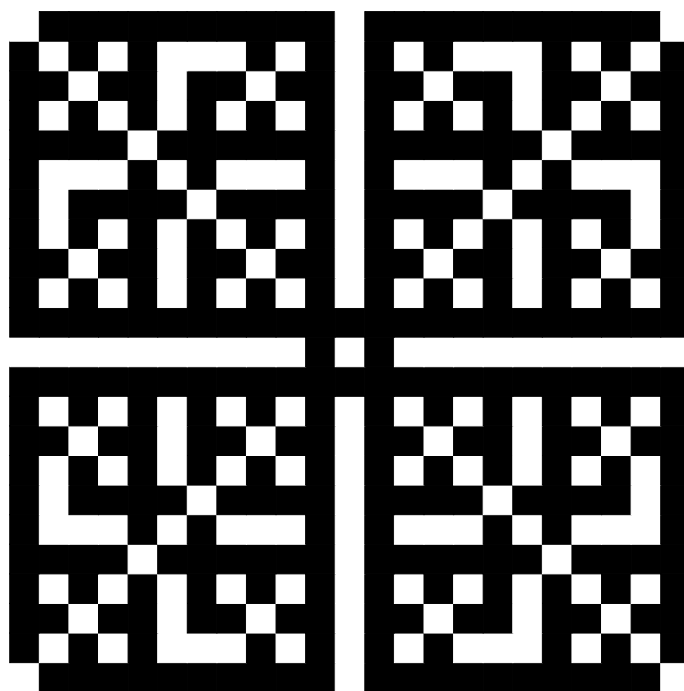

Lukuteoria 1



JOUNI PARKKONEN

LUENTOJA JYVÄSKYLÄN YLIOPISTOSSA

TALVELLA 2023

Sisällys

1	Jaollisuus	1
1.1	Kokonaisluvut ja luonnolliset luvut	1
1.2	Kokonaislukujen jaollisuus	2
1.3	Jakoyhtälö	3
1.4	Lukujärjestelmät	4
1.5	Jaollisuus kymmenjärjestelmässä	7
	Jaollisuus luvuilla 2, 5 ja 10	7
	Lohkaisuperiaate	8
	Jaollisuus luvulla 4	8
	Jaollisuus luvuilla 25, 50 ja 75	8
	Jaollisuus luvulla 8	9
	Jaollisuus luvuilla 3 ja 9	9
	Jaollisuus luvulla 11	10
	Jaollisuus luvulla 7	11
	Harjoitustehtäviä	12
2	Kokonaislukujen suurin yhteinen tekijä	15
2.1	Suurin yhteinen tekijä	15
2.2	Bézout'n yhtälö	16
2.3	Lineaarinen Diofantoksen yhtälö	18
2.4	Suhteelliset alkuluvut	20
2.5	Eukleideen algoritmi	21
2.6	Pienin yhteinen jaettava	23
	Harjoitustehtäviä	24
3	Alkuluvut	27
3.1	Alkuluvut ja yhdistetyt luvut	27
3.2	Aritmetiikan peruslause	29
3.3	Alkulukujen joukko on ääretön	31
3.4	Alkulukulause	32
3.5	Alkuluvut aritmeettisissa jonoissa	34
	Harjoitustehtäviä	36

4	Ratkaistuja ja ratkaisemattomia kysymyksiä alkuluvuista	39
4.1	Alkulukujen välissä olevista aukoista	39
4.2	Goldbachin otaksuma	40
4.3	Fermat'n luvut ja $n^2 + 1$ -otaksuma	41
4.4	Mersennen luvut	42
	Harjoitustehtäviä	43
5	Kongruenssi	45
5.1	Kongruenssi	45
5.2	Jaollisuussääntöjä kongruenssien avulla	48
5.3	Kongruenssiluokat	49
5.4	Fermat'n pieni lause	50
5.5	Wilsonin lause	52
5.6	Kokonaislukukertoimisista polynomeista	53
5.7	Kongruenssiluokkien laskutoimitukset	54
	Harjoitustehtäviä	55
6	Lineaariset kongruenssiyhtälöt	59
6.1	Lineaarinen kongruenssiyhtälö	59
6.2	Kiinalainen jäännöslause	62
6.3	Eulerin funktio	64
	Harjoitustehtäviä	67
	Kirjallisuutta	69

Johdanto

Tämä teksti on talven 2023 kurssin LUKUTEORIA 1 kurssimateriaali. Kurssilla käsittelemme kokonaislukujen jaollisuuteen liittyviä teemoja. Kurssille osallistuminen ei edellytä erityisiä esitietoja.

Luentojen pohjana 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 ja niinpä . Lisätietoja mainituista henkilöistä ja heidän matematiikastaan voi etsiä matematiikan historiaa käsittelevistä kirjoista ja esimerkiksi arkistosta [Mac]. Kurssin sisältö ei seuraa lukuteorian kehitystä historiallisessa aikajärjestyksessä ja esimerkiksi Gaussin¹ lemma esitetään ennen Eukleideen² lemmaa, joka on tämän kurssin kannalta Gaussin lemman seuraus.

¹Carl Friedrich Gauss (1777-1855).

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

Merkintöjä ja sopimuksia

Tässä esitellään merkintöjä joillekin 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.
- $\max A$ on joukon $A \subset \mathbb{Z}$ suurin alkio, jos sellainen on. Muuten $\max A = \infty$.
- $\#(A) \in \mathbb{N} \cup \{\infty\}$ joukon A alkioden 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.
- $\text{sy}(a, b)$ 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 .

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.

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

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

Luonnollisten lukujen järjestykselle pätee $a \leq b$, 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:

¹Lause 1.6.

²Monilla 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 $1, 2, \dots, k \in Q$ 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 $\{1, 2, \dots, k\} \subset A$ seuraa, että $k + 1 \in A$. Tällöin $A = \mathbb{N}$.*

Todistus. Väite seuraa induktioperiaatteesta tarkastelemalla joukkoa

$$B = \{n \in \mathbb{N} : \{0, 1, 2, \dots, n\} \subset A\}. \quad \square$$

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 $a \leq b$ 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 alkioita. Olkoon $B = \mathbb{N} - A$. Osoitamme induktiolla, että $B = \mathbb{N}$, jolloin siis $A = \emptyset$.

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

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) $1 \mid n$

$$(7) n \mid 0$$

$$(8) \text{ jos } 0 \mid n, \text{ niin } n = 0$$

$$(9) \text{ jos } d \mid n \text{ ja } n \neq 0, \text{ niin } |d| \leq |n| \text{ (VERTAILU)}$$

$$(10) \text{ jos } d \mid n \text{ ja } n \mid d, \text{ niin } |d| = |n|$$

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 $|k| \geq 1$. Siten

$$|n| = |dk| = |d||k| \geq |d|. \quad \square$$

Esimerkki 1.4. (1) Jos $u \mid 1$, niin Lauseen 1.3(9) nojalla $|u| \leq 1$, 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*

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

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

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

ei ole tyhjä. Tarkastelu jakautuu kolmeen tapaukseen.

- Jos $a \geq 0$, niin $a = a - 0 \cdot b \in S$.
- Jos $a \leq 0$ ja $b \geq 1$, niin $a - ab = a(1 - b) \geq 0$ ja siten $(a - ab) \in S$.
- Jos $a \leq 0$ ja $b \leq -1$,³ niin $(1 + b) \leq 0$. Nyt $a + ab = a(1 + b) \geq 0$ ja siten $(a + ab) \in S$.

³Muista, että $b \neq 0$.

Hyvän järjestyksen periaatteen⁴ 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 $r \geq b$, niin luku

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

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

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

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

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 $0 \leq r_1, r_2 < |b|$ pätee

$$a = q_1b + r_1 = q_2b + r_2.$$

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 $|r_2 - r_1| \geq |b|$. Tämä on mahdotonta, sillä $0 \leq r_1, r_2 < |b| - 1$. On siis $q_1 = q_2$ ja siten myös $r_1 = r_2$. \square

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

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

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 Jaollisuuslauseen⁵ 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 $n^2 = 4(N + 2) + 1$.

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 $a_0, a_1, \dots, a_s \in \mathbb{Z}$, joille $0 \leq a_i < k$ kaikilla $i = 0, 1, \dots, s$, $a_s > 0$ ja*

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

⁴Propositio 1.2

⁵Lause 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 $1, 2, \dots, n - 1$. Koska $k > 1$, niin Harjoitustehtävän 1.1 nojalla on yksikäsitteinen kokonaisluku $s \geq 0$, jolle

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

Jakoyhtälön⁶ perusteella on yksikäsitteiset $a_s, r \in \mathbb{Z}$, joille

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

missä $0 \leq r < k^s$. 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 $t \geq 0$ ja b_0, \dots, b_t , joille

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

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

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

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 $s, t \geq 0$, $a_0, a_1, \dots, a_s, b_0, b_1, \dots, b_t$ joille $0 \leq a_i < k$, kaikilla $i = 0, 1, \dots, s$, $0 \leq b_j < k$, kaikilla $j = 0, 1, \dots, t$, $a_s > 0$, $b_t > 0$ ja

$$n = a_s k^s + \dots + a_1 k + a_0 = b_t k^t + \dots + b_1 k + b_0. \quad (1.1)$$

Vähentämällä luvun n esitykset yhtälössä (1.1) saadaan

$$0 = e_m k^m + \dots + e_1 k + e_0, \quad (1.2)$$

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 $0 \leq a_i < k$ ja $0 \leq b_i < k$ kaikilla indekseillä i , niin

$$|e_i| = |a_i - b_i| \leq k - 1 \quad (1.3)$$

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

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

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

⁶Lause 1.6

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

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

Tällöin $\pm(a_N a_{N-1} \dots a_0)_b$ 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: $8^0, 8^1, 8^2, \dots$ 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

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

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

(2) Luku 2016_8 muunnetaan kymmenjärjestelmään seuraavasti

$$2016_8 = 2 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0 = 2 \cdot 512 + 1 \cdot 8 + 6 = 1038 .$$

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 A, B, C, D, E ja 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

$$1234 = 77 \cdot 16 + 2 = (4 \cdot 16 + 13) \cdot 16 + 2 = 4 \cdot 16^2 + 13 \cdot 16^1 + 2 \cdot 16^0 = 4D2_{16} = 4D2 .$$

(2) Luku $10B_{16} = 10B$ muunnetaan 10-järjestelmään seuraavasti

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

⁷Suomeksi: *on erikseen kerrottu*

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

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.

