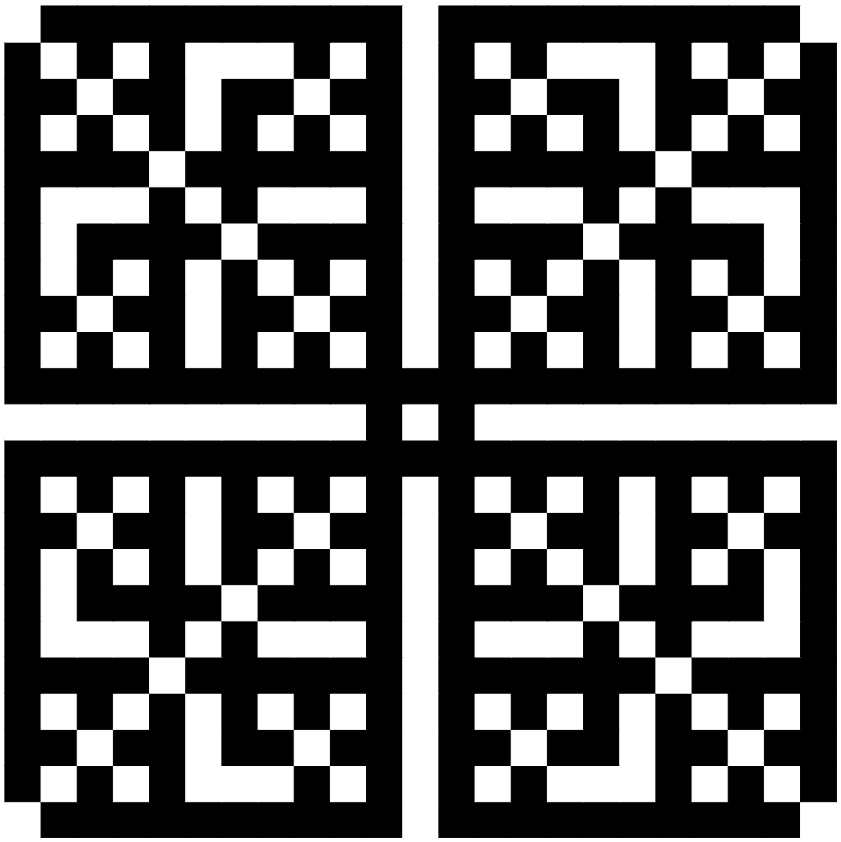
ainoa ratkaisu, jos $n \geqslant 3$. Wiles todisti tämän *Fermat'n suuren lauseen* 1990-luvulla. Tapaus $n = 4$ todistetaan osassa II luvussa 9.

2.4 Suhteelliset alkuluvut

Tässä luvussa todistamme Gaussin tärkeän tuloksen jaollisuudesta, kun kahden käsiteltävän luvun suurin yhteinen tekijä on 1.

Jos $a, b \in \mathbb{Z}$ ja $\operatorname{syt}(a, b) = 1$, niin a ja b ovat *suhteellisia alkulukuja* ja luvut a ja b ovat *keskenään jaottomia*.

Jos a ja b ovat suhteellisia alkulukuja, niin (a, b) on *suhteellinen alkulukupari*.



Kuva 2.2 — Suhteelliset alkulukuparit joukossa $\{(a, b) \in \mathbb{Z}^2 : -11 \leqslant a, b \leqslant 11\}$.

Huomautus 2.13. Bézout'n yhtälön[7] nojalla luvut $a, b \in \mathbb{Z}$ ovat keskenään jaottomia jos ja vain jos $xa + yb = 1$ jollain $x, y \in \mathbb{Z}$.

Seuraavat hyödylliset jaollisuustulokset pätevät vain keskenään jaottomille luvuille.[8]

Seuraus 2.14. *Olkoot $a, b \in \mathbb{Z}$ keskenään jaottomia ja $c \in \mathbb{Z}$. Tällöin*

[7] Seuraus 2.5

[8] Katso Harjoitustehtävä 2.10.

(1) Jos $a \mid c$ ja $b \mid c$, niin $ab \mid c$.

(2) Jos $a \mid bc$, niin $a \mid c$. *(Gaussin lemma)*

Todistus. Koska $\mathrm{syt}(a, b) = 1$, niin Bézout'n yhtälön mukaan $xa + yb = 1$ jollain $x, y \in \mathbb{Z}$, joten

$$c = c(xa + yb) = cxa + cyb. \tag{2.5}$$

((1)) Oletuksen nojalla on $k, l \in \mathbb{Z}$, joille $ka = c = lb$, joten yhtälön (2.5) nojalla

$$c = cxa + cyb = (lb)xa + (ka)yb = ab(lx + ky).$$

Siis $ab \mid c$.

((2)) Koska $a \mid a$ ja $a \mid bc$, niin kaavan (2.5) ja Lauseen 1.3 (3) nojalla $a \mid c$. □

Suhteellisilla alkuluvuilla on mielenkiintoinen tulo-ominaisuus, johon palaamme Luvussa 12.2.

Lause 2.15. *Olkoot $a, b, m \in \mathbb{Z}$. Jos $\mathrm{syt}(a, m) = \mathrm{syt}(b, m) = 1$, niin $\mathrm{syt}(ab, m) = 1$.*

Todistus. Bézout'n yhtälön nojalla on $x, y, z, w \in \mathbb{Z}$, joille $xa + ym = 1 = zb + wm$. Siis

$$(xa)(zb) = (1 - ym)(1 - wm) = 1 + \big(- (y + w) + ywm\big)m\,,$$

joten

$$(xz)(ab) + (y + w - ywm)m = 1\,.$$

Bézout'n yhtälön nojalla $\mathrm{syt}(ab, m) = 1$. □

2.5 Eukleideen algoritmi

Tekijöiden listaaminen ja suurimman yhteisen tekijän etsiminen yhteisten tekijöiden joukosta on isoilla luvuilla työlästä. Jakoyhtälöön ja seuraavaan lemmaan perustuva *Eukleideen algoritmi* on tehokkampi tapa.

Lemma 2.16. *Jos $a, b, q, r \in \mathbb{Z}$ ja $a = qb + r$, niin $\mathrm{syt}(a, b) = \mathrm{syt}(b, r)$.*

Todistus. Lauseen 1.3(3) nojalla jokainen lukujen b ja r yhteinen tekijä jakaa summan $qb + r = a$. Vastaavasti jokainen lukujen a ja b yhteinen tekijä jakaa luvun $a - qb = r$. Pareilla a, b ja b, r on siis samat yhteiset tekijät. Siten on myös $\mathrm{syt}(a, b) = \mathrm{syt}(b, r)$. □

Esimerkki 2.17. Määritetään lukujen 56 ja 32 suurin yhteinen tekijä Lemman 2.16 avulla. Seuraavassa laskussa esiintyviä lukuja on korostettu lisämerkinnöillä, että laskun logiikan seuraaminen helpottuisi.

$$\begin{aligned} 56 &= 1 \cdot \underline{32} + \boxed{24} \\ \underline{32} &= 1 \cdot \boxed{24} + \underline{\underline{8}} \\ \boxed{24} &= 3 \cdot \underline{\underline{8}}. \end{aligned}$$

Siis $\mathrm{syt}(56, 32) = 8$.

Eukleideen algoritmi

Olkoot $a, b \in \mathbb{Z}$, $a \neq 0$. Jos $b = 0$, niin $d = |a|$. Voidaan siis olettaa, että $a, b \neq 0$. Huomautuksen 2.2 nojalla voidaan olettaa, että $1 \leqslant b < a$.

Jakamalla a luvulla b jakoyhtälön[a] avulla saadaan yksikäsitteiset luvut $q_1, r_1 \in \mathbb{Z}$, joille

$$a = q_1 b + r_1 \quad \text{ja} \quad 0 \leqslant r_1 < b.$$

Jos $r_1 = 0$, niin $b \mid a$. Tällöin $\text{syt}(a, b) = b$ ja voimme lopettaa. Jos $r_1 > 0$, niin jaetaan b luvulla r_1. Jakoyhtälö antaa yksikäsitteiset luvut $q_2, r_2 \in \mathbb{Z}$, joille

$$b = q_2 r_1 + r_2 \quad \text{ja} \quad 0 \leqslant r_2 < r_1.$$

Lemman 2.16 nojalla $\text{syt}(a, b) = \text{syt}(b, r_1)$. Siten, jos $r_2 = 0$, niin $\text{syt}(a, b) = r_1$ voimme lopettaa. Jos $r_2 > 0$, jaetaan r_1 luvulla r_2. Jakoyhtälö antaa yksikäsitteiset luvut $q_3, r_3 \in \mathbb{Z}$, joille

$$r_1 = q_3 r_2 + r_3 \quad \text{ja} \quad 0 \leqslant r_3 < r_2.$$

Jatketaan kuten edellä. Koska jakoyhtälön antamien jakojäännösten jono (r_i) on aidosti vähenevä ja

$$b > r_1 > r_2 > \cdots \geqslant 0,$$

niin jollain n on oltava $r_n = 0$.[b] Viimeiset kaksi vaihetta ovat

$$\begin{aligned} r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, & 0 < r_{n-1} < r_{n-2}, \\ r_{n-2} &= q_n r_{n-1} + r_n, & r_n = 0. \end{aligned} \tag{2.6}$$

[a] Lause 1.6

[b] Eukleideen algoritmi siis päättyy korkeintaan b askeleen jälkeen.

Lause 2.18. *Olkoot $a, b \in \mathbb{N} - \{0\}$, $a > b$. Kun Eukleideen algoritmia sovelletaan lukuihin a ja b, niin viimeinen positiivinen jakojäännös on* $\text{syt}(a, b)$.

Todistus. Lemma 2.16 sovellettuna Eukleideen algoritmissa olevien lukujen $a, b, r_1, ..., r_{n-3}$ yhtälöihin kertoo, että

$$\text{syt}(a, b) = \text{syt}(b, r_1) = \text{syt}(r_1, r_2) = \cdots = \text{syt}(r_{n-2}, r_{n-1}). \tag{2.7}$$

Koska yhtälön (2.6) perusteella $r_{n-1} \mid r_{n-2}$, niin $\text{syt}(r_{n-2}, r_{n-1}) = r_{n-1}$. Yhtälöketjun (2.7) nojalla $\text{syt}(a, b) = r_{n-1}$. □

Jos $b \nmid a$, niin Eukleideen algoritmi *peruuttaen* antaa Bézout'n yhtälössä[9] esiintyvät kertoimet x ja y: Toiseksi viimeinen yhtälö ilmaisee suurimman yhteisen tekijän $d = r_{n-1}$ jakojäännösten r_{n-2} ja r_{n-3} kokonaislukukertoimisena lineaarikombinaationa. Edellinen yhtälö ilmaisee jakojäännöksen r_{n-2} jakojäännösten r_{n-3} ja r_{n-4} kokonaislukukertoimisena lineaarikombinaationa. Siis

$$r_{n-1} = r_{n-3} - q_{n-1} r_{n-2} = r_{n-3} - q_{n-1}(r_{n-4} - q_{n-2} r_{n-3}).$$

Jatkamalla näin päädytään haluttun esitykseen.

[9] Seuraus 2.5.

Esimerkki 2.19. Lasketaan syt$(18, 64)$ ja etsitään luvut $x, y \in \mathbb{Z}$, joille syt$(a, b) = xa + yb$. Eukleideen algoritmilla saadaan

$$\begin{aligned} 64 &= 3 \cdot \underline{18} + \boxed{10} & \qquad 10 &= 64 - 3 \cdot 18 \\ \underline{18} &= 1 \cdot \boxed{10} + \underline{\underline{8}} & \qquad 8 &= 18 - 10 \\ \boxed{10} &= 1 \cdot \underline{\underline{8}} + 2_* & \qquad 2 &= 10 - 8 \\ \underline{\underline{8}} &= 4 \cdot 2_* \end{aligned}$$

Siten syt$(18, 64) = 2$. *Peruuttamalla* algoritmissa saadaan

$$2 = 10 - 8 = 10 - (18 - 10) = 2 \cdot 10 - 18 = 2(64 - 3 \cdot 18) - 18 = 2 \cdot 64 - 7 \cdot 18.$$

2.6 Pienin yhteinen jaettava

Luku $c \in \mathbb{Z}$ on lukujen $a_1, a_2, \ldots, a_N \in \mathbb{Z} - \{0\}$ *yhteinen jaettava*, jos $a_i \mid c$ kaikilla $1 \leqslant i \leqslant N$.

Lukujen $a_1, a_2, \ldots, a_N \in \mathbb{Z} - \{0\}$ *pienin yhteinen jaettava*, pyj$(a_1, a_2, \ldots, a_N)$ on niiden pienin positiivinen yhteinen jaettava.

Kahden luvun tapauksessa luku $c \in \mathbb{Z}$ on lukujen $a, b \in \mathbb{Z} - \{0\}$ yhteinen jaettava, jos $a \mid c$ ja $b \mid c$. Lukujen a ja b pienin yhteinen jaettava pyj(a, b) on niiden pienin positiivinen yhteinen jaettava.

Seurausta 2.6 vastaava tulos pienimmälle yhteiselle jaettavalle on

Lause 2.20. *Olkoot $a, b, c \in \mathbb{Z}$ ja $a, b \neq 0$. Tällöin $a \mid c$ ja $b \mid c$ jos ja vain jos* pyj$(a, b) \mid c$.

Todistus. Jos pyj$(a, b) \mid c$, niin yhteisen jaettavan määritelmän ja Lauseen 1.3(2) nojalla $a \mid c$ ja $b \mid c$.

Oletetaan, että $a \mid c$ ja $b \mid c$. Jaollisuuslauseen nojalla on $q \in \mathbb{Z}$ ja $0 \leqslant r <$ pyj(a, b), joille $c = q\,$pyj$(a, b) + r$. Koska $a \mid$ pyj(a, b) ja $b \mid$ pyj(a, b), niin Lauseen 1.3 kohtien (2) ja (3) nojalla $a \mid r$ ja $b \mid r$, joten r on lukujen a ja b yhteinen jaettava. Koska $r <$ pyj(a, b), täytyy olla $r = 0$. Siis pyj$(a, b) \mid c$. □

Lemma 2.21. *Olkoot $a, b \in \mathbb{Z} - \{0\}$. Jos* syt$(a, b) = 1$, *niin* pyj$(a, b) = ab$.

Todistus. Jos $x \in \mathbb{Z}$, niin luvuilla x ja $-x$ on samat positiiviset tekijät ja jaettavat, joten voimme olettaa todistuksessa, että $a, b \in \mathbb{N} - \{0\}$. Koska $a \mid$ pyj(a, b), niin pyj$(a, b) = ka$ jollain $k \in \mathbb{N}$. Koska $b \mid$ pyj$(a, b) = ka$, niin Gaussin lemman[10] nojalla $b \mid k$. Lauseen 1.3(9) nojalla $k \geqslant b$, joten pyj$(a, b) = ka \geqslant ab$. Mutta ab on lukujen a ja b yhteinen jaettava, joten määritelmän nojalla pyj$(a, b) \leqslant ab$. □

Lemma 2.21 on erikoistapaus seuraavasta tuloksesta, jonka todistus tehdään hieman myöhemmin kurssilla.

Lause 2.22. *Olkoot $a, b \in \mathbb{N} - \{0\}$. Tällöin* syt$(a, b)$ pyj$(a, b) = ab$.

Todistus. Harjoitustehtävä 3.22 □

[10] Seuraus 2.14(2).

Harjoitustehtäviä

2.1. Määritä kokonaislukujen 126 ja 308 yhteiset tekijä ja suurin yhteinen tekijä.

2.2. Olkoon $(a_1, a_2, \ldots, a_N) \in \mathbb{Z}^N - \{0\}$. Oletetaan, että kaikilla $1 \leqslant i \neq j \leqslant N$ pätee $\operatorname{syt}(a_i, a_j) = 1$. Osoita, että

$$\operatorname{syt}(a_1, a_2, \ldots, a_N) = 1\,.$$

2.3. Anna esimerkki positiivisista luonnollisista luvuista $a_1, a_2, a_3 \in \mathbb{N} - \{0\}$, joille pätee $\operatorname{syt}(a_1, a_2) \neq 1$, $\operatorname{syt}(a_2, a_3) \neq 1$, $\operatorname{syt}(a_3, a_1) \neq 1$ ja $\operatorname{syt}(a_1, a_2, a_3) = 1$.

2.4. Onko yhtälöillä $126x - 308y = 1$ ja $93x + 11y = 1$ kokonaislukuratkaisuja?[11]

2.5. Olkoot $a, b \in \mathbb{Z}$ kokonaislukuja, joille $\operatorname{syt}(a, 4) = \operatorname{syt}(b, 4) = 2$. Määritä $\operatorname{syt}(a+b, 4)$.

2.6. Todista Seuraus 2.10.

2.7. Olkoon $n \in \mathbb{Z}$. osoita, että $6 \mid n(n+1)(n+2)$ ja $24 \mid n(n+1)(n+2)(n+3)$.[12]

2.8. Olkoon $N = a_n a_{n-1} \cdots a_1 a_0$ luvun $N \in \mathbb{N}$ esitys 10-järjestelmässä. Olkoon

$$N_1 = \frac{N - a_0}{10} - 2a_0\,.$$

Osoita, että $7 \mid N$, jos ja vain jos $7 \mid N_1$.

2.9. Tutki Harjoitustehtävän 2.8 menetelmällä, onko luku 158015 jaollinen luvulla 7.

2.10. (1) Etsi luvut $a, b, c \in \mathbb{Z}$, joille $\operatorname{syt}(a, b) > 1$, $a \mid c$ ja $b \mid c$ mutta $ab \nmid c$,
(2) Etsi luvut $a, b, c \in \mathbb{Z}$, joille $\operatorname{syt}(a, b) > 1$ ja $a \mid bc$ mutta $a \nmid b$ ja $a \nmid c$.[13]

2.11. Olkoot $a, b, c \in \mathbb{Z} - \{0\}$ siten, että $\operatorname{syt}(a, c) = 1$. Osoita, että $\operatorname{syt}(a, b) = \operatorname{syt}(a, bc)$.[14]

2.12. Olkoot $a, b, c, d, x, y, u, v \in \mathbb{Z}$ siten, että $ad - bc = 1$, $u = ax + by$ ja $v = cx + dy$. Osoita, että $\operatorname{syt}(x, y) = \operatorname{syt}(u, v)$.[15]

2.13. Laske $\operatorname{syt}(126, 308)$ Eukleideen algoritmilla. Etsi luvut $x, y \in \mathbb{Z}$, joille

$$\operatorname{syt}(126, 308) = 126x + 308y.$$

2.14. Laske $\operatorname{syt}(78, 123)$ Eukleideen algoritmilla. Etsi luvut $x, y \in \mathbb{Z}$, joille

$$\operatorname{syt}(78, 123) = 78x + 123y.$$

2.15. Laske $\operatorname{syt}(175, 441)$ Eukleideen algoritmilla. Etsi luvut $x, y \in \mathbb{Z}$, joille

$$\operatorname{syt}(175, 441) = 175x + 441y\,.$$

2.16. Laske $\operatorname{syt}(594, 814)$ Eukleideen algoritmilla. Etsi luvut $x, y \in \mathbb{Z}$, joille

$$\operatorname{syt}(594, 814) = 594x + 814y\,.$$

[11] Vihje: Tehtävä 2.1.
[12] Käytä Gaussin lemmaa.
[13] Tässä tehtävässä näytetään, että Seurauksen 2.14 väitteet eivät päde ilman oletusta $\operatorname{syt}(a, b) = 1$.
[14] Käytä Bézoutin yhtälön seurausta ja Gaussin lemmaa.
[15] Olkoon $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Auttaisivatko lineaarialgebra ja Bézout?

2.17. Laske syt$(234, 1026)$ Eukleideen algoritmilla. Etsi luvut $x, y \in \mathbb{Z}$, joille

$$\text{syt}(234, 1026) = 234x + 1026y\,.$$

2.18. Määritä Eukleideen algoritmin avulla syt$(1891, 651)$.

2.19. Etsi lineaarisen Diofantoksen yhtälön $654x - 9876y = 42$ ratkaisu.

2.20. Etsi lineaarisen Diofantoksen yhtälön $12345x + 54321y = 9$ ratkaisu.

2.21. Miten 6 cm mitataan mittatikuilla, joiden pituudet ovat 174 cm ja 72 cm?

Luku 3

Alkuluvut

Tässä luvussa määritellään alkuluvun käsite ja tutustutaan alkulukujen teorian perusasioihin. Osoitamme, että jokainen luonnollinen luku $n > 1$ voidaan esittää alkulukujen tulona täsmälleen yhdellä tavalla tekijöiden järjestystä vailla ja että alkulukuja on ääretömän monta. Lisäksi tutkitaan alkulukujen esiintymistiheyttä.

3.1 Alkuluvut ja yhdistetyt luvut

Luonnollinen luku $p > 1$ on *alkuluku*, jos sen ainoat positiiviset tekijät ovat 1 ja p.
Luonnollinen luku $p > 1$, joka ei ole alkuluku, on *yhdistetty luku*.
Jos $n \in \mathbb{Z} - \{0\}$ on jaollinen alkuluvulla p, niin p on luvun n *alkutekijä* tai *alkulukutekijä*.

Huomautus 3.1. (1) Luku 1 *ei* ole alkuluku *eikä* yhdistetty luku.

(2) 2 on ainoa parillinen alkuluku[1]

(3) Jos $p, q \in \mathbb{N}$ ovat alkulukuja ja $p \neq q$, niin $\text{syt}(p, q) = 1$. Erityisesti Seurauksen 2.14 seurauksena saadaan käyttökelpoinen tulos: Jos $a \in \mathbb{Z}$, $p \mid a$ ja $q \mid a$, niin $pq \mid a$. Harjoitustehtävässä 3.4 todistetaan tämän havainnon yleistys: Jos $p_1, p_2, \ldots, p_r$ ovat eri alkulukuja ja luvulle $a \in \mathbb{Z}$ pätee $p_k \mid a$ kaikilla $1 \leqslant k \leqslant r$. niin $p_1 p_2 \cdots p_r \mid a$.

Esimerkki 3.2. (1) 10 ensimmäistä alkulukua ovat $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.

(2) Luvulla 18 on (positiiviset) tekijät $1, 2, 3, 6, 9$ ja 18, joten se ei ole alkuluku.

Lemma 3.3. *Olkoon $n \in \mathbb{N}$, $n \geqslant 2$. Luku n on yhdistetty luku jos ja vain jos on alkuluku $p \leqslant \sqrt{n}$, joka jakaa luvun n.*

Todistus. Jos on sellainen alkuluku p, että $p \mid n$ ja $1 < p \leqslant \sqrt{n} < n$, niin n on yhdistetty luku.

Oletetaan, että $n \in \mathbb{N}$, $n \geqslant 2$, on yhdistetty luku. Olkoon p luvun n pienin alkutekijä. Tällöin on $k \in \mathbb{N}$, $k \geqslant p$, jolle $n = kp$. Nyt $n = kp \geqslant p^2$, joten $p \leqslant \sqrt{n}$. □

[1] The only even prime is the oddest prime!

Eratostheneen [a]seula

Lukua $x > 0$ pienemmät alkuluvut löydetään Eratostheneen seulan avulla seuraavasti:

(1) Kirjoitetaan taulukkoon luonnolliset luvut $n \leqslant x$.

(2) Luvun 2 positiiviset tekijät ovat 1 ja 2, joten 2 on alkuluku. Poistetaan luvun 2 monikerrat $2k$, joille $k \geqslant 2$.

(3) Ensimmäinen luku, jota ei ole poistettu on 3. Sen on oltava alkuluku. Poistetaan luvun 3 monikerrat $3k$, joille $k \geqslant 2$.

(4) Seuraava luku, jota ei ole poistettu on 3. Sen on oltava alkuluku. Poistetaan luvun 5 monikerrat $5k$, joille $k \geqslant 2$.

(5) Jatketaan näin, kunnes seuraava luku, jota ei ole poistettu on suurempi kuin $\sqrt{x}$.[b] Taulukon jäljelle jääneet luvut ovat lukua x pienemmät alkuluvut.

[a]Eratosthenes Kyreneläinen eli muun muuassa Aleksandriassa noin vuosina 276-199 eaa.
[b]Tämä riittää Lemman 3.3 nojalla.

Esimerkki 3.4. Etsitään alkuluvut p, joille $p \leqslant 40$. Riittää käydä läpi alkuluvut $p < 7$, sillä $6^2 = 36 < 40 < 49 = 7^2$.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~

Etsityt alkuluvut ovat siis $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$.

Monet pienet alkuluvut ovat muotoa $2^n \pm 1$, esimerkiksi $3, 5, 7, 17, 31$. Seuraavat tulokset osoittavat, että luvun 2^n esiintyminen kaavassa ei ole sattumaa.

Lause 3.5. *Olkoot $a, n \in \mathbb{N}$, $a, n \geqslant 2$. Jos $a^n - 1$ on alkuluku, niin $a = 2$ ja n on alkuluku.*

Todistus. Lemman 1.24 tai geometrisen summan kaavan nojalla $(a-1) \mid (a^n - 1)$. Luku $a^n - 1$ voi siis olla alkuluku vain, jos $a = 2$.

Jos olisi $n = km$ joillain $m, k \in \mathbb{N}$, $m, k > 1$, niin $2^n - 1 = (2^m)^k - 1$. Kuten edellä näemme siis, että $(2^m - 1) \mid (2^n - 1)$. Tämä ei ole mahdollista, jos $2^n - 1$ on alkuluku. □

Lause 3.6. *Olkoot $a, m \in \mathbb{N}$, $a \geqslant 2$. Jos $a^m + 1$ on alkuluku, niin a on parillinen ja $m = 2^n$ jollain $n \in \mathbb{N} \cup \{0\}$.*

Todistus. Jos a olisi pariton, niin a^m olisi pariton ja siten $a^m + 1 \geqslant 3 + 1 = 4$ olisi parillinen. Koska 2 on ainoa parillinen alkuluku, a ei siis voi olla pariton.

Jos luvulla m olisi pariton tekijä $k > 1$, niin olisi $m = 2^n k$ jollain kokonaisluvulla $n \geqslant 0$. Tällöin $a^m = (a^{2^n})^k$ ja $(-1)^k = -1$. Soveltamalla Lemmaa 1.24, kun $b = -1$, päättelemme, että $(a^{2^n} + 1) \mid (a^m + 1)$. Koska $a^m + 1$ on alkuluku, niin tämä on mahdotonta. Siis luvulla m ei ole parittomia tekijöitä. □

3.2 Aritmetiikan peruslause

Tässä luvussa osoitamme, että jokainen luonnollinen luku $n \geqslant 2$ voidaan esittää alkulukujen tulona järjestystä vaille yksikäsitteisellä tavalla.

Todistetaan ensin alkulukutekijäesityksen olemassaolo-osa.

Lemma 3.7. *Olkoon $n \in \mathbb{N}$, $n \geqslant 2$. Tällöin n on alkuluku tai alkulukujen tulo.*

Todistus. Todistetaan väite induktiolla. Koska 2 on alkuluku, niin väite on totta kun $n = 2$. Olkoon $k \in \mathbb{N}$, $k \geqslant 2$. Oletetaan, väite on totta luvuille $2, \ldots, k$. Pitää näyttää, että väite on totta luvulle $k+1$. Jos $k+1$ on alkuluku, niin väite on totta. Jos $k+1$ ei ole alkuluku, niin Lauseen 1.3 ((9)) nojalla on $a, b \in \mathbb{N}$, $1 < a, b \leqslant k$, joille

$$k + 1 = ab.$$

Induktio-oletuksen mukaan a ja b ovat alkulukujen tuloja (tai alkulukuja). Siten myös $k+1$ on alkulukujen tulo.

Induktioperiaatteen nojalla väite on totta kaikille $n \in \mathbb{N}$, $n \geqslant 2$. □

Luvun $n \in \mathbb{N} - \{0\}$, $n \geqslant 2$, esitys

$$n = p_1^{e_1} \cdots p_k^{e_k}, \tag{3.1}$$

missä $p_1 < \cdots < p_k$ ovat alkulukuja ja $e_1, \ldots e_k \in \mathbb{N} - \{0\}$, on luvun n *alkutekijäesitys*.

Esimerkki 3.8. Esitetään luku 80 alkulukujen tulona:

$$80 = 10 \cdot 8 = (2 \cdot 5) \cdot (2 \cdot 4) = (2 \cdot 5) \cdot (2 \cdot 2 \cdot 2) = 2^4 \cdot 5.$$

Jako voitaisiin tehdä myös seuraavasti

$$80 = 2 \cdot 40 = 2 \cdot 5 \cdot 8 = 2^4 \cdot 5.$$

Molemmilla tavoilla päädyttiin samaan esitykseen alkulukujen tulona.

Alkutekijäesityksen yksikäsitteisyyden todistus käyttää seuraavaa tulosta, joka on Luvussa 2.4 todistetun Gaussin lemman erikoistapaus.

Lemma 3.9 (Eukleideen lemma)**.** *(1) Olkoon p alkuluku ja olkoot $a, b \in \mathbb{Z}$. Jos $p \mid (ab)$, niin $p \mid a$ tai $p \mid b$.*

(2) Olkoot $a_i \in \mathbb{Z}$ kaikilla $1 \leqslant i \leqslant n$ ja olkoon p alkuluku. Jos $p \mid (a_1 \cdots a_n)$, niin $p \mid a_i$ jollain $1 \leqslant i \leqslant n$.

Todistus. (1) Jos $p \mid a$, niin väite pätee. Jos $p \nmid a$, niin $\operatorname{syt}(a, p) = 1$, joten väite seuraa Gaussin Lemmasta.[2]

(2) Harjoitustehtävä 3.3. □

[2]Seuraus 2.14(2)

Lause 3.10 (Aritmetiikan peruslause)**.** *Olkoon $n \in \mathbb{N}$, $n \geqslant 2$. On alkuluvut $p_1, \ldots, p_k$, $p_i \neq p_j$ kun $i \neq j$, ja $e_1, \ldots, e_k \in \mathbb{N}$, joille*

$$n = p_1^{e_1} \cdots p_k^{e_k}.$$

Esitys on tekijöiden järjestystä vaille yksikäsitteinen.

Todistus. Olkoon $n \in \mathbb{N}$, $n \geqslant 2$. Lemman 3.7 perusteella n on alkuluku tai alkulukujen tulo. Todistetaan esityksen yksikäsitteisyys induktiolla luvun n suhteen.

Luku $n = 2$ on alkuluku eikä sillä ole muita alkulukutekijöitä kuin 2, joten sen ainoa esitys alkulukujen tulona on $2 = 2$. Siis väite on totta kun $n = 2$.

Oletetaan, että esitys on yksikäsitteinen luvuilla $2, 3, \ldots, n-1$ ja näytetään, myös luvulla n on yksikäsitteinen esitys. Jos n on alkuluku, niin esitys on yksikäsitteinen, koska luvun n ainoa alkutekijä on n.

Voidaan siis olettaa, että n on yhdistetty luku. Oletetaan, että on alkuluvut p_i, q_j ja luvut $e_i, f_j \in \mathbb{N}$, $i = 1, \ldots, k$, $j = 1, \ldots, s$, joille $p_i \neq p_j$ ja $q_i \neq q_j$ kun $i \neq j$ ja

$$n = p_1^{e_1} \cdots p_k^{e_k} = q_1^{f_1} \cdots q_s^{f_s}. \tag{3.2}$$

Koska $p_1 \mid n$, niin Eukleideen lemman perusteella se jakaa jonkin luvuista q_j, $j \in \{1, \ldots, s\}$.

Numeroimalla luvut q_j tarvittaessa uudelleen voidaan olettaa, että $p_1 \mid q_1$. Koska p_1 ja q_1 ovat alkulukuja, niin on $p_1 = q_1$. Jakamalla yhtälön (3.2) molempien puolien lausekkeet luvulla p_1 saadaan

$$\tfrac{n}{p_1} = p_1^{e_1 - 1} \cdots p_k^{e_k} = q_1^{f_1 - 1} \cdots q_s^{f_s}.$$

Koska $p_1 \geqslant 2$ alkulukuna, niin $\frac{n}{p_1} \leqslant n - 1$.

Induktio-oletuksen mukaan luvulla n/p_1 on (järjestystä vailla) yksikäsitteinen esitys alkulukujen tulona. Järjestämällä tarvittaessa luvut p_i ja q_j suuruusjärjestykseen saadaan, että $k = s$, $p_i = q_i$ ja $e_i = f_i$ kaikilla $i = 1, \ldots, k$. Siten luvun $n + 1$ esitys on yksikäsitteinen. Väite seuraa induktioperiaatteesta. □

Huomautus 3.11. Alkutekijäesityksen yksikäsitteisyys on syy siihen, että lukua 1 ei kutsuta alkuluvuksi.

Esimerkki 3.12. Etsitään luvun $n = 156$ alkutekijäesitys. Koska n on parillinen, niin se ei ole alkuluku. Koska

$$12^2 = 144 < 156 < 169 = 13^2,$$

niin on $12 < \sqrt{n} < 13$. Siten luvulla 156 alkutekijä joukossa $\{2, 3, 5, 7, 11\}$. Nyt

$$156 = \begin{cases} 2 \cdot 78 = 2^2 \cdot 39 = 2^2 \cdot 3 \cdot 13 \\ 3 \cdot 52 = 3 \cdot 4 \cdot 13 = 2^2 \cdot 3 \cdot 13. \end{cases}$$

Tekijät 2 ja 3 löytyvät helposti luvun 1.5 jaollisuusääntöjen avulla.

Alkutekijäesityksen avulla voidaan helposti todistaa esimerkiksi luvun $\sqrt{2}$ irrationaalisuus.

Seuraus 3.13. *Olkoot $n, a \in \mathbb{N}$. Jos $\sqrt[n]{a}$ on rationaaliluku, niin $\sqrt[n]{a}$ on luonnollinen luku, erityisesti $a = r^n$ jollain $r \in \mathbb{N}$.*

Todistus. Koska $\sqrt[n]{a}$ on positiivinen rationaaliluku, niin on $r, s \in \mathbb{N}$ joille

$$\sqrt[n]{a} = \frac{r}{s}.$$

Seurauksen 2.10 nojalla voidaan olettaa, että $\text{syt}(r, s) = 1$.[3] Jos olisi $s > 1$, niin olisi alkuluku p, jolle $p \mid s$. Lauseen 1.3 ((3)) nojalla p jakaisi tulon $as^n = r^n$. Siten Eukleideen lemman perusteella $p \mid r$. Tämä on mahdotonta, sillä $\text{syt}(r, s) = 1$ ja p on alkuluku. On siis $s = 1$ ja siten $\sqrt[n]{a} = r$. □

Alkutekijäesityksessä kannattaa joskus sallia alkulukujen potenssina myös 0. Tästä on hyötyä suurimman yhteisen tekijän käsittelyssä.

Lause 3.14. *Olkoot $p_1, p_2, \ldots, p_r$ eri alkulukuja ja olkoot*

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \quad ja \quad b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$$

joillain $e_1, \ldots, e_r, f_1, \ldots, f_r \in \mathbb{N}$. Tällöin

$$\text{syt}(a, b) = p_1^{\min\{e_1, f_1\}} p_2^{\min\{e_2, f_2\}} \cdots p_r^{\min\{e_r, f_r\}}$$

ja

$$\text{pyj}(a, b) = p_1^{\max\{e_1, f_1\}} p_2^{\max\{e_2, f_2\}} \cdots p_r^{\max\{e_r, f_r\}}.$$

Todistus. Harjoitustehtävä 3.14 □

3.3 Alkulukujen joukko on ääretön

Tässä luvussa tutkitaan, kuinka paljon alkulukuja on ja kuinka ne sijoittuvat luonnollisten lukujen joukkoon.

Lause 3.15 (Eukleideen lause)**.** *Alkulukuja on äärettömän monta.*

Todistus. Näytetään, että minkä tahansa äärellisen alkulukujoukon ulkopuolella on alkuluku.

Olkoot $p_1, \ldots, p_n$ alkulukuja. Näytetään, että on alkuluku, joka ei ole mikään luvuista $p_1, \ldots, p_n$. Olkoon

$$N = p_1 \cdots p_n + 1.$$

Nyt $N \in \mathbb{N}$ ja $N > 2$, joten se on Lemman 3.7 mukaan joko alkuluku tai alkulukujen tulo.

Jos N on alkuluku, niin se on alkuluku, jolle $N > p_i$ kaikilla $1, 2, \ldots, n$. Jos N ei ole alkuluku, niin Lemman 3.7 mukaan on alkuluku q, jolle $q \mid N$. Jos $q = p_i$ jollain i, niin Lauseen 1.3 ((3)) perusteella q jakaisi luvun $N - p_1 \cdots p_n = 1$, mikä on mahdotonta. Siis $q \neq p_i$ kaikilla $i = 1, \ldots, n$, joten q on etsitty alkuluku. □

Huomautus 3.16. (1) Jos luvut p_i ovat n ensimmäistä alkulukua, niin Eukleideen lauseen todistus antaa suurinta lukua p_n isomman alkuluvun.

[3] Supistetaan mahdolliset yhteiset tekijät.

(2) Luku $N = p_1 \cdots p_n + 1$ ei välttämättä ole alkuluku. Jos 2 ei ole alkulukujen $p_1, p_2, \ldots, p_n$ joukossa, niin tulo $p_1 \cdots p_n$ on pariton. Tällöin $N = p_1 \cdots p_n + 1 > 2$ on parillinen eikä siten ole alkuluku. Esimerkiksi, jos aloitamme kahdella alkuluvulla $p_1 = 3$ ja $p_2 = 5$, niin

$$N = 3 \cdot 5 + 1 = 16 = 2^4.$$

Luvun N alkutekijä 2 on joukkoon $\{p_1, p_2\}$ kuulumaton alkuluku.

Eukleideen lauseen nojalla alkulukujen joukko on luonnollisten lukujen joukon ääretön osajoukko. Se on siis numeroituva ja luvut ovat luonnollisessa suuruusjärjestyksessä. Otamme käyttöön merkinnän, joka ei ole yleisesti käytössä.

Olkoon $\mathbf{p}_k$ k:s alkuluku kasvavassa suuruusjärjestyksessä.

Seuraava tulos antaa karkean ylärajan luvulle $\mathbf{p}_n$.

