Lukuteorian alkeita

Pentti Haukkanen

9/2025

Muokannut Inkeri Hanhela

Sisällys

Esipuhe

Tämän monisteen ensimmäinen versio on peräisin viime vuosituhannelta, jolloin Pentti Haukkanen luennoi algebran aineopintojen kurssia. Kurssin aiheina olivat lukuteorian, ryhmäteorian ja rengasteorian alkeet. Tämä moniste rajoittuu lukuteorian osuuteen. Se oli alun perin luentorunko, jota täydennettiin luennoilla esimerkeillä, avoimiksi jätettyjen tehtävien ratkaisuilla sekä todistuksilla, jotka oli monisteessa ohitettu.

Moniste ei perustu suoraan mihinkään yksittäiseen lähteeseen, vaan se heijastelee Pentti Haukkasen näkemystä lukuteorian perusteista. On hyvä huomata, että mukana ei ole niitä lukuteorian aiheita, jotka aikanaan kuuluivat ryhmä- ja rengasteorian osuuksiin. Vaikka ne olisivatkin tärkeä osa lukuteoriaa, niiden jättäminen pois tekee tästä monisteesta saavutettavamman: lukijalta ei edellytetä muuta kuin matemaattisen päättelyn perusteiden hallintaa.

Monisteen nykyinen versio on syntynyt, kun Inkeri Hanhela on osin Ari Virtasen ohjauksessa lisännyt puuttuvia todistuksia ja ratkaissut tehtäviä, jotka alkuperäisessä versiossa oli jätetty lukijan tehtäväksi.

1 Lukuteoriaa

Lukuteoria on karkeasti sanottuna matematiikan osa-alue, joka käsittelee kokonaislukujen ominaisuuksia. Tässä monisteessa paneudutaan varsinkin jaollisuuden problematiikkaan.

Kokonaislukujen joukkoa merkitsemme symbolilla $\mathbb{Z}$. Kaikki luvut ovat kokonaislukuja ellei toisin mainita.

1.1 Jaollisuus

Määritelmä 1.1.1. Luku a on luvun b *tekijä* (eli luku b on *jaollinen* luvulla a eli luku a jakaa luvun b), jos on olemassa sellainen $c \in \mathbb{Z}$, että $b = ac$.

Merkintä. Jos luku a on luvun b tekijä, niin merkitään $a \mid b$. Muussa tapauksessa $a \nmid b$.

Esimerkki 1.1.1. Koska $6 = 3 \cdot 2$, niin $3 \mid 6$. Koska yhtälö $7 = 3c$ ei ratkea millään kokonaisluvulla c, niin $3 \nmid 7$. Luvun 6 tekijöiksi löytyvät helposti luvut $1, 2, 3$ ja 6, ja koska esimerkiksi $6 = (-1) \cdot (-6)$, niin myös luvut $-1, -2, -3$ ja -6 ovat luvun 6 tekijöitä. Luvun -7 kaikki tekijät ovat $1, 7, -1$ ja -7.

Esimerkki 1.1.2. Olkoon n pariton kokonaisluku. Tiedetään, että

$$\sum_{i=1}^{n} i = n\left(\frac{n+1}{2}\right).$$

Koska n on pariton, niin $n + 1$ on parillinen, joten $\frac{n+1}{2}$ on kokonaisluku. Täten

$$n \mid \sum_{i=1}^{n} i,$$

kun n on pariton.

Esimerkki 1.1.3. Koska $0 = a \cdot 0$ kaikilla $a \in \mathbb{Z}$, niin $a \mid 0$ aina, kun $a \in \mathbb{Z}$. Koska $a = 1 \cdot a$ kaikilla $a \in \mathbb{Z}$, niin $1 \mid a$ aina, kun $a \in \mathbb{Z}$.

Lause 1.1.1. *Oletetaan, että $a, b, c \in \mathbb{Z}$. Silloin*

1) $a \mid b,\ a \mid c \Rightarrow a \mid b + c$,

2) $a \mid b,\ a \mid c \Rightarrow a \mid b - c$,

3) $a \mid b,\ c \mid d \Rightarrow ac \mid bd$,

4) $a \mid b \Rightarrow a \mid bd$.

Todistus.

1) Oletetaan, että $a \mid b$ ja $a \mid c$. Tällöin määritelmän 1.1.1 mukaan $b = ak$ ja $c = al$ joillakin $k, l \in \mathbb{Z}$. Näin ollen $b + c = ak + al = a(k + l)$, joten $a \mid b + c$.

2) Samoin oletuksin kuin kohdassa 1 saadaan $b - c = ak - al = a(k - l)$, joten $a \mid b - c$.

3) Oletetaan, että $a \mid b$ ja $c \mid d$. Tällöin $b = ak$ ja $d = cl$ joillakin $k, l \in \mathbb{Z}$. Näin ollen $bd = (ak)(cl) = (ac)(kl)$, joten $ac \mid bd$.