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

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

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

Esimerkki 1.13. Laaditaan kaksi- ja neljäjärjestelmien kertotaulut.

\cdot	1	10_2	\cdot	1	2	3	10_4
1	1	10_2	1	1	2	3	10_4
10_2	10_2	100_2	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 $s \geq 0$ ja a_0, a_1, \dots, a_s , joille

$$n = a_s 10^s + a_{s-1} 10^{s-1} + \dots + a_1 10 + a_0 = a_s a_{s-1} \dots a_0, \quad (1.4)$$

$0 \leq a_i \leq 9$ kaikilla $i = 0, 1, \dots, s$ ja $a_s > 0$. Tässä luvussa luvut a_0, \dots, 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 :

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

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 $10, 100, 1000, \dots$ tekijä, niin lohkaisutermit 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 lohkaisutermit valitaan luvun n täysiä satoja sisältävä osa $a_s a_{s-1} \dots a_2 00$. □

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 $9 = 10 - 1$, $99 = 100 - 1$, $999 = 1000 - 1, \dots$ 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 lohkaisutermien valinnan seurauksena *alkuperäisen luvun numeroiden summa*.

Jos

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

niin luku

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

on luvun n numerosumma.

Jos lohkaisutermiksi valitaan luvuilla 3 ja 9 jaollinen summa

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

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

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

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

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

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

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

$$a^m - b^m = (a - b)(a^{m-1} + a^{m-2}b + \dots + ab^{m-2} + b^{m-1}). \quad (1.8)$$

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

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

Kriittiseksi termiksi jää tällöin

$$a_0 - a_1 + a_2 - \dots + (-1)^s a_s, \quad (1.9)$$

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

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

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

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

ja luvulle -648 saadaan⁸

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

Luvun 648532 kriittinen termi on 1. ja 2. jaksotermien 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.

⁸huomaa etumerkki!

Yleisesti: Tutkittaessa luvun $n \in \mathbb{N}$ jaollisuutta luvulla 7, luku n jaetaan oikealta alkaen kolmen numeron ryhmiin $a_2a_1a_0, a_5a_4a_3, \dots$, (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 $a^{k-1} \leq b < a^k$.

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 $n \in \mathbb{N}, n \geq 2$. Olkoot $a_i, c_i \in \mathbb{Z}$ kaikilla $i = 1, 2, \dots, n$.

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

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

⁹Todista väite induktiolla luvun m suhteen.

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

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

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

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 luvuksi. 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 luvuksi. 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 $dcb a_7$ on jaollinen luvulla 6, jos ja vain jos

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

¹¹Tämän voi todistaa induktiolla luonnollisille luvuille ja negatiivisille kokonaisluville.

¹²Katso 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'n¹ 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

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

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

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

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

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

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

¹Étienne Bézout (1730-1783).

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

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 alkioita.

(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 kirjoitetaan $\text{syt}(a, b)$, 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 nolasta poikkeava.

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

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

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 periaatteen² 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

$$g = x_0a + y_0b \quad (2.1)$$

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

$$r = a - qg = a - q(x_0a + y_0b) = (1 - qx_0)a - qy_0b \in J.$$

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 $d \leq g$, joten $g = \text{syt}(a, b)$. \square

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

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

joillain $x, y \in \mathbb{Z}$. \square

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 $c \mid \text{syt}(a, b)$.*

Todistus. Olkoon c lukujen a ja b yhteinen jakaja. Tällöin $a = k_1c$ ja $b = k_2c$. Bézout'n yhtälön nojalla on luvut $x, y \in \mathbb{Z}$, joille pätee

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

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

Jos taas $c \mid \text{syt}(a, b)$, niin jaollisuuden transitiivisuuden³ nojalla $c \mid a$ ja $c \mid b$. \square

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 $k \text{syt}(a, b)$ jollain $k \in \mathbb{Z}$, voidaan esittää tällaisena summana.

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

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

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

²Propositio 1.2

³Lause 1.3(2)

Todistus. Olkoon $d = \text{syt}(a, b)$. 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

$$c = md = mxa + myb. \quad \square$$

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

(2) Koska $\text{syt}(18, 64) = 2$, 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*

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

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

$$\text{syt}(ca, cb) \geq c \text{syt}(a, b). \quad (2.2)$$

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

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

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

$$\text{syt}(ca, cb) \leq c \text{syt}(a, b). \quad (2.3)$$

Väite seuraa yhdistämällä epäyhtälöt (2.2) ja (2.3). □

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*

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

Erityisesti

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

Todistus. Harjoitustehtävä 2.6 □

2.3 Lineaarinen Diofantoksen yhtälö

Bézout'n yhtälö on erikoistapaus lukuteoriassa merkittävistä *Diofantoksen⁴ 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 $au + bv = c$.

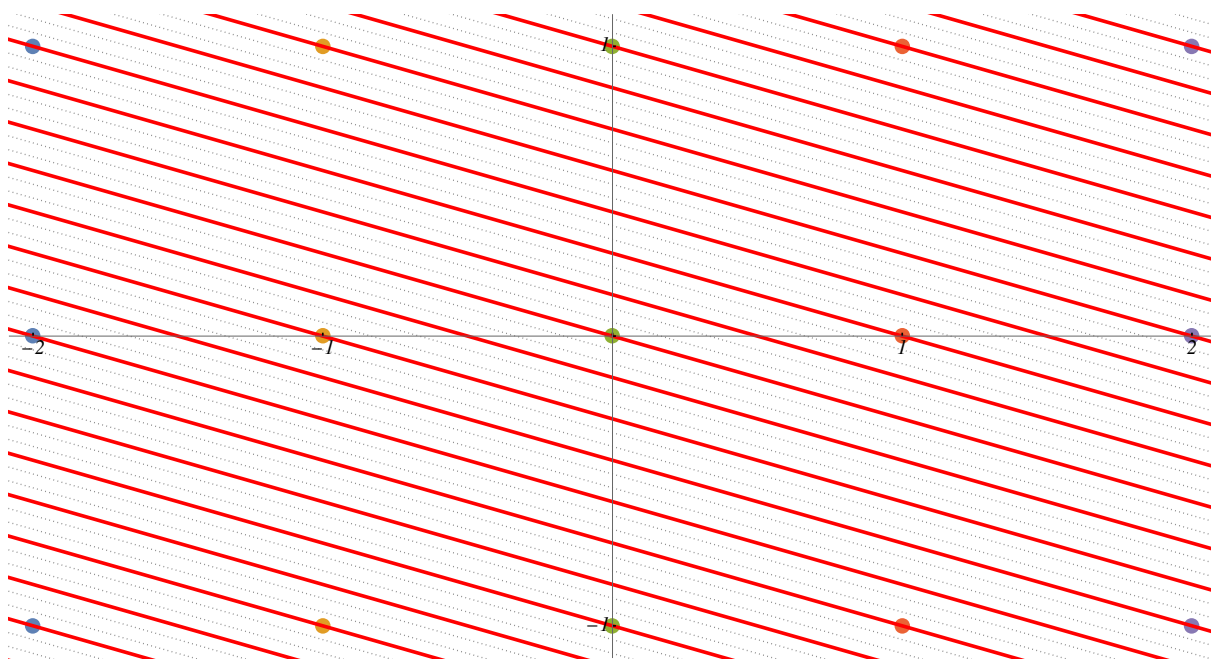
⁴Diofantos Aleksandrialainen oli kreikkalainen matemaatikko 200-luvulla Egyptissä.

Määritelmän mukaan lineaarisen Diofantoksen yhtälön ratkaisuksi hyväksytään ainoastaan kokonaislukupareja.

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

Todistus. Väite seuraa suoraan Lauseesta 2.7. □

Esimerkki 2.12. $\text{syta}(6, 21) = 3$, 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

$$x^2 + y^2 = z^2 \quad (2.4)$$

on äärettömän monta ratkaisua $(x, y, z) \in \mathbb{Z}^3$, joita kutsutaan *Pythagoraan⁵ kolmikoiksi*, koska Pythagoraan lauseen nojalla yhtälön ratkaisut ovat jonkin suorakulmaisen kolmion sivujen pituudet. On helppo tarkastaa, että esimerkiksi $(3, 4, 5)$ on Pythagoraan kolmikko.

Fermat⁶ kirjoitti 1600-luvulla Diofantoksen Arithmetica-kirjan marginaaliin löytäneensä todistuksen sille, että $(0, 0, 0)$ on Diofantoksen yhtälön

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

ainoa ratkaisu, jos $n \geq 3$. Wiles todisti tämän *Fermat'n suuren lauseen* 1990-luvulla.

⁵Pythagoras Samoslainen oli kreikkalainen filosofi, joka eli noin 570-490 eaa.

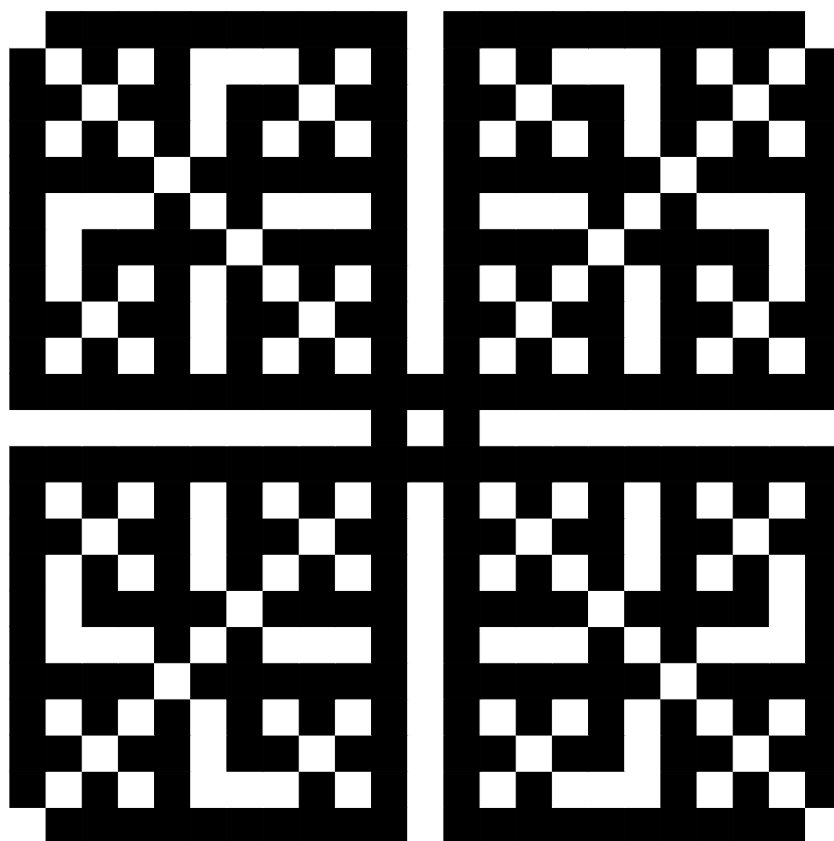
⁶Pierre de Fermat (1601-1665).