Lause 3.17. *Olkoon $n \in \mathbb{N}$. Tällöin $\mathbf{p}_n \leqslant 2^{2^{n-1}}$.*

Todistus. Todistetaan induktiolla luvun n suhteen.
(1) Kun $n = 1$, niin $\mathbf{p}_1 = 2 = 2^{2^0}$.
(2) Oletetaan, että arvio on totta alkuluvuille $\mathbf{p}_1, \ldots, \mathbf{p}_n$. Kuten Lauseen 3.15 todistuksessa huomataan, että luvulla

$$N = \mathbf{p}_1 \cdots \mathbf{p}_n + 1$$

on alkutekijä p ja että $p \neq \mathbf{p}_i$ kaikilla $i = 1, \ldots, n$. Koska alkuluku p ei ole n:n ensimmäisen alkuluvun joukossa, niin $\mathbf{p}_{n+1} \leqslant p$. Lausetta 1.3 (9), induktio-oletusta[4] ja geometrisen summan kaavaa käyttämällä saadaan

$$\begin{aligned} \mathbf{p}_{n+1} \leqslant p \leqslant \mathbf{p}_1 \cdots \mathbf{p}_n + 1 &\leqslant 2^{2^0} \cdot 2^{2^1} \cdots 2^{2^{n-1}} + 1 \\ &= 2^{1+2+4+\cdots+2^{n-1}} + 1 = 2^{2^n - 1} + 1 \\ &= \frac{1}{2} \cdot 2^{2^n} + 1 \leqslant 2^{2^n}. \end{aligned}$$

Induktioperiaatteen noijalla väite on totta kaikille $n \in \mathbb{N}$. □

Esimerkki 3.18. Edellisen lauseen arvio ei vaikuta kovin tarkalta: $3 = \mathbf{p}_2 \leqslant 2^{2^1} = 4$, $5 = \mathbf{p}_3 \leqslant 2^{2^2} = 2^4 = 16$, $7 = \mathbf{p}_4 \leqslant 2^{2^3} = 2^8 = 256$.

3.4 Alkulukulause

Funktio $\boldsymbol{\pi}\colon [0, \infty) \to \mathbb{N}$,

$$\boldsymbol{\pi}(x) = \#\{p : p \text{ on alkuluku, } p \leqslant x\},$$

on *alkulukujen lukumääräfunktio.*[a]

[a] Alkulukujen lukumääräfunktiota on tapana merkitä kreikkalaisella kirjaimella π. Reaalilukuun π sekoittamisen välttämiseksi käytämme hieman poikkeavaa merkintätapaa.

[4] $\mathbf{p}_i \leqslant 2^{2^{i-1}}$ kaikilla $i = 1, \ldots, n$

Esimerkki 3.19. (1) $\boldsymbol{\pi}(1) = 0$, $\boldsymbol{\pi}(2) = 1$, $\boldsymbol{\pi}(7) = 4$ (alkuluvut $2, 3, 5$ ja 7 ovat pienempiä tai yhtäsuuria kuin luku 7) ja $\boldsymbol{\pi}(7,5) = 4$.

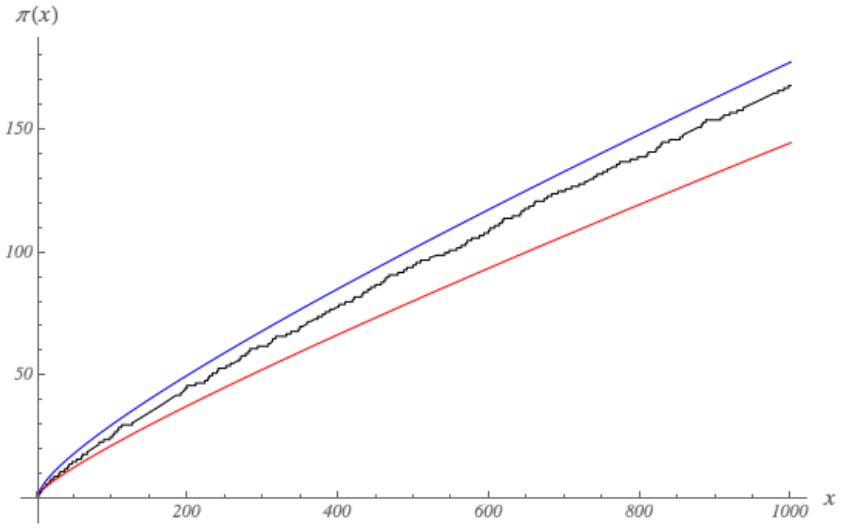
(2) $\boldsymbol{\pi}(\mathbf{p}_n) = n$.

Kuvassa 3.1 havainnollistettujen kokeilujen pohjalta oli arveltu jo pitkään, että arvoa $\boldsymbol{\pi}(x)$ voi arvioida melko hyvin luvulla $\frac{x}{\log x}$. Tämä pitääkin paikkansa. Itse asiassa seuraavan määritelmän funktio antaa tarkemman arvion.

Funktio $\mathrm{Li}\colon [2,\infty[\to \mathbb{R}$,

$$\mathrm{Li}(x) = \int_2^x \log t \, dt$$

on *(siirretty) logaritmin integraalifunktio.*



Kuva 3.1 — Funktioiden π (mustalla) , Li (sinisellä) ja $x \mapsto \frac{x}{\log x}$ (punaisella) kuvaajat välillä $[2, 1000]$.

Hadamard[5] ja de la Vallée Poussin[6] todistivat toisistaan riippumatta vuonna 1896 seuraavan vaativan tuloksen:

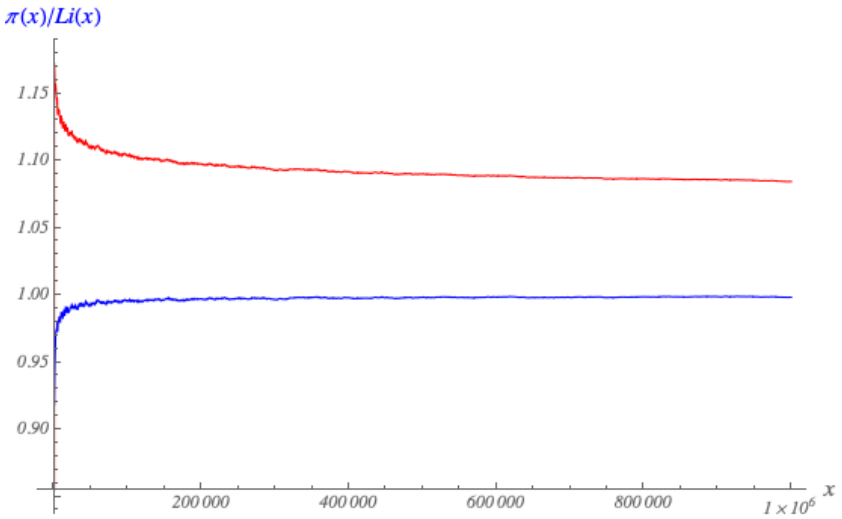
Lause 3.20 (Alkulukulause)**.**

$$\lim_{x\to\infty} \frac{\boldsymbol{\pi}(x)}{\mathrm{Li}(x)} = \lim_{x\to\infty} \frac{\log x}{x}\, \boldsymbol{\pi}(x) = 1\,.$$

Todistus. Katso esimerkiksi [Apo, Luku 13]. □

Kuva 3.2 havainnollistaa sitä, että logaritmin integraalifunktio Li antaa erittäin hyvän arvion funktiolle $\boldsymbol{\pi}$. Sen sijaan funktiolla $x \mapsto \frac{x}{\log x}$ tehtävän arvion virhe on suurempi.

[5] Jacques Hadamard (1865-1963).
[6] Charles de la Vallée Poussin (1866-1962).



Kuva 3.2 — Funktioiden $\frac{\pi(x)}{\mathrm{Li}(x)}$ (sinisellä) , $\frac{\log x}{x}\,\boldsymbol{\pi}(x)$ (punaisella) kuvaajat välillä $[2, 10^6]$.

Alkulukujen *esiintymistiheys* välillä $[0, x]$ on $\dfrac{\boldsymbol{\pi}(x)}{x}$.

Koska alkulukuja on äärettömän monta, niin $\boldsymbol{\pi}(x) \to \infty$ kun $x \to \infty$. Alkulukulauseen nojalla alkulukujen tiheys $\boldsymbol{\pi}(x)/x$ lähestyy nollaa kun x lähestyy ääretöntä mutta suppeneminen on melko hidasta kuten alla oleva taulukkokin havainnollistaa.

x	10	100	1000	10000	100000	10^6	$\cdots$	10^{13}
$\boldsymbol{\pi}(x)$	4	25	168	1229	9592	78498	$\cdots$	346065536839
$\frac{\pi(x)}{x}$	0.4	0.25	0.17	0.12	0, 096	0.078	$\cdots$	0.035

.

3.5 Alkuluvut aritmeettisissa jonoissa

Olkoot $a, b \in \mathbb{Z}$ ja olkoon $c_k^{a,b} = a + kb$ jokaisella $k \in \mathbb{N}$. Jono $c^{a,b} = (c_k^{a,b})_{k=0}^{\infty}$ on *aritmeettinen jono*.

Esimerkki 3.21. (1) Aritmeettisessa jono $c^{1,2}$ koostuu parittomista luonnollisista luvuista. Se sisältää äärettömän monta alkulukua, koska 2 on ainoa parillinen alkuluku.

(2) Kaikki lukua 2 suuremmat alkuluvut ovat muotoa $4k + 1$ tai $4k + 3$. Lukua 100 pienemmistä 24 parittomasta alkuluvusta alkuluvut $5, 13, 17, 29, 37, 41, 53, 61, 73, 89$ ja 97 (11 kappaletta) ovat muotoa $4k+1$ ja luvut $3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79$ ja 83 (13 kappaletta) ovat muotoa $4k + 3$. Tämän pienen otoksen nojalla vaikuttaisi uskottavalta, että molempia tyyppejä on äärettömän monta. Seuraavat tulokset osoittavat, että näin todella on.

Lause 3.22. *Muotoa*

$$4n + 3, \quad n \in \mathbb{N},$$

olevia alkulukuja on äärettömän monta.

Todistus. Olkoot $p_1, \ldots, p_k$ muotoa $4n + 3$ olevia alkulukuja, $n \geqslant 1$, ja olkoon

$$N = 4p_1 \cdots p_k + 3.$$

Luku N on muotoa $4n + 3$. Se ei ole jaollinen millään luvuista p_i, $i = 1, \ldots, k$, koska $p_i \mid 4p_1 \cdots p_k$ mutta $p_i \nmid 3$. Lisäksi N ei ole jaollinen alkuluvuilla 2 samasta syystä ja N ei ole jaollinen alkuluvulla 3, koska Eukleideen lemman[7] nojalla $3 \nmid 4p_1 \cdots p_k$.

Lauseen 3.10 nojalla $N = q_1 \cdots q_s$ joillain alkuluvuilla $q_1, \ldots, q_s$. Näytetään, että jokin luvun N alkutekijöistä q_i on muotoa $4n + 3$. Jakoyhtälön perusteella kaikilla $i = 1, \ldots, s$ on $n_i, r_i \in \mathbb{Z}$, joille

$$q_i = 4n_i + r_i \quad \text{ja} \quad 0 \leqslant r_i \leqslant 3.$$

Koska $2 \nmid N$, niin r_i ei voi olla 0 eikä 2. Jos olisi $r_i = 1$ kaikilla $i = 1, \ldots s$, niin N olisi muotoa $4n + 1$ olevien lukujen tulona myös muotoa $4n + 1$. Siis $q_i = 4n_i + 3$ jollain $i = 1, \ldots s$. Koska luvut $p_1, \ldots p_k$ eivät ole luvun N tekijöitä, niin q_i ei ole mikään luvuista p_i. Lisäksi $q_i \neq 3$, sillä muuten N olisi jaollinen luvulla 3 vastoin oletusta. □

Harjoitustehtävissä huomaamme, että samalla menetelmällä voidaan osoittaa, että monissa muissakin aritmeettisissa jonoissa on äärettömän monta alkulukua.

Esimerkki 3.23. Lauseen 3.22 todistuksen idea ei toimi, jos yritetään näyttää, että muotoa $4n + 1$ olevia alkulukuja on äärettömän monta: jos

$$N = 4p_1 \cdots p_k + 1$$

ja käytetään jakoyhtälöä luvun N alkutekijöihin, niin ei voida päätellä, että jokin tekijöistä olisi muotoa $4n + 1$. Esimerkiksi luku $21 = 3 \cdot 7 = 4 \cdot 5 + 1$ on muotoa $4n + 1$, mutta sen alkutekijät 3 ja $7 = 1 \cdot 4 + 3$ eivät ole muotoa $4n + 1$.

Yleisen aritmeettisen jonon tapauksen tarkastelu on haastava tehtävä. On selvää, että jonossa $c^{a,k}$ voi olla äärettömän monta alkulukua vain, jos $\operatorname{syt}(a, b) = 1$. Dirichlet[8] osoitti vuonna 1837, että tämä ehto on riittävä. Todistus käyttää edistyneitä analyyttisen lukuteorian menetelmiä, jotka eivät ole tällä kurssilla käytettävissä.

Lause 3.24 (Dirichlet'n lause alkuluvuista aritmeettisissa jonoissa)**.** *Jos $a, b \in \mathbb{Z}$, $a > 0$ ja $\operatorname{syt}(a, b) = 1$, niin muotoa*

$$p = an + b, \quad n \in \mathbb{N}$$

olevia alkulukuja on äärettömän monta.

Todistus. Katso esimerkiksi [Apo, Luku 7]. □

[7] Lemma 3.9.

[8] Gustav Lejeune Dirichlet (1805-1859).

Harjoitustehtäviä

3.1. Tee Eratostheneen seula luvuille $1 - 100$.

3.2. Tee Eratostheneen seula luvuille $101 - 200$.

3.3. Todista Lemma 3.9(2).

3.4. Olkoot $p_1, p_2, \ldots, p_r$ eri alkulukuja. Olkoon $n \in \mathbb{Z}$ kokonaisluku, jolle $p_k \mid n$ kaikilla $1 \leqslant k \leqslant r$. Osoita, että $p_1 p_2 \cdots p_r \mid n$.[9]

3.5. Määritä lukujen 117 ja 1005 alkutekijäesitykset.[10]

3.6. Muodosta luvun 158015 alkutekijäesitys.

3.7. Määritä luvun 22599 alkutekijäesitys.

3.8. Muodosta luvun 10573 alkutekijäesitys.[11]

3.9. Muodosta luvun 111111 alkutekijäesitys.

3.10. Luvut $3, 5$ ja 7 ovat muotoa $p, p+2, p+4$ oleva alkulukukolmikko. Miksi ei ole alkulukua $p > 3$, jolle luvut p, $p+2$ ja $p+4$ ovat alkulukuja? [12]

3.11. Montako muotoa $p = n^2 - 1$, $n \in \mathbb{N}$, olevaa alkulukua on?

3.12. Olkoon $p > 3$ alkuluku. Voiko $p^2 + 2$ olla alkuluku? [13]

3.13. Olkoon $p \geqslant 5$ alkuluku. Osoita, että $12 \mid (p^2 - 1)$.

3.14. Todista Lause 3.14.

3.15. Eukleideen lauseen todistuksessa haettiin alkulukujoukon $\{p_1, p_2, \ldots, p_n\}$ ulkopuolella olevaa alkulukua määrittelemällä

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

Etsi tällä menetelmällä alkulukuja aloittaen joukosta $\{2\}$. Jatka, kunnes olet löytänyt viisi uutta alkulukua.

3.16. Olkoon $n = 3k + 2 \in \mathbb{N} - \{0, 1\}$. Osoita, että luvun n alkutekijäesityksessä on ainakin yksi alkuluku p, jolle $p = 3a + 2$ jollain $a \in \mathbb{N}$.

3.17. Osoita, että joukossa $J = \{6k - 1 : k \in \mathbb{N}\}$ on äärettömän monta alkulukua.

3.18. Osoita, että joukossa $J = \{3k + 2 : k \in \mathbb{N}\}$ on äärettömän monta alkulukua.[14]

3.19. Olkoon $n \in \mathbb{N}$, $n \geqslant 2$, luku, joka jakaa luvun $(n-1)! + 1$. Osoita, että n on alkuluku.

3.20. Olkoon $n \in \mathbb{N}$, $n \geqslant 5$ yhdistetty luku. Osoita, että $n \mid (n-1)!$. Mitä tapahtuu, jos n on alkuluku?

[9] Seuraus 2.14(1) ja induktio.
[10] Joitain tekijöitä pitäisi nähdä vain katsomalla näitä lukuja...
[11] Tällä luvulla ei ole kovin pieniä alkutekijöitä.
[12] Tarkastele jakojäännöksiä sopivalla jakajalla.
[13] Tarkastele jaollisuutta luvulla 3.
[14] Miksi tämä tehtävä on tässä kohdassa?

3.21. Olkoon $n \in \mathbb{N} - \{0\}$. Osoita, että luvulla $n! + 1$ on alkutekijä p, jolle pätee $p > n$. Todista Lause 3.15 tämän havainnon avulla.

3.22. [15] Todista Lause 2.22.

3.23. Määritä luvut $\text{syt}(34086, 14630)$ ja $\text{pyj}(34086, 14630)$.

3.24. Määritä luvut $\text{syt}(11662, 95795)$ ja $\text{pyj}(11662, 95795)$.

[15] Lause 3.14

Luku 4

Ratkaistuja ja ratkaisemattomia kysymyksiä alkuluvuista

Landau[1] esitti vuonna 1912 kansainvälisessä matemaatikoiden kongressissa[2] neljä täsmällisesti muotoiltua lukuteorian ongelmaa, joiden ratkaisujen hän arvioi olevan saavuttamattomissa matematiikan tutkimuksen sen aikaisilla tunnetuilla menetelmillä.[3] Kaikki Landaun ongelmat ovat edelleen ratkaisemattomia talvella 2023. Tarkastelemme tässä luvussa lyhyesti Landaun ongelmia ja niiden lisäksi Mersennen alkulukuja ja täydellisiä lukuja koskevia ratkaisemattomia kysymyksiä.

4.1 Alkulukujen välissä olevista aukoista

Koska alkulukuja on melko harvassa suureten lukujen joukossa, joidenkin peräkkäisten alkulukujen välien tulee olla suuria.

Lause 4.1. *Kaikille $n \in \mathbb{N}$, $n \geqslant 2$, on $n-1$ peräkkäistä luonnollista lukua, joista mikään ei ole alkuluku.*

Todistus. Olkoon $n \in \mathbb{N}$, $n \geqslant 2$. Peräkkäisiä lukuja

$$n! + 2, n! + 3, \ldots, n! + n$$

on $n-1$ kappaletta. Nyt

$$n! + 2 = 2 \cdot 3 \cdots n + 2 = 2(3 \cdots n + 1)$$

on jaollinen luvulla 2,

$$n! + 3 = 2 \cdot 3 \cdots n + 3 = 3(2 \cdot 4 \cdots n + 1)$$

[1] Edmund Landau (1877-1938).
[2] International Congress of Mathematicians eli ICM
[3] Katso [Lan1, sivu 105]

on jaollinen luvulla 3, ja yleisesti

$$n! + i = 2 \cdot 3 \cdots n + i = i(2 \cdots (i-1)(i+1) \cdots n + 1)$$

on jaollinen luvulla i, $i = 2, 3 \ldots, n$. Siten mikään luvuista $n! + 2, n! + 3, \ldots, n! + n$ ei ole alkuluku. □

Koska 2 on ainoa parillinen alkuluku, ainoat peräkkäiset luonnolliset luvut, jotka ovat molemmat alkulukuja, ovat 2 ja 3. Mutta muita kahden peräkkäisen alkuluvun välejä esiintyy enemmän ja tämä on johtanut seuraavaan määritelmään. Kahden peräkkäisen lukua 2 suuremman alkuluvun erotus on aina parillinen, koska muuten toinen luvuista olisi parillinen.

Jos p ja $p + 2$ ovat alkulukuja, niin ne ovat *alkulukukaksosia*.
Jos p ja $p + 4$ ovat alkulukuja, niin ne ovat *alkulukuserkuksia*.

Esimerkki 4.2. (1) Alkulukukaksosia ovat esimerkiksi $(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)$ ja $(29, 31)$. Harjoitustehtävän 3.10 nojalla luku 5 on ainoa alkuluku, joka on kahdessa alkulukukaksosparissa.

(2) Alkulukuserkuksia ovat esimerkiksi $(3, 7)$, $(7, 11)$ ja $(13, 17)$.

(3) Suurin tunnettu alkulukukaksospari $2996863034895 \cdot 2^{1290000} \pm 1$ löydettiin syyskuussa 2016, katso [Cal].

Avoin kysymys 4.3 (Alkulukukaksosotaksuma)**.** *Onko alkulukukaksosia äärettömän monta?*

Yleisesti uskotaan, että alkulukukaksosia on äärettömän monta. Tämän vuoksi väitettä *alkulukukaksosia on äärettömän monta* kutsutaan alkulukuotaksumaksi eli alkulukukonjektuuriksi. Otaksumalla eli konjektuurilla tarkoitetaan todistamatonta väitettä, jonka uskotaan pitävän paikkansa esimerkiksi ahkeran kokeilemisen perusteella. Toinenkin Landaun kysymys käsittee alkulukujen välissä olevia lukuja:

Avoin kysymys 4.4 (Legendren otaksuma)**.** [4] *Onko lukujen n^2 ja $(n+1)^2$ välissä alkuluku kaikilla $n \in \mathbb{N}$?*

Tätä kysymystä on helppo tarkastella pienillä luvuilla. Yhtään vastaesimerkkiä ole löydetty vaikka kysymys on tarkastettu ainakin lukuun $n = 2 \cdot 10^9$ saakka. Kysymys on edelleen ratkaisematon.

4.2 Goldbachin otaksuma

Avoin kysymys 4.5 (Goldbachin otaksuma)**.** *Onko jokainen parillinen kokonaisluku $n \geqslant 4$ kahden alkuluvun summa?*

[4] Adrien-Marie Legendre (1752-1833).

Tämä kysymys esiintyy Goldbachin[5] kirjeessä Eulerille[6] vuonna 1742. Pienille parillisille luvuille on helppo löytää esitys kahden alkuluvun summana: $4 = 2+2$, $6 = 3+3$, $8 = 3+5$, $10 = 3+7$, ... Toisaalta väite ei selvästi päde ilman parillisuusehtoa: 11 ei ole kahden alkuluvun summa. Tiedetään, että kaikki parilliset luvut, jotka ovat pienempiä kuin $n < 4 \cdot 10^{18}$ ovat kahden alkuluvun summia. Helfgott[7] on toistaiseksi julkaisemattomassa käsikirjoituksessa todistanut *heikon Goldbachin konjektuurin*, jonka mukaan kaikki parittomat luvut $n \geqslant 7$ voidaan esittää kolmen alkuluvun summana.

4.3 Fermat'n luvut ja n^2+1-otaksuma

Olkoon $n \in \mathbb{N}$. Luku

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

on n:s *Fermat'n luku.*

Jos Fermat'n luku on alkuluku, niin se on *Fermat'n alkuluku.*

Fermat huomasi, että luvut

$$\begin{aligned} F_0 &= 2^1 + 1 = 3\,, \\ F_1 &= 2^2 + 1 = 5\,, \\ F_2 &= 2^4 + 1 = 17\,, \\ F_3 &= 2^8 + 1 = 257 \quad \text{ja} \\ F_4 &= 2^{16} + 1 = 65537 \end{aligned}$$

ovat alkulukuja. Tästä hän ajatteli keksineensä kaavan, joka tuottaa alkulukuja. Fermat esitti vuonna 1640 otaksuman eli, että kaikki luvut F_n ovat alkulukuja, kun $n \in \mathbb{N}$. Euler osoitti vuonna 1732, että

$$F_5 = 4294967297 = 641 \cdot 6700417\,.$$

Myöhemmin alkutekijäesitys on löydetty luvuille $F_5, \ldots, F_{11}$ ja lisäksi F_n on osoitettu yhdistetyksi luvuksi monilla muilla luvun n arvoilla, esimerkikisi, kun $5 \leqslant n \leqslant 32$.

Lemma 4.6. *Kaikille $m \in \mathbb{N} - \{0\}$ pätee $F_m = F_0 \cdot F_1 \cdots F_{m-1} + 2$.*

Todistus. Huomataan ensin, että $F_1 = 5 = 3 + 2 = F_0 + 2$. Oletetaan, että Väite pätee luvulle F_m. Tällöin

$$F_0 \cdot F_1 \cdots F_{m-1} F_m = (F_m - 2)F_m = (2^{2^m} - 1)(2^{2^m} + 1) = 2^{2^{m+1}} - 1 = F_{m+1} - 2\,.$$

Väite seuraa induktioperiaatteesta. □

Avoin kysymys 4.7. *Onko F_n yhdistetty luku kaikilla $n > 4$? Onko Fermat'n alkulukuja äärettömän monta, entä yhdistettyjä Fermat'n lukuja?*

[5] Christian Goldbach (1690-1764).
[6] Leonhard Euler (1707-1783).
[7] Harald Andrés Helfgott (1977-).

Melko yleisesti uskotaan, että kaikki Fermat'n alkuluvut tunnetaan jo. Olipa Fermat'n alkulukuja äärettömän monta tai ei, niin Fermat'n lukujen alkutekijöitä on äärettömän monta.

Lause 4.8. *Jos $n \neq m$, niin* $\operatorname{syt}(F_n, F_m) = 1$.

Todistus. Oletetaan, että $m < n$. Lemman 4.6 nojalla $F_n = F_0 \cdot F_1 \cdots F_m \cdots F_{n-1} + 2$. Olkoon d luvun F_m tekijä. Tällöin $d \neq 2$, joten joko $d \nmid 2$ tai $d = \pm 1$. Lauseen 1.3(3) nojalla[8] d ei ole luvun F_n tekijä, jos $d \neq 1$. □

Huomautus 4.9. Lauseen 4.8 perusteella mikä tahansa ääretön joukko Fermat'n lukuja antaa äärettömän monta alkulukua. Tämä antaa uuden todistuksen Eukleideen lauseelle 3.15.

Yksi Landaun ongelmista oli Fermat'n lukuja koskevan kysymyksen yleisempi versio:

Avoin kysymys 4.10 ((n^2+1)-konjektuuri)**.** *Onko muotoa n^2+1, $n \in \mathbb{N}$, olevia alkulukuja äärettömän monta?*

H. Iwaniec[9] osoitti vuonna 1978, että on äärettömän monta lukua $n \in \mathbb{N}$, joille $n^2 + 1$ on alkuluku tai kahden alkuluvun tulo.

4.4 Mersennen luvut

Olkoon p alkuluku. Luku $M_p = 2^p - 1$ on *Mersennen luku.*
Jos M_p on alkuluku, niin se on *Mersennen alkuluku.*

Lauseen 3.5 perusteella luku $2^n - 1$ voi olla alkuluku vain jos p on alkuluku. Ensimmäiset Mersennen luvut

$$\begin{aligned} M_2 &= 2^2 - 1 = 3\,, \\ M_3 &= 2^3 - 1 = 7\,, \\ M_5 &= 2^5 - 1 = 31 \quad \text{ja} \\ M_7 &= 2^7 - 1 = 127 \end{aligned}$$

ovat alkulukuja, mutta

$$M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$$

ei ole alkuluku.

Avoin kysymys 4.11. *Onko Mersennen alkulukuja äärettömän monta?*

Tämä kysymys ei ollut mukana Landaun listassa mutta kysymys muistuttaa Fermat'n lukujen äärettömyyskysymystä, joten sitä on luontevaa käsitellä tässä yhteydessä. Mersennen alkulukuja on löydetty 51 kpl. Suurin näistä on suurin tunnettu alkuluku $M_{82589933}$, joka löydettiin joulukuussa 2018. Vuoden 2022 loppuun mennessä kaikki eksponentit, jotka ovat korkeintaan $111 \cdot 10^6$ on tarkastettu ainakin kerran ja laskut esponenttiin $62 \cdot 10^6$ saakka on varmennettu, katso [GIM].

[8] Katso Harjoitustehtävä 1.12.
[9] Henryk Iwaniec (1947-).

Mersennen lukujen alkulukutestaukseen on tehokkaita testejä. Siksi suurimmat tunnetut alkuluvut ovat Mersennen alkulukuja.

Harjoitustehtäviä

4.1. Osoita yhtälöiden $641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$ avulla, että $2^{32} = 641k - 1$ jollain $k \in \mathbb{N}$.[10]

4.2. Olkoon $n \geqslant 2$. Osoita, että Fermat'n luvun F_n viimeinen numero on 7.

4.3. Olkoot p ja q alkulukuja, $p \neq q$. Määritä $\operatorname{syt}(M_p, M_q)$.

[10]Huomaa, että $2^{32} = 2^4 \cdot 2^{28}$. Käytä luvun 641 molempia esityksiä.

Luku 5

Kongruenssi

Tässä luvussa määriteltävä *kongruenssi* antaa keinon jaollisuutta ja erityisesti jakojäännöksiä käsittelevien kysymysten tarkasteluun. Todistamme Fermat'n pienen lauseen[1] ja sovellamme kongruenssia kokonaislukukertoimisen polynomin juurten tarkasteluun.

5.1 Kongruenssi

Olkoon $m \in \mathbb{N}$, $m \geqslant 1$. Kokonaisluvut $a \in \mathbb{Z}$ ja $b \in \mathbb{Z}$ ovat *kongruentteja luvun m suhteen* tai *kongruentteja modulo m*, jos $m \mid (b - a)$. Tällöin merkitään $a \equiv b \mod m$.
Luku m on kongruenssin *moduli*.

Koska 1 jakaa minkä tahansa kokonaisluvun, kaikille $a, b \in \mathbb{Z}$ pätee $a \equiv b \mod 1$. Sallimme kuitenkin luvun 1 kongruenssin määritelmässä, koska vältymme erikoistapausten listaamisesta esimerkiksi Lemmassa 5.8. Käytännössä olemme kuitenkin kiinnostuneita ainoastaan tapauksista, joissa $m \geqslant 2$.

Lemma 5.1. *Olkoon $m \in \mathbb{N} - \{0\}$. Tällöin*

(1) $a \equiv a \mod m$ *kaikilla* $a \in \mathbb{Z}$.

(2) Jos $a \equiv b \mod m$, *niin* $b \equiv a \mod m$

(3) Jos $a \equiv b \mod m$ *ja* $b \equiv c \mod m$, *niin* $a \equiv c \mod m$.

Todistus. Harjoitustehtävä 5.1. □

Olkoon A epätyhjä joukko. Joukon $A \times A$ osajoukko on *relaatio* joukossa A.
Relaatio $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : a \equiv b \mod m\}$ on *kongruenssi modulo* m.[a]

[a] Lemman 5.1 nojalla kongruenssi on *ekvivalenssirelaatio*. Tällä kurssilla emme käsittele (ekvivalenssi)relaatioiden yleistä teoriaa.

[1] Lause 5.23

Esimerkki 5.2. (1) $1 \equiv 6 \mod 5$, $1 \equiv -1 \mod 2$, $8 \equiv 5 \mod 3$,
(2) Kokonaisluku n on parillinen jos ja vain jos $n \equiv 0 \mod 2$ ja pariton jos ja vain jos $n \equiv 1 \mod 2$,

Lemma 5.3. *Olkoon $m \in \mathbb{N}$, $m \geqslant 1$ ja olkoot $a, b \in \mathbb{Z}$.*
(1) Jos $a \equiv b \mod m$ ja $d \mid m$, niin $a \equiv b \mod d$.
(2) Jos $a \equiv r \mod m$ ja $0 \leqslant r < m$, niin $a = qm + r$ jollain $q \in \mathbb{Z}$.
(3) $a \equiv 0 \mod m$, jos ja vain jos $m \mid a$.
(4) Jos $a \equiv b \mod m$ ja $c \in \mathbb{N} - \{0\}$, niin $ac \equiv bc \mod mc$

Todistus. (1) Jos $a \equiv b \mod m$, niin $m \mid (b-a)$. Koska lisäksi $d \mid m$, niin Lauseen 1.3(2) nojalla $d \mid (b-a)$, joten $a \equiv b \mod d$.
Kohdat (2) ja (3) seuraavat suoraan kongruenssin määritelmästä.
(4) Jos $a \equiv b \mod m$, niin $m \mid (a-b)$. Siis $a - b = mk$ jollain $k \in \mathbb{Z}$. Tällöin

$$ca - cb = c(a-b) = (cm)k\,,$$

joten $cm \mid (ca - cb)$. Siis $ca \equiv cb \mod cm$. □

Seuraava lause kertoo kongruenssin yhteensopivuudesta yhteenlaskun ja kertolaskun kanssa.

Lause 5.4 (Laskusäännöt)**.** *Olkoon $n \in \mathbb{N}$, $n \geqslant 1$ ja olkoot $a, b, c, d, x, y \in \mathbb{Z}$. Tällöin*

(1) jos $a \equiv b \mod n$ ja $c \equiv d \mod n$, niin $ax + cy \equiv bx + dy \mod n$,

(2) jos $a \equiv b \mod n$ ja $c \equiv d \mod n$, niin $ac \equiv bd \mod n$,

(3) jos $a \equiv b \mod n$, niin $a^m \equiv b^m \mod n$ kaikilla $m \in \mathbb{N}$.

Todistus. Oletuksen mukaan kohdissa (1) ja (2) $n \mid (b-a)$ ja $n \mid (d-c)$.
(1) Lauseen 1.3(3) nojalla n jakaa luvun

$$x(b-a) + y(d-c) = (bx + dy) - (ax + cy).$$

Siten $ax + cy \equiv bx + dy \mod n$.
(2) Lauseen 1.3(3) nojalla n jakaa luvun

$$(b-a)c + (d-c)b = bc - ac + bd - bc = bd - ac.$$

Siten $ac \equiv bd \mod n$.
(3) Todistetaan väite induktiolla eksponentin m suhteen. Jos $m = 1$, niin väite on sama kuin oletus. Oletetaan, että $a^m \equiv b^m \mod n$. Valitsemalla kohdassa ((2)) $c = a^m$ ja $d = b^m$, saadaan $aa^m \equiv bb^m \mod n$ eli $a^{m+1} \equiv b^{m+1} \mod n$. Induktioperiaatteen nojalla väite on totta kaikilla $m \in \mathbb{N}$. □

Seuraus 5.5. *Olkoon $m \in \mathbb{N}$, $m \geqslant 1$ ja olkoot $a_i, b_i \in \mathbb{Z}$ siten, että $a_i \equiv b_i \mod n$ kaikilla $i = 1, \ldots, k$. Tällöin*

$$\sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i \mod n \quad ja \quad a_1 a_2 \cdots a_k \equiv b_1 b_2 \cdots b_k \mod n\,.$$ □

Esimerkki 5.6. (1) $3^4 = 81 \equiv 1 \mod 10$, joten $3^{400} = (3^4)^{100} \equiv 1^{100} = 1 \mod 10$. Siis luvun 3^{400} viimeinen numero desimaaliesityksessä on 1.
(2) Koska $2 \equiv 5 \mod 3$, niin Lauseen 5.4 perusteella $2^{100} \equiv 5^{100} \mod 3$. Edelleen, Lauseesta 5.4 seuraa, että

$$2^{100} + 5 \equiv 5^{100} + 2 \mod 3.$$

Voimme sieventää lausekkeet kuten kohdassa (1): $2 \equiv -1 \mod 3$, joten

$$2^{100} \equiv (-1)^{100} \equiv 1^{100} \equiv 1 \mod 3\,.$$

Siis $2^{100} + 5 \equiv 6 \equiv 0 \mod 3$.

Lemma 5.7. *Olkoon $n \in \mathbb{N} - \{0\}$ ja olkoot $a, b \in \mathbb{Z}$ siten, että $a \equiv b \mod n$. Tällöin* $\operatorname{syt}(a, n) = \operatorname{syt}(b, n)$.

Todistus. Harjoitustehtävä 5.7. □

Kongruenssi ei yleensä ole yhteensopiva jakolaskun kanssa. Esimerkiksi $14 \equiv 8 \mod 6$, mutta $7 \not\equiv 4 \mod 6$. Lukua 2 ei siis voi supistaa pois. Seuraava tulos kertoo, milloin kongruenssi on yhteensopiva supistamisen kanssa.

Lause 5.8 (Supistussääntö)**.** *Olkoon $n \in \mathbb{N} - \{0\}$ ja olkoot $a, b, c \in \mathbb{Z}$. Tällöin $ac \equiv bc \mod n$, jos ja vain jos $a \equiv b \mod \frac{n}{\operatorname{syt}(n,c)}$.*

Todistus. Jos $ac \equiv bc \mod n$, niin $n \mid c(b-a)$. Koska $\operatorname{syt}(n, c)$ on lukujen n ja c yhteinen tekijä, saadaan Lauseen 1.3(5) nojalla

$$\frac{n}{\operatorname{syt}(n,c)} \;\Big|\; \frac{c}{\operatorname{syt}(n,c)}(b-a)\,.$$

Seurauksen 2.10 nojalla

$$\operatorname{syt}\left(\frac{n}{\operatorname{syt}(n,c)}, \frac{c}{\operatorname{syt}(n,c)}\right) = 1\,.$$

Gaussin Lemman[2] nojalla $\frac{n}{\operatorname{syt}(n,c)} \mid (b-a)$, joten $a \equiv b \mod \frac{n}{\operatorname{syt}(n,c)}$.

Jos taas $a \equiv b \mod \frac{n}{\operatorname{syt}(n,c)}$, niin Lemman 5.3(4) nojalla $ca \equiv cb \mod n\frac{c}{\operatorname{syt}(n,c)}$. Lemman 5.3(1) nojalla $ca \equiv cb \mod n$, koska $n \mid n\frac{c}{\operatorname{syt}(n,c)}$. □

Seuraus 5.9. *Olkoon $n \in \mathbb{N} - \{0\}$ ja olkoot $a, b, c \in \mathbb{Z}$ lukuja, joille $\operatorname{syt}(n, c) = 1$ ja $ac \equiv bc \mod n$. Tällöin $a \equiv b \mod n$.* □

Esimerkki 5.10. Luvun 2^{400} viimeisen numeron selvittäminen vaatii enemmän työtä kuin Esimerkki 5.6(1), koska $\operatorname{syt}(2, 10) = 2 \neq 1$. Lauseen 5.8 supistussäännön nojalla $2^{400} \equiv 2a \mod 10$, jos ja vain jos $2^{399} \equiv a \mod 5$. Koska $2^4 = 16 \equiv 1 \mod 5$, saadaan

$$2^{399} = 2^{396}2^3 = (2^4)^{99}2^3 \equiv 2^3 = 8 \equiv 3 \mod 5\,.$$

Siis $2^{400} \equiv 2 \cdot 3 = 6 \mod 10$.