2.4 Suhteelliset alkuluvut

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

Jos $a, b \in \mathbb{Z}$ ja $\text{syt}(a, b) = 1$, 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 $\{(a, b) \in \mathbb{Z}^2 : -11 \leq a, b \leq 11\}$.

Huomautus 2.13. Bézout'n yhtälön⁷ 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*

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

(2) *Jos $a \mid bc$, niin $a \mid c$. (GAUSSIN LEMMA)*

⁷Seuraus 2.5

⁸Katso Harjoitustehtävä 2.10.

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

$$c = c(xa + yb) = cxa + cyb. \quad (2.5)$$

((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 $a \mid c$. \square

Suhteellisilla alkuluvuilla on mielenkiintoinen tulo-ominaisuus, johon palaamme Luvussa 6.3.

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

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

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

joten

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

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

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

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

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.

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

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

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 $1 \leq b < a$.

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

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

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

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

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

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

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

$$b > r_1 > r_2 > \dots \geq 0,$$

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

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

^aLause 1.6

^bEukleideen 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 $a, b, r_1, \dots, r_{n-3}$ yhtälöihin kertoo, että

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

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 $\text{syt}(a, b) = r_{n-1}$. \square

Jos $b \nmid a$, niin Eukleideen algoritmi *peruuttaen* antaa Bézout'n yhtälössä⁹ 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 haluttuun esitykseen.

⁹Seuraus 2.5.

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

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

Siten $\text{sy}(18, 64) = 2$. *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 $a_1, a_2, \dots, a_N \in \mathbb{Z} - \{0\}$ yhteinen jaettava, jos $a_i \mid c$ kaikilla $1 \leq i \leq N$.

Lukujen $a_1, a_2, \dots, a_N \in \mathbb{Z} - \{0\}$ pienin yhteinen jaettava, $\text{pyj}(a_1, a_2, \dots, a_N)$ 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 $\text{pyj}(a, b)$ 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 $\text{pyj}(a, b) \mid c$.*

Todistus. Jos $\text{pyj}(a, b) \mid c$, 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 $0 \leq r < \text{pyj}(a, b)$, joille $c = q \text{pyj}(a, b) + r$. Koska $a \mid \text{pyj}(a, b)$ ja $b \mid \text{pyj}(a, b)$, 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 $r < \text{pyj}(a, b)$, täytyy olla $r = 0$. Siis $\text{pyj}(a, b) \mid c$. \square

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

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 $a \mid \text{pyj}(a, b)$, niin $\text{pyj}(a, b) = ka$ jollain $k \in \mathbb{N}$. Koska $b \mid \text{pyj}(a, b) = ka$, niin Gaussin lemmän¹⁰ nojalla $b \mid k$. Lauseen 1.3(9) nojalla $k \geq b$, joten $\text{pyj}(a, b) = ka \geq ab$. Mutta ab on lukujen a ja b yhteinen jaettava, joten määritelmän nojalla $\text{pyj}(a, b) \leq ab$. \square

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

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

Todistus. Harjoitustehtävä 3.22 \square

¹⁰Seuraus 2.14(2).

Harjoitustehtäviä

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

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

$$\text{sy}(a_1, a_2, \dots, a_N) = 1.$$

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

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

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

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 $\text{sy}(a, b) > 1$, $a \mid c$ ja $b \mid c$ mutta $ab \nmid c$,

(2) Etsi luvut $a, b, c \in \mathbb{Z}$, joille $\text{sy}(a, b) > 1$ 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 $\text{sy}(a, c) = 1$. Osoita, että $\text{sy}(a, b) = \text{sy}(a, bc)$.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 $\text{sy}(x, y) = \text{sy}(u, v)$.¹⁵

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

$$\text{sy}(126, 308) = 126x + 308y.$$

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

$$\text{sy}(78, 123) = 78x + 123y.$$

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

$$\text{sy}(175, 441) = 175x + 441y.$$

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

$$\text{sy}(594, 814) = 594x + 814y.$$

¹¹Vihje: Tehtävä 2.1.

¹²Käytä Gaussin lemmaa.

¹³Tässä tehtävässä näytetään, että Seurauksen 2.14 väitteet eivät päde ilman oletusta $\text{sy}(a, b) = 1$.

¹⁴Käytä Bézoutin yhtälön seurausta ja Gaussin lemmaa.

¹⁵Olkoon $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Auttaisivatko lineaarialgebra ja Bézout?

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

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

2.18. Määritä Eukleideen algoritmin avulla $\text{syt}(1891, 651)$.

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 alkuluku¹

(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, \dots, p_r ovat eri alkulukuja ja luvulle $a \in \mathbb{Z}$ pätee $p_k \mid a$ kaikilla $1 \leq k \leq r$, 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 $n \in \mathbb{N}$, $n \geq 2$. Luku n on yhdistetty luku jos ja vain jos on alkuluku $p \leq \sqrt{n}$, joka jakaa luvun n .*

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

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

¹The only even prime is the oddest prime!

Eratostheneen ^aseula

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

- (1) Kirjoitetaan taulukkoon luonnolliset luvut $n \leq x$.
- (2) Luvun 2 positiiviset tekijät ovat 1 ja 2, joten 2 on alkuluku. Poistetaan luvun 2 monikerrat $2k$, joille $k \geq 2$.
- (3) Ensimmäinen luku, jota ei ole poistettu on 3. Sen on oltava alkuluku. Poistetaan luvun 3 monikerrat $3k$, joille $k \geq 2$.
- (4) Seuraava luku, jota ei ole poistettu on 5. Sen on oltava alkuluku. Poistetaan luvun 5 monikerrat $5k$, joille $k \geq 2$.
- (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.

^aEratosthenes Kyreneläinen eli muun muuassa Aleksandriassa noin vuosina 276-199 eaa.

^bTämä riittää Lemman 3.3 nojalla.

Esimerkki 3.4. Etsitään alkuluvut p , joille $p \leq 40$. 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 $a, n \in \mathbb{N}$, $a, n \geq 2$. 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. \square

Lause 3.6. *Olkoot $a, m \in \mathbb{N}$, $a \geq 2$. 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 $a^m + 1 \geq 3 + 1 = 4$ 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 $n \geq 0$. 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. \square

3.2 Aritmetiikan peruslause

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

Todistetaan ensin alkulukutekijäesityksen olemassaolo-osa.

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

Todistus. Todistetaan väite induktiolla. Koska 2 on alkuluku, niin väite on totta kun $n = 2$. Olkoon $k \in \mathbb{N}$, $k \geq 2$. Oletetaan, väite on totta luvuille $2, \dots, k$. 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 $a, b \in \mathbb{N}$, $1 < a, b \leq k$, joille

$$k + 1 = ab.$$

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

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

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

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

missä $p_1 < \cdots < p_k$ ovat alkulukuja ja $e_1, \dots, e_k \in \mathbb{N} - \{0\}$, 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 yksikäsitteisyys todistus käyttää seuraavaa tulosta, joka on Luvussa 2.4 todistetun Gaussin lemmän 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 $1 \leq i \leq n$ ja olkoon p alkuluku. Jos $p \mid (a_1 \cdots a_n)$, niin $p \mid a_i$ jollain $1 \leq i \leq n$.*

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

(2) Harjoitustehtävä 3.3. □

²Seuraus 2.14(2)

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

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

Esitys on tekijöiden järjestyksestä vaille yksikäsitteinen.

Todistus. Olkoon $n \in \mathbb{N}$, $n \geq 2$. 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 $2, 3, \dots, n - 1$ 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 $e_i, f_j \in \mathbb{N}$, $i = 1, \dots, k$, $j = 1, \dots, s$, joille $p_i \neq p_j$ ja $q_i \neq q_j$ kun $i \neq j$ ja

$$n = p_1^{e_1} \cdots p_k^{e_k} = q_1^{f_1} \cdots q_s^{f_s}. \quad (3.1)$$

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

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 (3.1) molempien puolien lausekkeet luvulla p_1 saadaan

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

Koska $p_1 \geq 2$ alkulukuna, niin $\frac{n}{p_1} \leq n - 1$.

Induktio-oletuksen mukaan luvulla n/p_1 on (järjestyksestä vaille) 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 $i = 1, \dots, k$. Siten luvun $n + 1$ esitys on yksikäsitteinen. Väite seuraa induktioperiaatteesta. \square

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 $r, s \in \mathbb{N}$ jolle

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

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 $\text{sy}(r, s) = 1$ ja p on alkuluku. On siis $s = 1$ ja siten $\sqrt[n]{a} = r$. \square

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

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

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

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

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

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 \square

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, \dots, p_n alkulukuja. Näytetään, että on alkuluku, joka ei ole mikään luvuista p_1, \dots, 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 $1, 2, \dots, n$. 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 $i = 1, \dots, n$, joten q on etsitty alkuluku. \square

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

³Supistetaan 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, \dots, 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 äärettömän 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 $\mathbf{p}_n \leq 2^{2^{n-1}}$.*

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 $\mathbf{p}_1, \dots, \mathbf{p}_n$. 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 $i = 1, \dots, n$. Koska alkuluku p ei ole n :n ensimmäisen alkuluvun joukossa, niin $\mathbf{p}_{n+1} \leq p$. Lausetta 1.3 (9), induktio-oletusta⁴ ja geometrisen summan kaavaa käyttämällä saadaan

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

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

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

3.4 Alkulukulause

Funktio $\pi: [0, \infty) \rightarrow \mathbb{N}$,

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

on *alkulukujen lukumääräfunktio*.^a

^aAlkulukujen lukumääräfunktioita on tapana merkitä kreikkalaisella kirjaimella π . Reaalilukuun π sekoittamisen välttämiseksi käytämme hieman poikkeavaa merkintätapaa.

⁴ $\mathbf{p}_i \leq 2^{2^{i-1}}$ kaikilla $i = 1, \dots, n$

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

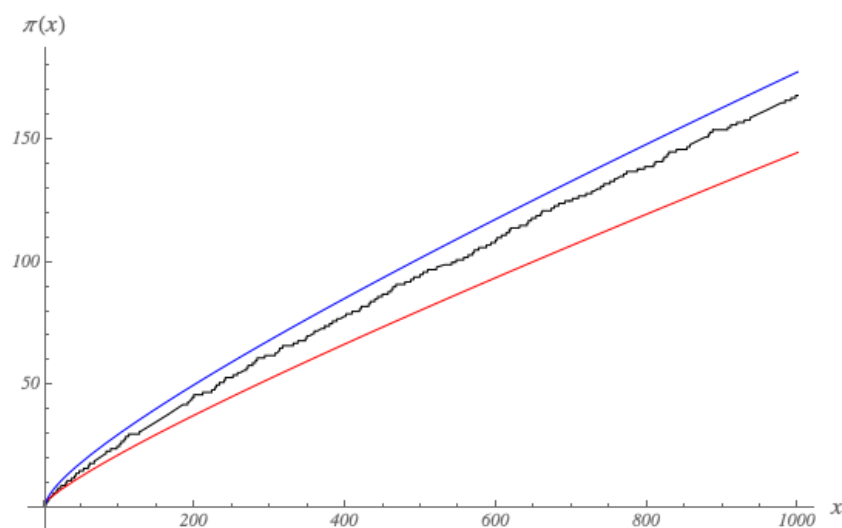
(2) $\pi(p_n) = n$.

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

Funktio Li: $[2, \infty[\rightarrow \mathbb{R}$,

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

on (siirretty) logaritmin integraalifunktio.



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

Hadamard⁵ ja de la Vallée Poussin⁶ todistivat toisistaan riippumatta vuonna 1896 seuraavan vaativan tuloksen:

Lause 3.20 (Alkulukulause).

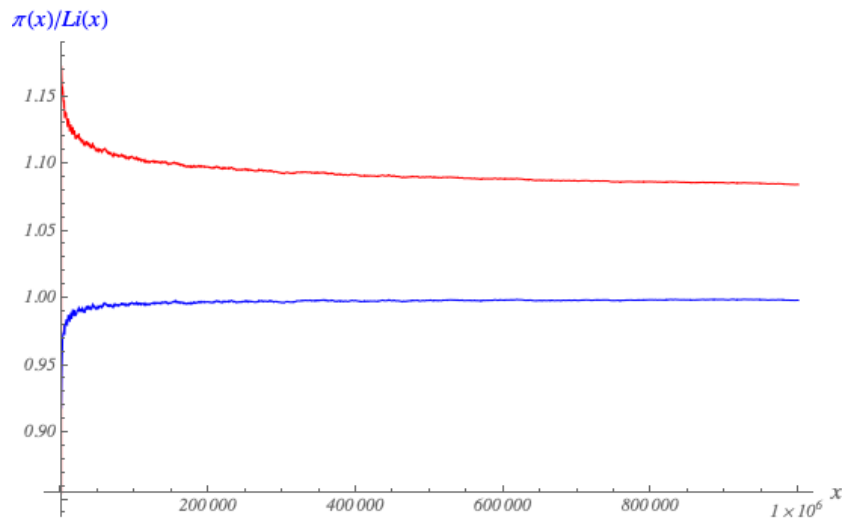
$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{\text{Li}(x)} = \lim_{x \rightarrow \infty} \frac{\log x}{x} \pi(x) = 1.$$

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

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

⁵Jacques Hadamard (1865-1963).

⁶Charles de la Vallée Poussin (1866-1962).



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

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

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

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

3.5 Alkuluvut aritmeettisissa jonoissa

Olko $a, b \in \mathbb{Z}$ 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) Aritmeettisessä 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 tyyppisiä 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, \dots, p_k muotoa $4n + 3$ olevia alkulukuja, $n \geq 1$, ja olkoon

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

Luku N on muotoa $4n + 3$. Se ei ole jaollinen millään luvuista p_i , $i = 1, \dots, k$, 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 lemmän⁷ nojalla $3 \nmid 4p_1 \cdots p_k$.

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

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

Koska $2 \nmid N$, niin r_i ei voi olla 0 eikä 2. Jos olisi $r_i = 1$ kaikilla $i = 1, \dots, s$, niin N olisi muotoa $4n + 1$ olevien lukujen tulona myös muotoa $4n + 1$. Siis $q_i = 4n_i + 3$ jollain $i = 1, \dots, s$. Koska luvut p_1, \dots, 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. \square

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 $\text{sy}(a, b) = 1$. Dirichlet⁸ 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 $\text{sy}(a, b) = 1$, niin muotoa*

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

olevia alkulukuja on äärettömän monta.

Todistus. Katso esimerkiksi [Apo, Luku 7]. \square

⁷Lemma 3.9.

⁸Gustav 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, \dots, p_r eri alkulukuja. Olkoon $n \in \mathbb{Z}$ kokonaisluku, jolle $p_k \mid n$ kaikilla $1 \leq k \leq r$. 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 $p \geq 5$ alkuluku. Osoita, että $12 \mid (p^2 - 1)$.
- 3.14.** Todista Lause 3.14.
- 3.15.** Eukleideen lauseen todistuksessa haettiin alkulukujoukon $\{p_1, p_2, \dots, p_n\}$ 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 $n \in \mathbb{N}$, $n \geq 2$, luku, joka jakaa luvun $(n - 1)! + 1$. Osoita, että n on alkuluku.
- 3.20.** Olkoon $n \in \mathbb{N}$, $n \geq 5$ yhdistetty luku. Osoita, että $n \mid (n - 1)!$. Mitä tapahtuu, jos n on alkuluku?

⁹Seuraus 2.14(1) ja induktio.

¹⁰Joitain tekijöitä pitäisi nähdä vain katsomalla näitä lukuja...

¹¹Tällä luvulla ei ole kovin pieniä alkutekijöitä.

¹²Tarkastele jakojäännöksiä sopivalla jakajalla.

¹³Tarkastele jaollisuutta luvulla 3.

¹⁴Miksi 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 $\text{sy}(34086, 14630)$ ja $\text{py}(34086, 14630)$.
- 3.24.** Määritä luvut $\text{sy}(11662, 95795)$ ja $\text{py}(11662, 95795)$.

¹⁵Lause 3.14

Luku 4

Ratkaistuja ja ratkaisemattomia kysymyksiä alkuluvuista

Landau¹ esitti vuonna 1912 kansainvälisessä matemaatikoiden kongressissa² 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 $n \in \mathbb{N}$, $n \geq 2$, on $n - 1$ peräkkäistä luonnollista lukua, joista mikään ei ole alkuluku.*

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

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

on $n - 1$ kappaletta. Nyt

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

on jaollinen luvulla 2,

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

¹Edmund Landau (1877-1938).

²International Congress of Mathematicians eli ICM

³Katso [Lan, 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 , $i = 2, 3, \dots, n$. Siten mikään luvuista $n! + 2, n! + 3, \dots, n! + n$ ei ole alkuluku. \square

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 väitetään *alkulukukaksosia on äärettömän monta* kutsutaan alkulukuotaksumaksi eli alkuluku-konjektuuriksi. Otaksumalla eli konjektuurilla tarkoitetaan todistamatonta väitettä, jonka uskotaan pitävän paikkansa esimerkiksi ahkeran kokeilemisen perusteella. Toisenkin Landaun kysymys käsittelee 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 $n \geq 4$ kahden alkuluvun summa?*

⁴Adrien-Marie Legendre (1752-1833).

Tämä kysymys esiintyy Goldbachin⁵ kirjeessä Eulerille⁶ 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. Helfgott⁷ on toistaiseksi julkaisemattomassa käsikirjoituksessa todistanut *heikon Goldbachin konjektuurin*, jonka mukaan kaikki parittomat luvut $n \geq 7$ 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

$$F_0 = 2^1 + 1 = 3,$$

$$F_1 = 2^2 + 1 = 5,$$

$$F_2 = 2^4 + 1 = 17,$$

$$F_3 = 2^8 + 1 = 257 \quad \text{ja}$$

$$F_4 = 2^{16} + 1 = 65537$$

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, \dots, F_{11} ja lisäksi F_n on osoitettu yhdistetyksi luvuksi monilla muilla luvun n arvoilla, esimerkiksi, kun $5 \leq n \leq 32$.

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?*

⁵Christian Goldbach (1690-1764).

⁶Leonhard Euler (1707-1783).

⁷Harald 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 $\text{syt}(F_n, F_m) = 1$.

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) nojalla⁸ d ei ole luvun F_n tekijä, jos $d \neq 1$. \square

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. Iwaniec⁹ 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

$$M_2 = 2^2 - 1 = 3,$$

$$M_3 = 2^3 - 1 = 7,$$

$$M_5 = 2^5 - 1 = 31 \quad \text{ja}$$

$$M_7 = 2^7 - 1 = 127$$

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].

⁸Katso Harjoitustehtävä 1.12.

⁹Henryk 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 $n \geq 2$. Osoita, että Fermat'n luvun F_n viimeinen numero on 7.
- 4.3.** Olkoot p ja q alkulukuja, $p \neq q$. Määritä $\text{syt}(M_p, M_q)$.

¹⁰Huomaa, 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 lauseen¹ ja sovellamme kongruenssia kokonaislukukertoimisen polynomin juurten tarkasteluun.

5.1 Kongruenssi

Olkoon $m \in \mathbb{N}$, $m \geq 1$. 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 $a \equiv b \pmod{m}$.

Luku m on kongruenssin *moduli*.

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

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

- (1) $a \equiv a \pmod{m}$ kaikilla $a \in \mathbb{Z}$.
- (2) Jos $a \equiv b \pmod{m}$, niin $b \equiv a \pmod{m}$.
- (3) Jos $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m}$, niin $a \equiv c \pmod{m}$.