Lause 5.11. *Olkoot $m_1, m_2, \ldots, m_r \in \mathbb{N} - \{0\}$ ja olkoot $x, y \in \mathbb{Z}$. Tällöin $x \equiv y \mod m_i$ kaikilla $1 \leqslant i \leqslant r$, jos ja vain jos $x \equiv y \mod \operatorname{pyj}(m_1, \ldots, m_r)$.*

[2]Seuraus 2.14(2)

Todistus. Oletetaan, että $x \equiv y \mod m_i$ kaikilla $1 \leqslant i \leqslant r$. Tällöin $m_i \mid (x-y)$ kaikilla $1 \leqslant i \leqslant r$, joten $x-y$ on lukujen $m_1, \ldots m_r$ yhteinen jaettava. Lauseen 2.20 nojalla $\operatorname{pyj}(m_1, m_2, \ldots, m_r) \mid (x-y)$. Siis $x \equiv y \mod \operatorname{pyj}(m_1, m_2, \ldots, m_r)$.

Oletetaan, että $x \equiv y \mod \operatorname{pyj}(m_1, m_2, \ldots, m_r)$. Yhteisen tekijän määritelmän nojalla $m_i \mid \operatorname{pyj}(m_1, m_2, \ldots, m_r)$ kaikilla $1 \leqslant i \leqslant r$. Lemman 5.3(1) nojalla $x \equiv y \mod m_i$ kaikilla $1 \leqslant i \leqslant r$. □

Seuraus 5.12. *Olkoot $m_1, m_2 \in \mathbb{N} - \{0,1\}$ suhteellisia alkulukuja ja olkoot $x, y \in \mathbb{Z}$. Tällöin $x \equiv y \mod m_1$ ja $x \equiv y \mod m_2$, jos ja vain jos $x \equiv y \mod m_1 m_2$.*

Todistus. Väite seuraa Lemman 2.21 nojalla Lauseesta 5.11. □

Seuraus 5.13. *Olkoot $p_1, p_2, \ldots, p_r$ eri alkulukuja ja olkoot $x, y \in \mathbb{Z}$. Tällöin $x \equiv y \mod p_k$ kaikilla $1 \leqslant k \leqslant r$, jos ja vain jos $x \equiv y \mod p_1 p_2 \cdots p_r$. Erityisesti $p_k \mid x$ kaikilla $1 \leqslant k \leqslant r$, jos ja vain jos $p_1 p_2 \cdots p_r \mid x$.*

Todistus. Väite seuraa Lauseesta 5.11, koska $\operatorname{pyj}(p_1, p_2, \ldots, p_r) = p_1 p_2 \cdots p_r$. □

5.2 Jaollisuussääntöjä kongruenssien avulla

Tässä luvussa palaamme lyhyesti Luvussa 1.5 käsiteltyihin jaollisuusääntöihin ja tarkastelemme niitä kongruenssin avulla.

Lemma 5.14. *Olkoon $n = (a_s a_{s-1} \ldots a_1 a_0)_{10} \in \mathbb{N}$. Tällöin*

(1) $(a_s a_{s-1} \ldots a_1 a_0)_{10} \equiv (a_1 a_0)_{10} \mod 4$.

(2) $(a_s a_{s-1} \ldots a_1 a_0)_{10} \equiv \sum_{k=0}^{s} a_k \mod 9$.

(3) $(a_s a_{s-1} \ldots a_1 a_0)_{10} \equiv \sum_{k=0}^{s} a_k \mod 3$.

(4) $(a_s a_{s-1} \ldots a_1 a_0)_{10} \equiv \sum_{k=0}^{s} (-1)^k a_k \mod 11$.

Todistus. (1) Koska $100 = 25 \cdot 4$ ja $10^k = 10^{k-2} \cdot 100 \equiv 0 \mod 4$ kaikilla $k \in \mathbb{N}$, $k \geqslant 2$, niin Lauseen 5.4 ja Seurauksen 5.5 perusteella on

$$\begin{aligned}(a_s a_{s-1} \ldots a_1 a_0)_{10} &= a_s 10^s + \cdots + a_2 10^2 + (a_1 a_0)_{10} \\ &\equiv 0 + 0 + \cdots + 0 + (a_1 a_0)_{10} = (a_1 a_0)_{10} \mod 4\,.\end{aligned}$$

(2) Huomataan ensin, että $10 \equiv 1 \mod 9$. Lauseen 5.4 ((3)) perusteella $10^k \equiv 1 \mod 9$ kaikilla $k \in \mathbb{N}$. Lauseen 5.4 ja Seurauksen 5.5 perusteella

$$(a_s a_{s-1} \ldots a_1 a_0)_{10} = \sum_{k=0}^{s} a_k 10^k \equiv \sum_{k=0}^{s} a_k \mod 9\,.$$

(3) Väite seuraa kohdasta (2) ja Lemmasta 5.3(1).

(4) Koska $10 \equiv -1 \mod 11$, Lauseen 5.4(3) nojalla saamme $10^k \equiv (-1)^k \mod 11$ kaikilla $k \in \mathbb{N}$. Seurauksen 5.5 nojalla

$$(a_s a_{s-1} \ldots a_1 a_0)_{10} = \sum_{k=0}^{s} a_k 10^k \equiv \sum_{k=0}^{s} a_k (-1)^k \mod 11\,.$$ □

Lauseen 1.22 todistus. Lemman 5.14 nojalla $3 \mid n$, jos ja vain jos $3 \mid \sum_{k=0}^{s} a_k$. Luvulla 9 jaollisuutta koskeva sääntö todistetaan samalla tavalla. □

Lauseet 1.14,1.16, 1.18, 1.20 ja 1.26 todistetaan samaan tapaan.

Esimerkki 5.15. Olet laskenut käsin kertolaskun

$$267539 \cdot 765927 = 204925343653\,. \tag{5.1}$$

Laskun mahdollisen virheen voi huomata kongruenssitarkastelun avulla. Koska

$$267539 \equiv 2+6+7+5+3+9 = 32 \equiv 5 \mod 9$$

ja

$$765927 \equiv 7+6+5+9+2+7 = 36 \equiv 0 \mod 9\,,$$

pitäisi Lauseen 5.4((2)) nojalla olla

$$0 = 5\cdot 0 \equiv 204925343653 \equiv 2+0+4+9+2+5+3+4+3+6+5+3 = 46 \equiv 1 \mod 9\,.$$

Laskussa (5.1) on siis virhe.[3]

5.3 Kongruenssiluokat

Olkoon $m \in \mathbb{N} - \{0\}$. Luvun $a \in \mathbb{Z}$ *kongruenssiluokka (modulo m)* on joukko

$$a + m\mathbb{Z} = \left\{b \in \mathbb{Z} : a \equiv b \mod n\right\}.$$

Seuraava tulos selittää, miksi valitsimme ylläolevan merkinnän kongruenssiluokille.

Lemma 5.16. *Olkoon $m \in \mathbb{N} - \{0\}$ ja olkoon $a \in \mathbb{Z}$. Tällöin*

$$a + m\mathbb{Z} = \{a + mk : k \in \mathbb{Z}\}\,.$$

Todistus. Harjoitustehtävä 5.11. □

Esimerkki 5.17. $4 + 5\mathbb{Z} = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$.

Lause 5.18. *Olkoon $n \in \mathbb{N}$ ja olkoot $a, b \in \mathbb{Z}$. Tällöin*

(1) $a \in a + n\mathbb{Z}$,

(2) $a \equiv b \mod n$, *jos ja vain jos* $a + n\mathbb{Z} = b + n\mathbb{Z}$.

(3) joko $a + n\mathbb{Z} = b + n\mathbb{Z}$ *tai* $(a + n\mathbb{Z}) \cap (b + n\mathbb{Z}) = \varnothing$.

[3] Oikea tulos on 204915343653.

Todistus. (1) on selvä.

(2) Oletetaan, että $a \equiv b \mod n$. Tällöin $a = b + m\ell$ jollain $\ell \in \mathbb{Z}$. Jos $x \in a + m\mathbb{Z}$, niin $x = a + mk$ jollain $k \in \mathbb{Z}$. Tällöin

$$x = a + mk = b + m(\ell + k) \in b + m\mathbb{Z}\,.$$

Siis $a + m\mathbb{Z} \subset b + m\mathbb{Z}$. Vastaavasti osoitetaan $b + m\mathbb{Z} \subset a + m\mathbb{Z}$. Siis $a + m\mathbb{Z} = b + m\mathbb{Z}$.

Jos $a + m\mathbb{Z} = b + m\mathbb{Z}$, niin $a \in b + m\mathbb{Z}$. Siis jollain $k \in \mathbb{Z}$ pätee $a = b + mk$, joten $a - b = mk$. Siis $a \equiv b \mod m$.

(3) Jos $(a + m\mathbb{Z}) \cap (b + m\mathbb{Z}) \neq \varnothing$, niin on $x \in (a + m\mathbb{Z}) \cap (b + m\mathbb{Z})$. Tällöin on luvut $k, \ell \in \mathbb{Z}$, joille $a + mk = x = b + m\ell$. Siis $b - a = m(k - \ell)$, joten $a \equiv b \mod m$. Kohdan (2) nojalla $a + m\mathbb{Z} = b + m\mathbb{Z}$. □

Lause 5.19. *Olkoon $n \in \mathbb{N}$. Kongruenssiluokat $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}$ ovat erillisiä ja niiden yhdiste on $\mathbb{Z}$.*

Todistus. Jos $0 \leqslant i < j \leqslant n-1$, niin $1 \leqslant j - i \leqslant n-1$. Siis $n \nmid (j-i)$, joten $j \not\equiv i \mod n$ ja Lauseen 5.18 nojalla $(i + n\mathbb{Z}) \cap (j + n\mathbb{Z}) = \varnothing$.

Toisaalta, jos $k \in \mathbb{Z}$, niin jakoyhtälön nojalla on luvut $q, r \in \mathbb{Z}$, joille $k = qn + r$ ja $0 \leqslant r \leqslant n-1$. Siten $k \equiv r \mod n$ ja $k \in r + n\mathbb{Z}$, joten

$$\mathbb{Z} = \bigcup_{i=0}^{n-1} (i + n\mathbb{Z})\,. \qquad \square$$

Lauseen 5.19 mukaan jokainen kongruenssiluokka vastaa yhtä luvulla n jaettaessa jäävää jakojäännöstä $0, 1, \ldots, n-1$. Jokainen kokonaisluku on kongruentti modulo n täsmälleen yhden kokonaisluvun $0, 1, \ldots n-1$ kanssa.

5.4 Fermat'n pieni lause

Tässä luvussa todistamme Fermat'n pienen lauseen, joka on hyödyllinen työkalu kongruenssien tarkastelussa.

Lemma 5.20. *Olkoot $a, b_1, b_2, n \in \mathbb{Z}$, $n \geqslant 1$ kokonaislukuja*

(1) Jos $\operatorname{syt}(a, n) = 1$*, niin on $b \in \mathbb{Z}$, jolle $ab \equiv 1 \mod n$.*

(2) Jos $\operatorname{syt}(a, n) > 1$*, niin yhtälöllä $ab \equiv 1 \mod n$ ei ole ratkaisua.*

(3) Jos $ab_1 \equiv 1 \mod n$ ja $ab_2 \equiv 1 \mod n$, niin $b_1 \equiv b_2 \mod n$.

Todistus. (1) Bezout'n yhtälön[4] nojalla on $b, k \in \mathbb{Z}$, joille pätee $ab + nk = 1$, joten $ab \equiv 1 \mod n$.

(2) Jos yhtälöllä $ab \equiv 1 \mod n$ on ratkaisu, niin on $k \in \mathbb{Z}$, jolle pätee $ab + nk = 1$. Siis Bézout'n yhtälön nojalla $\operatorname{syt}(a, n) = 1$.

(3) Kohdan (2) nojalla $\operatorname{syt}(a, n) = 1$. Seurauksen 5.9 nojalla $b_1 \equiv b_2 \mod n$. □

Lemma 5.21. *Olkoon p alkuluku ja olkoon $a \in \mathbb{Z}$ siten, että $p \nmid a$. Tällöin on $b \in \mathbb{Z}$, jolle $ab \equiv 1 \mod p$.*

[4] Seuraus 2.5

Todistus. Oletuksen nojalla $\text{syt}(a,p) = 1$, joten väite seuraa Lemmasta 5.20. □

Esimerkki 5.22. (1) Jos $p = 7$, niin Lemman 5.21 lupaamat luvut b on helppo löytää. Lauseiden 5.4((2)) ja 5.19 nojalla riittää tarkastella tapaukset $a \in \{1,2,3,4,5,6\}$. Kokeilemalla huomaamme, että

$$\begin{aligned} 1 \cdot 1 &\equiv 1 \mod 7\,, & 2 \cdot 4 &\equiv 1 \mod 7\,,\\ 3 \cdot 5 &\equiv 1 \mod 7\,, & 6 \cdot 6 &\equiv (-1)^2 = 1 \mod 6\,. \end{aligned}$$

(2) Lemman 5.21 väite ei päde, jos $\text{syt}(a,n) > 1$. Esimerkiksi, kun $n = 6$ huomaamme, että

$$\begin{aligned} 2 \cdot 1 &= 2 \not\equiv 1\,, & 2 \cdot 2 &= 4 \not\equiv 1\,, & 2 \cdot 3 &= 6 \equiv 0 \not\equiv 1\,,\\ 2 \cdot 4 &= 8 \equiv 2 \not\equiv 1\,, & 2 \cdot 5 &= 10 \equiv 4 \not\equiv 1\,, \end{aligned}$$

joten yhtälöllä $2x \equiv 1 \mod 6$ ei ole ratkaisua.

Lause 5.23 (Fermat'n pieni lause)**.** *Olkoon p alkuluku. Tällöin $a^p \equiv a \bmod p$ jokaiselle $a \in \mathbb{Z}$. Erityisesti, jos $p \nmid a$, niin $a^{p-1} \equiv 1 \bmod p$.*

Todistus. Jos $a \equiv 0$, niin $a^p \equiv 0^p = 0 \equiv a$, joten voimme olettaa, että $p \nmid a$. Lemman 5.21 nojalla on $b \in \mathbb{Z}$, jolle $ab \equiv 1 \mod p$. Olkoot $1 \leqslant x, y \leqslant p$ siten, että $ax \equiv ay \mod p$. Tällöin Lauseen 5.4((2)) nojalla

$$x \equiv bax \equiv bay \equiv y \mod p\,,$$

joten $x = y$. Siis $ax \not\equiv ay \mod p$ kaikilla $1 \leqslant x < y \leqslant p$.

Lauseen 5.19 nojalla jokaisella $1 \leqslant k \leqslant p-1$ on $1 \leqslant x_k \leqslant p-1$, jolle $ak \equiv x_k \bmod p$. Edellä näimme, että $x_k \neq x_\ell$, jos $1 \leqslant k, \ell \leqslant p-1$ ja $k \neq \ell$, joten

$$\{x_1, x_2, \ldots, x_{p-1}\} = \{1, 2, \ldots, p-1\}\,.$$

Lauseen 5.4((2)) nojalla

$$a^{p-1}(p-1)! = (a \cdot 1)(a \cdot 2) \cdots (a(p-1)) \equiv x_1 x_2 \cdots x_{p-1} = (p-1)! \mod p\,.$$

Seurauksen 5.9 nojalla $a^{p-1} \equiv 1 \bmod p$, josta seuraa $a^p \equiv a \bmod p$ □

Esimerkki 5.24. Fermat'n pienen lauseen ja Lauseen 5.4((2)) nojalla $a^{k+p-1} \equiv a^k \bmod p$ jokaiselle $a \in \mathbb{Z}$, $k \in \mathbb{N}$ ja jokaiselle alkuluvulle p.

(1) Esimerkiksi $2^0 = 1 \mod 5$, $2^1 = 2 \mod 5$, $2^2 = 4 \mod 5$, $2^3 = 8 \equiv 3 \mod 5$, $2^4 \equiv 6 \equiv 1 \mod 5$ ja siten $2^5 = 2^4 \cdot 2 \equiv 2 \mod 5$ ja potenssin $2^k \mod 5$ arvo muuttuu jaksolla 4, kun k kasvaa.

(2) Toisaalta $4^0 = 1$, $4^1 = 4$, $4^2 = 16 \equiv 2 \mod 7$, $4^3 \equiv 4 \cdot 2 \equiv 1 \mod 7$, $4^4 \equiv 4 \mod 7$ ja potenssin $4^k \mod 7$ arvo muuttuu 3-jaksollisesti ja siis myös 6-jaksollisesti.

Fermat'n pienen lauseen nojalla $n \in \mathbb{N}$ ei ole alkuluku, jos esimerkiksi $2^n \not\equiv 2 \mod n$. Tuloksen avulla saadaan yksinkertainen alkulukutesti, joka tosin voi vain osoittaa, että testattava luku ei ole alkuluku.

Fermat'n alkulukutesti

Luonnollinen luku n ei ole alkuluku, jos $a^{n-1} \not\equiv 1$ jollain $2 \leqslant a \leqslant n-1$.

Esimerkki 5.25. On yhdistettyjä lukuja $n \in \mathbb{N}$, joille $2^n \equiv 2 \mod n$. Pienin tällainen esimerkki on $341 = 11 \cdot 31$. Nimittäin Fermat'n pienen lauseen nojalla $2^{10} \equiv 1 \mod 11$ ja on helppo huomata, että $2^5 = 32 \equiv 1 \mod 31$, joten Lauseen 5.4(2) nojalla $2^{10} \equiv 1 \mod 31$. Seurauksen 5.13 nojalla $2^{10} \equiv 1 \mod 341$. Siis $2^{340} \equiv 1 \mod 341$. Yhdistetty luku 341 läpäisee siis Fermat'n alkulukutestin kannassa 2, joten sitä sanotaan *valealkuluvuksi kannassa* 2.

Huomaa, että Fermat'n pieni lause antaa tiedon $2^{30} \equiv 1 \mod 31$ mutta tästä tiedosta ei ole hyötyä tässä esimerkissä, sillä $30 \nmid 340$.

Yhdistetty luku $n \in \mathbb{N} - \{0,1\}$ on *(Fermat'n) valealkuluku kannassa* $a \in \{2,3,\ldots,n-1\}$, jos $a^{n-1} \equiv 1 \mod n$.

Esimerkki 5.26. (1) Yhdistetty luku 341 on Esimerkin 5.25 nojalla valealkuluku kannassa 2. Kuitenkin lasku osoittaa, että $3^{340} \equiv 56 \mod 341$, joten 341 ei ole valealkuluku kannassa 3.

(2) Samaan tapaan nähdään, että 4 on valealkuluku kannassa 5: $4 \equiv -1 \mod 5$, joten $4^4 \equiv (-1)^4 = 1 \mod 5$.

Yhdistetty luku $m \in \mathbb{N} - \{0,1\}$ on *Carmichaelin luku* eli *Fermat'n valealkuluku*, jos kaikille $a \in \mathbb{Z}$, joille $\operatorname{syt}(a,m) = 1$, pätee $a^{m-1} \equiv 1 \mod m$.

Esimerkki 5.27. Yhdistetty luku $561 = 3 \cdot 11 \cdot 17$ on Carmichaelin[5] luku: Olkoon $a \in \mathbb{Z}$ siten, että $\operatorname{syt}(a, 561) = 1$. Tällöin $3 \nmid a$, $11 \nmid a$ ja $17 \nmid a$. Fermat'n pienen lauseen nojalla $a^2 \equiv 1 \mod 3$, $a^{10} \equiv 1 \mod 11$ ja $a^{16} \equiv 1 \mod 17$ Siis

$$\begin{aligned} a^{560} &= (a^2)^{280} \equiv 1^{280} = 1 \mod 3\,, \\ a^{560} &= (a^{10})^{56} \equiv 1^{56} = 1 \mod 11 \quad \text{ja} \\ a^{560} &= (a^{16})^{35} \equiv 1^{35} = 1 \mod 17\,. \end{aligned}$$

Seurauksen 5.13 nojalla $a^{560} \equiv 1 \mod 561$.

Carmichaelin lukuja kutsutaan valealkuluvuiksi, koska ne läpäisevät Fermat'n alkulukutestin kaikilla kantaluvuilla, jotka eivät ole niiden kanssa suhteellisia alkulukuja. Alford, Granville ja Pomerance[6] osoittivat vuonna 1994, että Carmichaelin lukuja on äärettömän monta.

[5] Robert Carmichael (1879-1967).
[6] William Alford (1940-2005), Andrew Granville (1962-), Carl Pomerance (1944-).

5.5 Wilsonin lause

Lemma 5.28. *Olkoon p alkuluku. Kongruenssiyhtälön $x^2 \equiv 1 \mod p$ ratkaisut ovat $x \equiv \pm 1 \mod p$.*

Todistus. Jos $x \equiv \pm 1 \mod p$, niin Lauseen 5.4(2) nojalla $x^2 \equiv 1 \mod p$. Osoitetaan, että muita ratkaisuja ei ole. Jos $x^2 \equiv 1 \mod p$, niin $(x-1)(x+1) \equiv 0 \mod p$. Siis $p \mid (x-1)(x+1)$. Eukleideen lemman[7] nojalla $p \mid (x-1)$ tai $p \mid (x+1)$. Siis $x \equiv 1 \mod p$ tai $x \equiv -1 \mod p$. □

Ilmeisesti Wilson[8] arvasi kokeilujen perusteella, että kaikki alkuluvut p toteuttavat kongruenssiyhtälön $(p-1)! \equiv -1 \mod p$. Lagrange[9] esitti ensimmäisen tunnetun todistuksen seuraavalle Wilsonin mukaan nimetylle tulokselle vuonna 1773.

Lause 5.29 (Wilsonin lause)**.** *Luonnollinen luku $n \in \mathbb{N} - \{0,1\}$ on alkuluku, jos ja vain jos $(n-1)! \equiv -1 \bmod n$.*

Todistus. Harjoitustehtävässä 3.20 osoitettiin, että $(n-1)! \equiv 0 \mod n$, jos $n \geqslant 5$ on yhdistetty luku. Lisäksi $(4-1)! = 6 \equiv 2 \mod 4$, joten $(n-1)! \not\equiv -1 \mod n$, jos n on yhdistetty luku.

Olkoon n alkuluku. Lemman 5.21 nojalla jokaisella $1 \leqslant a \leqslant n-1$ on yksikäsitteinen $1 \leqslant b(a) \leqslant n-1$ siten, että $ab \equiv 1 \mod p$. Lemman 5.28 nojalla $b(a) = a$, jos ja vain jos $a = \pm 1 \mod p$. Siis jokaiselle $2 \leqslant a \leqslant p-2$ on yksikäsitteinen $b(a) \neq a$, $1 \leqslant b(a) \leqslant n-1$, jolle $ab \equiv 1 \mod p$. Siis

$$(n-1)! = 1 \cdot (2 \cdot 3 \cdots (n-2))\,(n-1) \equiv n-1 \equiv -1 \mod n\,. \qquad \square$$

Esimerkki 5.30. Wilsonin lauseen todistuksessa jokaisella luvulla $2 \leqslant a \leqslant p-2$ on $2 \leqslant b \leqslant p-2$, jolle $ab \equiv 1 \mod p$. Esimerkiksi, kun $p = 11$, saadaan

$$\begin{aligned} 10! &= 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \\ &= (2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8)10 \\ &\equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot (-1) = -1 \mod 11\,. \end{aligned}$$

Wilsonin lause antaa testin, jolla voidaan todeta, onko jokin luku alkuluku vai ei. Käytännössä yhtälön $(n-1)! \equiv 0 \mod n$ tarkastaminen on niin raskasta suurille luvuille n, että Wilsonin lauseen merkitys alkulukujen selvittämisessä jää teoreettiseksi.

5.6 Kokonaislukukertoimisista polynomeista

Lause 5.31. *Olkoot $n, k \in \mathbb{N}$ ja olkoot $a, b \in \mathbb{Z}$. Olkoon P kokonaislukukertoiminen polynomi,*

$$P(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_k x^k, \quad c_0, c_1, \ldots, c_k \in \mathbb{Z}.$$

Jos $a \equiv b \mod n$, niin $P(a) \equiv P(b) \mod n$.

[7] Lemma 3.9

[8] John Wilson (1741-1793).

[9] Joseph-Louis Lagrange (1736-1813).

Todistus. Koska $a \equiv b \mod n$, niin Lauseen 5.4 nojalla $a^i \equiv b^i \mod n$ kaikilla $i \in \mathbb{N}$ ja siten $c_i a^i \equiv c_i b^i \mod n$ kaikilla i. Seurauksen 5.5 nojalla $\sum_{i=0}^{k} c_i a^i \equiv \sum_{i=0}^{k} c_i b^i \mod n$. Siten $P(a) \equiv P(b) \mod n$. □

Luku $a \in \mathbb{Z}$ on kokonaislukukertoimisen polynomin $P(x)$ *juuri*, jos $P(a) = 0$.

Jos kokonaislukukertoimisella polynomilla $P(x)$ on juuri $a \in \mathbb{Z}$, niin $P(a) \equiv 0 \mod n$ kaikilla $n \in \mathbb{N}$. Lauseen 5.31 avulla voidaan joskus päätellä, että polynomilla ei ole kokonaislukujuuria.

Seuraus 5.32. *Jos on $n \in \mathbb{N}$, jolle yhtälöllä $P(x) \equiv 0 \mod n$ ei ole kokonaislukuratkaisua, niin polynomilla P ei ole juuria.* □

Esimerkki 5.33. Olkoon $P(x) = x^5 - x^2 + x - 3$. Näytetään, että polynomilla P ei ole kokonaislukujuuria. Huomaamme ensin, että $P(1) = -2 \equiv 0 \mod 2$ ja $P(0) = 3 \equiv 0 \mod 3$, joten kongruenssilaskut modulo 2 tai modulo 3 eivät anna haluttua tulosta. Sen sijaan $P(0) = -3 \not\equiv 0 \mod 4$, $P(1) = -2 \not\equiv 0 \mod 4$, $P(2) = 27 \not\equiv 0 \mod 4$ ja $P(-1) = -6 \not\equiv 0 \mod 4$. Lauseen 5.31 yhtälöllä

$$P(x) = x^5 - x^2 + x - 3 \equiv 0 \mod 4$$

ei ole ratkaisua. Seurauksen 5.32 nojalla $P(x) = x^5 - x^2 + x - 3 \neq 0$ kaikilla $x \in \mathbb{Z}$.

Esimerkki 5.34. Ei ole kokonaislukukertoimista polynomia $P(x) = a_n x^n + \ldots a_1 x + a_0$, $n \in \mathbb{N}$, $a_n \neq 0$, jolle $P(k)$ on alkuluku kaikilla $k \in \mathbb{Z}$. Osoitamme tämän kongruenssin avulla. Todistuksessa käytämme kurssilla Renkaat ja Kunnat todistettavaa tietoa, että millä tahansa polynomilla, jonka aste on n on korkeintaan n juurta.[10]

Oletetaan, että P on kokonaislukukertoiminen polynomi, jolle $P(k)$ on alkuluku kaikilla $k \in \mathbb{Z}$. Olkoon $k \in \mathbb{Z}$. Nyt $P(k) = q$ on alkuluku. Jos $b \in \mathbb{Z}$ siten, että $b \equiv k \mod q$, niin Lauseen 5.31 nojalla $P(b) \equiv P(k) \mod q$. Koska $P(k) = q \equiv 0 \mod q$, niin $q \mid P(b)$.

Koska oletimme, että $P(b)$ on alkuluku, niin $q = P(b)$. Kongruenssiluokassa $k + q\mathbb{Z}$ on äärettömän monta kokonaislukua, joten tästä seuraa, että polynomilla $Q(x) = P(x) - q$ on äärettömän monta juurta, mikä on mahdotonta.

5.7 Kongruenssiluokkien laskutoimitukset

Tässä luvussa tarkastelemme kongruenssiluokkia algebralliselta kannalta. Tätä aihepiiriä käsitellään tarkemmin algebran kursseilla Renkaat ja kunnat ja Ryhmät.

Olkoon A epätyhjä joukko. Kuvaus $*\colon A \times A \to A$ on *joukon A laskutoimitus* tai *laskutoimitus joukossa A*.

Olkoon $n \in \mathbb{N} - \{0\}$. Kongruenssiluokkien joukko

$$\mathbb{Z}/n\mathbb{Z} = \{i + n\mathbb{Z} : i \in \mathbb{Z}\}$$

on *kokonaisluvut modulo n* tai *jäännösluokkarengas modulo n*.

[10] Katso esimerkiksi [Par, Lause 6.20].

Lauseen 5.19 nojalla joukossa $\mathbb{Z}/n\mathbb{Z}$ on n alkiota.

Esimerkki 5.35. $\mathbb{Z}/2\mathbb{Z} = \{0 + 2\mathbb{Z}, 1 + 2\mathbb{Z}\}$.

Lauseesta 5.4 seuraa, että kokonaislukujen luonnolliset laskutoimitukset määräävät laskutoimituksia kongruenssiluokkien joukoissa.

Olkoon $n \in \mathbb{N} - \{0\}$ ja olkoot $a, b \in \mathbb{Z}$. Määritellään laskutoimitukset joukossa $\mathbb{Z}/n\mathbb{Z}$ seuraavasti

$$\begin{aligned}(a + n\mathbb{Z}) + (b + n\mathbb{Z}) &= (a + b) + n\mathbb{Z},\\ (a + n\mathbb{Z}) - (b + n\mathbb{Z}) &= (a - b) + n\mathbb{Z},\\ (a + n\mathbb{Z})(b + n\mathbb{Z}) &= ab + n\mathbb{Z}\end{aligned} \tag{5.2}$$

Jotta laskutoimitukset olisivat hyvin määriteltyjä, kohdan (5.2) kaavojen oikeat puolet saavat riippua vain kongruenssiluokista $a + n\mathbb{Z}$ ja $b + n\mathbb{Z}$, eivät kongruenssiluokkien edustajista a ja b.

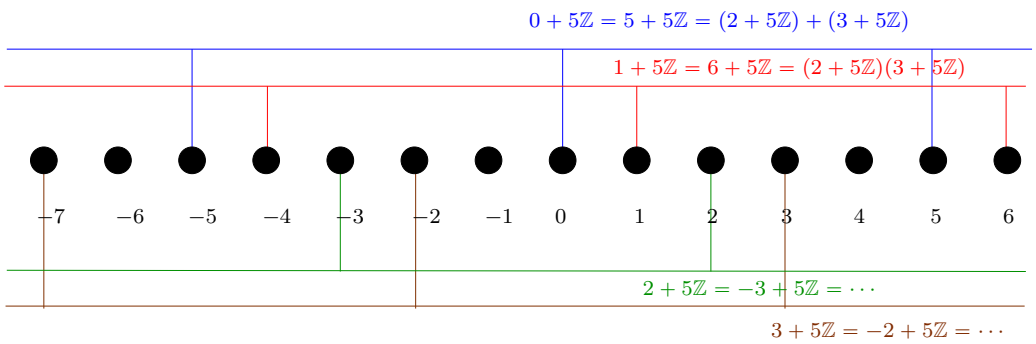
Lemma 5.36. *Kongruenssiluokkien yhteenlasku on hyvin määritelty.*

Todistus. Oletetaan, että $a + n\mathbb{Z} = a' + n\mathbb{Z}$ ja $b + n\mathbb{Z} = b' + n\mathbb{Z}$. Lauseen 5.18 ((2)) nojalla $a \equiv a' \mod n$ ja $b \equiv b' \mod n$, joten Lauseen 5.4 ((1)) perusteella $a + b \equiv a' + b' \mod n$. Seurauksen 5.18 ((2)) toinen suunta kertoo, että $(a + b) + n\mathbb{Z} = (a' + b') + n\mathbb{Z}$. □

Kongruenssiluokkien kertolaskun tuloksen riippumattomuus kongruenssiluokkien edustajista todistetaan samalla tavalla.

Esimerkki 5.37. Esimerkkejä kongruessiluokkien yhteen- ja kertolaskusta:

$$\begin{aligned}(1 + 3\mathbb{Z}) + (2 + 3\mathbb{Z}) &= (1 + 2) + 3\mathbb{Z} = 3 + 3\mathbb{Z} = 0 + 3\mathbb{Z}\\ (2 + 5\mathbb{Z})(4 + 5\mathbb{Z}) &= (2 \cdot 4) + 5\mathbb{Z} = 8 + 5\mathbb{Z} = 3 + 5\mathbb{Z}\,.\end{aligned}$$



Kuva 5.1 — Kongruenssiluokat modulo 5 ja esimerkkejä laskutoimituksista.

Harjoitustehtäviä

5.1. Todista Lemma 5.1.

5.2. Olkoon $p \geqslant 5$ alkuluku. Osoita, että $p \equiv \pm 1 \mod 6$.

5.3. Onko $46^{78} + 89^{67}$ jaollinen luvulla 5?

5.4. Onko $20^{2022} + 22^{2022}$ jaollinen luvulla 7?

5.5. Määritä jakojäännökset, kun
(1) 2^{345} jaetaan luvulla 5 ja
(2) 3^{456} jaetaan luvulla 6.

5.6. Osoita yhtälöiden $641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$ avulla, että $2^{32} \equiv -1 \mod 641$.

5.7. Todista Lemma 5.7.

5.8. Olkoon p alkuluku. Osoita, että $(x + y)^p \equiv x^p + y^p \mod p$ kaikille $x, y \in \mathbb{Z}$.

5.9. Miksi Harjoitustehtävässä 5.8 ei väitetä, että $(x + y)^n \equiv x^n + y^n \mod n$ kaikille $x, y \in \mathbb{Z}$ ja kaikille $n \in \mathbb{N} - \{0, 1\}$?

5.10. Osoita, että

$$\sum_{i=1}^{100} i^5 \equiv 0 \mod 4\,.$$

5.11. Todista Lemma 5.16.

5.12. Osoita, että $4 \mid (a_s a_{s-1} \ldots a_1 a_0)_{10}$, jos ja vain jos $4 \mid (2a_1 + a_0)$.

5.13. Olkoon p alkuluku, joka ei ole 2 eikä 5. Osoita, että
(1) p jakaa äärettömän monta luvuista 9, 99, 999, 9999, 9999, ...[11].
(2) p jakaa äärettömän monta luvuista 11, 111, 1111, 11111, ...[12]

5.14. Osoita, että 645 on valealkuluku kannassa 2.

5.15. Osoita, että 91 on valealkuluku kannassa 3.

5.16. Osoita, että 1105 on Carmichaelin luku.

5.17. Osoita, että 2821 on Carmichaelin luku.

5.18. Olkoot $p_1, p_2, \ldots, p_n$ eri alkulukuja, $n \geqslant 2$, ja olkoon $m = p_1 p_1 \cdots p_n$. Oletetaan, että $(p_k - 1) \mid (m - 1)$ kaikilla $1 \leqslant k \leqslant n$. Osoita, että m on Carmichaelin luku.

5.19. Näytä kongruenssien avulla, että polynomeilla $P(x) = x^3 - x + 1$ ja $Q(x) = x^3 + x^2 - x + 1$ ei ole kokonaislukujuuria.

5.20. Olkoon $n \in \mathbb{Z}$. Osoita, että $30 \mid n^5 - n$.[13]

5.21. Olkoon $n \in \mathbb{Z}$. Osoita, että $42 \mid n^7 - n$.[14]

5.22. Olkoon $n \in \mathbb{Z}$ siten, että n ei ole jaollinen millään luvuista 5, 7 ja 11. Osoita, että $385 \mid n^{60} - 1$.

[11] Esimerkki 5.24
[12] Olisiko kohdan (1) tuloksesta hyötyä?
[13] Vihje: $30 = 2 \cdot 3 \cdot 5$ ja Seuraus 5.13.
[14] Vihje: $30 = 2 \cdot 3 \cdot 7$ ja Seuraus 5.13.

Luku 6

Lineaariset kongruenssiyhtälöt

Lemman 5.20 todistuksessa osoitimme, että lineaarisella kongruenssiyhtälöllä $ax \equiv 1 \mod n$ on ratkaisu, jos $\text{syt}(a, n) = 1$. Tässä luvussa tarkastelemme tämän yhtälön yleistyksiä ja samalla palaamme luvussa 2.2 tarkasteltujen lineaaristen Diofantoksen yhtälöiden tarkasteluun. Kurssin lopuksi tarkastelemme lineaaristen kongruenssiyhtälöiden ryhmiä ja Eulerin ϕ-funktiota.

6.1 Lineaarinen kongruenssiyhtälö

Olkoon $n \in \mathbb{N} - \{0\}$ ja olkoot $a, b \in \mathbb{Z}$, $a \neq 0$. Luku $x \in \mathbb{Z}$, joka toteuttaa ehdon

$$ax \equiv b \mod n\,, \tag{6.1}$$

on *(yhden muuttujan) lineaarisen kongruenssiyhtälön* $ax \equiv b \mod n$ *ratkaisu.*
Jos $x \in \mathbb{Z}$ ja $y \in \mathbb{Z}$ ovat yhtälön (6.1) ratkaisuja ja $x \equiv y \mod n$, niin ne ovat yhtälön *sama ratkaisu* $\mod n$.

Kokonaisluku x on kongruenssiyhtälön $ax \equiv b \mod n$ ratkaisu, jos ja vain jos

$$ax + ny = b$$

jollain $y \in \mathbb{Z}$.

Esimerkki 6.1. Ainakin luvut $x = 3$, $x = 9$ ja $x = 15$ ovat kongruenssiyhtälön $2x \equiv 6 \mod 12$ ratkaisuja. Koska $15 \equiv 3 \mod 12$, niin se 3 ja 15 ovat kongruenssimielessä sama ratkaisu mod 3.

(2) Kongruenssiyhtälöllä $2x \equiv 3 \mod 4$ ei ole ratkaisuja, koska $2x$ on parillinen kaikilla $x \in \mathbb{Z}$, 3 on pariton ja moduli 4 on parillinen.

Lemma 6.2. *Jos $c \in \mathbb{Z}$, niin joko kongruenssiluokan $c + n\mathbb{Z}$ kaikki luvut ovat lineaarisen kongruenssiyhtälön* (6.1) *ratkaisuja tai mikään luvuista $x \in c + n\mathbb{Z}$ ei ole ratkaisu.*

Todistus. Jos $x \equiv y \mod n$, niin Lemman 5.4(1) nojalla $ax \equiv ay$. □

Koska jokaisen luvun $x \in \mathbb{Z}$ jakojäännökselle r modulo n pätee $x \equiv r \mod n$, niin haettaessa ratkaisua yhtälöön (6.1) riittää Lemman (6.2) perusteella tutkia luvut $0, 1, \ldots, n-1$. Se, että Esimerkin 6.1((2)) yhtälöllä ei ole ratkaisuja, voitaisiin perustella myös tarkastamalla, että mikään luvuista $0, 1, 2, 3$ ei ole yhtälön ratkaisu modulo 4.

Lemman 6.2 perusteella kongruenssiyhtälön ratkaisuista voidaan käyttää myös toisenlaista sanastoa:

Kongruenssiluokka $c + n\mathbb{Z}$ on kongruenssiyhtälön $ax \equiv b$ *ratkaisu*, jos $ay \equiv b \mod n$ kaikilla $y \in c + n\mathbb{Z}$.

Esimerkki 6.3. Kongruenssiluokat $3 + 12\mathbb{Z}$ ja $9 + 12\mathbb{Z}$ ovat Esimerkin 6.1((1)) yhtälön $2x \equiv 6 \mod 12$ ratkaisuja.

Lause 6.4. *Olkoon $n \in \mathbb{N} - \{0\}$, olkoot $a, b \in \mathbb{Z}$, $a \neq 0$.*

(1) Jos $\operatorname{syt}(a, n) \nmid b$, niin lineaarisella kongruenssiyhtälöllä $ax \equiv b \mod n$ ei ole ratkaisua.

(2) Jos $\operatorname{syt}(a, n) \mid b$, niin lineaarisella kongruenssiyhtälöllä $ax \equiv b \mod n$ on $\operatorname{syt}(a, n)$ ratkaisua modulo n. Jos x_0 on ratkaisu, niin kaikki ratkaisut saadaan kaavalla

$$x \equiv x_0 + i \frac{n}{\operatorname{syt}(a, n)} \mod n, \quad i = 0, 1, \ldots, \operatorname{syt}(a, n) - 1 \,. \tag{6.2}$$

Todistus. (1) Lauseen 2.7 mukaan yhtälöllä

$$b = ax + ny \,,$$

ei ole kokonaislukuratkaisua $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, jos $\operatorname{syt}(a, n) \nmid b$.

(2) Bézout'n yhtälön nojalla on $k_0, \ell_0 \in \mathbb{Z}$, joille

$$ak_0 + n\ell_0 = \operatorname{syt}(a, n) \,.$$

Kertomalla tämä yhtälö puolittain luvulla $\frac{b}{\operatorname{syt}(a,n)} \in \mathbb{Z}$ saadaan

$$a \frac{b}{\operatorname{syt}(a, n)} k_0 + n \frac{b}{\operatorname{syt}(a, n)} \ell_0 = b \,. \tag{6.3}$$

Siten $x_0 \equiv \frac{b\,k_0}{\operatorname{syt}(a,n)} \mod n$ on kongruenssiyhtälön $ax \equiv b \mod n$ ratkaisu.

Koska $\operatorname{syt}(a, n) \mid a$ ja $cn \equiv 0 \mod n$ kaikilla $c \in \mathbb{Z}$, niin Lauseen 5.4 nojalla kaikille $j \in \mathbb{Z}$ pätee

$$a\Big(x_0 + j \frac{n}{\operatorname{syt}(a, n)}\Big) = ax_0 + j \frac{a}{\operatorname{syt}(a, n)} n \equiv ax_0 \equiv b \mod n \,.$$

Siis $x_0 + j \frac{n}{\operatorname{syt}(a,n)}$ on ratkaisu kaikilla $j \in \mathbb{Z}$. Ratkaisut $x_0 + i \frac{n}{\operatorname{syt}(a,n)}$ ja $x_0 + j \frac{n}{\operatorname{syt}(a,n)}$ luvuille $i, j \in \mathbb{Z}$ ovat kongruentteja mod n, jos ja vain jos $\operatorname{syt}(a, n) \mid (i - j)$, joten jokaiselle $j \in \mathbb{Z}$ pätee $x_0 + j \frac{n}{\operatorname{syt}(a,n)} \equiv x_0 + i \frac{n}{\operatorname{syt}(a,n)}$ jollain $i \in \{0, 1, 2, \ldots, \operatorname{syt}(a, n) - 1\}$.

Näytetään vielä, että muita ratkaisuja ei ole. Olkoon $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ yhtälön $ax+ny = b$ ratkaisu. Jos k_0, ℓ_0 ja x_0 ovat kuten yllä ja $y_0 = \frac{b\,\ell_0}{\mathrm{syt}(a,n)}$, niin yhtälön (6.3) nojalla

$$a(x - x_0) + n(y - y_0) = ax + ny - (ax_0 + ny_0) = 0\,.$$

Koska $\mathrm{syt}(a, n)$ on lukujen a ja n tekijä, niin

$$\frac{a}{\mathrm{syt}(a,n)}(x - x_0) = -\frac{n}{\mathrm{syt}(a,n)}(y - y_0)\,,$$

joten $\frac{n}{\mathrm{syt}(a,n)} \mid \frac{a}{\mathrm{syt}(a,n)}(x - x_0)$. Seurausten 2.10 ja 2.14 nojalla $\frac{n}{\mathrm{syt}(a,n)} \mid (x - x_0)$. Siten on $i \in \mathbb{Z}$, jolle

$$x = x_0 + i\frac{n}{\mathrm{syt}(a,n)}\,. \qquad \square$$

Seuraus 6.5. *Jos $n \in \mathbb{N}$, $a \in \mathbb{Z}$ ja $\mathrm{syt}(a, n) = 1$, niin lineaarisella kongruenssiyhtälöllä $ax \equiv b \mod n$ on ratkaisu kaikilla $b \in \mathbb{Z}$. Ratkaisu on yksikäsitteinen modulo n.*

Todistus. Lause 6.4. $\square$

Esimerkki 6.6. (1) Koska $\mathrm{syt}(7, 12) = 1$, niin Lauseen 6.4 nojalla yhtälöllä $7x \equiv 3 \mod 12$ on täsmälleen yksi ratkaisu. Samaan tapaan kuin Lauseen 6.4(2) todistuksessa ratkaisemme ensin kongruenssiyhtälön $7x \equiv 1 \mod 12$. Tarkastelemme Bézout'n yhtälöä

$$7x + 12y = 1\,. \tag{6.4}$$

Eukleideen algoritmilla saamme

$$\begin{aligned} 12 &= 7 + 5 \\ 7 &= 5 + 2 \\ 5 &= 2 \cdot 2 + 1\,, \end{aligned}$$

josta peruuttamalla löydämme Bézout'n yhtälön (6.4) ratkaisun $(-5) \cdot 7 + 3 \cdot 12 = 1$. Lauseen 6.4 nojalla yhtälön $7x \equiv 3 \mod 12$ ainoa ratkaisu on $x \equiv 3 \cdot (-5) = -15 \equiv 9 \mod 12$.

(2) Koska $\mathrm{syt}(10, 12) = 2$ ja $2 \mid 6$, niin Lauseen 6.4 nojalla yhtälöllä $10x \equiv 6 \mod 12$ on kaksi ratkaisua modulo 12. Tässä tapauksessa näemme helposti, että $-1 \cdot 10 + 1 \cdot 12 = 2$, joten $x_0 = 3 \cdot (-1) = -3 \equiv 9$ on yksi ratkaisu. Toinen ratkaisu on lausekkeen (6.2) nojalla $x_1 \equiv x_0 + \frac{12}{2} \mod 12$ eli $x_1 \equiv 3 \mod 12$.

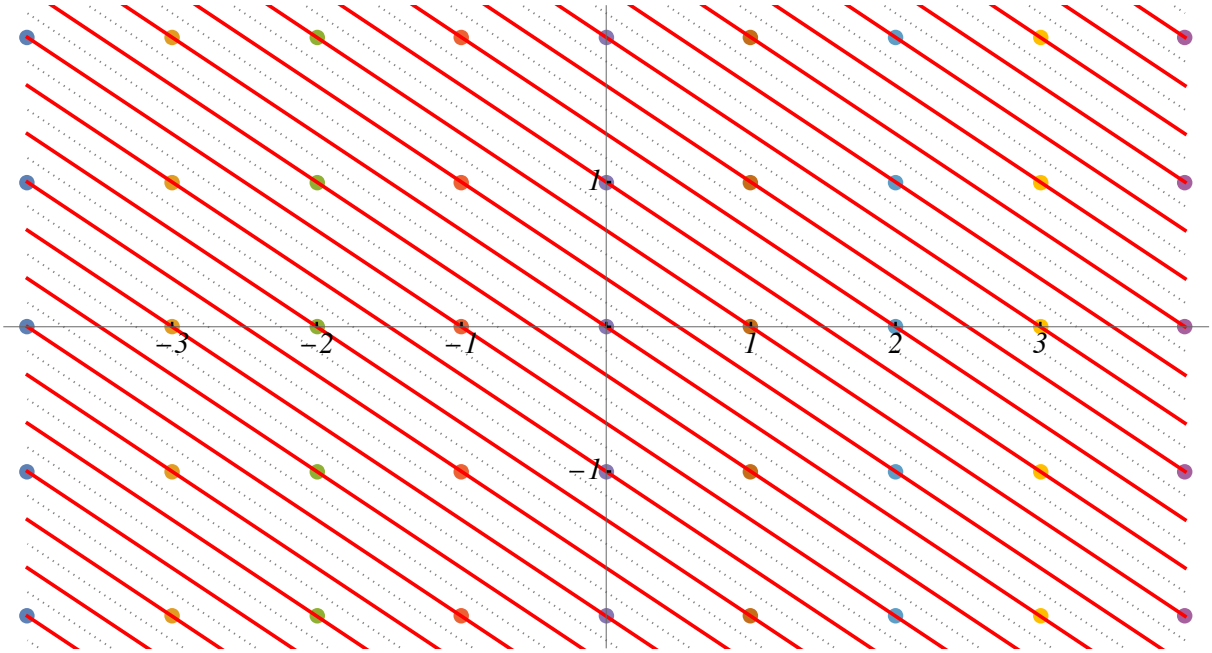
Lauseen 6.4 todistuksessa todistimme myös seuraavan tuloksen, joka täydentää Seurauksen 2.11 tuloksen lineaaristen Diofantoksen yhtälöiden ratkaisuista.

Seuraus 6.7. *Olkoot $(a, b) \in \mathbb{Z}^2 - \{(0, 0)\}$ ja $c \in \mathbb{Z}$. Lineaarisella Diofantoksen yhtälöllä $ax + by = c$ on ratkaisu $(x, y) \in \mathbb{Z}^2$, jos ja vain jos $\mathrm{syt}(a, b) \mid c$. Jos (x_0, y_0) on on yhtälön ratkaisu, niin kaikki ratkaisut saadaan kaavalla*

$$(x, y) = \left(x_0 + i\,\frac{b}{\mathrm{syt}(a,b)}\,,\; y_0 - i\,\frac{a}{\mathrm{syt}(a,b)}\right), \quad i \in \mathbb{Z}. \qquad \square$$

Esimerkki 6.8. (1) Esimerkin 6.6 ja Seurauksen 6.7 nojalla lineaarisen Diofantoksen yhtälön $7x + 12y = 3$ kaikki ratkaisut ovat $(-5 + 12k, 3 - 7k) = (-5, 3) + k(12, -7)$, $k \in \mathbb{Z}$.

(2) Lineaarisella Diofantoksen yhtälöllä $4x + 6y = c$ on ratkaisuja täsmälleen silloin, kun c on parillinen. Jos $4x_0 + 6y_0 = c$, niin Seurauksen 6.7 nojalla kaikki yhtälön ratkaisut ovat $(x_0 + 3k, y_0 - 2k)$, $k \in \mathbb{Z}$.



Kuva 6.1 — Lineaarisen Diofantoksen yhtälön $4x+6y = c$ ratkaisuja vakion c eri arvoilla. Jokainen punainen suora vastaa luvun c jotain parillista arvoa.

6.2 Kiinalainen jäännöslause

Tässä luvussa tarkastelemme kongruenssiyhtälöiden muodostamia yhtälöryhmiä.

Esimerkki 6.9. (1) Tarkastellaan lineaaristen kongruenssiyhtälöiden ryhmää

$$\begin{cases} x \equiv 2 \mod 3, \\ x \equiv 3 \mod 5 \\ x \equiv 2 \mod 7 \end{cases}. \tag{6.5}$$

Lauseen 6.4 nojalla jokaisella ryhmän 6.5 kongruenssiyhtälöllä on yksikäsitteinen ratkaisu kunkin yhtälön oman modulin suhteen, koska kaikissa yhtälöissä muuttujan x kerroin on 1. Ensimmäisen yhtälön ratkaisuja ovat luvut $x = 2+3k$, $k \in \mathbb{Z}$. Sijoitetaan tällainen ratkaisu toiseen yhtälöön, jolloin saadaan uusi yhtälö $2 + 3k \equiv 3 \mod 5$, joka on yhtäpitävä yhtälön $3k \equiv 1 \mod 5$ kanssa. Tämän yhtälön ratkaisu on $k = 2 + 5\ell$, $\ell \in \mathbb{Z}$. Siis luvut $x = 2 + 3(2 + 5\ell) = 8 + 15\ell$ ovat kongruenssiyhtälöparin

$$\begin{cases} x \equiv 2 \mod 3, \\ x \equiv 3 \mod 5 \end{cases} \tag{6.6}$$

ratkaisuja kaikilla $\ell \in \mathbb{Z}$. Kun tämä ratkaisu sijoitetaan kolmanteen yhtälöön, päädytään yhtälöön $8 + 15\ell \equiv 2 \mod 7$, joka on yhtäpitävä yhtälön $\ell \equiv 15\ell \equiv -6 \equiv 1 \mod 7$ kanssa. Siis $\ell = 1 + 7m$, $m \in \mathbb{Z}$. Sijoittamalla tämä yhtälöparin (6.6) ratkaisuun, saadaan yhtälöryhmän (6.5) ratkaisu $x = 23 + 105m$, $m \in \mathbb{Z}$.

(2) Kongruenssiyhtälöparilla

$$\begin{cases} x \equiv 3 \mod 9 \\ x \equiv 2 \mod 6 \end{cases}$$

ei ole ratkaisua. Jos $x \equiv 3 \mod 9$, niin $3 \mid (3-x)$ ja siten 3 jakaa luvun x. Jos $x \equiv 2 \mod 6$, niin $3 \mid (2-x)$. Jos $3 \mid x$, niin 3 jakaisi luvun 2, mikä ei ole totta.

Esimerkin 6.9(1) ongelma ja sen ratkaisu esitetään *Mestari Sunin*[1] *matemaattisessa oppaassa*, joka lienee kirjoitettu Kiinassa noin 2000 vuotta sitten. Tällaisten kysymysten ratkeavuutta käsittelevä lause tunnetaankin nimellä *kiinalainen jäännöslause*.

Lause 6.10 (Kiinalainen jäännöslause)**.** *Olkoon $k \in \mathbb{N}$. Olkoot $n_1, \ldots, n_k \in \mathbb{N} - \{0,1\}$ ja $b_1, \ldots, b_k \in \mathbb{Z}$. Jos* $\operatorname{syt}(n_i, n_j) = 1$ *aina, kun $i \neq j$, niin kongruenssiyhtälöryhmällä*

$$\begin{cases} x \equiv b_1 \mod n_1 \\ x \equiv b_2 \mod n_2 \\ \quad \vdots \qquad \vdots \\ x \equiv b_k \mod n_k \end{cases} \tag{6.7}$$

on yksikäsitteinen ratkaisu modulo $n = n_1 \cdots n_k$.

Todistus. Olkoon

$$c_i = \frac{n}{n_i}, \quad i = 1, 2, \ldots, k.$$

Koska $\operatorname{syt}(n_i, n_j) = 1$ aina, kun $i \neq j$, niin Lauseen 2.15 tai Lauseen 3.14 ja induktion avulla näemme, että $\operatorname{syt}(c_i, n_i) = 1$ kaikilla $i = 1, 2, \ldots, k$. Seurauksen 6.5 perusteella yhtälöllä

$$c_i x \equiv 1 \mod n_i$$

on yksikäsitteinen ratkaisu $d_i \mod n_i$.

Olkoon

$$x_0 = b_1 c_1 d_1 + b_2 c_2 d_2 + \cdots + b_k c_k d_k \,. \tag{6.8}$$

Jos $i \neq j$, niin $n_i \mid c_j$ ja siten $b_j c_j d_j \equiv 0 \mod n_i$. Luvun x_0 määritelmän mukaan on siis $x_0 \equiv b_i c_i d_i \equiv b_i \mod n_i$. Siis x_0 on kaikkien ryhmän kongruenssiyhtälöiden ratkaisu mod n.

Näytetään seuraavaksi, että muita ratkaisuja ei ole. Olkoon $x \in \mathbb{Z}$ yhtälöryhmän ratkaisu. Koska tällöin $x \equiv b_i \mod n_i$ ja $x_0 \equiv b_i \mod n_i$, niin $x_0 \equiv x \mod n_i$ ja siten $n_i \mid (x - x_0)$ kaikilla $i = 1, 2, \ldots, k$. Koska $\operatorname{syt}(n_i, n_j) = 1$, niin Seurauksen 2.14 perusteella luku $n = n_1 \cdots n_k$ jakaa luvun $x - x_0$ eli $x \equiv x_0 \mod n$. Siis x_0 on ainoa ratkaisu modulo n. □

Esimerkki 6.11. Luku $x = 23$ toteuttaa Esimerkin 6.9 lineaariset kongruenssiyhtälöt. Kiinalaisen jäännöslauseen perusteella 23 on yhtälöryhmän yksikäsitteinen ratkaisu modulo 105. Asian voi myös ilmaista hieman toisin toteamalla, että kongruenssiluokka $23 + 105\mathbb{Z}$ on yhtälöryhmän yksikäsitteinen ratkaisu.

Yhtälöryhmän (6.5) ratkaisun voi etsiä myös Kiinalaisen jäännöslauseen todistuksen menetelmällä. Todistuksen merkinnöillä $n = 3 \cdot 5 \cdot 7 = 105$, $c_1 = 35$, $c_2 = 21$ ja $c_3 = 15$.

[1] Sun Zi eli ilmeisesti 400-luvulla.

Yhtälön $35x \equiv 2x \equiv 1 \mod 3$ ratkaisu on $d_1 \equiv 2 \mod 3$. Yhtälön $21x \equiv x \equiv 1 \mod 5$ ratkaisu on $d_2 \equiv 1 \mod 5$. Yhtälön $15x \equiv x \equiv 1 \mod 7$ ratkaisu on $d_3 \equiv 1 \mod 7$. Kaavan (6.8) mukaan ratkaisuksi saadaan

$$x_0 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \mod 105\,.$$

Harjoitustehtäviä

6.1. Ratkaise lineaarinen kongruenssiyhtälö $3x \equiv 5 \mod 11$.

6.2. Ratkaise lineaariset kongruenssiyhtälöt

(a) $5x \equiv 2 \mod 7$,

(b) $4x \equiv 5 \mod 6$.

6.3. Ratkaise lineaarinen kongruenssiyhtälö $12x \equiv 9 \mod 15$.

6.4. Ratkaise lineaarinen kongruenssiyhtälö $240x \equiv 21 \mod 561$.

6.5. Ratkaise lineaarinen Diofantoksen yhtälö $6x + 21y = 15$. Etsi kaikki ratkaisut.

6.6. Ratkaise lineaarinen kongruenssiyhtälöpari

$$\begin{cases} x \equiv 3 \mod 7, \\ x \equiv 5 \mod 9 \end{cases}$$

6.7. Ratkaise lineaarinen kongruenssiyhtälöryhmä

$$\begin{cases} x \equiv 0 \mod 3, \\ x \equiv 1 \mod 4 \\ x \equiv 5 \mod 7 \end{cases}$$

6.8. Ratkaise lineaarinen kongruenssiyhtälöryhmä

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 2 \mod 17 \\ x \equiv 7 \mod 25 \end{cases}$$

6.9. Ratkaise lineaarinen kongruenssiyhtälöryhmä

$$\begin{cases} x \equiv 3 \mod 13 \\ x \equiv 7 \mod 20 \end{cases}$$

Osa II

Luku 7

Kahden neliön summat

7.1 Additiivisesta lukuteoriasta

Additiivisessa lukuteoriassa tarkastellaan esimerkiksi seuraavanlaisia kysymyksiä: Olkoot $A, B \subset \mathbb{Z}$.

(1) Voidaanko kaikki luvut $n \in B$ esittää summina

$$n = a_1 + a_2 + \cdots + a_s \,,$$

kun $a_1, a_2, \ldots, a_s \in A$ ja s on rajoittamaton tai rajoittamalla $s \leqslant N$ jollain $N \in \mathbb{N}^*$ tai $s = M$ jollain $M \in \mathbb{N}^*$?

(2) Monellako eri tavalla n voidaan esittää tällaisena summana? Tässä kysymyksessä voidaan valita laskea summat, joissa on samat yhteenlaskettavat eri järjestyksessä, samaksi tai eri esitykseksi.

Esimerkki 7.1. (1) Olkoot $A = B = \mathbb{N}^*$. Tarkastelemme siis positiivisten luonnollisten lukujen esittämistä positiivisten luonnollisten lukujen summina. Tällöin kysymyksessä (1) ei ole mitään tarkastelemista mutta kysymys (2) on mielekäs. Jos yhteenlaskettavien lukujen määrää ei rajoiteta eikä samojen lukujen eri järjestyksiä huomioida, niiin esimerkiksi luku 5 voidaan esittää seitsemällä tavalla

$$5 = 1+1+1+1+1 = 1+1+1+2 = 1+2+2 = 1+1+3 = 2+3 = 1+4\,.$$

Tällaisia esityksiä kutsutaan luonnollisten lukujen *rajoittamattomiksi osituksiksi*.

Jos luonnollinen luku esitetään positiivisten luonnollisten lukujen summana ja samojen yhteenlaskettavien eri järjestykset lasketaan erikseen, niin luvun 5 esityksiä on $1+1+4+3+3+2+2 = 16$. Tällöin siis $1+1+1+2$, $1+1+2+1$, $1+2+1+1$ ja $2+1+1+1$ lasketaan eri esityksiksi.

(2) Goldbachin otaksuma[1] on esimerkki kysymyksestä, jossa yhteenlaskettavien lukumäärää rajoitetaan. Tässä ongelmassa $A \subset \mathbb{N}$ on alkulukujen joukko, $B = \{k \in 2\mathbb{N} : k \geqslant 4\}$ ja $M = 2$.

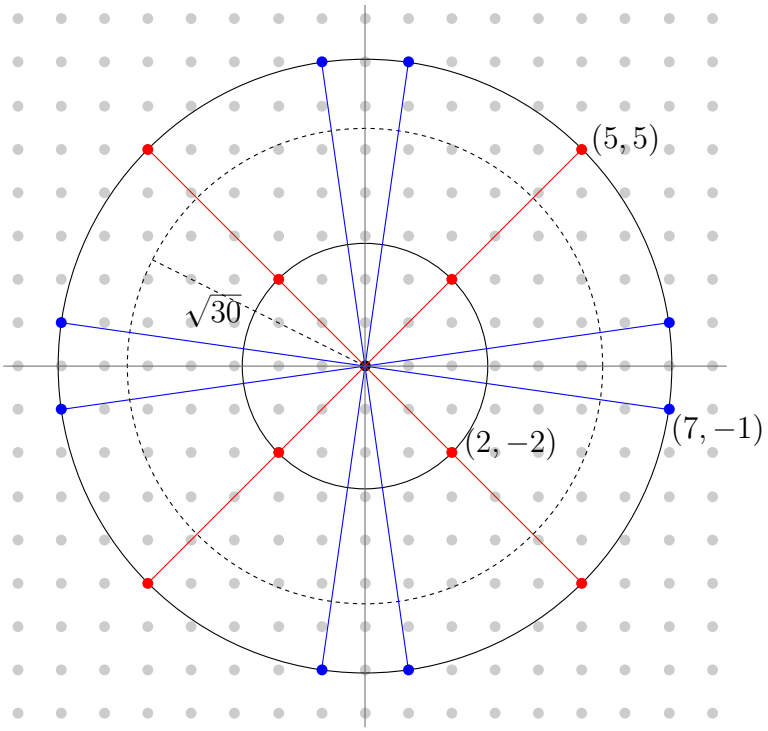
[1] Katso luku 4.2.

7.2 Kahden neliön lause

Luonnollinen luku n on *kahden neliön summa*, jos on $a, b \in \mathbb{Z}$, joille $n = a^2 + b^2$.
Funktio $r_2 \colon \mathbb{N} \to \mathbb{N}$ määritellään asettamalla jokaiselle $n \in \mathbb{N}$

$$r_2(n) = \#\{(a,b) \in \mathbb{Z}^2 : a^2 + b^2 = n\}\,.$$

Kahden neliön summassa sallitaan, että $a = 0$ tai $b = 0$, joten kokonaislukujen neliöt ovat kahden neliön summia. Kahden neliön summalla on geometrinen tulkinta, jota Kuva 7.1 havainnollistaa.



Kuva 7.1 — Luku 8 on kahden neliön summa 4 eri tavalla. Luku 50 on kahden neliön summa 12 eri tavalla. Luku 30 ei ole kahden neliön summa. Tämä näkyy kuvassa siten, että origokeskinen $\sqrt{30}$-säteinen ympyrä ei kulje yhdenkään kokonaislukukertoimisen pisteen kautta.

Luonnollinen luku on kahden neliön summa, jos ja vain jos se on euklidisen tason kokonaislukukertoimisen pisteen normin neliö.

Taulukko 7.1 antaa esityksiä kahden neliön summana niille positiivisillle luonnollisille luvuille $1 \leqslant n \leqslant 60$, joilla tällaisia esityksiä on. Taulukossa annetaan myös arvo $r_2(n)$, joka kertoo, kuinka monella eri tavalla luku n voidaan esittää kahden neliön summana, kun esitykset $a^2 + b^2$ ja $b^2 + a^2$ lasketaan eri esityksiksi, jos $a \neq b$.

Lause 7.2 (Kahden neliön lause)**.** *Positiivinen kokonaisluku n on kahden neliön summa, jos ja vain jos jokaisen alkuluvun $p \equiv 3 \bmod 4$ eksponentti luvun n alkutekijäesityksessä on parillinen.*

Lause 7.2 todistetaan luvussa 7.5. Seuraavissa kahdessa luvussa valmistelemme tarvittavia aputuloksia.

n		$r_2(n)$	alkutekijäesitys	n		$r_2(n)$	alkutekijäesitys
1	0^2+1^2	4	1	31	•	0	31^1
2	1^2+1^2	4	2^1	32	4^2+4^2	4	2^5
3	•	0	3^1	33	•	0	$3^1 11^1$
4	0^2+2^2	4	2^2	34	3^2+5^2	8	$2^1 17^1$
5	1^2+2^2	8	5^1	35	•	0	$5^1 7^1$
6	•	0	$2^1 3^1$	36	0^2+6^2	4	$2^2 3^2$
7	•	0	7^1	37	1^2+6^2	8	37^1
8	2^2+2^2	4	2^3	38	•	0	$2^1 19^1$
9	0^2+3^2	4	3^2	39	•	0	$3^1 13^1$
10	1^2+3^2	8	$2^1 5^1$	40	2^2+6^2	8	$2^3 5^1$
11	•	0	11^1	41	4^2+5^2	8	41^1
12	•	0	$2^2 3^1$	42	•	8	$2^1 3^1 7^1$
13	2^2+3^2	8	13^1	43	•	0	43^1
14	•	0	$2^1 7^1$	44	•	0	$2^2 11^1$
15	•	0	$3^1 5^1$	45	3^2+6^2	8	$3^3 5^1$
16	0^2+4^2	4	2^4	46	•	0	$2^1 23^1$
17	1^2+4^2	8	17^1	47	•	0	47^1
18	3^2+3^2	4	$2^1 3^2$	48	•	0	$2^4 3^1$
19	•	0	19^1	49	0^2+7^2	4	7^2
20	2^2+4^2	8	$2^2 5^1$	50	$5^2+5^2, 1^2+7^2$	12	$2^1 5^2$
21	•	0	$3^1 7^1$	51	•	0	$3^1 17^1$
22	•	0	$2^1 11^1$	52	4^4+6^2	8	$2^2 13^1$
23	•	0	23^1	53	2^2+7^2	8	53^1
24	•	0	$2^3 3^1$	54	•	0	$2^1 3^3$
25	$0^2+5^2, 3^2+4^2$	12	5^2	55	•	0	$5^1 11^1$
26	1^2+5^2	8	$2^1 13^1$	56	•	0	$2^3 7^1$
27	•	0	3^3	57	•	0	$3^1 19^1$
28	•	0	$2^2 7^1$	58	3^2+7^2	8	$2^1 29^1$
29	2^2+5^2	8	29^1	59	•	0	59^1
30	•	0	$2^1 3^1 5^1$	60	•	0	$2^2 3^1 5^1$

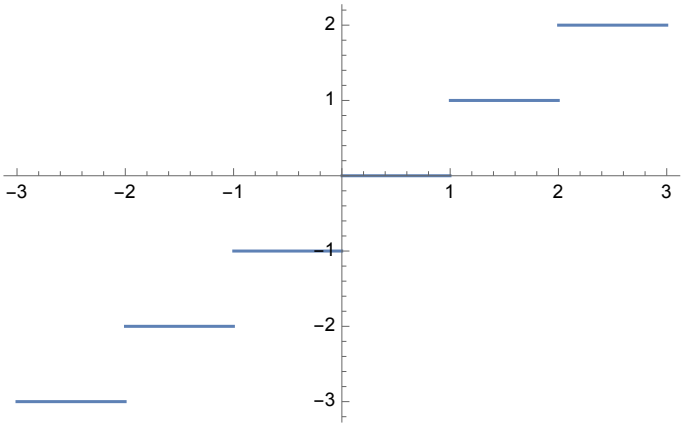
Taulukko 7.1 — Luonnollisten lukujen $1 \leqslant n \leqslant 60$ esityksiä kahden neliön summana. Merkki • tarkoittaa, että luku ei ole kahden neliön summa. Alkutekijäesityksen punaiset termit 3^1, 7^1, 11^1, 19^1, 23^1, 31^1, 43^1, 47^1, 59^1 ja 3^3 antavat viitteitä siitä, mikä alkutekijäesityksen ominaisuus on ratkaiseva kahden neliön summien lukuteoreettisessa luonnehdinnassa. Tässä taulukossa ei esitetä kaikkia tapoja kirjoittaa luku kahden neliön summana, lisää esityksiä saa vaihtamalla neliöitävien lukujen merkkejä ja useimmissa tapauksissa myös niiden järjestystä.

7.3 Kokonaisosa

Olkoon $x \in \mathbb{R}$. Olkoon

$$\lfloor x \rfloor = \max\{k \in \mathbb{Z} : k \leqslant x\}\,.$$

Jos $x > 0$, niin $\lfloor x \rfloor$ on luvun x *kokonaisosa*.



Kuva 7.2 — Funktion $x \mapsto \lfloor x \rfloor$ kuvaajaa. Huomaa, että esimerkiksi $\lfloor -0.5 \rfloor = -1$.

Lemma 7.3. *Olkoon $x \in \mathbb{R}$. Tällöin:*
(1) $0 \leqslant x - \lfloor x \rfloor < 1$.
(2) $\lfloor x \rfloor + \lfloor y \rfloor \leqslant \lfloor x + y \rfloor \leqslant \lfloor x \rfloor + \lfloor y \rfloor + 1$.
(3) Jos $m \in \mathbb{N}^*$, niin $\left\lfloor \dfrac{x}{m} \right\rfloor = \left\lfloor \dfrac{\lfloor x \rfloor}{m} \right\rfloor$.

Todistus. Harjoitustehtävä 7.3. □

Lemma 7.4 (Thuen lemma).[2] *Olkoon p alkuluku ja olkoon $a \in \mathbb{Z}$, $p \nmid a$. Tällöin kahden muuttujan kongruenssiyhtälöllä*

$$ax \equiv y \mod p$$

on ratkaisu $(x_0, y_0) \in \mathbb{Z}^2$, jolle pätee $0 < |x_0|, |y_0| < \sqrt{p}$.

Todistus. Olkoon $f_a \colon \left\{0, 1, 2, \ldots, \lfloor \sqrt{p} \rfloor\right\}^2 \to \mathbb{Z}/p\mathbb{Z}$,

$$f_a(u, v) = u + av \mod p\,.$$

Lemman 7.3(1) nojalla $(\lfloor \sqrt{p} \rfloor + 1)^2 > p$. Kyyhkyslakkaperiaatteen[3] nojalla f_a ei ole injektio, joten on $(u_1, v_1), (u_2, v_2) \in [0, \lfloor \sqrt{p} \rfloor]^2$, joille $u_1 + av_1 \equiv u_2 + av_2 \bmod p$ ja $(u_1, v_1) \neq (u_2, v_2)$. Siis $u_1 - u_2 \equiv a(v_2 - v_1) \bmod p$. Lisäksi $0 \leqslant u_1, v_1, u_2, v_2 < \sqrt{p}$, joten $|u_1 - u_2| < \sqrt{p}$ ja $|v_2 - v_1| < \sqrt{p}$. Siis luvut $x_0 = u_1 - u_2$ ja $y_0 = v_2 - v_1$ toteuttavat väitteen ehdot. □

[2] Axel Thue (1863-1922).

[3] *Kyyhkyslakkaperiaate* eli *lokeroperiaate*: Jos $N + 1$ palloa jaetaan N lokeroon, niin ainakin yhteen lokeroon tulee kaksi palloa.

7.4 Neliönjäännökset

Olkoon $n \in \mathbb{N} - \{0,1\}$. Luku $0 \leqslant r \leqslant n-1$ on *neliönjäännös* $\bmod n$, jos $r \equiv x^2 \bmod n$ jollain $x \in \mathbb{Z}$.[a]

[a] Lukua 0 ei aina lasketa neliönjäännökseksi. Lisäksi, jos n ei ole alkuluku, saatetaan rajoittua lukuihin $1 \leqslant a \leqslant n-1$, joille $\operatorname{syt}(a,n) = 1$.

Kun halutaan määrittää neliönjäännökset $\bmod n$, riittää tarkastella lukujen $0 \leqslant x \leqslant n-1$ neliönjäännökset $\bmod n$, koska $(x+kn)^2 \equiv x^2 \bmod n$ kaikilla $k \in \mathbb{Z}$.

Lemma 7.5. *Olkoon $n \in \mathbb{N} - \{0,1\}$.*

(1) Jos n on parillinen, niin on korkeintaan $\frac{n}{2}+1$ neliönjäännöstä $\bmod n$.

(2) Jos n on pariton, niin on korkeintaan $\frac{n+1}{2}$ neliönjäännöstä $\bmod n$.

(3) Jos p on pariton alkuluku, niin neliönjäännöksiä $\bmod p$ on $\frac{p+1}{2}$.

Todistus. (1) Kaikille $1 \leqslant k \leqslant \frac{n}{2}-1$ pätee $k^2 = (-k)^2 \equiv (n-k)^2 \bmod n$. Lisäksi neliönjäännöksiä antavat 0 ja $\frac{n}{2}$. Siis neliönjäännöksiä on korkeintaan $\frac{n}{2} - 1 + 2 = \frac{n}{2} + 1$.

(2) Todistetaan samaan tapaan kuin kohta (1). Harjoitustehtävä 7.4.

(3) Harjoitustehtävä 7.4. □

Esimerkki 7.6. (1) Luvut $0 = 0^2$, $1 = 1^2 \equiv 4^2 \bmod 5$ ja $4 = 2^2 \equiv 3^2 \bmod 5$ ovat neliönjäännökset $\bmod 5$.

(2) Luvut $0 = 0^2$, $1 = 1^2 \equiv 4^2 \equiv 5^2 \bmod 6$, $3 \equiv 3^2 \bmod 6$ ja $4 = 2^2$ ovat neliönjäännökset $\bmod 6$. Neliöjäännöksiä $\bmod 6$ on suurin mahdollinen määrä $4 = \frac{6}{2}+1$.

(3) Luvut $0 = 0^2$, $1 = 1^2 \equiv 5^2 \equiv 7^2 \equiv 11^2 \bmod 6$,$4 = 2^2 \equiv 4^2 \equiv 8^2 \equiv 10^2 \bmod 12$ ja $9 = 3^2 \equiv 9^2 \bmod 12$ ovat neliönjäännökset $\bmod 12$. Neliöjäännöksiä $\bmod 12$ on siis 4, joka on vähemmän kuin Lemman 7.5 antama yläraja $7 = \frac{12}{2}+1$.

Propositio 7.7. *Olkoon p alkuluku. Tällöin -1 on neliönjäännös $\bmod p$, jos ja vain jos $p = 2$ tai $p \equiv 1 \bmod 4$.*

Todistus. Olkoon $p \equiv 1 \bmod 4$ alkuluku. Olkoon $a = (\frac{p-1}{2})!$. Oletuksen mukaan $\frac{p-1}{2}$ on parillinen, joten Wilsonin lauseen[4] nojalla

$$a^2 = \left(\left(\frac{p-1}{2}\right)!\right)^2 = \left(\frac{p-1}{2}\right)!\left((-1)(-2)\cdots\left(-\frac{p-1}{2}\right)\right) \equiv (p-1)! \equiv -1 \mod p\,.$$

Harjoitustehtävässä 7.6 osoitetaan, että -1 ei ole neliönjäännös $\bmod p$, jos $p \equiv 3 \bmod 4$. Lisäksi $-1 \equiv 1 = 1^2 \bmod 2$. □

Seuraus 7.8. *Olkoot $a, b \in \mathbb{Z}$ ja olkoon $p \equiv 3 \bmod 4$ alkuluku. Jos $p \mid a^2+b^2$, niin $p \mid a$ ja $p \mid b$. Erityisesti $p^2 \mid a^2+b^2$.*

Todistus. Olkoon p alkuluku siten, että $p \mid a^2+b^2$ ja $p \nmid a$. Oletuksen nojalla pätee $a^2 \equiv -b^2 \bmod p$ ja Lemman 5.21 nojalla on $c \in \mathbb{Z}$, jolle $ac \equiv 1 \bmod p$. Siis

$$1 \equiv (ac)^2 = a^2c^2 \equiv -b^2c^2 = -(bc)^2 \mod p\,,$$

joten -1 on neliönjäännös $\bmod p$. Proposition 7.7 nojalla $p = 2$ tai $p \equiv 1 \bmod 4$. □

[4] Lause 5.29.