Todistus. Harjoitustehtävä 5.1. □

Olkoon A epätyhjä joukko. Joukon $A \times A$ osajoukko on *relaatio* joukossa A .

Relaatio $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : a \equiv b \pmod{m}\}$ on *kongruenssi modulo m* .^a

^aLemman 5.1 nojalla kongruenssi on *ekvivalenssirelaatio*. Tällä kurssilla emme käsittele (ekvivalenssi)relaatioiden yleistä teoriaa.

¹Lause 5.23

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

Lemma 5.3. *Olkoon $m \in \mathbb{N}$, $m \geq 1$ ja olkoot $a, b \in \mathbb{Z}$.*

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

Todistus. (1) Jos $a \equiv b \pmod{m}$, niin $m \mid (b - a)$. Koska lisäksi $d \mid m$, niin Lauseen 1.3(2) nojalla $d \mid (b - a)$, joten $a \equiv b \pmod{d}$.

Kohdat (2) ja (3) seuraavat suoraan kongruenssin määritelmästä.

(4) Jos $a \equiv b \pmod{m}$, 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 $ca \equiv cb \pmod{cm}$. □

Seuraava lause kertoo kongruenssin yhteensopivuudesta yhteenlaskun ja kertolaskun kanssa.

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

- (1) jos $a \equiv b \pmod{n}$ ja $c \equiv d \pmod{n}$, niin $ax + cy \equiv bx + dy \pmod{n}$,
 (2) jos $a \equiv b \pmod{n}$ ja $c \equiv d \pmod{n}$, niin $ac \equiv bd \pmod{n}$,
 (3) jos $a \equiv b \pmod{n}$, niin $a^m \equiv b^m \pmod{n}$ 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 $ax + cy \equiv bx + dy \pmod{n}$.

(2) Lauseen 1.3(3) nojalla n jakaa luvun

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

Siten $ac \equiv bd \pmod{n}$.

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

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

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

Esimerkki 5.6. (1) $3^4 = 81 \equiv 1 \pmod{10}$, joten $3^{400} = (3^4)^{100} \equiv 1^{100} = 1 \pmod{10}$. Siis luvun 3^{400} viimeinen numero desimaaliesityksessä on 1.

(2) Koska $2 \equiv 5 \pmod{3}$, niin Lauseen 5.4 perusteella $2^{100} \equiv 5^{100} \pmod{3}$. Edelleen, Lauseesta 5.4 seuraa, että

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

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

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

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

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

Todistus. Harjoitustehtävä 5.7. □

Kongruenssi ei yleensä ole yhteensopiva jakolaskun kanssa. Esimerkiksi $14 \equiv 8 \pmod{6}$, mutta $7 \not\equiv 4 \pmod{6}$. 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 $ac \equiv bc \pmod{n}$, jos ja vain jos $a \equiv b \pmod{\frac{n}{\text{syt}(n,c)}}$.*

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

$$\frac{n}{\text{syt}(n, c)} \mid \frac{c}{\text{syt}(n, c)}(b - a).$$

Seurauksen 2.10 nojalla

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

Gaussin Lemman² nojalla $\frac{n}{\text{syt}(n, c)} \mid (b - a)$, joten $a \equiv b \pmod{\frac{n}{\text{syt}(n, c)}}$.

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

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

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

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

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

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

²Seuraus 2.14(2)

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

Oletetaan, että $x \equiv y \pmod{\text{pyj}(m_1, m_2, \dots, m_r)}$. Yhteisen tekijän määritelmän nojalla $m_i \mid \text{pyj}(m_1, m_2, \dots, m_r)$ kaikilla $1 \leq i \leq r$. Lemman 5.3(1) nojalla $x \equiv y \pmod{m_i}$ kaikilla $1 \leq i \leq r$. \square

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

Todistus. Väite seuraa Lemman 2.21 nojalla Lauseesta 5.11. \square

Seuraus 5.13. *Olko p_1, p_2, \dots, p_r eri alkulukuja ja olko $x, y \in \mathbb{Z}$. Tällöin $x \equiv y \pmod{p_k}$ kaikilla $1 \leq k \leq r$, jos ja vain jos $x \equiv y \pmod{p_1 p_2 \cdots p_r}$. Erityisesti $p_k \mid x$ kaikilla $1 \leq k \leq r$, jos ja vain jos $p_1 p_2 \cdots p_r \mid x$.*

Todistus. Väite seuraa Lauseesta 5.11, koska $\text{pyj}(p_1, p_2, \dots, p_r) = p_1 p_2 \cdots p_r$. \square

5.2 Jaollisuussääntöjä kongruenssien avulla

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

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

- (1) $(a_s a_{s-1} \dots a_1 a_0)_{10} \equiv (a_1 a_0)_{10} \pmod{4}$.
- (2) $(a_s a_{s-1} \dots a_1 a_0)_{10} \equiv \sum_{k=0}^s a_k \pmod{9}$.
- (3) $(a_s a_{s-1} \dots a_1 a_0)_{10} \equiv \sum_{k=0}^s a_k \pmod{3}$.
- (4) $(a_s a_{s-1} \dots a_1 a_0)_{10} \equiv \sum_{k=0}^s (-1)^k a_k \pmod{11}$.

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

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

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

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

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

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

$$(a_s a_{s-1} \dots a_1 a_0)_{10} = \sum_{k=0}^s a_k 10^k \equiv \sum_{k=0}^s a_k (-1)^k \pmod{11}. \quad \square$$

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. \square

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

Esimerkki 5.15. Olet laskenut käsin kertolaskun

$$267539 \cdot 765927 = 204925343653. \quad (5.1)$$

Laskun mahdollisen virheen voi huomata kongruenssitarkastelun avulla. Koska

$$267539 \equiv 2 + 6 + 7 + 5 + 3 + 9 = 32 \equiv 5 \pmod{9}$$

ja

$$765927 \equiv 7 + 6 + 5 + 9 + 2 + 7 = 36 \equiv 0 \pmod{9},$$

pitäisi Lauseen 5.4((2)) nojalla olla

$$0 = 5 \cdot 0 \equiv 204925343653 \equiv 2 + 0 + 4 + 9 + 2 + 5 + 3 + 4 + 3 + 6 + 5 + 3 = 46 \equiv 1 \pmod{9}.$$

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

$$a + m\mathbb{Z} = \{b \in \mathbb{Z} : a \equiv b \pmod{m}\}.$$

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. \square

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

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

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

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

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

³Oikea tulos on 204915343653.

Todistus. (1) on selvä.

(2) Oletetaan, että $a \equiv b \pmod n$. 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 $a \equiv b \pmod m$.

(3) Jos $(a + m\mathbb{Z}) \cap (b + m\mathbb{Z}) \neq \emptyset$, 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 $a \equiv b \pmod m$. Kohdan (2) nojalla $a + m\mathbb{Z} = b + m\mathbb{Z}$. \square

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

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

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

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

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

5.4 Fermat'n pieni lause

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

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

- (1) *Jos $\text{sy}(a, n) = 1$, niin on $b \in \mathbb{Z}$, jolle $ab \equiv 1 \pmod n$.*
- (2) *Jos $\text{sy}(a, n) > 1$, niin yhtälöllä $ab \equiv 1 \pmod n$ ei ole ratkaisua.*
- (3) *Jos $ab_1 \equiv 1 \pmod n$ ja $ab_2 \equiv 1 \pmod n$, niin $b_1 \equiv b_2 \pmod n$.*

Todistus. (1) Bezout'n yhtälön⁴ nojalla on $b, k \in \mathbb{Z}$, joille pätee $ab + nk = 1$, joten $ab \equiv 1 \pmod n$.

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

(3) Kohdan (2) nojalla $\text{sy}(a, n) = 1$. Seurauksen 5.9 nojalla $b_1 \equiv b_2 \pmod n$. \square

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

⁴Seuraus 2.5

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

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

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

(2) Lemman 5.21 väite ei päde, jos $\text{sy}(a, n) > 1$. 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 $2x \equiv 1 \pmod{6}$ ei ole ratkaisua.

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

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 $ab \equiv 1 \pmod{p}$. Olkoot $1 \leq x, y \leq p$ siten, että $ax \equiv ay \pmod{p}$. Tällöin Lauseen 5.4((2)) nojalla

$$x \equiv bax \equiv bay \equiv y \pmod{p},$$

joten $x = y$. Siis $ax \not\equiv ay \pmod{p}$ kaikilla $1 \leq x < y \leq p$.

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

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

Lauseen 5.4((2)) nojalla

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

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

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

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

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

Fermat'n pienen lauseen nojalla $n \in \mathbb{N}$ ei ole alkuluku, jos esimerkiksi $2^n \not\equiv 2 \pmod{n}$. 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 $2 \leq a \leq n-1$.

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

Huomaa, että Fermat'n pieni lause antaa tiedon $2^{30} \equiv 1 \pmod{31}$ 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* $a \in \{2, 3, \dots, n-1\}$, jos $a^{n-1} \equiv 1 \pmod n$.

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

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

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

Esimerkki 5.27. Yhdistetty luku $561 = 3 \cdot 11 \cdot 17$ on Carmichaelin⁵ luku: Olkoon $a \in \mathbb{Z}$ siten, että $\text{sy}(a, 561) = 1$. Tällöin $3 \nmid a$, $11 \nmid a$ ja $17 \nmid a$. Fermat'n pienen lauseen nojalla $a^2 \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$ ja $a^{16} \equiv 1 \pmod{17}$ Siis

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

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

Carmichaelin lukuja kutsutaan valealkuluvuiksi, koska ne läpäisevät Fermat'n alkulukutestin kaikilla kantaluvuilla, jotka eivät ole niiden kanssa suhteellisia alkulukuja. Alford, Granville ja Pomerance⁶ osoittivat vuonna 1994, että Carmichaelin lukuja on äärettömän monta.

5.5 Wilsonin lause

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

⁵Robert Carmichael (1879-1967).

⁶William Alford (1940-2005), Andrew Granville (1962-), Carl Pomerance (1944-).

Todistus. Jos $x \equiv \pm 1 \pmod{p}$, niin Lauseen 5.4(2) nojalla $x^2 \equiv 1 \pmod{p}$. Osoitetaan, että muita ratkaisuja ei ole. Jos $x^2 \equiv 1 \pmod{p}$, niin $(x-1)(x+1) \equiv 0 \pmod{p}$. Siis $p \mid (x-1)(x+1)$. Eukleideen lemman⁷ nojalla $p \mid (x-1)$ tai $p \mid (x+1)$. Siis $x \equiv 1 \pmod{p}$ tai $x \equiv -1 \pmod{p}$. \square

Ilmeisesti Wilson⁸ arvasi kokeilujen perusteella, että kaikki alkuluvut p toteuttavat kongruenssiyhtälön $(p-1)! \equiv -1 \pmod{p}$. Lagrange⁹ 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 $(n-1)! \equiv -1 \pmod{n}$.*

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

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

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

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

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

Wilsonin lause antaa testin, jolla voidaan todeta, onko jokin luku alkuluku vai ei. Käytännössä yhtälön $(n-1)! \equiv 0 \pmod{n}$ 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,*

$$P(x) = c_0 + c_1x + c_2x^2 + \cdots + c_kx^k, \quad c_0, c_1, \dots, c_k \in \mathbb{Z}.$$

Jos $a \equiv b \pmod{n}$, niin $P(a) \equiv P(b) \pmod{n}$.

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

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

⁷Lemma 3.9

⁸John Wilson (1741-1793).

⁹Joseph-Louis Lagrange (1736-1813).

Jos kokonaislukukertoimisella polynomilla $P(x)$ on juuri $a \in \mathbb{Z}$, niin $P(a) \equiv 0 \pmod n$ 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 $P(x) \equiv 0 \pmod n$ ei ole kokonaislukuratkaisua, niin polynomilla P ei ole juuria. \square

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

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

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 $P(x) = a_n x^n + \dots + a_1 x + a_0$, $n \in \mathbb{N}$, $a_n \neq 0$, 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 $b \equiv k \pmod q$, niin Lauseen 5.31 nojalla $P(b) \equiv P(k) \pmod q$. Koska $P(k) = q \equiv 0 \pmod q$, 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 $*$: $A \times A \rightarrow A$ 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* .

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

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.

¹⁰Katso esimerkiksi [Par, Lause 6.20].

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 .

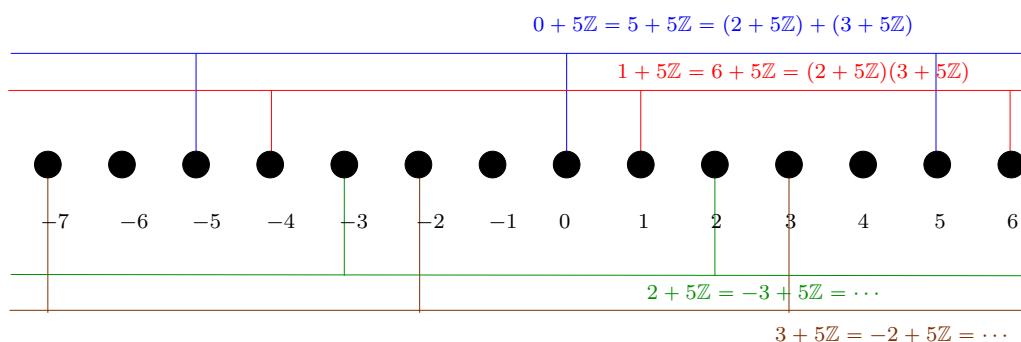
Lemma 5.36. *Kongruenssiluokkien yhteenlasku on hyvin määritelty.*

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

Kongruenssiluokkien kertolaskun tuloksen riippumattomuus kongruenssiluokkien edustajista todistetaan samalla tavalla.

Esimerkki 5.37. Esimerkkejä kongruenssiluokkien 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 $p \geq 5$ alkuluku. Osoita, että $p \equiv \pm 1 \pmod{6}$.
- 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 $2^{32} \equiv -1 \pmod{641}$.

5.7. Todista Lemma 5.7.

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

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

5.10. Osoita, että

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

5.11. Todista Lemma 5.16.

5.12. Osoita, että $4 \mid (a_s a_{s-1} \dots a_1 a_0)_{10}$, 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, \dots ¹¹.

(2) p jakaa äärettömän monta luvuista 11, 111, 1111, 11111, \dots 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, \dots, p_n eri alkulukuja, $n \geq 2$, ja olkoon $m = p_1 p_2 \dots p_n$. Oletetaan, että $(p_k - 1) \mid (m - 1)$ kaikilla $1 \leq k \leq n$. 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.

Olkoon $n \in \mathbb{N} - \{0, 1\}$. Luku $0 \leq r \leq n - 1$ on *neliönjäännös* mod n , jos $r \equiv x^2 \pmod{n}$ jollain $x \in \mathbb{Z}$.

5.20. Olkoot $a, b \in \mathbb{Z}$ parittomia lukuja. Osoita, että $a^2 + b^2 \neq c^2$ kaikilla $c \in \mathbb{Z}$.¹³

5.21. Olkoot $a, b \in \mathbb{Z}$, $a \not\equiv 0 \pmod{3}$ ja $b \not\equiv 0 \pmod{3}$. Osoita, että $a^2 + b^2 \neq c^2$ kaikilla $c \in \mathbb{Z}$.

5.22. Määritä neliönjäännökset mod 10.¹⁴

5.23. Olkoon $n \in \mathbb{Z}$. Osoita, että $30 \mid n^5 - n$.¹⁵

5.24. Määritä neliönjäännökset mod 8.

¹¹Esimerkki 5.24

¹²Olisiko kohdan (1) tuloksesta hyötyä?

¹³Tarkastele kysymystä mod 4.

¹⁴Jos $x, y \in \mathbb{Z}$, $x \equiv y \pmod{n}$, niin Lauseen 5.4 nojalla $x^2 \equiv y^2 \pmod{n}$.

¹⁵Vihje: $30 = 2 \cdot 3 \cdot 5$ ja Seuraus 5.13.

5.25. Olkoot $x, y, z \in \mathbb{Z}$.

(1) Osoita, että $x^2 + y^2 + z^2 \not\equiv 7 \pmod{8}$.

(2) Olkoot $x, y, z \in \mathbb{Z}$ siten, että $4 \mid x^2 + y^2 + z^2$. Osoita, että $x \equiv y \equiv z \equiv 0 \pmod{2}$.

5.26. 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.¹⁶

5.27. Olkoon $n \in \mathbb{Z}$. Osoita, että $42 \mid n^7 - n$.¹⁷

¹⁶Harjoitustehtävä 5.25 ja induktio.

¹⁷Vihje: $30 = 2 \cdot 3 \cdot 7$ ja Seuraus 5.13.

Luku 6

Lineaariset kongruenssiyhtälöt

Lemman 5.20 todistuksessa osoitimme, että lineaarisella kongruenssiyhtälöllä $ax \equiv 1 \pmod{n}$ on ratkaisu, jos $\text{sy}(a, n) = 1$. 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

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

on (yhden muuttujan) lineaarisen kongruenssiyhtälön $ax \equiv b \pmod{n}$ ratkaisu.

Jos $x \in \mathbb{Z}$ ja $y \in \mathbb{Z}$ ovat yhtälön (6.1) ratkaisuja ja $x \equiv y \pmod{n}$, niin ne ovat yhtälön sama ratkaisu \pmod{n} .

Kokonaisluku x on kongruenssiyhtälön $ax \equiv b \pmod{n}$ 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 $2x \equiv 6 \pmod{12}$ ratkaisuja. Koska $15 \equiv 3 \pmod{12}$, niin se 3 ja 15 ovat kongruenssimielessä sama ratkaisu $\pmod{12}$.

(2) Kongruenssiyhtälöllä $2x \equiv 3 \pmod{4}$ 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 kongruenssiyhtälön $ax \equiv b \pmod{n}$ kaikki luvut ovat lineaarisen kongruenssiyhtälön (6.1) ratkaisuja tai mikään luvuista $x \in c + n\mathbb{Z}$ ei ole ratkaisu.

Todistus. Jos $x \equiv y \pmod{n}$, niin Lemman 5.4(1) nojalla $ax \equiv ay$. \square

Koska jokaisen luvun $x \in \mathbb{Z}$ jakojäännökselle r modulo n pätee $x \equiv r \pmod{n}$, niin haettaessa ratkaisua yhtälöön (6.1) riittää Lemman (6.2) perusteella tutkia luvut $0, 1, \dots, n-1$. 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 ratkaisuisia voidaan käyttää myös toisenlaista sanastoa:

Kongruenssiluokka $c + n\mathbb{Z}$ on kongruenssiyhtälön $ax \equiv b \pmod{n}$ ratkaisu, jos $ay \equiv b \pmod{n}$ 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 $2x \equiv 6 \pmod{12}$ ratkaisuja.

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

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

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

$$x \equiv x_0 + i \frac{n}{\text{syt}(a, n)} \pmod{n}, \quad i = 0, 1, \dots, \text{syt}(a, n) - 1. \quad (6.2)$$

Todistus. (1) Lauseen 2.7 mukaan yhtälöllä

$$b = ax + ny,$$

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

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

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

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

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

Siten $x_0 \equiv \frac{bk_0}{\text{syt}(a, n)} \pmod{n}$ on kongruenssiyhtälön $ax \equiv b \pmod{n}$ ratkaisu.

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

$$a \left(x_0 + j \frac{n}{\text{syt}(a, n)} \right) = ax_0 + j \frac{a}{\text{syt}(a, n)} n \equiv ax_0 \equiv b \pmod{n}.$$

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

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 $y_0 = \frac{b\ell_0}{\text{syt}(a,n)}$, niin yhtälön (6.3) nojalla

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

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

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

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

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

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

Todistus. Lause 6.4. □

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

$$7x + 12y = 1. \quad (6.4)$$

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 $7x \equiv 3 \pmod{12}$ ainoa ratkaisu on $x \equiv 3 \cdot (-5) = -15 \equiv 9 \pmod{12}$.

(2) Koska $\text{syt}(10, 12) = 2$ ja $2 \mid 6$, niin Lauseen 6.4 nojalla yhtälöllä $10x \equiv 6 \pmod{12}$ 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 $x_1 \equiv x_0 + \frac{12}{2} \pmod{12}$ eli $x_1 \equiv 3 \pmod{12}$.