7.5 Kahden neliön lauseen todistus

Lause 7.9 (Fermat)**.** *Olkoon $p \geqslant 3$ alkuluku. Tällöin p on kahden neliön summa, jos ja vain jos $p \equiv 1 \bmod 4$.*

Todistus. Esimerkissä 1.7 havaittiin, että jokaisen parittoman luvun neliö on kongruentti luvun 1 kanssa mod 4 ja lisäksi jokaisen parillisen luvun neliö on jaollinen luvulla 4. Jos x on kahden neliön summa, niin Lauseen 5.4(1) nojalla pätee $x \equiv 0 \bmod p$, $x \equiv 1 \bmod p$ tai $x \equiv 2 \bmod p$. Siis mikään luku, joka on kongruentti luvun 3 kanssa mod 4, ei ole kahden neliön summa.

Olkoon $p \equiv 1 \bmod 4$ alkuluku ja olkoon $a = (\frac{p-1}{2})!$. Proposition 7.7 nojalla $a^2 \equiv -1 \bmod p$. Thuen lemman[5] nojalla on $x_0, y_0 \in \mathbb{Z}$, joille pätee

$$0 < |x_0|, |y_0| < \sqrt{p} \tag{7.1}$$

ja $ax_0 \equiv y_0 \bmod p$. Siis Lauseen 5.4(3) nojalla

$$-x_0^2 \equiv a^2 x_0^2 = (ax_0)^2 \equiv y_0^2 \mod p\,,$$

joten $p \mid x_0^2 + y_0^2$. Epäyhtälön (7.1) nojalla $0 < x_0^2 + y_0^2 < p + p = 2p$. Siis $x_0^2 + y_0^2 = p$. □

Lemma 7.10 (Diofantos)**.** *Olkoot $a, b, c, d \in \mathbb{Z}$. Tällöin*

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

Todistus. Tämän voi todistaa suoralla laskulla, Harjoitustehtävä 7.7.[6] □

Seuraus 7.11. *Jos luonnolliset luvut x ja y ovat kahden neliön summia, niin xy on kahden neliön summa.* □

Lauseen 7.2 todistus. Harjoituksissa osoitetaan Lauseen 7.9 ja Seurauksen 7.11 avulla, että n on kahden neliön summa, jos jokaisen alkuluvun $p \equiv 3 \bmod 4$ eksponentti luvun n alkutekijäesityksessä on parillinen.

Olkoon $p \equiv 3 \bmod 4$ alkuluku, jolle $p \mid n = a^2 + b^2$. Seurauksen 7.8 nojalla $a = pa_1$ ja $b = pb_1$ joillain $a_1, b_1 \in \mathbb{Z}$, joten $n = p^2(a_1^2 + b_1^2)$.

Olkoon

$$\alpha = \max\{k \in \mathbb{N} : p^k \mid n\}\,.$$

Tällöin $n = p^\alpha n_0$ ja $\operatorname{syt}(p, n_0) = 1$. Jos $\alpha = 2\beta + 1$ on pariton, niin edellä tehty lasku osoittaa, että on luonnolliset luvut a_β, b_β, joille $pn_0 = a_\beta^2 + b_\beta^2$. Seurauksen 7.8 nojalla $p \mid n_0$, mutta tämä on ristiriita. Siis α on parillinen. □

[5] Lemma 7.4.

[6] Algebrallisempi tapa todistaa tämä yhtälö on osoittaa, että Gaussin kokonaislukujen renkaan $\mathbb{Z}[i]$ algebrallinen normi $z \mapsto |z|^2 = z\overline{z}$ on homomorfismi $(\mathbb{Z}[i] - \{0\}, \cdot) \to \mathbb{R}^\times$.

Harjoitustehtäviä

7.1. Määritä luvun 6 rajoittamattomien ositusten lukumäärä.

7.2. Osoita, että luku $n \in \mathbb{N}^*$ voidaan esittää positiivisten kokonaislukujen summana 2^{n-1} tavalla, kun samojen yhteenlaskettavien eri järjestykset lasketaan erikseen kuten Esimerkin 7.1 lopussa. [7]

7.3. Todista Lemma 7.3.

7.4. Todista Lemman 7.5 kohdat (2) ja (3).

7.5. Määritä neliönjäännökset $\bmod 8$.

7.6. Olkoon $p > 2$ alkuluku. Osoita, että $p \equiv 1 \bmod 4$, jos -1 on neliönjäännös $\bmod p$.[8]

7.7. Todista Lemma 7.10.

7.8. (1) Olkoon x kahden neliön summa ja olkoon $y \in \mathbb{Z}$. Osoita, että xy^2 on kahden neliön summa.

(2) Olkoon $n \in \mathbb{N} - \{0\}$ luonnollinen luku, jonka alkutekijäesityksessä (3.1) jokaisen alkuluvun $p \equiv 3 \bmod 4$ eksponentti on parillinen. Osoita, että n on kahden neliön summa.

7.9. Esitä luku 10285 kahden neliön summana.

7.10. Esitä luku 1517 kahden neliön summana.

7.11. Mitkä luvuista 105, 2205 ja 5951 ovat kahden neliön summia?[9]

7.12. Olkoot $x, y, z \in \mathbb{Z}$.

(1) Osoita, että $x^2 + y^2 + z^2 \not\equiv 7 \mod 8$.

(2) Olkoot $x, y, z \in \mathbb{Z}$ siten, että $4 \mid x^2 + y^2 + z^2$. Osoita, että $x \equiv y \equiv z \equiv 0 \mod 2$.

7.13. Olkoon $n = 4^a(8\,b + 7) \in \mathbb{N}$ joillain $a, b \in \mathbb{N}$. Osoita, että n ei ole kolmen kokonaisluvun neliön summa.[10]

[7] Aseta n palikkaa jonoon. Niiden väleissä on $n - 1$ rakoa, joista palikoiden jono voidaan jakaa asettamalla siihen erottaja. Jokaiseen rakoon siis valitaan, laitetaanko siihen erottaja vai ei. Tämän valinnan voi koodata luvuilla 1 ja 0 ...

[8] Fermat'n pieni lause, Lause 5.23.

[9] Esityksiä kahden neliön summina ei kysytä.

[10] Harjoitustehtävä 7.12 ja induktio.

Luku 8

Neljän neliön summat

Luvussa 7 selvitimme, mitkä luonnolliset luvut ovat kahden neliön summia. Tässä luvussa todistamme, että kaikki luonnolliset luvut ovat neljän neliön summia.

8.1 Neljän neliön lause

Lause 8.1 (Lagrange)**.** *Jokainen luonnollinen luku on neljän neliön summa.*

Lauseen todistus palautetaan alkulukujen tarkasteluun Diofantoksen lemman 7.10 vastineen avulla.

Lemma 8.2 (Euler)**.** *Olkoot $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{Z}$. Tällöin*

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = \\ (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ + (x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2)^2 + (x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1)^2 .\end{aligned}$$

Todistus. Harjoitustehtävä 8.1. □

Seuraus 8.3. *Jos luonnolliset luvut x ja y ovat neljä neliön summia, niin xy on neljän neliön summa.* □

Seurauksen 8.3 nojalla riittää näyttää, että jokainen alkuluku on neljän neliön summa.

Lemma 8.4. *Olkoon p alkuluku ja olkoon $m \in \mathbb{N}^*$ parillinen luku, jolle*

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = mp$$

joillain $y_1, y_2, y_3, y_4 \in \mathbb{Z}$. Tällöin yhtälöllä

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = \frac{m}{2}\, p$$

on ratkaisu.

n		$m_2(n)$		n		$r_2(n)$	
1	1^2	1		31	$5^2+2^2+1^2+1^2$	4	$3\cdot 8+7$
2	1^2+1^2	2		32	4^2+4^2	2	
3	$1^2+1^2+1^2$	3		33	$4^2+4^2+1^2$	3	
4	2^2	1		34	5^2+3^2	2	
5	2^2+1^2	2		35	$5^2+3^2+1^2$	3	
6	$2^2+1^2+1^2$	3		36	6^2	1	
7	$2^2+1^2+1^2+1^2$	4	7	37	6^2+1^2	2	
8	2^2+2^2	2		38	$6^2+1^2+1^2$	3	
9	3^2	1		39	$6^2+1^2+1^2+1^2$	4	$4\cdot 8+7$
10	3^2+1^2	2		40	6^2+2^2	2	
11	$3^2+1^2+1^2$	3		41	5^2+4^2	2	
12	$2^2+2^2+2^2$	3		42	$5^2+4^2+1^2$	3	
13	3^2+2^2	2		43	$5^2+3^2+3^2$	3	
14	$3^2+2^2+1^2$	3		44	$6^2+2^2+2^2$	3	
15	$3^2+2^2+1^2+1^2$	4	$8+7$	45	6^2+3^2	2	
16	4^2	1		46	6^2+3^2+1	3	
17	4^2+1^2	2		47	$6^2+3^2+1+1^2$	4	$5\cdot 8+7$
18	3^2+3^2	2		48	$4^2+4^2+4^2$	3	
19	$3^2+3^2+1^2$	3		49	7^2	1	
20	4^2+2^2	2		50	7^2+1^2	2	
21	$4^2+2^2+1^2$	3		51	$7^2+1^2+1^2$	3	
22	$3^2+3^2+2^2$	3		52	6^2+4^2	2	
23	$3^2+3^2+2^2+1^2$	4	$2\cdot 8+7$	53	7^2+2^2	2	
24	$4^2+2^2+2^2$	3		54	$7^2+2^2+1^2$	3	
25	5^2	1		55	$7^2+2^2+1^2+1^2$	4	$6\cdot 8+7$
26	5^2+1^2	2		56	$6^2+4^2+2^2$	3	
27	$5^2+1^2+1^2$	3		57	$7^2+2^2+2^2$	3	
28	$5^2+1^2+1^2+1^2$	4	$4\cdot 7$	58	7^2+3^2	2	
29	5^2+2^2	2		59	$7^2+3^2+1^2$	3	
30	$5^2+2^2+1^2$	3		60	$7^2+3^2+1^2+1^2$	4	$4\,(8+7)$

Taulukko 8.1 — Luonnollisten lukujen $1 \leqslant n \leqslant 60$ esityksiä neliöiden summina. Luku $m_2(n)$ on pienin määrä neliöitä, joiden summana n voidaan esittää. Lauseen 8.1 nojalla luvun n arvoille pätee $m_2(n) \leqslant 4$. Taulukon 60 luvusta yhdeksälle pätee $m_2(n) = 4$. Neljäs ja kahdeksas sarake antavat lukujen esitykset kolmen neliön lauseessa esiintyvässä muodossa.

.

Todistus. Luku mp on parillinen, joten 0, 2 tai 4 luvuista y_1, y_2, y_3, y_4 on parillisia. Erityisesti voimme olettaa, että $y_1 \equiv y_2 \bmod 2$ ja $y_3 \equiv y_4 \bmod 2$. Tällöin luvut

$$x_1 = \frac{y_1 - y_2}{2}\,, \quad x_2 = \frac{y_1 + y_2}{2}\,, \quad x_3 = \frac{y_3 - y_4}{2} \quad \text{ja} \quad x_4 = \frac{y_3 + y_4}{2}$$

ovat kokonaislukuja ja niille pätee

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &= \Big(\frac{y_1 - y_2}{2}\Big)^2 + \Big(\frac{y_1 + y_2}{2}\Big)^2 + \Big(\frac{y_3 - y_4}{2}\Big)^2 + \Big(\frac{y_3 + y_4}{2}\Big)^2 \\ &= \frac{y_1^2 + y_2^2 + y_3^2 + y_4^2}{2} = \frac{m}{2}\,p\,. \end{aligned}$$

□

Propositio 8.5. *Olkoon p alkuluku ja olkoot $a, b, c \in \mathbb{Z}$. Kongruenssiyhtälöllä*

$$ax^2 + by^2 + cz^2 \equiv 0 \mod p$$

on ratkaisu $(x, y, z) \in \mathbb{Z}^3 - \{0, 0, 0\}$.

Todistus. Jos $a \equiv 0 \bmod p$, niin $x = 1$, $y = 0 = z$ on ratkaisu ja vastaavasti saadaan ratkaisuja, jos $b = 0$ tai $c = 0$. Siis voimme olettaa, että $a, b, c \not\equiv 0 \mod p$.

Jos $p = 2$, niin juuri tehdyn oletuksen nojalla $a \equiv b \equiv c \equiv 1 \bmod 2$. Esimerkiksi $a + b \equiv 1 + 1 \equiv 0 \mod 2$, joten $x = 1 = y$, $z = 0$ on ratkaisu.

Jos $p > 2$, niin $p - 1$ on parillinen. Olkoot

$$\mathscr{S} = \Big\{a + by^2 : 0 \leqslant y \leqslant \frac{p-1}{2}\Big\}$$

ja

$$\mathscr{T} = \Big\{ -cz^2 : 0 \leqslant z \leqslant \frac{p-1}{2}\Big\}\,.$$

Jos $a + by_1 \equiv a + by_2^2$, niin Lauseen 5.4(1) nojalla

$$0 \equiv by_1 - by_2^2 = b(y_1 + y_2)(y_1 - y_2)\,.$$

Supistussäännön[1] nojalla $y_1 \equiv y_2$ tai $y_1 \equiv -y_1$. Joukkojen $\mathscr{S}$ ja $\mathscr{T}$ määritelmien nojalla $0 \leqslant y_1, y_2 \leqslant \frac{p-1}{2}$, joten saamme $y_1 = y_2$. Siis joukossa $\mathscr{S}$ on $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ alkiota, jotka ovat kaikki eri kongruenssiluokissa. Samalla tavalla nähdään, että joukossa $\mathscr{T}$ on myös $\frac{p+1}{2}$ alkiota, jotka ovat kaikki eri kongruenssiluokissa. Kongruenssiluokkia $\bmod p$ on $p < p + 1 = \frac{p+1}{2} + \frac{p+1}{2}$, joten kyyhkyslakkaperiaatteen nojalla on $0 \leqslant y_0, z_0 \leqslant \frac{p-1}{2}$, joille $a + by_0^2 \equiv -cz_0^2 \mod p$. Siis $a\,1^2 + by_0^2 + cz_0^2 \equiv 0 \mod p$, joten $(1, y_0, z_0)$ on haluttu ratkaisu. □

Lemma 8.6. *Olkoon p pariton alkuluku. On pariton luonnollinen luku $0 < m < p$, jolle yhtälöllä*

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp$$

on ratkaisu

[1] Seuraus 5.9.

Todistus. Proposition 8.5 nojalla on $x_2, x_3 \in \mathbb{N}$, $0 \leqslant x_2, x_3 \leqslant \frac{p-1}{2}$ ja $k \in \mathbb{N}^*$, joille pätee

$$kp = 1 + x_2^2 + x_3^2 + 0^2 \leqslant 1 + \frac{(p-1)^2}{4} + \frac{(p-1)^2}{4} < \frac{p^2}{2}\,.$$

Siis haluttu yhtälö pätee jollain luonnollisella luvulla $0 < k < p$.

Jos k on pariton, niin väite on todistettu. Oletetaan siis, että k on parillinen. Lemman 8.4 nojalla yhtälöllä

$$1 + x_2^2 + x_3^2 + 0^2 = \frac{k}{2}\,p$$

on ratkaisu. Jos $\frac{k}{2}$ on pariton, väite on todistettu. Muuten voimme soveltaa Lemmaa 8.4 riittävän monta kertaa kunnes päädymme parittomaan lukuun $\frac{k}{2^\ell}$. □

Propositio 8.7. *Jokainen alkuluku on neljän neliön summa.*

Todistus. Alkuluku $p = 2 = 1^2 + 1^2 + 0^2 + 0^2$ on neljän neliön summa.

Olkoon p pariton alkuluku. Lemman 8.6 nojalla on pariton $m \in \mathbb{N}^*$, $m < p$, ja kokonaisluvut x_1, x_2, x_3, x_4, joille pätee

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp\,. \tag{8.1}$$

Oletetaan, että $m > 1$. Olkoot

$$-\frac{m}{2} < a_1, a_2, a_3, a_4 < \frac{m}{2}$$

siten, että $a_i \equiv x_i \bmod m$ kaikilla $1 \leqslant i \leqslant 4$.[2] Tällöin

$$a_1^2 + a_2^2 + a_3^3 + a_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \mod m\,.$$

Siis on $\ell \in \mathbb{N}$, jolle $a_1^2 + a_2^2 + a_3^3 + a_4^2 = \ell m$.

Luvut a_1, a_2, a_3, a_4 valittiin siten, että

$$a_1^2 + a_2^2 + a_3^3 + a_4^2 < 4\left(\frac{m}{2}\right)^2 = m^2$$

joten $\ell < m$. Jos $\ell = 0$, niin $a_1 = a_2 = a_3 = a_4 = 0$. Tällöin $x_1, x_2, x_3, x_4 \equiv 0 \bmod m$. Yhtälön (8.1) nojalla siis pätee $m^2 \mid mp$, joten $m \mid p$, mutta tämä on mahdotonta, koska $1 < m < p$ ja p on alkuluku. Siis $0 < \ell < m$.

Lemman 8.2 nojalla

$$\begin{aligned} m^2\ell p = mp\ell m =& \left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right)\left(a_1^2 + a_2^2 + a_3^3 + a_4^2\right) && (8.2)\\ =& (x_1a_1 + x_2a_2 + x_3a_3 + x_4a_4)^2 + (x_1a_2 - x_2a_1 + x_3a_4 - x_4a_3)^2 && (8.3)\\ &+ (x_1a_3 - x_2a_4 - x_3a_1 + x_4a_2)^2 + (x_1a_4 + x_2a_3 - x_3a_2 - x_4a_1)^2\,. && (8.4) \end{aligned}$$

Lukujen a_1, a_2, a_3, a_4 valinnan nojalla

$$\begin{aligned} x_1a_1 + x_2a_2 + x_3a_3 + x_4a_4 &\equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \equiv 0 \mod m\\ x_1a_2 - x_2a_1 + x_3a_4 - x_4a_3 &\equiv x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3 = 0 \mod m\\ x_1a_3 - x_2a_4 - x_3a_1 + x_4a_2 &\equiv x_1x_3 - x_2x_4 - x_3x_1 + x_4x_2 = 0 \mod m \text{ ja}\\ x_1a_4 + x_2a_3 - x_3a_2 - x_4a_1 &\equiv x_1x_4 + x_2x_3 - x_3x_2 - x_4x_1 = 0 \mod m\,, \end{aligned}$$

[2] Huomaa, että $\frac{m}{2}$ ei ole kokonaisluku.

joten valitsemalla

$$y_1 = \frac{x_1a_1 + x_2a_2 + x_3a_3 + x_4a_4}{m} \in \mathbb{Z}\,,$$
$$y_2 = \frac{x_1a_2 - x_2a_1 + x_3a_4 - x_4a_3}{m} \in \mathbb{Z}\,,$$
$$y_3 = \frac{x_1a_3 - x_2a_4 - x_3a_1 + x_4a_2}{m} \in \mathbb{Z} \quad \text{ja}$$
$$y_4 = \frac{x_1a_4 + x_2a_3 - x_3a_2 - x_4a_1}{m} \in \mathbb{Z}\,,$$

saamme yhtälön (8.2) nojalla

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = \frac{m^2\ell p}{m^2} = \ell p\,.$$

Lemman 8.4 nojalla voimme olettaa, että ℓ on pariton. Jos $\ell > 1$, niin voimme toistaa edellä tehdyn päättelyn ja löytää ratkaisun yhtälölle

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = mp\,,$$

jollain parittomalla luvulla $1 \leqslant m < \ell$. Näin jatkettu prosessi päättyy äärellisen monen askeleen jälkeen ja antaa lopulta ratkaisun yhtälölle $y_1^2 + y_2^2 + y_3^2 + y_4^2 = p$. □

Lauseen 8.1 todistus. Väite seuraa Propositiosta 8.7 ja Lemmasta 8.2. □

8.2 Waringin ongelma

Olkoon $k \in \mathbb{N}^*$ ja olkoon

$$g(k) = \inf\left\{\ell \in \mathbb{N}^* : \forall n \in \mathbb{N}\ \exists\ x_1, x_2, \ldots, x_\ell \in \mathbb{N}^*, \text{ joille } n = \sum_{j=1}^{\ell} x_j^k\right\}.$$

Jos $g(k) \neq \infty$, niin se antaa pienimmän määrän ℓ, jolla kaikki luonnolliset luvut voidaan esittää ℓ kokonaisluvun k. potenssin summana. Luvun $g(k)$ äärellisyyskysymys on *Waringin*[3] *ongelma*. Hilbert ratkaisi vuonna sen 1909.

Lause 8.8 (Hilbert)**.** *Luku $g(k)$ on äärellinen jokaisella $k \in \mathbb{N}$.*

Esimerkki 8.9. Neljän neliön lauseen nojalla $g(2) \leqslant 4$. Toisaalta 7 ei ole kolmen neliön summa, koska ainoat neliöt, jotka ovat korkeintaan 7 ovat $1 = 1^2$ ja $2 = 2^2$, joista 7 saadaan ainoastaan summana $7 = 2^2 + 1^2 + 1^2 + 1^2$. Siis $g(2) = 4$.

Esimerkissä 8.9 tehty havainto voidaan laajentaa kolmen neliön summien täydelliseksi kuvailuksi.

Lause 8.10 (Kolmen neliön lause)**.** *Jokainen positiivinen luonnollinen luku, joka ei ole muotoa $4^a(8k + 7)$ joillain $a, k \in \mathbb{N}$, on kolmen neliön summa.*

Todistus. Harjoitustehtävässä 7.13 osoitetaan, että luku $4^a(8k + 7)$ ei ole kolmen neliön summa millään $a, k \in \mathbb{N}$. Toinen suunta on vaativampi. Se todistetaan esimerkiksi lähteissä [Lan2, Thm. 187] ja [TB, Thm. 9.8]. □

[3] Edward Waring (1736-1798).

8.3 Diofantoksen ja Eulerin lemmoista

Tässä luvussa oletamme, että kompleksilukujen perusominaisuudet ovat tunnettuja. Ne on esitetty tiiviisti esimerkiksi lähteen [Par] luvussa 1.8. Olkoot $z = x+iy, w = u+iv \in \mathbb{C}$. Tällöin

$$zw = (x + iy)(u + iv) = (xu - yv) + i(xv + yu)\,. \tag{8.5}$$

Kompleksiluvun $z = x + iy \in \mathbb{C}$ *algebrallinen normi* on

$$\mathbf{n}(z) = z\overline{z} = x^2 + y^2\,.$$

Lemma 8.11. *Olkoot $z, w \in \mathbb{C}$. Tällöin $\mathbf{n}(zw) = \mathbf{n}(z)\mathbf{n}(w)$.* □

Gaussin kokonaisluvut on kompleksilukujen kunnan alirengas[a]

$$\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}\,.$$

[a] Katso [Par, Luku 4.3].

Lemma 8.12. *Luonnollinen luku n on kahden neliön summa, jos ja vain jos $n = \mathbf{n}(z)$ jollekin $z \in \mathbb{Z}[i]$.* □

Diofantoksen lemman 7.10 toinen todistus. Olkoot m ja n kahden neliön summia. Lemman 8.12 nojalla on $z = x + iy, w = u + iv \in \mathbb{Z}[i]$, joille $m = \mathbf{n}(z)$ ja $n = \mathbf{n}(z)$. Tällöin Lemman 8.11 ja yhtälön (8.5) nojalla

$$mn = \mathbf{n}(z)\mathbf{n}(w) = \mathbf{n}(zw) = \mathbf{n}((xu - yv) + i(xv + yu)) = (xu - yv)^2 + (xv + yu)^2$$

on kahden neliön summa. □

Eulerin lemma 8.2 voidaan todistaa samaan tapaan kuin Diofantoksen lemma käyttämällä kompleksilukujen sijaan *Hamiltonin kvaternioita*

$$\mathbb{H} = \{x_0 + x_1\mathbf{i} + x_2\,\mathbf{j} + x_3\,\mathbf{k} : x_0, x_1, x_2, x_3 \in \mathbb{R}\}\,,$$

missä $\mathbf{i}$,$\mathbf{j}$ ja $\mathbf{k}$ toteuttavat yhtälöt

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 \tag{8.6}$$

ja

$$\mathbf{ij} = \mathbf{k} = -\mathbf{ji}, \quad \mathbf{ki} = \mathbf{j} = -\mathbf{ik}, \quad \mathbf{jk} = \mathbf{i} = -\mathbf{kj}. \tag{8.7}$$

Kvaternioiden yhteenlasku määritellään kuten avaruudessa $\mathbb{R}^4$ ja niiden kertolasku määritellään ottaen huomioon yhtälöt (8.6) ja (8.7). Gaussin kokonaislukujen sijaan tarkastellaan *Lipschitzin kokonaislukuja*

$$L = \{x_0 + x_1\mathbf{i} + x_2\,\mathbf{j} + x_3\,\mathbf{k} : x_0, x_1, x_2, x_3 \in \mathbb{Z}\}\,.$$

Harjoitustehtäviä

8.1. Todista Lemma 8.2.

8.2. Esitä luku 2024 neljän neliön summana.

8.3. Esitä luku 29887 neljän neliön summana.

8.4. Osoita, että $g(3) \geqslant 9$ ja $g(4) \geqslant 19$.[4]

[4]Katso luku 8.2.

Luku 9

Pythagoraan kolmikot ja Fermat'n suuri lause

Tässä luvussa tarkastelemme epälineaarisia Diofantoksen yhtälöitä

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

kun $n \geqslant 2$. Tapauksessa $n = 2$ yhtälöllä on äärettömän monta ratkaisua, joita kutsutaan Pythagoraan kolmikoiksi. Parametrisoimme nämä ratkaisut luvussa 9.1. Jos $n \geqslant 3$, niin $(0, 0, 0)$ on ainoa ratkaisu. Tämä on *Fermat'n suuri lause*, johon tutustumme luvussa 9.2. Todistamme tapauksen $n = 4$ Pythagoraan kolmikoiden avulla.

9.1 Pythagoraan kolmikot

Olkoot $a, b, c \in \mathbb{N}^*$. Jos

$$a^2 + b^2 = c^2,$$

niin (a, b, c) on *Pythagoraan kolmikko*. Jos lisäksi $\operatorname{syt}(a, b, c) = 1$, niin (a, b, c) on *primitiivinen Pythagoraan kolmikko*.

Esimerkki 9.1. (1) $(3, 4, 5)$, $(5, 12, 13)$ ja $(8, 15, 17)$ ovat primitiivisiä Pythagoraan kolmikoita.

(2) Jos (a, b, c) on Pythagoraan kolmikko ja $k \in \mathbb{N}^*$, niin (ka, kb, kc) on Pythagoraan kolmikko, joka ei ole primitiivinen, jos $k \geqslant 2$.

(3) Jaollisuussäännöistä ja Pythagoraan kolmikot määrittelevästä yhtälöstä seuraa, että $\operatorname{syt}(a, b, c) > 1$, jos $\operatorname{syt}(a, b) > 1$, $\operatorname{syt}(b, c) > 1$ tai $\operatorname{syt}(a, c) > 1$.

Tässä luvussa osoitamme, että Pythagoraan kolmikot voi parametrisoida parittomien luonnollisten lukujen pareilla, jotka ovat suhteellisia alkulukupareja. Sitä ennen pohdimme, mitä lukuja primitiivisessä kolmikossa (a, b, c) voi olla.

Lemma 9.2. *(1) Olkoon (a, b, c) Pythagoraan kolmikko. Tällöin $a \geqslant 3$, $b \geqslant 3$ ja $c \geqslant 3$.*
(2) Olkoon $a \in \mathbb{N}$, $a \geqslant 3$. Tällöin on $b, c \in \mathbb{N}^*$ siten, että (a, b, c) on Pythagoraan kolmikko.

Todistus. (1) Kaksi ensimmäistä neliöä 1^2 ja $2^2 = 4$ eivät ole kahden neliön summia, joten jokaiselle Pythagoraan kolmikolle pätee $c \geqslant 3$.

Koska $a^2 < a^2 + 1^2 < (a+1)^2$, niin $a^2 + 1^2$ ei ole neliö millään $a \in \mathbb{N}^*$. Siis $b \geqslant 2$. Vastaavasti nähdään, että $a \geqslant 2$.

Jos $b = 2$, niin tietoa $a \geqslant 2$ käyttäen saadaan

$$a^2 < a^2 + b^2 = a^2 + 4 < (a+1)^2 ,$$

joen $a^2 + b^2$ ei ole neliö. Siis $b > 2$. Samaan tapaan nähdään, että $a > 2$.

(2) Jos $a \geqslant 3$ on pariton, niin a^2 on pariton ja $\frac{a^2+1}{2}, \frac{a^2-1}{2} \in \mathbb{N}^*$. Lasku osoittaa, että

$$\Big(\frac{a^2+1}{2}\Big)^2 - \Big(\frac{a^2-1}{2}\Big)^2 = a^2 ,$$

joten $(a, \frac{a^2-1}{2}, \frac{a^2+1}{2})$ on Pythagoraan kolmikko. Jos a on parillinen, niin $\frac{a^2}{4} \in \mathbb{N}^*$ ja

$$\Big(\frac{a^2}{4} + 1\Big)^2 - \Big(\frac{a^2}{4} - 1\Big)^2 = a^2 ,$$

joten $(a, \frac{a^2}{4} - 1, \frac{a^2}{4} + 1)$ on Pythagoraan kolmikko. □

Esimerkki 9.3. Taulukko 9.1 luettelee Lemman 9.2 antamat Pythagoraan kolmikot parametrin a arvoilla $3 \leqslant a \leqslant 20$. Lauseen 9.5 todistuksessa näemme, että parametrin a parittomat arvot antavat primitiivisia Pythagoraan kolmikoita. Sen sijaan kaikki parilliset parametrin a arvot eivät anna primitiivisiä kolmikoita.

a	(a, b, c)	a	(a, b, c)
3	$(3, 4, 5)$	4	$(4, 3, 5)$
5	$(5, 12, 13)$	6	$(6, 8, 10)$
7	$(7, 24, 25)$	8	$(8, 15, 17)$
9	$(9, 40, 41)$	10	$(10, 24, 26)$
11	$(11, 60, 61)$	12	$(12, 35, 37)$
13	$(13, 84, 85)$	14	$(14, 48, 50)$
15	$(15, 112, 113)$	16	$(16, 63, 65)$
17	$(17, 144, 145)$	18	$(18, 80, 82)$
19	$(19, 180, 181)$	20	$(20, 99, 101)$

Taulukko 9.1 — Lemman 9.2 antamia Pythagoraan kolmikoita.

Lemma 9.4. *Olkoon (a, b, c) primitiivinen Pythagoraan kolmikko. Tällöin $a \not\equiv b \bmod 2$ ja $c \equiv 1 \bmod 2$.*

Todistus. (1) Jos $a \equiv b \equiv 0 \bmod 2$, niin $a^2 \equiv b^2 \equiv 0 \bmod 2$. Siten $c^2 = a^2 + b^2 \equiv 0 \mod 2$, joten Eukleideen lemman[1] nojalla $c \equiv 0 \mod 2$. Tämä on mahdotonta, sillä primitiiviselle Pythagoraan kolmikolle pätee $\operatorname{syt}(a, b, c) = 1$.

Jos $a \equiv b \equiv 1 \mod 2$, niin $a^2 \equiv b^2 \equiv 1 \mod 2$, joten $c^2 = a^2 + b^2 \equiv 0 \mod 2$. Tällöin[2]

$$2 \equiv a^2 + b^2 = c^2 \equiv 0 \mod 4\,.$$

Tämä on mahdotonta. □

Olkoon

$$J = \{(s,t) \in \mathbb{N}^* \times \mathbb{N}^* : s \equiv t \equiv 1 \bmod 2\,,\ \operatorname{syt}(s,t) = 1\,,\ s > t\}$$

ja olkoon $\mathrm{P}\colon J \to (\mathbb{N}^*)^3$,

$$\mathrm{P}(s,t) = \left(st, \frac{s^2 - t^2}{2}, \frac{s^2 + t^2}{2}\right).$$

Lause 9.5. *Kuvaus* P *on injektio ja sen kuvajoukko* $\mathrm{P}(J)$ *on niiden primitiivisten Pythagoraan kolmikoiden joukko, joilla* a *pariton.*

Todistus. Olkoon (a, b, c) primitiivinen Pythagoraan kolmikko. Tällöin

$$a^2 = c^2 - b^2 = (c - b)(c + b). \tag{9.1}$$

Näytetään, että $\operatorname{syt}(c - b, c + b) = 1$ ja että $c - b$ ja $c + b$ ovat neliöitä eli $c + b = s^2$ ja $c - b = t^2$ joillain $s, t \in \mathbb{N}$.

Jos d on alkuluku, jolle $d \mid (c - b)$ ja $d \mid (c + b)$, niin jaollisuuslauseen perusteella d jakaa myös luvut

$$(c + b) + (c - b) = 2c \quad \text{ja} \quad (c + b) - (c - b) = 2b.$$

Siten $d \mid 2c$ ja $d \mid 2b$. Eukleideen lemman ja Esimerkin 9.1(3) nojalla $d = 2$. Koska toisaalta d jakaa myös luvun $(c - b)(c + b) = a^2$ ja a^2 on pariton, niin $d \neq 2$. On siis $\operatorname{syt}(c - b, c + b) = 1$.

Koska $\operatorname{syt}(c - b, c + b) = 1$ ja $(c - b)(c + b) = a^2$, niin alkutekijäesityksen yksikäsitteisyydestä seuraa, että $c - b$ ja $c + b$ ovat neliöitä eli on luvut $s, t \in \mathbb{N}^*$, $s > t$, joille

$$c + b = s^2 \quad \text{ja} \quad c - b = t^2.$$

Nyt

$$c = \frac{s^2 + t^2}{2}, \qquad b = \frac{s^2 - t^2}{2}$$

ja siten yhtälön (9.1) nojalla

$$a = \sqrt{(c - b)(c + b)} = st.$$

Toisaalta, jos s, t, a, b ja c ovat kuten oletuksissa, niin

$$a^2 + b^2 = s^2t^2 + \frac{s^4 - 2s^2t^2 + t^4}{4} = \frac{s^4 + 2s^2t^2 + t^4}{4} = c^2$$

[1] Lemma 3.9.

[2] Katso Esimerkki 1.7.

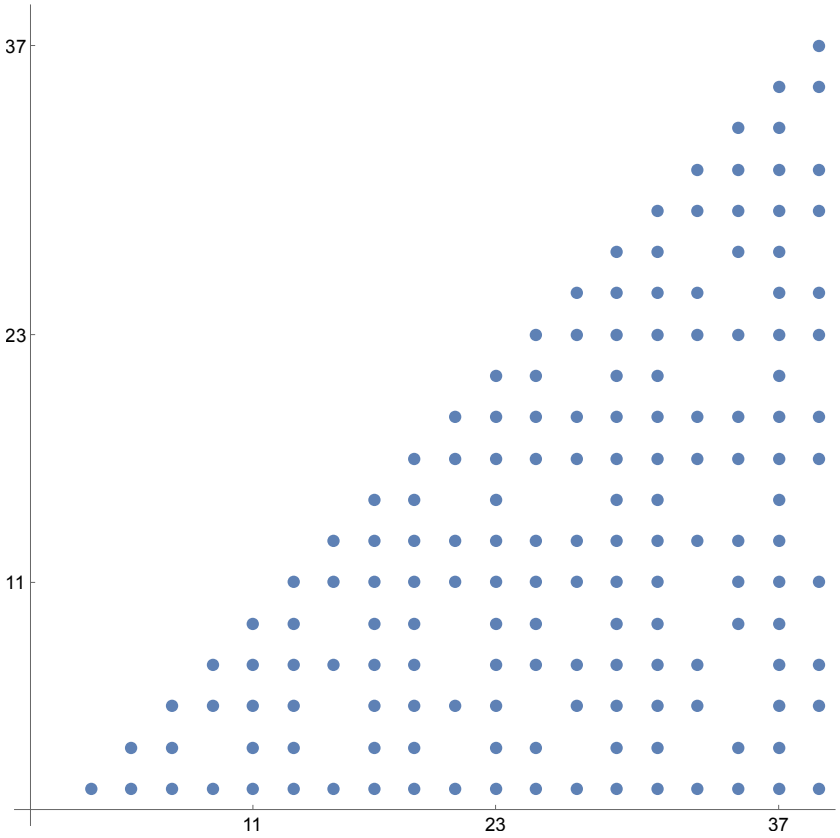
eli (a, b, c) on Pythagoraan kolmikko.

Osoitetaan, että näin saatu Pythagoraan kolmikko on primitiivinen. Oletetaan, että on alkuluku p, jolle $p \mid a$ ja $p \mid b$. Koska s ja t ovat parittomia, niin a on pariton ja siten p on pariton. Jaollisuuslauseen nojalla $p \mid c^2$ ja Eukleideen lemman nojalla $p \mid c$. Siten p jakaa luvun $b + c = s^2$. Eukleideen lemmasta seuraa, että $p \mid s$. Jaollisuuslauseen nojalla p jakaa myös luvun $2b - s^2 = t^2$ ja Eukleideen lemman perusteella $p \mid t$. Tämä on mahdotonta, sillä $\text{syt}(s, t) = 1$. Siis (a, b, c) on primitiivinen.