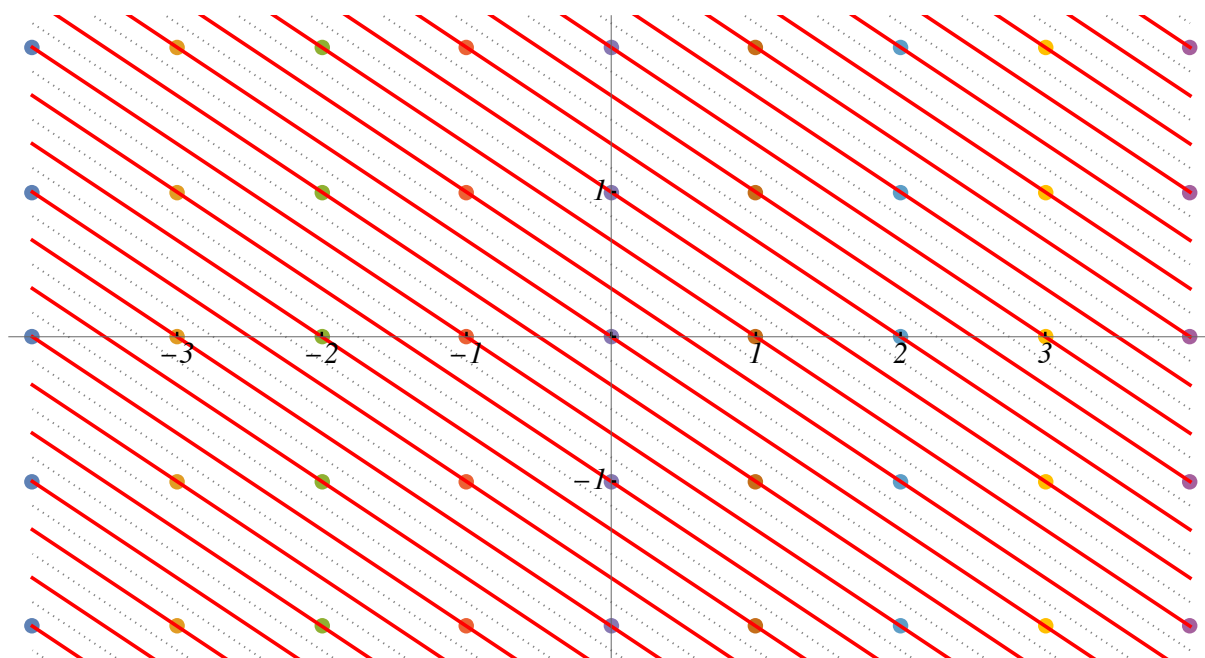
Lauseen 6.4 todistuksessa todistimme myös seuraavan tuloksen, joka täydentää Seurausten 2.11 tuloksen lineaaristen Diofantoksen yhtälöiden ratkaisuihin.

Seuraus 6.7. Olkoot $(a, b) \in \mathbb{Z}^2 - \{(0, 0)\}$ ja $c \in \mathbb{Z}$. Lineaarilla Diofantoksen yhtälöllä $ax + by = c$ on ratkaisu $(x, y) \in \mathbb{Z}^2$, jos ja vain jos $\text{syt}(a, b) \mid c$. Jos (x_0, y_0) on yhtälön ratkaisu, niin kaikki ratkaisut saadaan kaavalla

$$(x, y) = \left(x_0 + i \frac{b}{\text{syt}(a, b)}, y_0 - i \frac{a}{\text{syt}(a, b)} \right), \quad i \in \mathbb{Z}. \quad \square$$

Esimerkki 6.8. (1) Esimerkin 6.6 ja Seurausten 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) Lineaarilla Diofantoksen yhtälöllä $4x + 6y = c$ on ratkaisuja täsmälleen silloin, kun c on parillinen. Jos $4x_0 + 6y_0 = c$, niin Seurausten 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

$$\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases} . \quad (6.5)$$

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 $2 + 3k \equiv 3 \pmod{5}$, joka on yhtäpitävä yhtälön $3k \equiv 1 \pmod{5}$ 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

$$\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5} \end{cases} \quad (6.6)$$

ratkaisuja kaikilla $\ell \in \mathbb{Z}$. Kun tämä ratkaisu sijoitetaan kolmanteen yhtälöön, päädytään yhtälöön $8 + 15\ell \equiv 2 \pmod{7}$, joka on yhtäpitävä yhtälön $\ell \equiv 15\ell \equiv -6 \equiv 1 \pmod{7}$ 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

$$\begin{cases} x \equiv 3 \pmod{9} \\ x \equiv 2 \pmod{6} \end{cases}$$

ei ole ratkaisua. Jos $x \equiv 3 \pmod{9}$, niin $3 \mid (3 - x)$ ja siten 3 jakaa luvun x . Jos $x \equiv 2 \pmod{6}$, 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 tunnetaan nimellä *kiinalainen jäännöslause*.

Lause 6.10 (Kiinalainen jäännöslause). *Olkoon $k \in \mathbb{N}$. Olkoot $n_1, \dots, n_k \in \mathbb{N} - \{0, 1\}$ ja $b_1, \dots, b_k \in \mathbb{Z}$. Jos $\text{sy}(n_i, n_j) = 1$ aina, kun $i \neq j$, niin kongruenssiyhtälöryhmällä*

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \vdots \\ x \equiv b_k \pmod{n_k} \end{cases} \quad (6.7)$$

on yksikäsitteinen ratkaisu modulo $n = n_1 \cdots n_k$.

Todistus. Olkoon

$$c_i = \frac{n}{n_i}, \quad i = 1, 2, \dots, k.$$

Koska $\text{sy}(n_i, n_j) = 1$ aina, kun $i \neq j$, niin Lauseen 2.15 tai Lauseen 3.14 ja induktion avulla näemme, että $\text{sy}(c_i, n_i) = 1$ kaikilla $i = 1, 2, \dots, k$. Seurauksen 6.5 perusteella yhtälöllä

$$c_i x \equiv 1 \pmod{n_i}$$

on yksikäsitteinen ratkaisu $d_i \pmod{n_i}$.

Olkoon

$$x_0 = b_1 c_1 d_1 + b_2 c_2 d_2 + \cdots + b_k c_k d_k. \quad (6.8)$$

Jos $i \neq j$, niin $n_i \mid c_j$ ja siten $b_j c_j d_j \equiv 0 \pmod{n_i}$. Luvun x_0 määritelmän mukaan on siis $x_0 \equiv b_i c_i d_i \equiv b_i \pmod{n_i}$. Siis x_0 on kaikkien ryhmän kongruenssiyhtälöiden ratkaisu modulo n .

Näytetään seuraavaksi, että muita ratkaisuja ei ole. Olkoon $x \in \mathbb{Z}$ yhtälöryhmän ratkaisu. Koska tällöin $x \equiv b_i \pmod{n_i}$ ja $x_0 \equiv b_i \pmod{n_i}$, niin $x_0 \equiv x \pmod{n_i}$ ja siten $n_i \mid (x - x_0)$ kaikilla $i = 1, 2, \dots, k$. Koska $\text{sy}(n_i, n_j) = 1$, niin Seurauksen 2.14 perusteella luku $n = n_1 \cdots n_k$ jakaa luvun $x - x_0$ eli $x \equiv x_0 \pmod{n}$. Siis x_0 on ainoa ratkaisu modulo n . \square

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 $c_3 = 15$.

¹Sun Zi eli ilmeisesti 400-luvulla.

Yhtälön $35x \equiv 2x \equiv 1 \pmod{3}$ ratkaisu on $d_1 \equiv 2 \pmod{3}$. Yhtälön $21x \equiv x \equiv 1 \pmod{5}$ ratkaisu on $d_2 \equiv 1 \pmod{5}$. Yhtälön $15x \equiv x \equiv 1 \pmod{7}$ ratkaisu on $d_3 \equiv 1 \pmod{7}$. Kaavan (6.8) mukaan ratkaisuksi saadaan

$$x_0 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}.$$

6.3 Eulerin funktio

Suhteellisten alkulukujen tarkastelusta päätyy luontevasti tärkeän lukuteoreettisen funktion määritelmään:

Kuvaus $\phi: \mathbb{N} - \{0\} \rightarrow \mathbb{N}$,

$$\phi(n) = \#\{1 \leq k \leq n : \text{syt}(k, n) = 1\}$$

on Eulerin ϕ -funktio.

Eulerin funktion avulla voimme muotoilla Eulerin yleistyksen Fermat'n pienelle lauseelle.² Todistuksen idea on sama. Olkoon

$$\mathcal{R}(n) = \{1 \leq k \leq n : \text{syt}(k, n) = 1\}$$

luvun $n \in \mathbb{N} - \{0\}$ kanssa jaottomien positiivisten luonnollisten lukujen joukko. Määritelmän nojalla siis $\phi(n) = \#\mathcal{R}(n)$.

Lause 6.12. *Olkoot $a, n \in \mathbb{N} - \{0\}$ siten, että $\text{syt}(a, n) = 1$. Tällöin $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Todistus. Olkoon $\mathcal{R}(n) = \{b_1, b_2, \dots, b_{\phi(n)}\}$. Kuten Fermat'n lauseen todistuksessa näemme Lauseen 6.4(2) nojalla, että jokaiselle b_k , $1 \leq k \leq \phi(n)$, on $1 \leq x_k \leq n - 1$, jolle $ab_k \equiv x_k \pmod{n}$ ja että $x_i \neq x_j$, jos $i \neq j$. Lauseen 2.15 nojalla $x_k \in \mathcal{R}(n)$ jokaisella $1 \leq k \leq \phi(n)$, joten $\{x_1, x_2, \dots, x_{\phi(n)}\} = \mathcal{R}(n)$.