Kuvauksen P injektiivisyys seuraa siitä, että $s^2 = b + c$ ja $t^2 = c - b$, joten nämä parametrit määräävät luvut s ja t yksikäsitteisesti joukossa J. □

Seuraus 9.6. *Primitiivisien Pythagoraan kolmikoiden joukko on ääretön.*

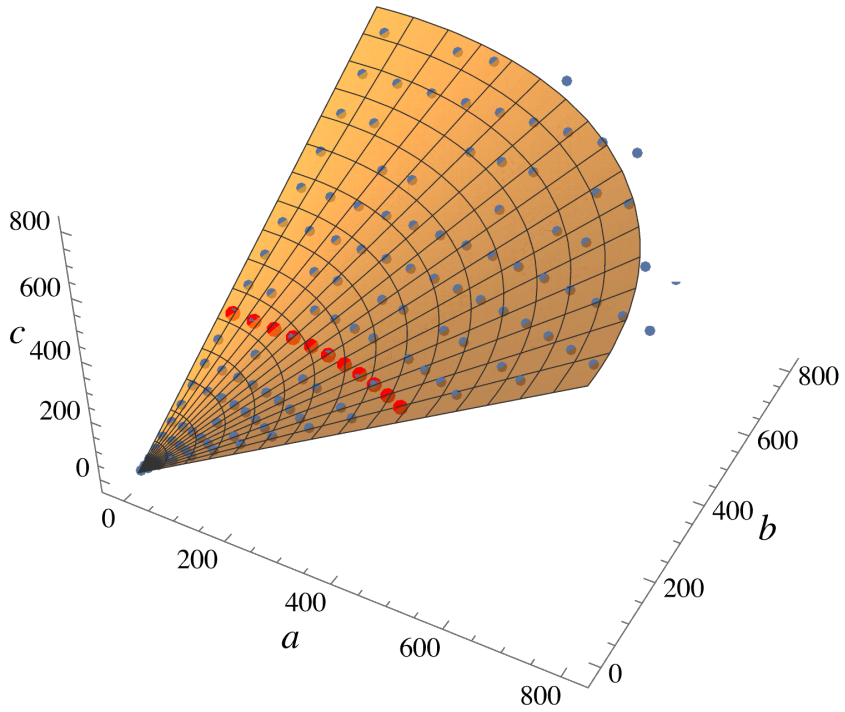
Todistus. Joukko J on ääretön, koska se sisältää esimerkiksi joukon $\{(2k+1, 1) : k \in \mathbb{N}^*\}$. Väite seuraa, koska kuvaus P on injektio. □



Kuva 9.1 — Joukko J.

(s, t)	(a, b, c)
$(23, 1)$	$(23, 264, 265)$
$(23, 3)$	$(69, 260, 269)$
$(23, 5)$	$(115, 252, 277)$
$(23, 7)$	$(161, 240, 289)$
$(23, 9)$	$(207, 224, 305)$
$(23, 11)$	$(253, 204, 325)$
$(23, 13)$	$(299, 180, 349)$
$(23, 15)$	$(345, 152, 377)$
$(23, 17)$	$(391, 120, 409)$
$(23, 19)$	$(437, 84, 445)$
$(23, 21)$	$(483, 44, 485)$

Taulukko 9.2 — Pythagoraan kolmikoita, jotka vastaavat parametreja, joissa $s = 23$.



Kuva 9.2 — Pythagoraan kolmikoita, joille $s \leqslant 39$ kartiolla $a^2 + b^2 = c^2$. Kolmikot, jotka vastaavat parametreja, joissa $s = 23$, on merkitty punaisella.

9.2 Fermat'n lause - tapaus $n = 4$

Lause 9.7 (Fermat'n suuri lause)**.** *Olkoon $n \geqslant 3$ luonnollinen luku. Diofantoksen yhtälöllä*

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

ei ole ratkaisua, jolle $xyz \neq 0$.

Todistus. Tämän lauseen todistus on erittäin syvällinen ja pitkä, emmekä käsittele sitä tällä kurssilla. Todistuksessa käytettävää matematiikkaa esitellään esimerkiksi kirjassa [Hel]. □

Lause 9.8. *Diofantoksen yhtälöllä $x^4 + y^4 = z^2$ ei ole ratkaisua, jolle $xyz \neq 0$.*

Lause 9.8 antaa välittämänä seurauksena Fermat'n lauseen erikoistapauksen, jossa $n = 4$.

Seuraus 9.9. *Diofantoksen yhtälöllä*

$$x^4 + y^4 = z^4$$

ei ole ratkaisua, jolle $xyz \neq 0$. □

Lauseen 9.8 todistus. Oletetaan, että yhtälöllä on muita ratkaisuja. Jos (x, y, z) on ratkaisu, niin $\big(|x|, |y|, |z|\big)$ on ratkaisu, joten riittää tarkastella *positiivisia* ratkaisuja, joissa kaikki luvut ovat positiivisia. Olkoon (a, b, c) positiivinen ratkaisu, jossa

$$c = \min\{z \in \mathbb{N}^* : x^4 + y^4 = z^2 \text{ joillain } x, y \in \mathbb{N}^*\}\,.$$

Tällöin (a, b, c) on *minimaalinen ratkaisu*.

Jaollisuuslauseen 1.3 nojalla $\operatorname{syt}(a, b)^4 \mid c^2$. Jos $\operatorname{syt}(a, b) > 1$, niin jollekin alkuluvulle p pätee $p \mid \operatorname{syt}(a, b)$. Tällöin $p^4 \mid c^2$, joten Eukleideen lemman[3] nojalla $p^2 \mid c$. Siis

$$\left(\frac{a}{p}\right)^4 + \left(\frac{b}{p}\right)^4 = \left(\frac{c}{p^2}\right)^2,$$

joten (a, b, c) ei ole minimaalinen ratkaisu. Siis $\operatorname{syt}(a, b) = 1$, joten (a^2, b^2, c) on primitiivinen Pythagoraan kolmikko.

Oletamme siis, että a on pariton ja b on parillinen. Lauseen 9.5 nojalla on parittomat keskenään jaottomat luonnolliset luvut $t < s$, joille

$$a^2 = st\,, \tag{9.2}$$

$$b^2 = \frac{s^2 - t^2}{2} \quad \text{ja} \tag{9.3}$$

$$c = \frac{s^2 + t^2}{2}\,. \tag{9.4}$$

Esimerkin 1.7 nojalla $st \equiv 1 \bmod 4$, joten

$$s \equiv t \equiv 1 \bmod 4 \quad \text{tai} \quad s \equiv t \equiv 3 \bmod 4\,. \tag{9.5}$$

Yhtälön (9.3) nojalla

$$2b^2 = s^2 - t^2 = (s - t)(s + t)\,. \tag{9.6}$$

[3]Lemma 3.9.

Tulon tekijät $s-t$ ja $s+t$ ovat parillisia, koska $s \equiv t \equiv 1 \bmod 2$, joten $\operatorname{syt}(s-t, s+t) \geqslant 2$. Lisäksi vaihtoehtojen (9.5) nojalla $s - t \equiv 0 \bmod 4$. Jos $d \mid (s - t)$ ja $d \mid s + t$, niin $d \mid \operatorname{syt}(2s, 2t)$. Lemman 2.9 nojalla $\operatorname{syt}(2s, 2t) = 2\operatorname{syt}(s, t) = 2$, joten $d \leqslant 2$. Siis

$$\operatorname{syt}(s - t, s + t) = 2\,. \tag{9.7}$$

Yhtälön (9.6) nojalla on $u, v \in \mathbb{N}^*$, joille $s + t = 2u^2$, $s - t = 4v^2$ ja $\operatorname{syt}(u, 2v) = 1$. Tällöin $s = u^2 + 2v^2$ ja $t = u^2 - 2v^2$, joten yhtälön (9.2) nojalla $a^2 = u^4 - 4v^4$. Siis

$$a^2 + (2v^2)^2 = a^2 + 4v^4 = u^4 = (u^2)^2\,, \tag{9.8}$$

joten $(a, 2v^2, u^2)$ on primitiivinen Pythagoraan kolmikko. Huomaa, että $u < c$, koska $v \geqslant 1$ ja yhtälön (9.4) nojalla $c = u^4 + 4v^2$.

Lauseen 9.5 nojalla on parittomat keskenään jaottomat luonnolliset luvut $T < S$, joille

$$a = ST\,, \quad 2v^2 = \frac{S^2 - T^2}{2} \text{ ja } u^2 = \frac{S^2 + T^2}{2}\,. \tag{9.9}$$

Keskimmäisen yhtälön (9.9) nojalla

$$4v^2 = S^2 - T^2 = (S - T)(S + T)\,. \tag{9.10}$$

Samalla tavalla kuin yhtälö (9.7), saamme $\operatorname{syt}(S - T, S + T) = 2$, joten yhtälön (9.10) nojalla joillakin $A, B \in \mathbb{N}^*$ pätee $S - T = 2A^2$ ja $S + T = 2B^2$. Siis $S = A^2 + B^2$ ja $T = A^2 - B^2$, joten oikeanpuoleisen yhtälön (9.9) nojalla

$$u^2 = \frac{(A^2 + B^2)^2 + (A^2 - B^2)^2}{2} = A^4 + B^4\,.$$

Edellä näimme, että $0 < u < c$, joten (a, b, c) ei ole minimaalinen ratkaisu ja olemme päätyneet ristiriitaan. □

Lauseen 9.8 todistuksessa käytettävä *Fermat'n äärettömän laskeutumisen menetelmä* on tärkeä todistustekniikka. Tässä menetelmässä oletetaan jonkin väitteen pätevän luonnollisella luvulla $n \geqslant 1$, jonka oletetaan olevan minimaalinen. Sitten osoitetaan, että n ei ole minimaalinen.

Harjoitustehtäviä

9.1. Olkoon (a, b, c) primitiivinen Pythagoraan kolmikko. Osoita, että a tai b on jaollinen luvulla 3, mutta c ei ole jaollinen luvulla 3.

9.2. Olkoon (a, b, c) primitiivinen Pythagoraan kolmikko. Osoita, että a tai b on jaollinen luvulla 4, mutta c ei ole jaollinen luvulla 4.

9.3. Olkoon (a, b, c) primitiivinen Pythagoraan kolmikko. Osoita, että täsmälleen yksi luvuista a, b tai c on jaollinen luvulla 5.

9.4. Olkoon (a, b, c) Pythagoraan kolmikko. Osoita, että $a \neq b$.

9.5. Oletetaan tunnetuksi, että Diofantoksen yhtälön

$$x^p + y^p = z^p$$

ainoa ratkaisu on $(0,0,0)$ millä tahansa parittomalla alkuluvulla p. Todista Lause 9.7.

9.6. Olkoon (a,b,c) Pythagoraan kolmikko. Osoita, että

$$(ab)^4 + (bc)^4 + (ca)^4 = (c^4 - a^2b^2)^2 \,.$$

9.7. Osoita, että Diofantoksen yhtälöllä

$$x^2 + y^2 = 3z^2$$

ei ole ratkaisuja, joille $xyz \neq 0$.[4]

9.8. Osoita äärettömän laskeutumisen menetelmällä, että $\sqrt{2}$ on irrationaaliluku.[5]

Olkoot $a,b,c,d \in \mathbb{N}^*$. Jos

$$a^2 + b^2 + c^2 = d^2,$$

niin (a,b,c,d) on *Pythagoraan nelikko*. Jos lisäksi $\operatorname{syt}(a,b,c,d) = 1$, niin (a,b,c,d) on *primitiivinen Pythagoraan nelikko*.

9.9. Olkoot $m,n,p \in \mathbb{N}^*$ ja olkoot

$$\begin{aligned} a &= 2mp \\ b &= 2np \\ c &= p^2 - (m^2 + n^2) \\ d &= p^2 + (m^2 + n^2)\,. \end{aligned}$$

Osoita, että (a,b,c,d) on Pythagoraan nelikko.

9.10. Tarkasta, että $(36,8,3,37)$ on Pythagoraan nelikko. Osoita, että tehtävän 9.9 kaava ei anna tätä nelikkoa.

Olkoot

$$U = \begin{pmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}, \quad D = \begin{pmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{pmatrix}.$$

9.11. Osoita, että U, A ja D ovat kääntyviä matriiseja ja määritä niiden käänteismatriisit.

9.12. Olkoon (a,b,c) Pythagoraan kolmikko. Osoita, että $U\,{}^t a$, $A\,{}^t a$ ja $D\,{}^t a$ ovat Pythagoraan kolmikoita.

9.13. Olkoon (a,b,c) primitiivinen Pythagoraan kolmikko. Osoita, että $U\,{}^t a$, $A\,{}^t a$ ja $D\,{}^t a$ ovat primitiivisia Pythagoraan kolmikoita.

[4] Käytä äärettömän laskeutumisen menetelmää. Tarkastele kysymystä mod 3.

[5] Muotoile väite Diofantoksen yhtälön avulla.

Luku 10

Diofantoksen approksimaatio

Tässä luvussa tarkastelemme reaalilukujen arvioimista rationaaliluvuilla.

10.1 Johdantoa

Rationaaliluku $p/q \in \mathbb{Q}$ on *supistetussa muodossa*, jos $q \in \mathbb{N}^*$ ja $\operatorname{syt}(p,q) = 1$.

Rationaalilukujen joukko $\mathbb{Q}$ on tunnetusti reaalilukujen joukon $\mathbb{R}$ tiheä osajoukko, kun lukujen $x, y \in \mathbb{R}$ etäisyytenä käytetään niiden erotuksen itseisarvoa $|x-y|$. Jos $x \in \mathbb{R}-\mathbb{Q}$ on irrationaaliluku ja $\varepsilon > 0$, niin epäyhtälöllä

$$\left|x - \frac{p}{q}\right| < \varepsilon$$

on äärettömän monta ratkaisua $\frac{p}{q} \in \mathbb{Q}$.

Diofantoksen approksimaatiossa tarkastellaan irrationaaliluvun arvioimista rationaaliluvulla *mahdollisimman tarkasti* arvioinnissa käytettävän rationaaliluvun *nimittäjästä riippuvan funktion suhteen.*

Olkoon $\psi\colon \mathbb{N}^* \to]0,\infty[$. Diofantoksen approksimaatiossa tarkastellaan epäyhtälöiden

$$\left|\alpha - \frac{p}{q}\right| < \psi(q)$$

rationaalisten ratkaisuiden $\frac{p}{q} \in \mathbb{Q}$ lukumäärää reaaliluvuilla α. Yleensä α on irrationaaliluku ja ψ on monotoninen ja $\lim_{q\to\infty} \psi(q) = 0$. Tyypillisesti

$$\psi(q) = \frac{c}{q^\beta}$$

joillain vakioilla $c, \beta > 0$.

Propositio 10.1. *Olkoon $x \in \mathbb{R}$ ja olkoon $q \in \mathbb{N}^*$. Epäyhtälöllä*

$$\left|x - \frac{p}{q}\right| \leqslant \frac{1}{2q}$$

on ratkaisu. Jos x on irrationaalikulu, niin yhtälöllä

$$\left|x - \frac{p}{q}\right| < \frac{1}{2q}$$

on ratkaisu.

Todistus. Koska

$$\mathbb{R} = \bigcup_{a \in \mathbb{Z}} \left[\frac{a}{q}, \frac{a+1}{q}\right],$$

niin jokaiselle $x \in \mathbb{R}$ on $a \in \mathbb{Z}$, jolle $a \leqslant x \leqslant a+1$. Kolmioepäyhtälön nojalla pätee $|x-a| \leqslant \frac{1}{2}$ tai $|(a+1)-x| \leqslant \frac{1}{2}$. Molemmissa yhtälöissä pätee yhtäsuuruus ainoastaan välin $\left[\frac{a}{q}, \frac{a+1}{q}\right]$ keskipisteessä $\frac{2a+1}{2q} \in \mathbb{Q}$. Kaikilla muilla reaaliluvuilla pätee siis toinen aidoista epäyhtälöistä jollain $a \in \mathbb{Z}$. □

10.2 Dirichlet'n approksimaatiolause

Tässä luvussa osoitamme, että irrationaaliluvuille voimme käyttää funktioita ψ, jotka menevät nollaan äärettömyydessä nopeammin kuin $q \mapsto \frac{1}{q}$.

Propositio 10.2. *Olkoon $\alpha \in \mathbb{R}$ ja olkoon $N \in \mathbb{N}^*$. Tällöin on $p, q \in \mathbb{Z}$, $0 < q \leqslant N$, joille pätee*

$$|q\,\alpha - p| < \frac{1}{N}\,.$$

Todistus. Kyyhkyslakkaperiaatteen nojalla on $k_1, k_2 \in \{k \in \mathbb{N} : k \leqslant N\}$, $k_1 < k_2$, ja kokonaisluku $0 \leqslant s \leqslant N-1$, joille

$$k_1\alpha - \lfloor k_1\alpha \rfloor, k_2\alpha - \lfloor k_2\alpha \rfloor \in \left[\frac{s}{N}, \frac{s+1}{N}\right[\,.$$

Tällöin

$$\left|(k_1-k_2)\alpha - (\lfloor k_1\alpha \rfloor - \lfloor k_2\alpha \rfloor)\right| = \left|k_1\alpha - \lfloor k_1\alpha \rfloor - (k_2\alpha - \lfloor k_2\alpha \rfloor)\right| < \frac{1}{N}$$

Väite seuraa valitsemalla $p = \lfloor k_2\alpha \rfloor - \lfloor k_1\alpha \rfloor$ ja $q = k_2 - k_1$. □

Esimerkki 10.3. Olkoot $\alpha = \sqrt{2}$ ja $N = 8$ kuten Propositiossa 10.2.

k	0	1	2	3	4	5	6	7	8
$k\alpha - \lfloor k\alpha \rfloor$	0	$\sqrt{2}-1$	$2\sqrt{2}-2$	$3\sqrt{2}-4$	$4\sqrt{2}-5$	$5\sqrt{2}-7$	$6\sqrt{2}-8$	$7\sqrt{2}-9$	$8\sqrt{2}-11$
$\approx$	0	0.41421	0.82843	0.24264	0.65685	0.071068	0.48528	0.89949	0.31371
s	0	3	6	1	5	0	3	7	2

Lasku osoittaa, että lokeroissa 0 ja 3 on kummassakin kaksi murto-osaa:

$$0 \leqslant 0 < 5\sqrt{2} - 7 < \frac{1}{8}$$

ja

$$\frac{3}{8} < \sqrt{2} - 1 < 6\sqrt{2} - 8 < \frac{3}{8}\,.$$

Näistä pareista saadaan sama arvio $\frac{7-0}{5-0} = \frac{7}{5} = \frac{8-1}{6-1}$ luvulle $\sqrt{2}$. Lauseen 10.4 mukaisesti $|\sqrt{2} - \frac{7}{5}| \approx 0.0142 < 0.04 = \frac{1}{5^2}$ ja Proposition 10.2 mukaisesti $|5\alpha - 7| \approx 0.071 < 0.125 = \frac{1}{8}$.

Lause 10.4 (Dirichlet'n approksimaatiolause)**.** *Olkoon $\alpha \in \mathbb{R} - \mathbb{Q}$. Epäyhtälö*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2} \tag{10.1}$$

pätee äärettömän monelle $\frac{p}{q} \in \mathbb{Q}$.

Todistus. Proposition 10.2 nojalla jokaisella $N \in \mathbb{N}^*$ on $p \in \mathbb{Z}$ ja $q \in \mathbb{N}^*$, $1 \leqslant q \leqslant N$, joille

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qN} \leqslant \frac{1}{q^2}\,. \tag{10.2}$$

Osoitetaan, että epäyhtälö pätee äärettömän monella rationaaliluvulla $\frac{q}{p} \in \mathbb{Q}$. Olkoot rationaaliluvut $\frac{p_1}{q_1}, \ldots, \frac{p_M}{q_M}$ epäyhtälön (10.3) ratkaisuja. Koska α ei ole rationaaliluku, $\min\left\{|\alpha - \frac{p_i}{q_i}| : 1 \leqslant i \leqslant M\right\} > 0$, joten on $Q \in \mathbb{N}^*$, jolle pätee

$$\left|\alpha - \frac{p_i}{q_i}\right| > \frac{1}{Q}$$

kaikilla $1 \leqslant i \leqslant M$.

Edellä tehdystä havainnosta (10.2) valinnalla $N = Q$ seuraa, että on $\frac{p}{q} \in \mathbb{Q}$, $1 \leqslant q \leqslant Q$, jolle

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{q\,Q} \leqslant \frac{1}{Q}\,.$$

Siis

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{q^2}\,,$$

mutta $\frac{p}{q} \neq \frac{p_i}{q_i}$ kaikilla $1 \leqslant i \leqslant M$. Tästä seuraa, että epäyhtälön (10.3) ratkaisujen joukko ei ole äärellinen. □

Propositio 10.5. *Olkoon $\frac{a}{b} \in \mathbb{Q}$. Epäyhtälön*

$$\left|\frac{a}{b} - \frac{p}{q}\right| < \frac{1}{q^2} \tag{10.3}$$

ratkaisujen joukko on äärellinen.

Todistus. Harjoitustehtävä 10.2. □

10.3 Huonosti arvioituvat luvut

Reaaliluku $x \in \mathbb{R}$ on *algebrallinen luku*, jos se on kokonaislukukertoimisen polynomin juuri.

Jos x on jonkin n. asteen kokonaislukukertoimisen polynomin juuri, mutta ei ole minkään alemman asteen kokonaislukukertoimisen polynomin juuri, niin x on *n. asteen algebrallinen luku*.

Esimerkki 10.6. (1) Rationaaliluvut ovat täsmälleen ensimmäisen asteen algebralliset luvut.

(2) Harjoitustehtävässä 9.8 osoitimme tunnetun tuloksen, että $\sqrt{2}$ ei ole rationaaliluku. Siis se ei ole ensimmäisen asteen algebrallinen luku. Määritelmänsä nojalla $\sqrt{2}$ on kokonaislukukertoimisen polynomin $X^2 - 2$ juuri, joten se on toisen asteen algebrallinen luku.

Toisen asteen polynomin $P(X) = aX^2 + bX + c$ *diskriminantti* on

$$\operatorname{Disc}(P(X)) = b^2 - 4ac\,.$$

Lemma 10.7. *Olkoot $a, b, c \in \mathbb{R}$, $a \neq 0$ ja olkoot α ja α' polynomin $P(X) = aX^2 + bX + c$ juuret. Tällöin*

$$\operatorname{Disc}(P(X)) = a^2(\alpha - \alpha')^2\,.$$

Todistus. Harjoitustehtävä 10.3. □

Propositio 10.8. *Olkoon $P(X)$ kokonaislukukertoiminen toisen asteen polynomi, jonka diskriminantti on D, ja olkoon $A > \sqrt{D}$. Olkoon irrationaaliluku α polynomin $P(X)$ juuri. Epäyhtälöllä*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Aq^2} \tag{10.4}$$

on vain äärellisen monta ratkaisua.

Todistus. Olkoon $P(X) = aX^2 + bX + c$ ja olkoon α' polynomin $P(X)$ toinen juuri. Tällöin polynomin $\operatorname{Disc}(P(X)) = a^2(\alpha - \alpha')^2 > 0$.

Olkoon $\frac{p}{q}$ epäyhtälön (10.4) rationaalinen ratkaisu. Koska $P(\frac{p}{q}) \neq 0$, pätee

$$\left|P\Big(\frac{p}{q}\Big)\right| = \left|\frac{ap^2 + bpq + cq^2}{q^2}\right| \geqslant \frac{1}{q^2}\,. \tag{10.5}$$

Epäyhtälön (10.5), polynomin juuriesityksen ja sen nojalla, että $\frac{p}{q}$ on ratkaisu, saamme kolmioepäyhtälöstä arvion

$$\begin{aligned}\frac{1}{q^2} &\leqslant \left|P\Big(\frac{p}{q}\Big)\right| = \left|\alpha - \frac{p}{q}\right| \left|a\big(\alpha' - \frac{p}{q}\big)\right| < \frac{1}{Aq^2}\left|a(\alpha - \alpha') + a\big(\alpha - \frac{p}{q}\big)\right| \\ &\leqslant \frac{\sqrt{D}}{Aq^2} + \frac{|a|}{A^2q^4}\,.\end{aligned}$$

Saatu epäyhtälö pätee, jos ja vain jos $q^2 < \frac{|a|}{A(A-\sqrt{D})}$, joten nimittäjän q mahdollisten arvojen joukko on äärellinen. □

Kuva 10.1 — Kultaisen leikkauksen suhde jakaa janan niin, että pidemmän palan pituuden suhde koko janan pituuteen on sama kuin lyhyemmän janan pituuden suhde pidemmän janan pituuteen: $\frac{1}{\varphi} = \frac{\varphi-1}{1}$.

Irrationaaliluku x on *huonosti arvioituva luku*, jos on $c > 0$ jolle epäyhtälöllä $|x - \frac{p}{q}| < \frac{c}{q^2}$ ei ole ratkaisuja.

Lause 10.9. *Toisen asteen irrationaaliluvut ovat huonosti arvioituvia.*

Todistus. Harjoitustehtävä 10.4. □

Esimerkki 10.10. Kokonaislukukertoimisen polynomin $P(X) = X^2 - X - 1$ juuret ovat *kultaisen leikkauksen luku* $\varphi = \frac{1+\sqrt{5}}{2}$ ja sen *konjugaatti* $\widehat{\varphi} = \frac{1-\sqrt{5}}{2}$. Polynomin $P(X)$ diskriminantti on 5, joten epäyhtälön

$$\left|\varphi - \frac{p}{q}\right| < \frac{\beta}{\sqrt{5}q^2}$$

ratkaisujen joukko on äärellinen kaikille $0 < \beta < 1$.

Kultaisen leikkauksen lukua voi arvioida rationaaliluvuilla, joita saadaan seuraavalla prosessilla: Kirjoitetaan yhtälö $\varphi^2 - \varphi - 1 = 0$ muodossa $\varphi = 1 + \frac{1}{\varphi}$. Iteroimalla tätä saamme yhtälöketjun

$$\varphi = 1 + \frac{1}{\varphi} = 1 + \frac{1}{1+\frac{1}{\varphi}} = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{\varphi}}} = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{\varphi}}}} = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{\varphi}}}}} = \cdots$$

Kun jätämme jokaisesta yhtälöketjussa esiintyvästä murtolausekkeesta pois termin $\frac{1}{\varphi}$, saamme rationaaliluvut

$$\begin{aligned}
\frac{P_1}{Q_1} &= \frac{1}{1}, \\
\frac{P_2}{Q_2} &= 1 + \frac{1}{1} = 2, \\
\frac{P_3}{Q_3} &= 1 + \frac{1}{1+\frac{1}{1}} = \frac{3}{2}, \\
\frac{P_4}{Q_4} &= 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1}}} = \frac{5}{3}, \\
\frac{P_5}{Q_5} &= 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1}}}} = \frac{8}{5},
\end{aligned}$$

jotka antavat hyviä arvioita luvulle φ kuten Taulukossa 10.10 kootut laskut osoittavat.

k	$\frac{P_k}{Q_k}$	$\varphi - \frac{P_k}{Q_k}$	$\frac{1}{\sqrt{5}Q_k^2}$	
1	$\frac{1}{1}$	0.618034	0.447214	
2	$\frac{2}{1}$	−0.381966	0.447214	•
3	$\frac{3}{2}$	0.118034	0.111803	
4	$\frac{5}{3}$	−0.0486327	0.0496904	•
5	$\frac{8}{5}$	0.018034	0.0178885	
6	$\frac{13}{8}$	−0.00696601	0.00698771	•
7	$\frac{21}{13}$	0.00264937	0.00264623	
8	$\frac{34}{21}$	−0.00101363	0.00101409	•
9	$\frac{55}{34}$	0.00038693	0.000386863	
10	$\frac{89}{55}$	−0.000147829	0.000147839	•

Taulukko 10.1 — Ketjumurtoluvuilla saatavia kultaisen leikkauksen luvun φ arvioita. Viimeisessä sarakkeessa oleva merkki • osoittaa, että sillä rivillä oleva rationaaliluku $\frac{P_k}{Q_k}$ on epäyhtälön $|\varphi - \frac{P_k}{Q_k}| < \frac{1}{\sqrt{5}Q_k^2}$ ratkaisu.

Harjoitustehtäviä

10.1. Etsi ratkaisu epäyhtälölle

$$|\sqrt{3} - \frac{p}{q}| < \frac{1}{q^2}$$

siten, että $|q\sqrt{3} - p| < \frac{1}{9}$.[1]

10.2. Todista Propositio 10.5.

10.3. Todista Lemma 10.7.

10.4. Todista Lause 10.9.

Reaaliluku on *transkendenttiluku*[a], jos se ei ole algebrallinen luku.

[a] Toinen mahdollinen kirjoitusasu on *transsendenttiluku*.

10.5. Osoita, että transkendenttilukujen joukko on ylinumeroituva.

[1] Esimerkki 10.3.

Olkoot $F_0 = 0$ ja $F_1 = 1$ ja asetetaan kaikille $n \geqslant 2$

$$F_n = F_{n-1} + F_{n-2}\,.$$

Lukujono $(F_n)_{n\in\mathbb{N}}$ on *Fibonaccin jono*.

10.6. Todista,[2] että

$$F_n = \frac{\varphi^n - \widehat{\varphi}^n}{\sqrt{5}}$$

kaikilla $n \in \mathbb{N}$.

10.7. Todista, että

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \varphi\,.$$

10.8. Todista, että

$$F_{n+2}F_n - F_{n+1}^2 = (-1)^{n+1}$$

kaikilla $n \in \mathbb{N}$.

10.9. Mitä edelliset tehtävät kertovat siitä, kuinka hyvin jono $(\frac{F_{n+1}}{F_n})_{n\in\mathbb{N}}$ arvioi kultaisen leikkauksen lukua φ?

[2] Induktio.

Luku 11

Fordin ympyrät ja Hurwitzin lause

Tässä luvussa todistamme Hurwitzin approksimaatiolauseen todistuksella, jossa käytetään geometrista menetelmää.

11.1 Rationaaliluvun naapurit

Rationaaliluvut $\frac{a}{c}, \frac{b}{d} \in \mathbb{Q}$ ovat *naapureita*, jos $|ad - bc| = 1$.

Esimerkki 11.1. Luvut $\pm\frac{1}{n}$ ovat rationaaliluvun $0 = \frac{0}{1}$ naapureita.

Jos $\frac{a}{c}$ ja $\frac{b}{d}$ ovat naapureita, niin $\frac{a+b}{c+d}$ on niiden *mediantti*.

Lemma 11.2. *Jos rationaaliluvut $\frac{a}{c}$ ja $\frac{b}{d}$ ovat naapureita, niin niiden mediantti on kummankin naapuri.*

Todistus. Jos $ad - cb = 1$, niin

$$(a + b)c - a(c + d) = -(ad - bc) = -1$$

ja

$$(a + b)d - b(c + d) = ad - bc = 1\,. \qquad \square$$

Lemma 11.3. *Jokaisella rationaaliluvulla on äärettömän monta naapuria. Jos $\frac{b}{d}$ on luvun $\frac{a}{c}$ naapuri, niin luvun $\frac{a}{c}$ naapurien joukko on*

$$\mathbf{N}\left(\frac{a}{c}\right) = \left\{\frac{b + ka}{d + kc} : k \in \mathbb{Z}\right\}.$$

Todistus. Olkoon $\frac{a}{c} \in \mathbb{Q}$ supistetussa muodossa. Lineaarisella Diofantoksen yhtälöllä

$$ax - cy = 1 \tag{11.1}$$

on Bézout'n yhtälön[1] nojalla ratkaisu, koska $\operatorname{syt}(a,c) = 1$. Jos (b,d) on yhtälön (11.1) ratkaisu, niin Seurauksen 6.7 nojalla yhtälön (11.1) ratkaisujen joukko on

$$\big\{(b+ak, d+ck) : k \in \mathbb{Z}\big\}\,.$$

Vastaavasti saadaan yhtälön $ax - cy = -1$ ratkaisut. □

Esimerkki 11.4. (1) Jos $\frac{a}{c} = \frac{0}{1}$, niin Lemman 11.3 todistuksessa löydetty ratkaisujen joukko sisältää myös parin $(1,0)$, joka ei vastaa rationaalilukua. Näin käy itse asiassa täsmälleen silloin, kun $\frac{a}{b} \in \mathbb{Z}$. Jos nimittäin $d + ck = 0$, niin $d = -kc$ ja saadaan

$$\pm 1 = ad - bc = -(ak+b)c\,,$$

joten $c = 1$.

On kätevää ajatella, että kokonaisluvuilla on äärettömän monen rationaalilukunaapurin lisäksi myös naapuri $\infty = \frac{1}{0}$, joka ei ole rationaaliluku.

(2) On helppo tarkastaa, että $\frac{0}{1}$ on rationaaliluvun $\frac{1}{2}$ naapuri. Lemman 11.3 nojalla

$$\begin{aligned}\mathbf{N}\Big(\frac{1}{2}\Big) = \left\{\frac{k}{1+2k} : k \in \mathbb{Z}\right\} &= \left\{\ldots, \frac{-3}{-5}, \frac{-2}{-3}, \frac{-1}{-1}, \frac{0}{1}, \frac{1}{3}, \frac{2}{5}, \frac{3}{7}, \ldots\right\} \\ &= \left\{\ldots, \frac{3}{5}, \frac{2}{3}, \frac{1}{1}, \frac{0}{1}, \frac{1}{3}, \frac{2}{5}, \frac{3}{7}, \ldots\right\}\end{aligned}$$

(3) Jos $\frac{a}{c}$ ja $\frac{b}{d}$ ovat naapureita, niin

$$\lim_{k\to\infty} \frac{b+ka}{d+kc} = \frac{a}{c} = \lim_{k\to-\infty} \frac{b+ka}{d+kc}\,.$$

Lemma 11.5. *Jos $\frac{a}{c}$ ja $\frac{b}{d}$ ovat naapureita, niin $\frac{b+ka}{d+kc}$ ja $\frac{b+(k+1)a}{d+(k+1)c}$ ovat naapureita.*

Todistus. Harjoitustehtävä 11.3. □

Lemma 11.6. *Jos $q \geqslant 2$, niin täsmälleen kahdella luvun $\frac{p}{q}$ naapurilla on nimittäjä, joka on pienempi kuin q.*

Todistus. Harjoitustehtävä 11.5. □

11.2 Fordin ympyrät

Ford[2] esitteli geometrisen menetelmän Diofantoksen approksimaation tarkastelemiseen. Tässä menetelmässä jokaiseen rationaalilukuun liitetää *suljettuun ylempään puolitasoon*

$$\overline{\mathbb{H}} = \{(x,y) \in \mathbb{R}^2 : y \geqslant 0\}$$

sisältyvä ympyrä.

[1] Katso Seuraus 2.5.
[2] Lester R. Ford (1886-1967).

Olkoon $\frac{p}{q} \in \mathbb{Q}$ supistetussa muodossa. *Fordin kiekko* pisteessä $\frac{p}{q}$ on

$$\mathscr{H}_{\frac{p}{q}} = \left\{(x,y) \in \mathbb{R}^2 : \left\| w - \left(\frac{p}{q}, \frac{1}{2q^2}\right)\right\| \leqslant \frac{1}{2q^2}\right\}.$$

Fordin kiekon $\mathscr{H}_{\frac{p}{q}}$ reuna $\partial\mathscr{H}_{\frac{p}{q}}$ on *Fordin ympyrä* pisteessä $\frac{p}{q}$.

Puolitaso

$$\mathscr{H}_{\frac{1}{0}} = \{(x,y) \in \mathbb{R}^2 : y \geqslant 1\}$$

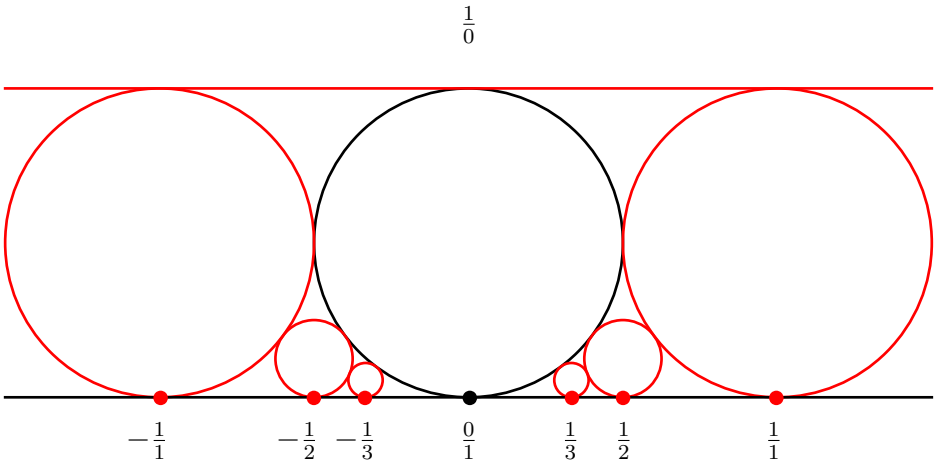
on *Fordin kiekko äärettömyydessä.*

On helppo tarkastaa, että Fordin ympyrä $\partial\mathscr{H}_{\frac{p}{q}}$ on ympyrä, jonka säde on $\frac{1}{2q^2}$ ja joka sivuaa x-akselia pisteessä $\left(\frac{p}{q}, 0\right)$. Koko Fordin kiekko sisältyy ylempään puolitasoon.

Samastamme reaalilukujen joukon x-akselin $\{(x,y) \in \mathbb{R}^2 : y = 0\}$ kanssa.

Lemma 11.7. *Jos $\frac{a}{c}, \frac{b}{d} \in \mathbb{Q} \cup \{\infty\}$ ovat naapureita, niin Fordin kiekot $\mathscr{H}_{\frac{a}{c}}$ ja $\mathscr{H}_{\frac{b}{d}}$ sivuavat toisiaan. Muuten kiekot $\mathscr{H}_{\frac{a}{c}}$ ja $\mathscr{H}_{\frac{b}{d}}$ ovat erillisiä.*

Todistus. Harjoitustehtävä 11.6. □



Kuva 11.1 — Rationaaliluvun $\frac{0}{1}$ naapureita vastaavia Fordin ympyröitä.

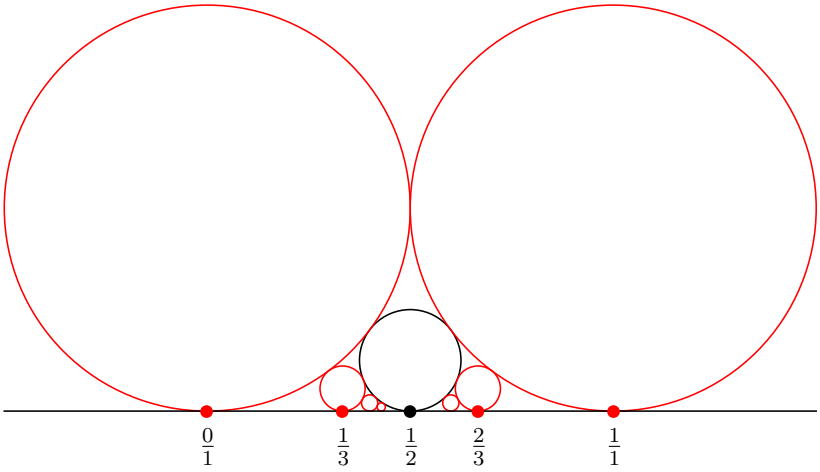
Jos $r, s, t \in \mathbb{Q} \cup \{\infty\}$ ovat pareittain naapureita, niin (r,s,t) on *naapurikolmikko. Naapurikolmikoiden joukko* on $\mathbf{N}_3$.

Jos (r,s,t) on naapurikolmikko, niin kiekkojen $\mathscr{H}_r$, $\mathscr{H}_s$ ja $\mathscr{H}_t$ rajaama kompakti joukko tasossa $\mathbb{R}^2$ on *Fordin kolmio* $\Delta(r,s,t)$.

Esimerkki 11.8. $(\frac{0}{1}, \frac{1}{1}, \frac{1}{2})$ ja $(\frac{0}{1}, \frac{1}{1}, \frac{0}{1})$ ovat naapurikolmikoita.

Propositio 11.9.

$$\mathbb{H} - \bigcup_{r \in \mathbb{Q} \cup \{\infty\}} \mathscr{H}_r = \bigcup_{(r,s,t) \in \mathbf{N}_3} \Delta(r,s,t)\,.$$



Kuva 11.2 — Rationaaliluvun $\frac{1}{2}$ naapureita vastaavia Fordin ympyröitä.

Todistus. Olkoon $(x, y) \in \mathbb{H} - \bigcup_{r\in\mathbb{Q}\cup\{\infty\}} \mathscr{H}_r$. Olkoon

$$\widehat{y} = \min\left\{z > y : (x, z) \in \bigcup_{r\in\mathbb{Q}\cup\{\infty\}} \mathscr{H}_r\right\}.$$

Tällöin $(x, \widehat{y}) \in \partial\mathscr{H}_s$ jollain $s \in \mathbb{Q} \cup \{\infty\}$. Lemmojen 11.3 ja 11.5 nojalla $(x, y) \in \Delta(s, t, u)$ joillain $t, u \in \mathbf{N}(s)$, jotka ovat naapureita keskenään. □

11.3 Hurwitzin approksimaatiolause

Seuraava Dirichlet'n approksimaatiolauseen[3] vahvennus havainnollistaa Fordin ympyröiden käyttökelpoisuutta Diofantoksen approksimaatiossa.

Lause 11.10. *Olkoon $\alpha \in \mathbb{R} - \mathbb{Q}$. Epäyhtälö*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2} \tag{11.2}$$

pätee äärettömän monelle $\frac{p}{q} \in \mathbb{Q}$.

Todistus. Olkoon $\rho_\alpha\colon [0, \infty[\to \mathbb{H} = \{(x, y) : y > 0\}$, $\rho_\alpha(s) = (\alpha, e^{-s})$. Kuvauksen ρ_α kuvajoukko

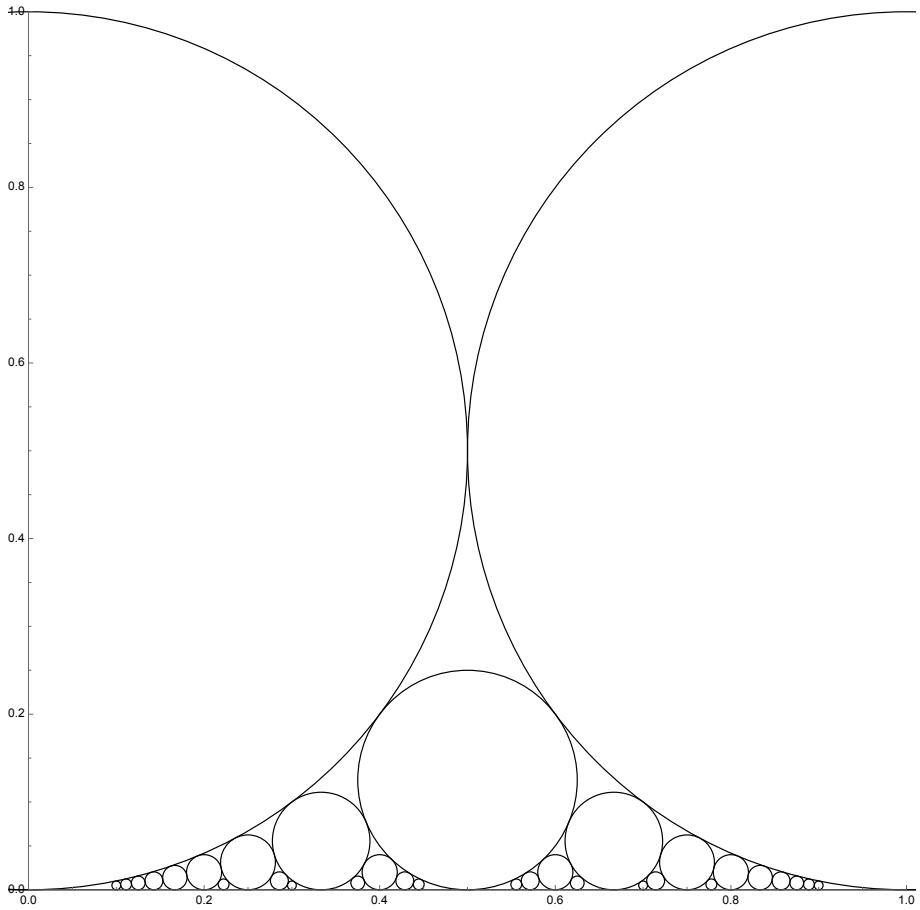
$$V_\alpha = \rho_\alpha([0, \infty[) = \{(\alpha, t) : t > 0\}$$

on pystysuora jana ja

$$\lim_{s\to\infty} \rho_\alpha(s) = (\alpha, 0) \in \mathbb{R} \times \{0\}.$$

Jos $V_\alpha \cap \mathscr{H}_{\frac{p}{q}} \neq \varnothing$ jollain $\frac{p}{q} \in \mathbb{Q}$, niin $I_{\frac{p}{q}} = \rho_\alpha^{-1}(V_\alpha \cap \mathscr{H}_{\frac{p}{q}})$ on kompakti jana, koska muuten $\alpha = \frac{p}{q} \in \mathbb{Q}$. Samoin kuvajoukon V_α leikkaus jokaisen Fordin kolmion kanssa on kompakti, koska kolmiot ovat kompakteja. Siis käyrä V_α leikkaa äärettömän montaa Fordin kiekkoa.

[3] Lause 10.4.



Kuva 11.3 — Fordin ympyröitä, joiden sivuamispiste on yksikkövälillä $[0, 1]$.

Jana V_α ei sivua Fordin kiekkoja, koska Fordin kiekon ja x-akselin sivuamispisteen koordinaatit ja niiden säteet ovat rationaalilukuja. Jos $V_\alpha \cap \operatorname{int} \mathscr{H}_{\frac{p}{q}}$, niin $|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$. □

Mikään nimittäjä q ei esiinny Lauseen 11.10 todistuksessa saatavassa jonossa enempää kuin kerran, koska näitä rationaalilukuja vastaavien Fordin kiekkojen säteet olisivat samat. Tällöin ainoa mahdollisuus olisi, että V_α sivuaisi molempia kiekkoja niiden sivuamispisteessä. Tämä ei ole mahdollista, sillä sivuamispisteen x-koordinaatti on rationaaliluku.

Seuraavassa todistuksessa tarkastelemme janan V_α ja Fordin kolmioiden leikkauksia yksityiskohtaisemmin.

Lause 11.11. *Olkoon $\alpha \in \mathbb{R} - \mathbb{Q}$. Epäyhtälö*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2} \tag{11.3}$$

pätee äärettömän monelle $\frac{p}{q} \in \mathbb{Q}$. Jos $c < 1$, niin on $\omega \in \mathbb{R} - \mathbb{Q}$, jolle epäyhtälön

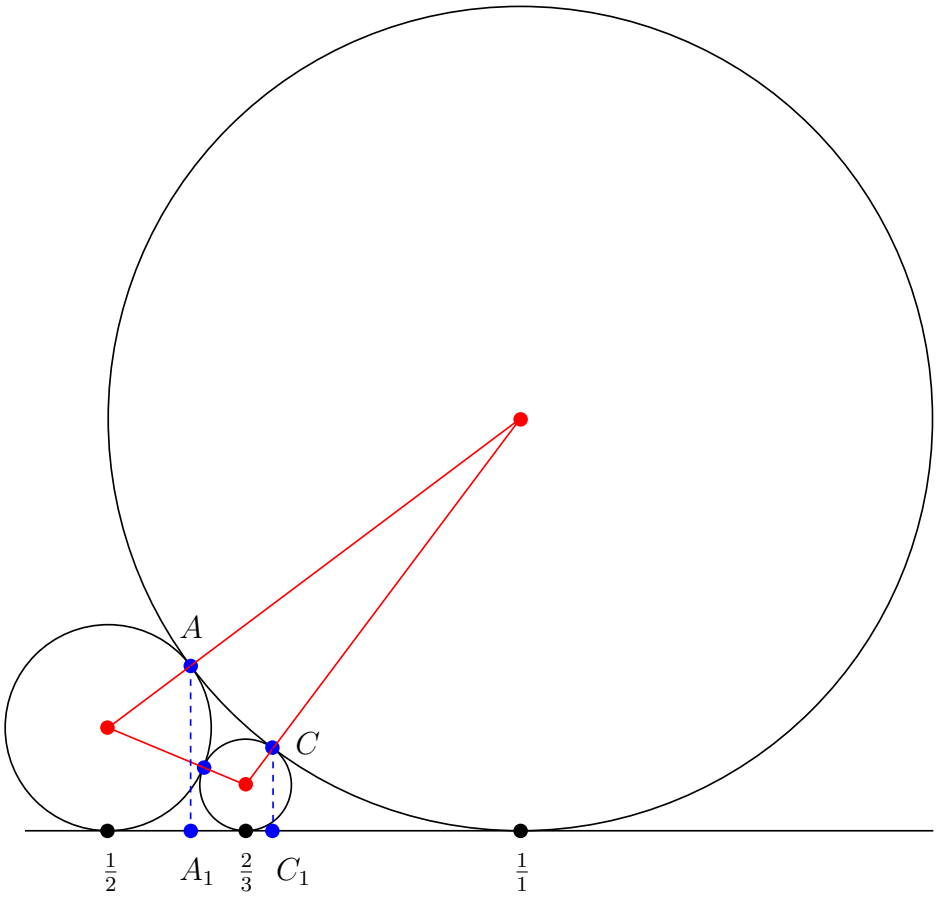
$$\left|\omega - \frac{p}{q}\right| < \frac{c}{\sqrt{5}q^2} \tag{11.4}$$

ratkaisujen joukko on äärellinen

Todistus. Oletetaan, että $V_\alpha \cap \Delta(\frac{p}{q}, \frac{r}{s}, \frac{t}{u}) \neq \varnothing$. Oletetaan lisäksi, että

$$q \leqslant s < u = q + s \tag{11.5}$$

ja että $\frac{p}{q} > \frac{r}{s}$, jolloin $ps - qr = 1$.



Kuva 11.4 — Esimerkki tapauksesta $A_1 < B_1$. Tässä $\frac{p}{q} = \frac{1}{1}$, $\frac{r}{s} = \frac{1}{2}$ ja $\frac{t}{u} = \frac{2}{3}$.

Olkoot Fordin kolmion $\Delta = \Delta(\frac{p}{q}, \frac{r}{s}, \frac{t}{u})$ kärjet

$$\begin{aligned} A &= (A_1, A_2) = \mathscr{H}_{\frac{p}{q}} \cap \mathscr{H}_{\frac{r}{s}}\,, \\ B &= (B_1, B_2) = \mathscr{H}_{\frac{r}{s}} \cap \mathscr{H}_{\frac{t}{u}} \quad \text{ja} \\ C &= (C_1, C_2) = \mathscr{H}_{\frac{t}{u}} \cap \mathscr{H}_{\frac{p}{q}}\,. \end{aligned}$$

Tällöin[4]

$$A_1 = \frac{pq + rs}{q^2 + s^2}\,, \quad B_1 = \frac{rs + tu}{s^2 + u^2} \quad \text{ja} \quad C_1 = \frac{tu + pq}{u^2 + q^2}\,, \tag{11.6}$$

joten

$$B_1 - A_1 = \frac{s^2 - qs - q^2}{(s^2 + q^2)(s^2 + u^2)} = \left(\left(\frac{s}{q}\right)^2 - \frac{s}{q} - 1\right)\frac{q^2}{(s^2 + q^2)(s^2 + u^2)}\,.$$

[4]Harjoitustehtävä 11.7.

Olkoon $x = \frac{s}{q} > 0$. Lausekkeen $B_1 - A_1$ merkki on sama kuin lausekkeen[5]

$$x^2 - x - 1 = (x - \varphi)(x - \widehat{\varphi})$$

merkki.

Jos $A_1 < B_1$, niin $A_1 < \alpha < \frac{p}{q}$, joten

$$\left|\alpha - \frac{p}{q}\right| < \frac{p}{q} - A_1 = \frac{s}{q(s^2+q^2)} = \frac{x}{x^2+1}\,\frac{1}{q^2}\,.$$

Lauseen ensimmäinen väite pätee, jos voimme osoittaa, että $\frac{x}{x^2+1} < \frac{1}{\sqrt{5}}$.[6] Jos

$$\frac{x}{x^2+1} > \frac{1}{\sqrt{5}}\,,$$

niin epäyhtälö saadaan helposti muotoon

$$(x-\varphi)\Big(x - \frac{\sqrt{5}-1}{2}\Big) = s^2 - \sqrt{5}x + 1 < 0\,.$$

Oletuksesta $A_1 < B_1$ seuraa $x^2 - x - 1 > 0$, joten $x > \varphi$, koska $\widehat{\varphi} < 0 < x$. Toisaalta $0 < \frac{\sqrt{5}-1}{2} < \varphi$, joten $(x-\varphi)\Big(x - \frac{\sqrt{5}-1}{2}\Big) > 0$ ja on päädytty ristiriitaan.

Tapaus $A_1 > B_1$ käsitellään samaan tapaan. Tällöin $x < \varphi$. Nyt osoitamme, että $\frac{t}{u}$ on haettu ratkaisu. Nythän $B_1 < \alpha < C_1$. Huomaamme, että $\frac{t}{u} - B_1 > C_1 - \frac{t}{u}$, koska oska $C_2 > B_2$. Käyttämällä yhtälöä (11.5), saamme

$$\left|\frac{t}{u} - \alpha\right| < \frac{t}{u} - B_1 = \frac{s}{u(s^2+u^2)} = \frac{x(x+1)}{x^2+(x+1)^2}\,\frac{1}{u^2}\,.$$

Jos $\frac{x(x+1)}{x^2+(x+1)^2} > \frac{1}{\sqrt{5}}$, niin

$$(\sqrt{5}-2)x^2 + (\sqrt{5}-2)x - 1 > 0\,.$$

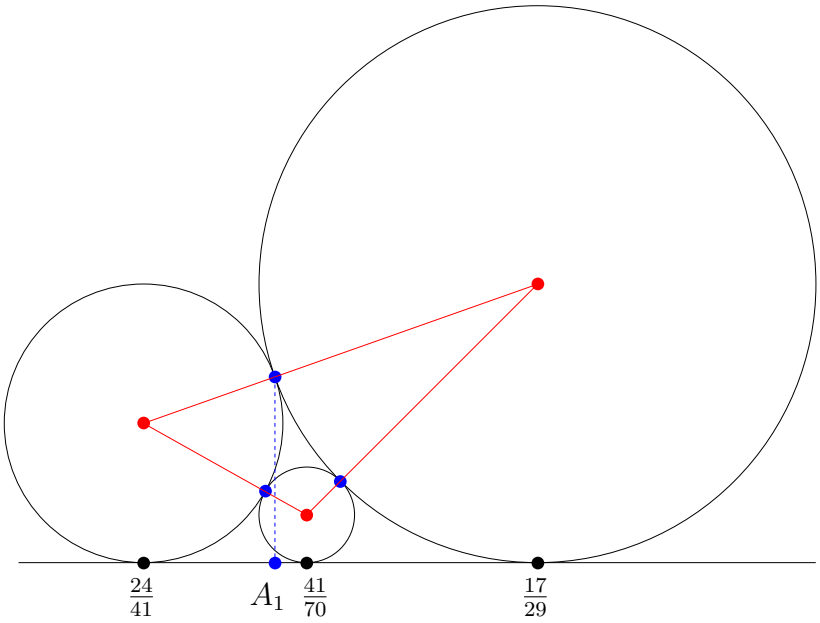
Siis

$$\Big(x + \frac{\sqrt{5}+3}{2}\Big)(x-\varphi) = x^2 + x - (\sqrt{5}+2) > 0\,,$$

mutta tämä on ristiriita, koska $x + \frac{\sqrt{5}+3}{2} > 0$ ja oletuksen mukaan $x - \varphi < 0$.

[5]Tässä φ on kultainen leikkaus ja $\widehat{\varphi}$ on sen konjugaatti. Katso Esimerkki 10.10.

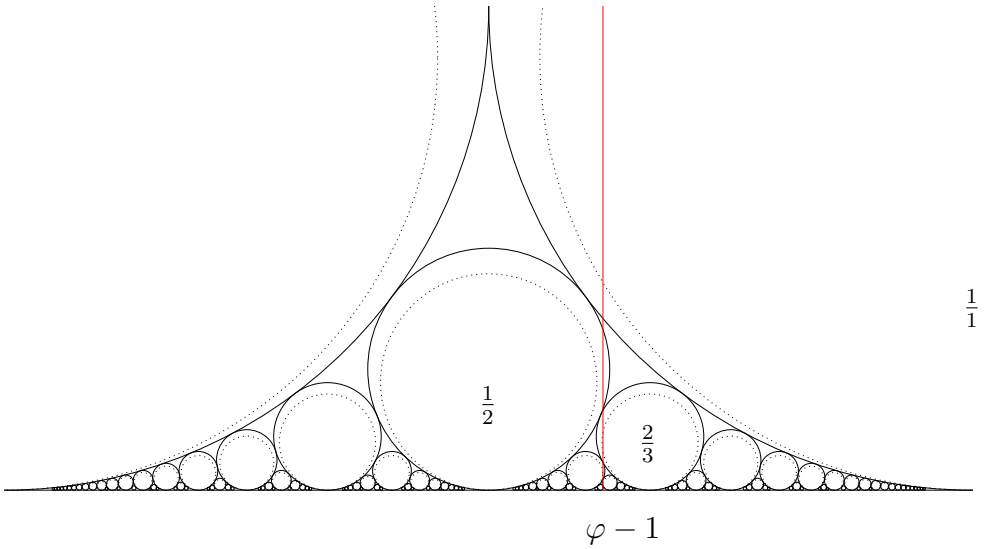
[6]Huomaa, että yhtäsuuruus ei ole mahdollista, koska verrataan rationaalilukua ja irrationaalilukua.



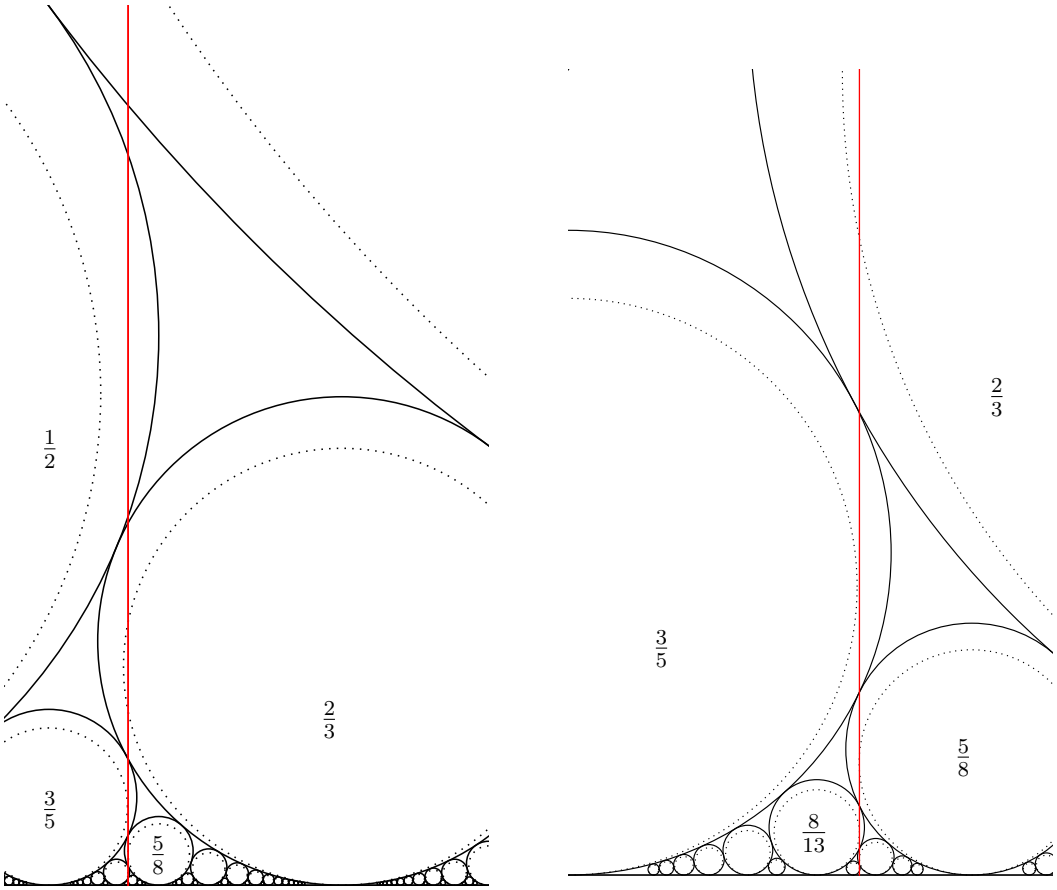
Kuva 11.5 — Esimerkki tapauksesta $A_1 < B_1$.

Lauseen toinen väite seuraa Esimerkistä 10.10. □

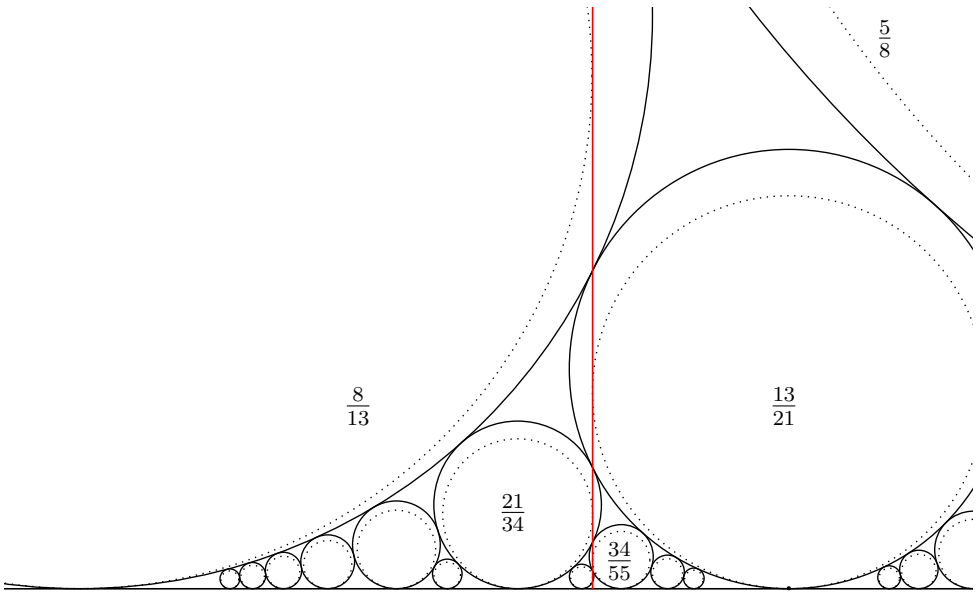
Esimerkki 11.12. Olkoon $\alpha = \frac{1}{\varphi} = \varphi - 1 = \frac{\sqrt{5}-1}{2} \approx 0.618$. Seuraavista kuvista näkee, että ainakin $\frac{1}{1}$ ja $\frac{2}{3}$ arvioivat lukua $\varphi - 1$ Hurwitzin lauseen lupaamalla tarkkuudella. Saamme jonon rationaalilukuja, jotka toteuttavat Lauseen 11.10 ehdon luvulle $\varphi - 1$: $\frac{1}{1}, \frac{1}{2}, \frac{2}{3}, \frac{3}{5}, \frac{5}{8}, \frac{8}{13}, \frac{21}{34}, \frac{34}{55}, \ldots$.



Kuva 11.6 — Irrationaaliluvun $\varphi - 1$ arviointia. Fordin kiekon $\mathscr{H}_{\frac{p}{q}}$ sisällä olevan pisteviivalla piirretyn ympyrän säde on $\frac{1}{\sqrt{5}q^2}$.



Kuva 11.7 — Irrationaaliluvun $\varphi - 1$ arviointia, lähikuvia.



Kuva 11.8 — Irrationaaliluvun $\varphi - 1$ arviointia, lähikuva.

11.4 Fareyn sarja

Olkoon $n \in \mathbb{N}^*$. Kertaluvun n *Fareyn*[a] *jono* on

$$\mathfrak{F}_n = \left\{ \frac{p}{q} \in \mathbb{Q} : 0 \leqslant p \leqslant q, \ ; q \leqslant n \right\}.$$

[a] John Farey (1766-1826) oli englantilainen geologi.

Esimerkki 11.13. Ensimmäiset Fareyn jonot ovat

$$\mathfrak{F}_1 = \left\{ \frac{0}{1}, \frac{1}{1} \right\},$$
$$\mathfrak{F}_2 = \left\{ \frac{0}{1}, \frac{1}{2}, \frac{1}{1} \right\},$$
$$\mathfrak{F}_3 = \left\{ \frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1} \right\},$$
$$\mathfrak{F}_4 = \left\{ \frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1} \right\}.$$

Fareyn jonoja voidaan käyttää Hurwitzin lauseen todistuksessa ilman Fordin ympyröitä. Todistamme joitain niiden perusominaisuuksia tämän luvun tulosten avulla.

Propositio 11.14. *(1) Fareyn jonossa $\mathfrak{F}_n$ peräkkäin esiintyvät luvut ovat naapureita. (2) Olkoot $\frac{b}{d} < \frac{e}{f} < \frac{a}{c}$ kolme peräkkäistä lukua Fareyn jonossa $\mathfrak{F}_n$. Tällöin $\frac{e}{f} = \frac{a+b}{c+d}$.*

Todistus. Harjoitustehtävät 11.9 ja 11.10. □

Harjoitustehtäviä

11.1. Määritä rationaaliluvun $\frac{2}{3}$ naapurit.

11.2. Määritä rationaaliluvun $\frac{23}{41}$ naapurit.

11.3. Todista Lemma 11.5.

11.4. Olkoot $r, s \in \mathbb{Q} \cup \{\frac{1}{0}\}$ naapureita. Osoita, että on niillä on täsmälleen kaksi yhteistä naapuria, joista toinen on niiden mediantti.

11.5. Todista Lemma 11.6.[7]

11.6. Todista Lemma 11.7.

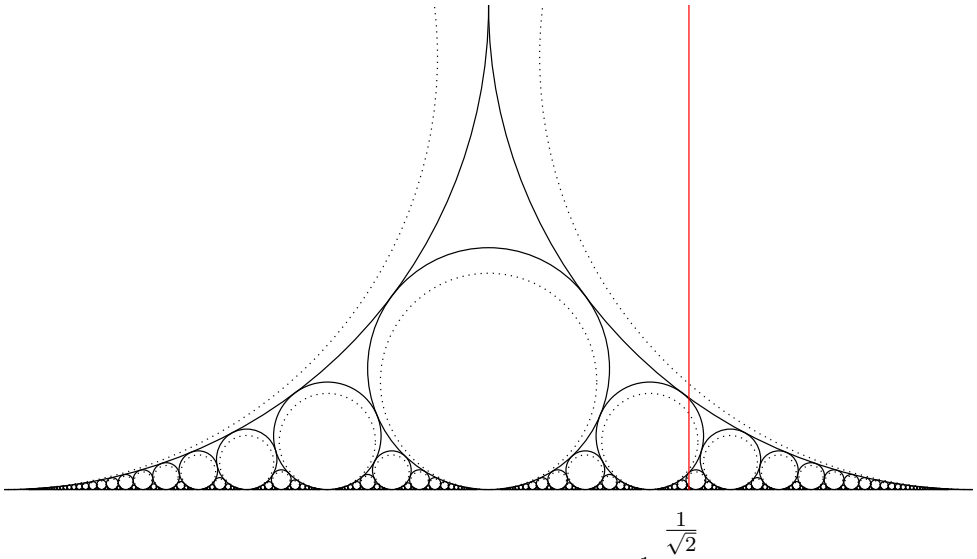
11.7. Todista yhtälöt (11.6).

11.8. Etsi neljä rationaalista ratkaisua epäyhtälölle

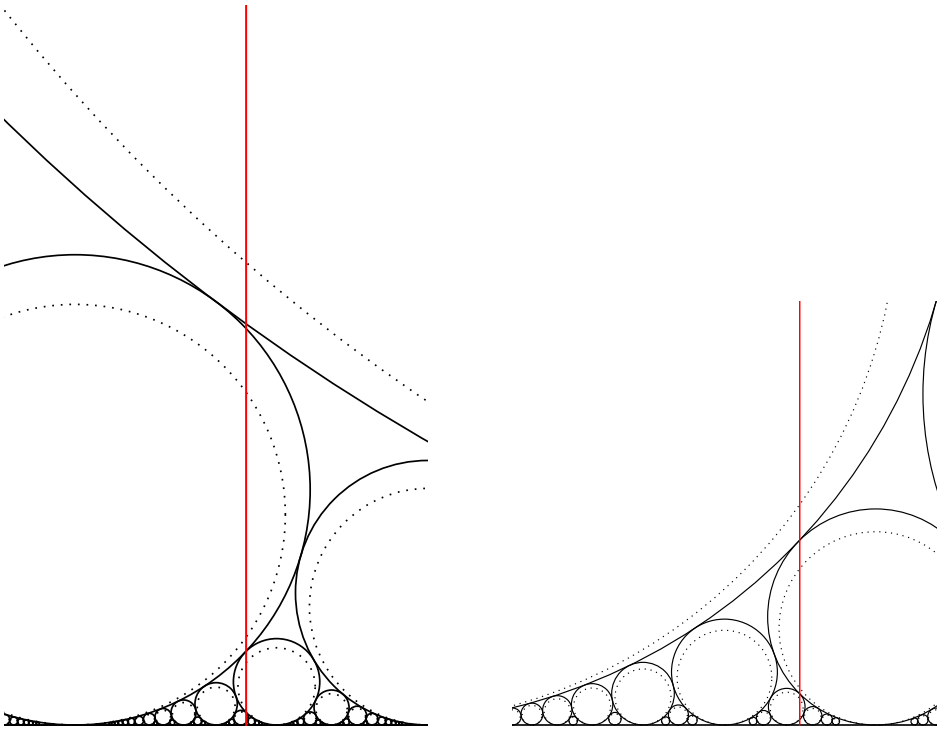
$$\left| \frac{1}{\sqrt{2}} - \frac{p}{q} \right| < \frac{1}{2q^2}$$

kuvien 11.9 ja 11.10 avulla.

[7] Lemma 11.3.



Kuva 11.9 — Irrationaaliluvun $\frac{1}{\sqrt{2}}$ arviointia.



Kuva 11.10 — Irrationaaliluvun $\frac{1}{\sqrt{2}}$ arviointia, lähikuvia.

11.9. Todista Propositio 11.14(1).[8]

11.10. Todista Propositio 11.14(2).

[8]Käytä Fordin ympyröitä ja sopivaa janaa.

Luku 12

Lukuteoreettisia funktioita

Olkoon $M \subset \mathbb{C}$, $M \neq \varnothing$. Funktio $f\colon \mathbb{N}^* \to M$ on *lukuteoreettinen funktio* eli *aritmeettinen funktio*.

Yleensä ajatellaan, että lukuteoreettinen funktio kuvaa jotain luonnollisten lukujen *lukuteoreettista ominaisuutta*[1] Kaikki funktiot $f\colon \mathbb{N}^* \to \mathbb{N}$, $f\colon \mathbb{N}^* \to \mathbb{Z}$, $f\colon \mathbb{N}^* \to \mathbb{Q}$ ja $f\colon \mathbb{N}^* \to \mathbb{R}$ ovat aritmeettisia funktioita, koska niiden määrittelyjoukko on $\mathbb{N}^*$ ja niiden maalijoukko on kompleksilukujen joukon osajoukko.

12.1 Multiplikatiiviset funktiot

Tässä luvussa tarkastelemme yleisellä tasolla tärkeää aritmeettisten funktioiden luokkaa.

Funktio $f\colon \mathbb{N} - \{0\} \to \mathbb{Z}$ on *multiplikatiivinen funktio*, jos $f(1) = 1$ ja

$$f(mn) = f(m)f(n)$$

kaikille $m, n \in \mathbb{N}$, joille $\operatorname{syt}(m, n) = 1$.

Esimerkki 12.1. (1) Olkoon $\alpha \in \mathbb{C}$. Aritmeettinen funktio id^α,

$$\mathrm{id}^\alpha(n) = n^\alpha\,,$$

on multiplikatiivinen. Erityisesti vakiofunktio $\mathbf{1} = \mathrm{id}^0\colon \mathbb{N}^* \to \mathbb{Z}$,

$$\mathbf{1}(n) = 1\,,$$

on multiplikatiivinen funktio.

[1] Itse asiassa Hardy ja Wright[HW, §16.1] sisällyttävät tämän ajatuksen lukuteoreettisen funktion määritelmään. Tällöin määritelmä ei kuitenkaan ole erityisen täsmällinen.

(2) Aritmeettinen funktio

$$\delta(k) = \begin{cases} 1 & , \text{kun } k = 1 \\ 0 & \text{muuten} \end{cases}$$

on multiplikatiivinen funktio.

Propositio 12.2. *Olkoon f multiplikatiivinen funktio. Jos luvun n alkutekijäesitys on*

$$n = p_1^{e_1} \cdots p_k^{e_k} ,$$

missä $p_1 < \cdots < p_k$ ovat alkulukuja ja $e_1, \ldots e_k \in \mathbb{N} - \{0\}$,

$$f(n) = f(p_1^{e_1}) \cdots f(p_k^{e_k}) .$$

Todistus. Harjoitustehtävä 12.1. □

Multiplikatiivisen funktion f summafunktio on $F\colon \mathbb{N} - \{0\} \to \mathbb{Z}$,

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

Propositio 12.3. *Multiplikatiivisen funktion summafunktio on multiplikatiivinen funktio.*

Todistus. Olkoot $a, b \in \mathbb{N} - \{0\}$ suhteellisia alkulukuja. Tällöin $d \mid ab$, jos ja vain jos $d = d_a d_b$ siten, että $d_a \mid a$ ja $d_b \mid b$. Siis

$$\begin{aligned} F(ab) &= \sum_{d|ab} f(d) = \sum_{d_a|a} \sum_{d_b|b} f(d_a d_b) \\ &= \sum_{d_a|a} \sum_{d_b|b} f(d_a) f(d_b) = \sum_{d_a|a} f(d_a) \sum_{d_b|b} f(d_b) = F(a)F(b) . \end{aligned}$$ □

12.2 Eulerin funktio

Suhteellisten alkulukujen tarkastelusta esimerkiksi Fareyn sarjan[2] yhteydessä päätyy luontevasti tärkeän lukuteoreettisen funktion määritelmään:

Kuvaus $\phi\colon \mathbb{N} - \{0\} \to \mathbb{N}$,

$$\phi(n) = \#\big\{1 \leqslant k \leqslant n : \operatorname{syt}(k, n) = 1\big\}$$

on *Eulerin ϕ-funktio*.

Olkoon

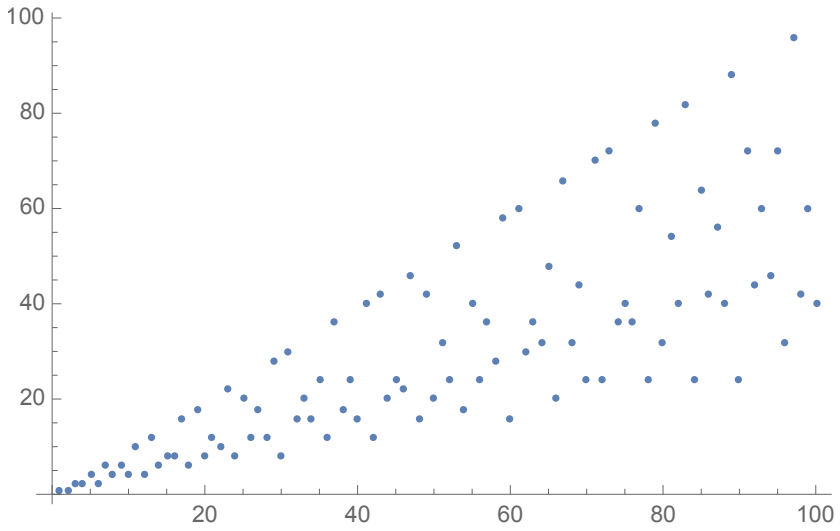
$$\mathscr{R}(n) = \big\{1 \leqslant k \leqslant n : \operatorname{syt}(k, n) = 1\big\}$$

luvun $n \in \mathbb{N} - \{0\}$ kanssa jaottomien positiivisten luonnollisten lukujen joukko. Määritelmän nojalla siis $\phi(n) = \#\mathscr{R}(n)$.

Taulukko 12.1 ja Kuva 12.1 näyttävät, että Eulerin funktion arvot vaihtelevat melko paljon peräkkäisillä luvuilla.

n	1	2	3	4	5	6	7	8	9	10	11	12	23	14	15	16	17	18	19	20
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8
n	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
$\phi(n)$	12	10	22	8	20	12	18	12	28	8	30	16	20	16	24	12	36	18	24	16

Taulukko 12.1 — Eulerin ϕ-funktion arvot $\phi(n)$, kun $1 \leqslant n \leqslant 40$.