Lauseen 5.4((2)) nojalla

$$a^{\phi(n)} b_1 b_2 \cdots b_{\phi(n)} = ab_1 \cdot ab_2 \cdots ab_{\phi(n)} \equiv b_1 b_2 \cdots b_{\phi(n)} \pmod{n},$$

joten väite seuraa Seurauksen 5.9 nojalla □

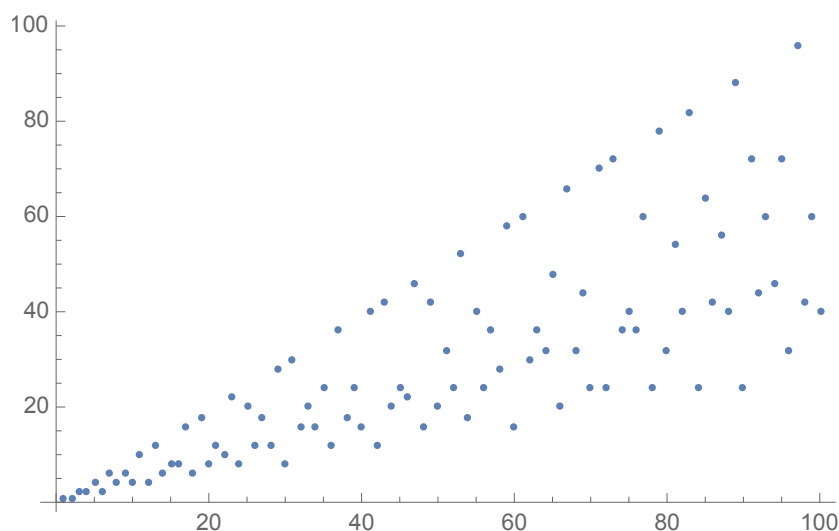
Seuraava taulukko ja Kuva 6.2 näyttävät, että Eulerin funktion arvot vaihtelevat melko paljon peräkkäisillä luvuilla.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	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

Kuitenkin Eulerin funktion käyttäytymisessä näyttää olevan jotain säännönmukaisuuksia, sillä esimerkiksi

$$\begin{aligned} \phi(15) &= 8 = \phi(3)\phi(5) = 2 \cdot 4 = 8 \quad \text{ja} \\ \phi(18) &= 6 = \phi(2)\phi(9) \neq \phi(3)\phi(6). \end{aligned}$$

²Lause 5.23



Kuva 6.2 — Eulerin ϕ -funktion arvot $\phi(n)$, kun $1 \leq n \leq 100$.

Funktio $f: \mathbb{N} - \{0\} \rightarrow \mathbb{Z}$ (tai $f: \mathbb{N} \rightarrow \mathbb{Z}$) on *multiplikatiivinen funktio*, jos

$$f(mn) = f(m)f(n)$$

kaikille $m, n \in \mathbb{N}$, joille $\text{syt}(m, n) = 1$.

Lause 6.13. Eulerin ϕ -funktio on multiplikatiivinen funktio.

Todistus. Olkoot $m_1, m_2 \in \mathbb{N} - \{0\}$ siten, että $\text{syt}(m_1 m_2) = 1$. Olkoon $x \in \mathcal{R}(m_1 m_2)$. Määritelmän nojalla $1 \leq x \leq m_1 m_2$ ja $\text{syt}(x, m_1 m_2) = 1$. Tällöin

$$\text{syt}(x, m_1) = 1 = \text{syt}(x, m_2),$$

koska lukujen m_1 ja m_2 tekijät ovat luvun $m_1 m_2$ tekijöitä. Jakoyhtälön³ nojalla on luvut $0 \leq r_1 \leq m_1 - 1$ ja $0 \leq r_2 \leq m_2 - 1$ siten, että $r_1 \equiv x \pmod{m_1}$ ja $r_2 \equiv x \pmod{m_2}$. Lemman 5.7 nojalla

$$\text{syt}(r_1, m_1) = \text{syt}(x, m_1) = 1 = \text{syt}(x, m_2) = \text{syt}(r_2, m_2),$$

joten $r_1 \in \mathcal{R}(m_1)$ ja $r_2 \in \mathcal{R}(m_2)$. Siis kuvaus $F: \mathcal{R}(m_1 m_2) \rightarrow \mathcal{R}(m_1) \times \mathcal{R}(m_2)$,

$$F(x) = (r_1, r_2),$$

on hyvin määritelty.

Olkoot $r_1 \in \mathcal{R}(m_1)$ ja $r_2 \in \mathcal{R}(m_2)$. Kiinalaisen jäännöslauseen nojalla on yksikäsitteinen $1 \leq x \leq m_1 m_2$, jolle $x \equiv r_1 \pmod{m_1}$ ja $x \equiv r_2 \pmod{m_2}$. Lemman 5.7 nojalla

$$\text{syt}(x, m_1) = \text{syt}(r_1, m_1) = 1 = \text{syt}(r_2, m_2) = \text{syt}(x, m_2).$$

Lauseen 2.15 nojalla $\text{syt}(x, m_1 m_2) = 1$. Nyt siis $F(x) = (r_1, r_2)$, joten F on bijektio. Siis

$$\begin{aligned} \phi(m_1 m_2) &= \#\mathcal{R}(m_1 m_2) = \#F(\mathcal{R}(m_1 m_2)) = \#(\mathcal{R}_1 \times \mathcal{R}_2) = \#\mathcal{R}(m_1) \#\mathcal{R}(m_2) \\ &= \phi(m_1)\phi(m_2). \end{aligned}$$

□

³Lause 1.6

Lemma 6.14. *Olkoon p on alkuluku. Tällöin $\phi(p^k) = p^{k-1}(p-1)$ kaikille $k \in \mathbb{N} - \{0\}$.*

Todistus. Harjoitustehtävä 6.9. □

Olkoon $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ luvun $n \in \mathbb{N} - \{0, 1\}$ alkutekijäesitys. Olkoon $f: \mathbb{N} \rightarrow \mathbb{R}$. Tällöin käytetään merkintää

$$\prod_{p|n} f(p) = f(p_1)f(p_2) \cdots f(p_k).$$

Lause 6.15. *Olkoon $n \in \mathbb{N} - \{0, 1\}$. Tällöin*

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Todistus. Olkoon $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Lauseen 6.13 ja Lemman 6.14 nojalla

$$\begin{aligned} \phi(n) &= \phi(p_1^{e_1}) \phi(p_2^{e_2}) \cdots \phi(p_k^{e_k}) \\ &= p_1^{e_1-1}(p_1-1) p_2^{e_2-1}(p_2-1) \cdots p_k^{e_k-1}(p_k-1) \\ &= p_1^{e_1} \left(1 - \frac{1}{p_1}\right) p_2^{e_2} \left(1 - \frac{1}{p_2}\right) \cdots p_k^{e_k} \left(1 - \frac{1}{p_k}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right). \end{aligned} \quad \square$$

Esimerkki 6.16. Koska $\text{sy}(3, 10) = 1$ ja $\phi(10) = 4$, voimme selvittää luvun 3^{1000} viimeisen desimaalin Lauseen 6.12 avulla:

$$3^{1000} = 3^{250\phi(10)} = (3^{\phi(10)})^{250} \equiv 1^{250} = 1 \pmod{10}.$$

Siis viimeinen luku desimaaliesityksessä on 1.

Lause 6.17. *Olkoon $n \in \mathbb{N} - \{0\}$. Tällöin $\sum_{d|n} \phi(d) = n$.*

Todistus. Olkoon

$$\mathcal{S}_\delta = \{1 \leq a \leq n : \text{sy}(a, n) = \delta\}$$

jokaiselle luvun n tekijälle δ . Seurauksen 2.10 nojalla $a \in \mathcal{S}_\delta$, jos ja vain jos δ on lukujen a ja n yhteinen tekijä ja $\text{sy}\left(\frac{a}{\delta}, \frac{n}{\delta}\right) = 1$. Siis $\#\mathcal{S}_\delta = \phi\left(\frac{n}{\delta}\right)$. Koska joukot \mathcal{S}_δ ovat erillisiä ja

$$\bigcup_{\delta|n} \mathcal{S}_\delta = \{1 \leq b \leq n : b \in \mathbb{N}\},$$

saamme

$$n = \sum_{\delta|n} \phi\left(\frac{n}{\delta}\right) = \sum_{d|n} \phi(d),$$

sillä $\left\{\frac{n}{\delta} : \delta \in \mathbb{N}, \delta | n\right\} = \{d \in \mathbb{N} : d | n\}$. □

Harjoitustehtäviä

6.1. Ratkaise lineaarinen kongruenssiyhtälö $3x \equiv 5 \pmod{11}$.

6.2. Ratkaise lineaariset kongruenssiyhtälöt

(a) $5x \equiv 2 \pmod{7}$,

(b) $4x \equiv 5 \pmod{6}$.

6.3. Ratkaise lineaarinen kongruenssiyhtälö $12x \equiv 9 \pmod{15}$.

6.4. Ratkaise lineaarinen kongruenssiyhtälö $240x \equiv 21 \pmod{561}$.

6.5. Ratkaise lineaarinen Diofantoksen yhtälö $6x + 21y = 15$. Etsi kaikki ratkaisut.

6.6. Ratkaise lineaarinen kongruenssiyhtälöpari

$$\begin{cases} x \equiv 3 \pmod{7}, \\ x \equiv 5 \pmod{9} \end{cases}$$

6.7. Ratkaise lineaarinen kongruenssiyhtälöryhmä

$$\begin{cases} x \equiv 0 \pmod{3}, \\ x \equiv 1 \pmod{4} \\ x \equiv 5 \pmod{7} \end{cases}$$

6.8. Ratkaise lineaarinen kongruenssiyhtälöryhmä

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 2 \pmod{17} \\ x \equiv 7 \pmod{25} \end{cases}$$

6.9. Todista Lemma 6.14.

6.10. Määritä $\phi(1000)$ ja $\phi(2343)$.

6.11. Määritä $\phi(75141)$.

6.12. Mitkä ovat luvun 3^{400} desimaaliesityksen kaksi viimeistä numeroa?

6.13. Olkoot $m, n \in \mathbb{N}$ ja olkoon $s = \prod_{p|m \text{ ja } p|n} p$. Osoita, että

$$\phi(mn) = s \frac{\phi(m)\phi(n)}{\phi(s)}.$$

6.14. Olkoot $m, n \in \mathbb{N} - \{0, 1\}$ siten, että $\phi(mn) = \phi(n)$. Osoita, että $m = 2$ ja n on pariton.

6.15. Ratkaise lineaarinen kongruenssiyhtälöryhmä

$$\begin{cases} x \equiv 3 \pmod{13} \\ x \equiv 7 \pmod{20} \end{cases}$$

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.
- [JJ] G. A. Jones and J. M. Jones. *Elementary number theory*. Springer Undergraduate Mathematics Series. Springer-Verlag London, Ltd., London, 1998.
- [Lan] 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.
- [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.
- [Par] J. Parkkonen. Algebra. <http://users.jyu.fi/~parkkone/Algebra2021/Algebra2021R.pdf>, 2021.