Kuva 12.1 — Eulerin ϕ-funktion arvot $\phi(n)$, kun $1 \leqslant n \leqslant 100$.

Eulerin funktion avulla voimme muotoilla Eulerin yleistyksen Fermat'n pienelle lauseelle.[3] Todistuksen idea on sama.

Lause 12.4. *Olkoot* $a, n \in \mathbb{N} - \{0\}$ *siten, että* $\operatorname{syt}(a, n) = 1$. *Tällöin* $a^{\phi(n)} \equiv 1 \bmod n$.

Todistus. Olkoon $\mathscr{R}(n) = \{b_1, b_2, \ldots, b_{\phi(n)}\}$. Kuten Fermat'n lauseen todistuksessa näemme Lauseen 6.4(2) nojalla, että jokaiselle b_k, $1 \leqslant k \leqslant \phi(n)$, on $1 \leqslant x_k \leqslant n-1$, jolle $ab_k \equiv x_k \mod n$ ja että $x_i \neq x_j$, jos $i \neq j$. Lauseen 2.15 nojalla $x_k \in \mathscr{R}(n)$ jokaisella $1 \leqslant k \leqslant \phi(n)$, joten $\{x_1, x_2, \ldots, x_{\phi(n)}\} = \mathscr{R}(n)$.

Lauseen 5.4((2)) nojalla

$$a^{\phi(n)} b_1 b_2 \cdots b_{\phi(n)} = ab_1 \cdot ab_2 \cdots ab_{\phi(n)} \equiv b_1 b_2 \cdots b_{\phi(n)} \mod n\,,$$

joten väite seuraa Seurauksen 5.9 nojalla □

Esimerkki 12.5. Koska $\operatorname{syt}(3, 10) = 1$ ja $\phi(10) = 4$, voimme selvittää luvun 3^{1000} viimeisen desimaalin Lauseen 12.4 avulla:

$$3^{1000} = 3^{250\phi(10)} = (3^{\phi(10)})^{250} \equiv 1^{250} = 1 \mod 10\,.$$

Siis viimeinen luku desimaaliesityksessä on 1.

[2]Katso luku 11.4.
[3]Lause 5.23

Eulerin funktion käyttäytymisessä on helppo nähdä multiplikatiivisuuteen viittaavia säännönmukaisuuksia, sillä esimerkiksi

$$\phi(15) = 8 = \phi(3)\phi(5) = 2 \cdot 4 = 8 \quad \text{ja}$$
$$\phi(18) = 6 = \phi(2)\phi(9) \neq \phi(3)\phi(6)\,.$$

Lause 12.6. *Eulerin ϕ-funktio on multiplikatiivinen funktio.*

Todistus. Olkoot $m_1, m_2 \in \mathbb{N}^*$ siten, että $\operatorname{syt}(m_1, m_2) = 1$. Olkoon

$$S_r = \{km_1 + r : 0 \leqslant k \leqslant m_2 - 1\}$$

jokaisella $1 \leqslant r \leqslant m_1$. Tällöin $\bigcup_{r=1}^{m_1} S_r = \{1, 2, 3, \ldots, m_1 m_2\}$.

S_1	1	$m_1 + 1$	$2m_1 + 1$	$\cdots$	$(m_2 - 1)m_1 + 1$
S_2	2	$m_1 + 2$	$2m_1 + 2$	$\cdots$	$(m_2 - 1)m_1 + 2$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
S_r	r	$m_1 + r$	$2m_1 + r$	$\cdots$	$(m_2 - 1)m_1 + r$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
S_{m_1}	m_1	$2m_1$	$3m_1$	$\cdots$	$m_1 m_2$

Jos $\operatorname{syt}(m_1, r) > 1$, niin $\operatorname{syt}(km_1 + r, m_1 m_2) > 1$ kaikille $0 \leqslant k \in \mathbb{Z}$. Siis $S_r \cap \mathscr{R}(m_1 m_2) = \varnothing$, jos $\operatorname{syt}(m_1, r) > 1$, joten

$$\mathscr{R}(m_1 m_2) \subset \bigsqcup_{r \in \mathscr{R}(m_1)} S_r\,. \tag{12.1}$$

Olkoon $r \in \mathscr{R}(m_1)$. Tällöin kaikille $s \in S_r$ pätee $\operatorname{syt}(s, m_1) = 1$. Harjoitustehtävän 12.2 nojalla mitkään kaksi joukon S_r alkiota eivät ole kongruentteja $\bmod m_2$, joten joukossa S_r on edustaja jokaisesta kongruenssiluokasta $\bmod m_2$. Siis $\phi(m_2)$ joukon S_r alkioista on luvun m_2 kanssa suhteellisia alkulukuja jokaisella $r \in \mathscr{R}(m_1)$.[4] Lauseen 2.15 nojalla nämä $\phi(m_2)$ lukua ovat suhteellisia alkulukuja luvun $m_1 m_2$ kanssa. Jos taas $\operatorname{syt}(s, m_2) > 1$, niin $\operatorname{syt}(s, m_1 m_2) > 1$, joten inkluusion (12.1) nojalla

$$\phi(m_1 m_2) = \#\mathscr{R}(m_1 m_2) = \phi(m_1)\phi(m_2)\,. \qquad \square$$

Proposition 12.2 nojalla Eulerin funktion arvot voidaan laskea, kunhan tunnetaan sen arvot alkulukujen potensseilla.

Lemma 12.7. *Olkoon p on alkuluku. Tällöin $\phi(p^k) = p^{k-1}(p-1)$ kaikille $k \in \mathbb{N} - \{0\}$.*

Todistus. Harjoitustehtävä 12.3. $\square$

Seuraus 12.8. *Olkoon $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ luvun n alkutekijäesitys. Tällöin*

$$\phi(n) = \phi(p_1^{e_1})\,\phi(p_2^{e_2}) \cdots \phi(p_k^{e_k})\,.$$

[4] Huomaa, että luku $\phi(m_2)$ on riippumaton luvusta $r \in \mathscr{R}((m_1)$.

Todistus. Väite seuraa Lauseesta 12.6, Lemmasta 12.7 ja Propositiosta 12.2. □

Esimerkki 12.9. Koska $4312 = 2^3 7^2 11$, saamme Seurauksen 12.8 nojalla

$$\phi(4312) = \phi(2^3)\phi(7^2)\phi(11) = 2^2(2-1)\,7\,(7-1)(11-1) = 1680\,.$$

Olkoon $n = p_1^{e_1}\,p_2^{e_2}\cdots p_k^{e_k}$ luvun $n \in \mathbb{N} - \{0,1\}$ alkutekijäesitys. Olkoon $f\colon \mathbb{N} \to \mathbb{R}$. Tällöin käytetään merkintää

$$\prod_{p|n} f(p) = f(p_1)f(p_2)\cdots f(p_k)\,.$$

Lause 12.10. *Olkoon $n \in \mathbb{N} - \{0,1\}$. Tällöin*

$$\phi(n) = n\prod_{p|n}\Big(1 - \frac{1}{p}\Big)\,.$$

Todistus. Olkoon $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$. nojalla

$$\begin{aligned}
\phi(n) &= \phi(p_1^{e_1})\,\phi(p_2^{e_2})\cdots\phi(p_k^{e_k}) \\
&= p_1^{e_1-1}(p_1-1)\,p_2^{e_2-1}(p_2-1)\cdots p_k^{e_k-1}(p_k-1) \\
&= p_1^{e_1}\Big(1-\frac{1}{p_1}\Big)\,p_2^{e_2}\Big(1-\frac{1}{p_2}\Big)\cdots p_k^{e_k}\Big(1-\frac{1}{p_k}\Big) \\
&= n\,\Big(1-\frac{1}{p_1}\Big)\Big(1-\frac{1}{p_2}\Big)\cdots\Big(1-\frac{1}{p_k}\Big)\,.
\end{aligned}$$

□

Lause 12.11. *Olkoon $n \in \mathbb{N} - \{0\}$. Tällöin $\sum_{d|n}\phi(d) = n$.*

Todistus. Olkoon

$$\mathscr{R}_\delta(n) = \{1 \leqslant a \leqslant n : \operatorname{syt}(a,n) = \delta\}$$

jokaiselle luvun n tekijälle δ. Seurauksen 2.10 nojalla $a \in \mathscr{S}_\delta$, jos ja vain jos δ on lukujen a ja n yhteinen tekijä ja $\operatorname{syt}(\frac{a}{\delta},\frac{n}{\delta}) = 1$. Siis $\#\mathscr{R}_\delta(n) = \phi(\frac{n}{\delta})$. Koska joukot $\mathscr{R}_\delta(n)$ ovat erillisiä ja

$$\bigcup_{\delta|n}\mathscr{R}_\delta(n) = \{b \in \mathbb{N}^* : b \leqslant n\}\,,$$

saamme

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

sillä $\{\frac{n}{\delta} : \delta \in \mathbb{N},\ \delta \mid n\} = \{d \in \mathbb{N} : d \mid n\}$. □

12.3 Tekijäfunktiot

Olkoon $k \in \mathbb{N}$. Luonnollisten lukujen k:s *tekijäfunktio*[a] on $\sigma_k\colon \mathbb{N} - \{0\} \to \mathbb{N}$,

$$\sigma_k(n) = \sum_{d|n} d^k\,.$$

Funktio $d = \sigma_0$ on *tekijöiden lukumääräfunktio* ja $\sigma = \sigma_1$ on *tekijöiden summafunktio.*

[a] Sitä olisi ehkä selvempi kutsua pidemmällä nimellä *tekijäpotenssisummafunktio.*

Propositio 12.12. *Funktio σ_k on multiplikatiivinen jokaisella $k \in \mathbb{N}$.*

Todistus. Funktio σ_k on multiplikatiivisen funktion id^k summafunktio, joten väite seuraa Propositiosta 12.3. □

Esimerkki 12.13. Jos p on alkuluku ja $k \in \mathbb{N}$, niin luvun p^k positiiviset tekijät ovat $1, p, \ldots, p^k$. Siten geometrisen summan osasummana on

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

Propositio 12.14. *Olkoon luvun $n \in \mathbb{N}^*$ alkutekijäesitys $n = p_1^{e_1} \cdots p_r^{e_r}$. Tällöin*

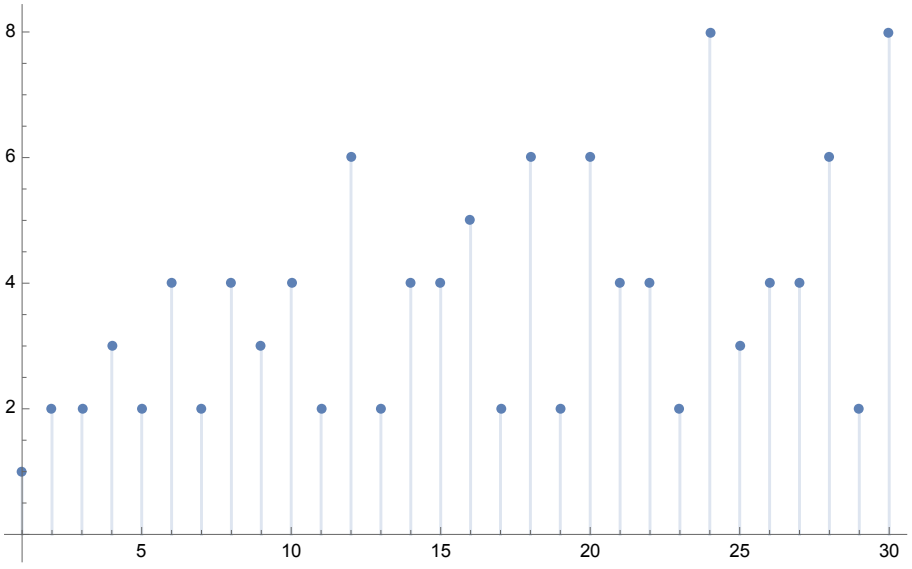
$$\sigma_0(n) = \prod_{j=1}^{r} (e_j + 1)\,.$$

Todistus. Multiplikatiivisuuden nojalla väite seuraa havainnosta, että luvun p^a tekijät ovat $1, p, p^2, \ldots, p^a$, jos p on alkuluku ja $a \in \mathbb{N}^*$. □

Propositio 12.15. *Olkoon $k > 1$. Olkoon luvun $n \in \mathbb{N}^*$ alkutekijäesitys $n = p_1^{e_1} \cdots p_r^{e_r}$. Tällöin*

$$\sigma_k(n) = \prod_{j=1}^{r} \frac{p_r^{k(e_j+1)} - 1}{p_r^k - 1}.$$

Todistus. Harjoitustehtävä 12.9. □



Kuva 12.2 — Tekijöiden lukumääräfunktion arvot $\sigma_0(n)$, kun $1 \leqslant n \leqslant 30$.

Luku $n \in \mathbb{N}^*$ on *täydellinen luku*[a], jos $\sigma(n) = 2n$. Se on *runsas luku*, jos $\sigma_1(n) > 2n$ ja *vajaa luku*, jos $\sigma_1(n) < 2n$.

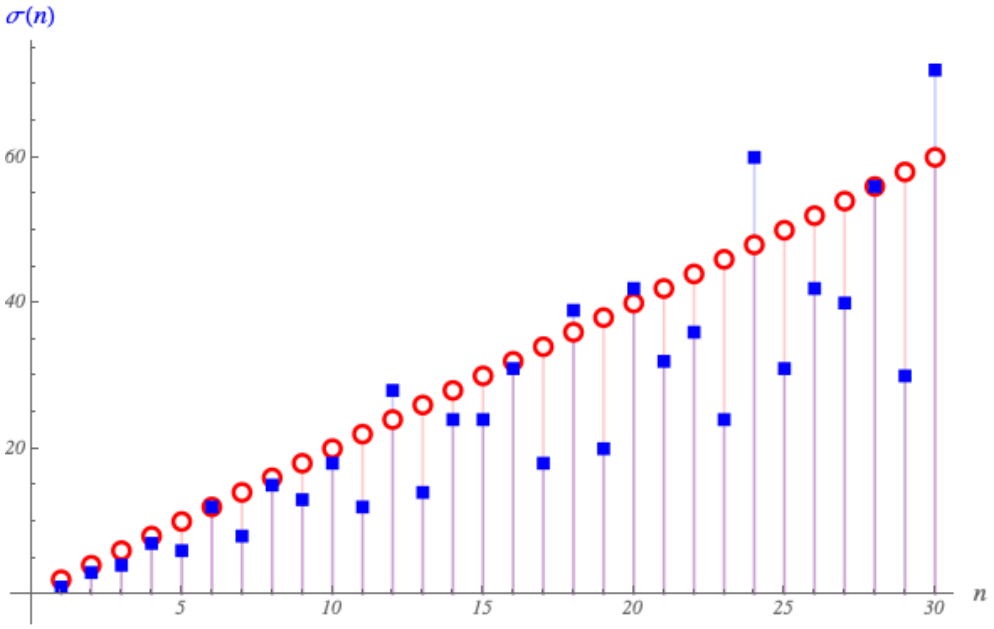
[a] Täydellisten lukujen käsite lienee peräisin Pythagoraan koulukunnalta.

Lemma 12.16. *Positiivinen luonnollinen luku n on täydellinen luku, jos ja vain jos se on itseään aidosti pienempien positiivisten tekijöidensä summa.* □

Esimerkki 12.17. (1) Täydellisiä lukuja ovat esimerkiksi

$$\begin{aligned} 6 &= 2(2^2-1) = 1+2+3, \\ 28 &= 2^2(2^3-1) = 1+2+4+7+14, \\ 496 &= 2^4(2^5-1) = 1+2+4+8+16+31+62+124+248 \quad \text{ja} \\ 8128 &= 2^6(2^7-1)\,. \end{aligned}$$

(2) Kaikki alkuluvut ovat vajaita lukuja. Lisäksi esimerkiksi $\sigma(4) = 1+2+4 = 7 < 8 = 2\cdot 4$, joten 4 on vajaa luku.
(3) $\sigma(12) = 1+2+3+4+6+12 = 28 > 24 = 2\cdot 12$, joten 12 on runsas luku.



Kuva 12.3 — Tekijöiden summafunktion arvot $\sigma(n)$, kun $1 \leqslant n \leqslant 30$ sinisellä. Punaiset ympyrät osoittavat luvun $2n$ jokaisella n. Sininen neliö punaisessa ympyrässä osoittaa täydelliset luvut 6 ja 28.

Joulukuussa 2018 tehdyn löydön jälkeen tunnetaan 51 täydellistä lukua. Ne ovat kaikki parillisia. Jos parittomia täydellisiä lukuja on, niin ne ovat suurempia kuin 10^{1500} ja niillä on ainakin 10 eri alkutekijää.[5]

Avoin kysymys 12.18. *Onko täydellisten lukujen joukko ääretön? Onko parittomia täydellisiä lukuja?*

Seuraava lause kytkee täydelliset luvut Mersennen alkulukuihin.[6] Ensimmäinen kohta on Eukleideksen tulos ja jälkimmäinen kohta on Eulerin tulos vuodelta 1849.

[5]Katso [OR].
[6]Katso luku 4.4.

Lause 12.19. *(1) Jos $2^p - 1$ on alkuluku, niin luku $n = 2^{p-1}(2^p - 1)$ on täydellinen.*
(2) Jos n on parillinen täydellinen luku, niin $n = 2^{p-1}(2^p - 1)$ jollain Mersennen alkuluvulla $M_p = 2^p - 1$.

Todistus. (1) Olkoon $n = 2^{p-1}(2^p - 1)$. Koska $\operatorname{syt}(2^{p-1}, 2^p - 1) = 1$ ja $2^p - 1$ on alkuluku, niin Proposition 12.12 ja Esimerkin 12.13 perusteella on

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

Siten n on täydellinen.
(2) Koska n on parillinen, niin on $p, q \in \mathbb{N}$, siten, että $p \geqslant 2$, q on pariton ja

$$n = 2^{p-1}q.$$

Luvun n täydellisyyttä, Propositiota 12.12 ja Esimerkkiä 12.13 käyttäen saadaan

$$2^p q = 2n = \sigma(n) = \sigma(2^{p-1})\sigma(q) = (2^p - 1)\sigma(q), \tag{12.2}$$

mistä seuraa, että $(2^p - 1) \mid 2^p q$. Koska $\operatorname{syt}(2^p - 1, 2^p) = 1$, niin Seurauksen 2.14 perusteella $(2^p - 1) \mid q$. On siis $r \in \mathbb{N}$, jolle $q = (2^p - 1)r$ ja siten yhtälön (12.2) nojalla

$$2^p r = \sigma(q).$$

Nyt q ja r ovat luvun q kaksi eri positiivistä tekijää ja

$$q + r = (2^p - 1)r + r = 2^p r = \sigma(q).$$

Funktion σ määritelmän mukaan q ja r ovat luvun q ainoat tekijät. Siten luku q on alkuluku, $r = 1$ ja $q = 2^p - r = 2^p - 1$. Siis $n = 2^{p-1}(2^p - 1)$. Koska $2^p - 1$ on alkuluku, niin Lauseen 3.5 nojalla myös p on alkuluku. □

Seuraus 12.20. *Mersennen alkulukujen joukko on ääretön, jos ja vain jos parillisten täydellisten lukujen joukko on ääretön.* □

Mersennen lukujen joukon äärettömyys on Avoimen kysymyksen 4.11 aihe. Mersennen lukuja tunnetaan 51, joten parillisia täydellisiä lukuja tunnetaan yhtä monta.

Esimerkki 12.21. Esimerkin 12.17 täydelliset luvut vastaavat neljää ensimmäistä Mersennen alkulukua. Seuraavat täydelliset luvut ovat

$$2^{12}(2^{13} - 1) = 2^{12}M_{13} = 33550336$$

ja

$$2^{16}(2^{17} - 1) = 2^{16}M_{17} = 8589869056\,.$$

12.4 Aritmeettinen funktio r_2

Lukuteoreettinen funktio r_2, jolle $r_2(n)$ on luvun n esitysten lukumäärä kahden neliön summina, ei ole multiplikatiivinen funktio, koska $r_2(1) = 4$.

Taulukossa 7.1 näimme, että funktion r_2 arvot eivät käyttäydy säännöllisesti. Kuvat 12.4 ja 12.5 havainnollistavat tätä ilmiötä. Sen sijaan funktion r_2 *keskimääräinen käyttäytyminen* on hyvin säännöllistä.

Aritmeettiset funktiot f ja g ovat *asymptoottisia*, jos $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$. Jos f ja g ovat asymptoottisia, käytetään merkintää $f \sim g$.

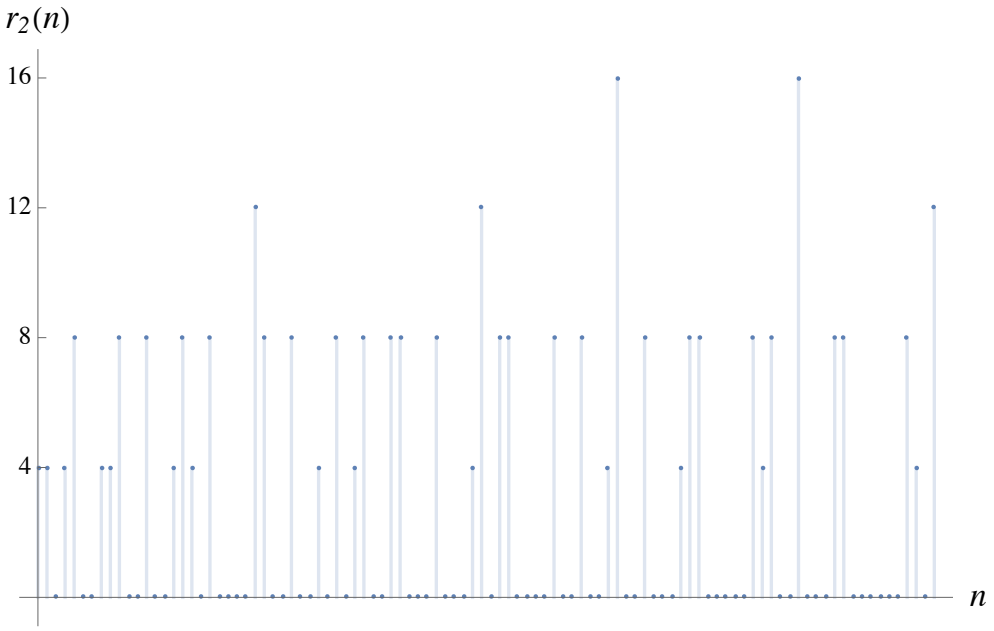
olkoot f ja F aritmeettisia funktioita. Jos funktiot F ja

$$n \mapsto \frac{1}{n} \sum_{k=1}^{n} f(k)$$

ovat asymptoottisia, niin F on funktion f *keskimääräinen kertaluku*[a]

[a] Englanniksi *average order*.

Keskimääräisen kasvunopeuden määritelmässä käytetään yleensä mahdollisimman yksinkertaista funktion F lauseketta, esimerkiksi $F(n) = Cn^\alpha$ joillain $C, \alpha \in \mathbb{R}$, $F(n) = Cn^\alpha \log(n)^\beta$ joillain $C, \alpha, \beta \in \mathbb{R}$ tai $F(n) = Ce^{\alpha n}$ joillain $C, \alpha \in \mathbb{R}$.



Kuva 12.4 — Funktion r_2 arvot kun $1 \leqslant n \leqslant 100$.

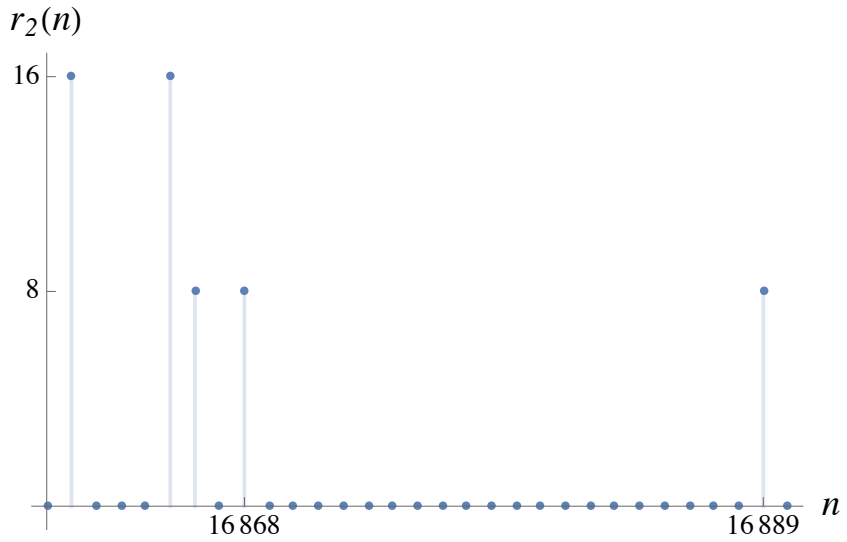
Lause 12.22. *Funktion r_2 keskimääräinen kertaluku on π.*

Todistus. Jos $x \in \mathbb{R}^2$, niin olkoon $I(x) = [x_1, x_1 + 1] \times [x_2, x_2 + 1]$. Määritelmän nojalla

$$\begin{aligned}\sum_{k=1}^{n} r_2(k) &= \sum_{k=1}^{n} \#\{(a,b) \in \mathbb{Z}^2 : a^2 + b^2 = k\} \\ &= \#\{(a,b) \in \mathbb{Z}^2 : a^2 + b^2 \leqslant n\} - 1 \\ &= \text{Ala} \bigcup_{(a,b)\in\mathbb{Z}^2 \,:\, a^2+b^2\leqslant n} I(a,b) - 1\,.\end{aligned}$$

On helppo tarkastaa, että

$$B(0, \sqrt{n} - \sqrt{2}) \subset \bigcup_{(a,b)\in\mathbb{Z}^2 \,:\, a^2+b^2\leqslant n} I(a,b) \subset B(0, \sqrt{n} - \sqrt{2})\,,$$



Kuva 12.5 — Funktion r_2 arvot kun $16860 \leqslant n \leqslant 18890$. Kahden neliön summien joukossa on tällä välillä 20 luvun pituinen aukko.

joten

$$\pi(\sqrt{n}-\sqrt{2})^2 - 1 \leqslant \sum_{k=1}^{n} r_2(k) \leqslant \pi(\sqrt{n}+\sqrt{2})^2 - 1\,.$$

Väite seuraa tästä, sillä $(\sqrt{n} \pm \sqrt{2})^2 = n + \mathrm{O}(\sqrt{n})$. □

Lause 12.23. *Tekijöiden lukumääräfunktion σ_0 keskimääräinen kertaluku on* $\log n$.

Todistus. Katso [HW, Theorem 319]. □

Lause 12.24. *Eulerin ϕ-funktion keskimääräinen kertaluku on* $\frac{3n}{\pi}$.

Todistus. Katso [HW, Theorem 330]. □

Harjoitustehtäviä

12.1. Todista Propositio 12.2.

12.2. Olkoot $r, m, n \in \mathbb{Z}$, $n \geqslant 2$. Osoita, että mitkään kaksi joukon

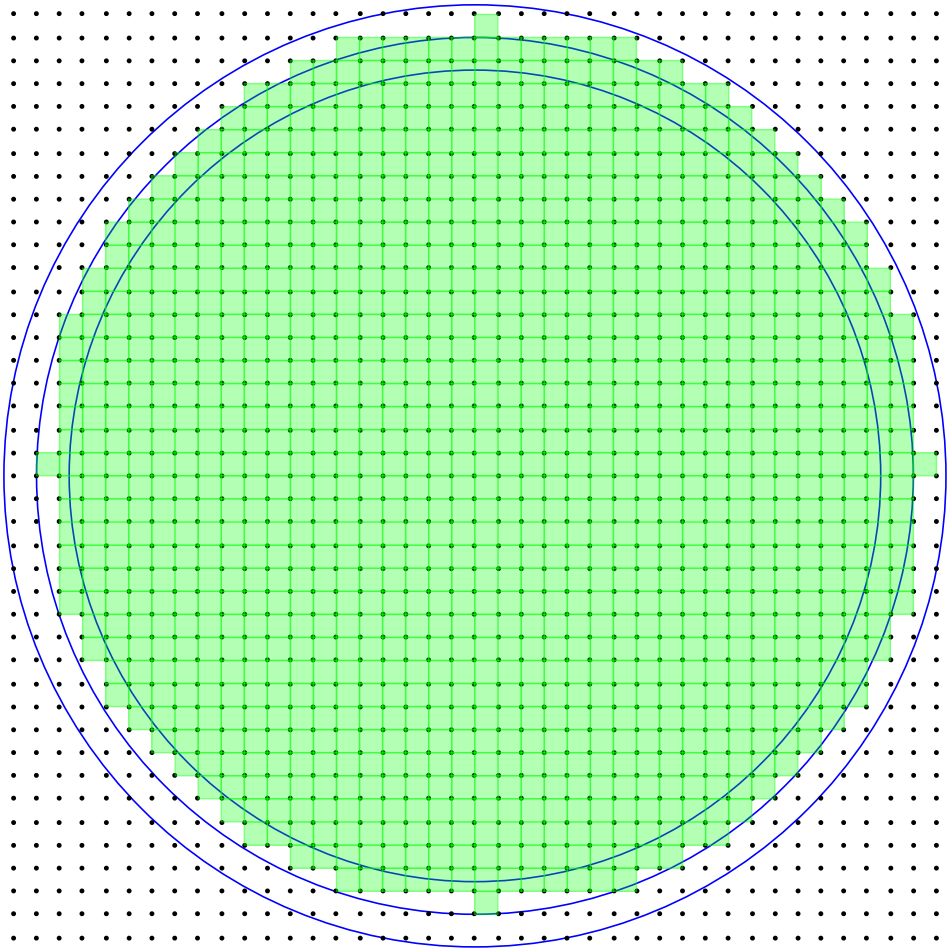
$$\{km + r : 0 \leqslant k \leqslant n-1\}$$

alkiota eivät ole kongruentteja mod n.

12.3. Todista Lemma 12.7.

12.4. Määritä $\phi(1000)$ ja $\phi(2343)$.

12.5. Määritä $\phi(75141)$.



Kuva 12.6 — Lauseen 12.22 todistuksen idea.

12.6. Mitkä ovat luvun 3^{400} desimaaliesityksen kaksi viimeistä numeroa?

12.7. Olkoot $m, n \in \mathbb{N}$ ja olkoon $s = \prod_{p|m \text{ ja } p|n} p$. Osoita, että

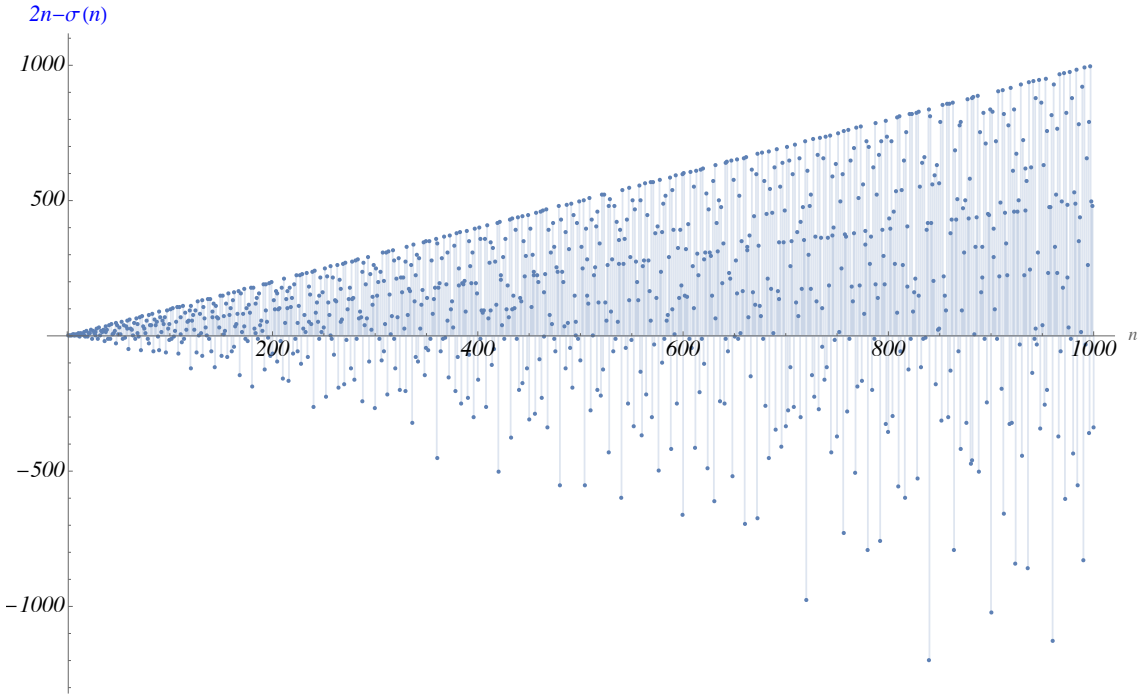
$$\phi(mn) = s\,\frac{\phi(m)\phi(n)}{\phi(s)}\,.$$

12.8. Olkoot $m, n \in \mathbb{N} - \{0, 1\}$ siten, että $\phi(mn) = \phi(n)$. Osoita, että $m = 2$ ja n on pariton.

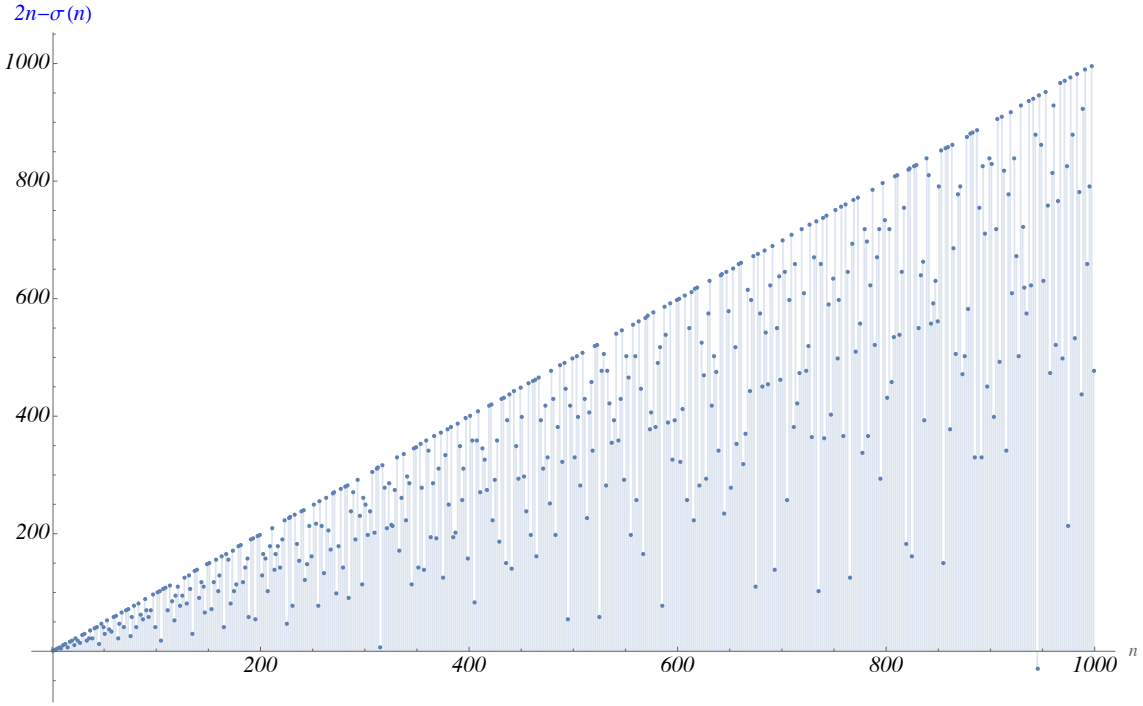
12.9. Todista Propositio 12.15.

12.10. Anna esimerkki parittomasta runsaasta luvusta.[7]

[7]Kuvat 12.7 ja 12.8.



Kuva 12.7 — Lausekkeen $2n - \sigma_1(n)$ arvot luvuilla $1 \leqslant n \leqslant 999$.



Kuva 12.8 — Lausekkeen $2n - \sigma_1(n)$ arvot parittomilla luvuilla $1 \leqslant n \leqslant 999$.

Kirjallisuutta

[GIM] Great Internet Mersenne Prime Search. `https://www.mersenne.org/report_milestones/`.

[Mac] MacTutor History of Mathematics Archive. `https://mathshistory.st-andrews.ac.uk/`.

[Apo] T. M. Apostol. *Introduction to analytic number theory.* Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[Cal] C. K. Caldwell. Twin Primes. The Prime Pages. `https://primes.utm.edu/top20/page.php?id=1`.

[Dud] U. Dudley. *A guide to elementary number theory*, volume 41 of *The Dolciani Mathematical Expositions*. Mathematical Association of America, Washington, DC, 2009. MAA Guides, 5.

[HW] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers.* Oxford University Press, Oxford, sixth edition, 2008.

[Hel] Y. Hellegouarch. *Invitation to the mathematics of Fermat-Wiles.* Academic Press, Inc., San Diego, CA, 2002. Translated from the second (2001) French edition by Leila Schneps.

[JJ] G. A. Jones and J. M. Jones. *Elementary number theory.* Springer Undergraduate Mathematics Series. Springer-Verlag London, Ltd., London, 1998.

[Lan1] E. Landau. Gelöste und ungelöste Probleme aus der Theorie der Primzahlverteilung und der Riemannschen Zetafunktion. In *Proceedings of the fifth International Congress of Mathematicians*, pages 93–108. Cambridge Univ. Press, 1913.

[Lan2] E. Landau. *Elementary number theory.* Chelsea Publishing Co., New York, N.Y., 1958.

[LeV] W. J. LeVeque. *Topics in number theory. Vols. 1 and 2.* Addison-Wesley Publishing Co., Inc., Reading, Mass., 1956.

[Nev] V. Nevanlinna. Lukuteorian alkeet. Luentomoniste 8. Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, 2004.

[OR] P. Ochem and M. Rao. Odd perfect numbers are greater than 10^{1500}. *Math. Comp.*, 81(279):1869–1877, 2012.

[Par] J. Parkkonen. Algebra. `http://users.jyu.fi/~parkkone/Algebra2021/Algebra2021R.pdf`, 2021.

[TB] R. Takloo-Bighash. *A Pythagorean introduction to number theory*. Undergraduate Texts in Mathematics. Springer, Cham, 2018. Right triangles, sums of squares, and arithmetic.