4) Oletetaan, että $a \mid b$. Tällöin $b = ak$ jollakin $k \in \mathbb{Z}$. Näin ollen $bd = (ak)d = a(kd)$, joten $a \mid bd$.

□

Lause 1.1.2. *Oletetaan, että $a, b, c \in \mathbb{Z}_+$. Silloin*

1) $a \mid a$ *(refleksiivisyys),*

2) $a \mid b, b \mid a \Rightarrow a = b$ *(antisymmetrisyys),*

3) $a \mid b, b \mid c \Rightarrow a \mid c$ *(transitiivisuus).*

Todistus.

1) Koska $a = a \cdot 1$, niin $a \mid a$.

2) Oletetaan, että $a \mid b$ ja $b \mid a$. Tällöin $b = ak$ ja $a = bl$ joillakin $k, l \in \mathbb{Z}_+$. Näin ollen $a = bl = akl$, joten täytyy olla $kl = 1$. Koska kyseessä ovat positiiviset kokonaisluvut, täytyy olla $k = l = 1$. Tästä seuraa, että $b = a \cdot 1$ ja $a = b \cdot 1$, joten $a = b$.

3) Oletetaan, että $a \mid b$ ja $b \mid c$. Tällöin $b = ak$ ja $c = bl$ joillakin $k, l \in \mathbb{Z}_+$. Näin ollen $c = bl = akl$, joten $a \mid c$.

□

Huomautus. Lauseen 1.1.2 mukaan jaollisuusrelaatio | on osittainen järjestysrelaatio joukossa $\mathbb{Z}_+$.

Huomautus. Lauseen 1.1.2 kaavaa 2 voi käyttää lukuteoreettisten yhtälöiden todistamiseen. (Vrt. joukko-opissa $A = B \Leftrightarrow A \subseteq B, B \subseteq A$ ja logiikassa $(p \Leftrightarrow q) \Leftrightarrow (p \Rightarrow q, q \Rightarrow p)$.

Esimerkki 1.1.4. Todistetaan, että

1) $a \mid b, a \mid c \Rightarrow a \mid xb + yc$ aina, kun $x, y \in \mathbb{Z}$,

   Oletetaan, että $a \mid b$ ja $a \mid c$. Lauseen 1.1.1 kohdan 4 mukaan tällöin $a \mid xb$ ja $a \mid yc$ kaikilla $x, y \in \mathbb{Z}$, ja saman lauseen kohdan 1 nojalla tästä seuraa, että $a \mid xb + yc$.

2) $a \mid b, c \mid d \nRightarrow a + c \mid b + d$,

   Osoitetaan vastaesimerkillä, että $a \mid b, c \mid d \Rightarrow a + c \mid b + d$ ei aina päde. Valitaan $a = 2, b = 4, c = 3, d = 9$. Tällöin $2 \mid 4$ ja $3 \mid 9$, mutta $5 \nmid 13$.

3) $a \mid b, a \nmid c \Rightarrow a \nmid b + c$,

   Oletetaan, että $a \mid b$ ja $a \nmid c$. Todistetaan, että $a \nmid b + c$. Tehdään vastaoletus, että $a \mid b + c$. Silloin lauseen 1.1.1 kohdan 2 perusteella $a \mid ((b + c) - b)$ eli $a \mid c$, joka on ristiriita. Siten vastaoletus on väärin ja väite oikein.

4) $a \mid (-a)$.

   Väite seuraa suoraan siitä, että $-a = a \cdot (-1)$.

1.2 Suurin yhteinen tekijä

Määritelmä 1.2.1. Olkoot a ja b kokonaislukuja, joista ainakin toinen on nollasta eroava. Silloin c on lukujen a ja b *suurin yhteinen tekijä*, jos

1) $c \mid a, c \mid b$ ja

2) $d \mid a, d \mid b \Rightarrow d \leq c$.

Merkintä. Lukujen a ja b suurinta yhteistä tekijää merkitään symbolilla (a, b), $\text{syt}(a, b)$ tai $\gcd(a, b)$. Huom. $(a, b) = (b, a)$.

Palautetaan mieleen hyvinjärjestysperiaate, jota tarvitaan myöhemmissä todistuksissa.

Hyvinjärjestysperiaate. Jokainen luonnollisten lukujen epätyhjä osajoukko sisältää pienimmän alkion.

Huomautus. Hyvinjärjestysperiaatteen pienin alkio on yksikäsitteinen. Tämän todistamiseksi oletetaan, että S on hyvinjärjestetty joukko ja että $s_1 \in S$ ja $s_2 \in S$ ovat kumpikin joukon S pienimpiä alkioita. Tällöin $s_1 \leq s$ aina, kun $s \in S$, ja $s_2 \leq s$ aina, kun $s \in S$. Näin ollen, erityisesti $s_1 \leq s_2$ ja $s_2 \leq s_1$, joten antisymmetrisyyden nojalla $s_1 = s_2$. Siis joukon S pienin alkio on yksikäsitteinen.

Lause 1.2.1. *Olkoot a ja b kokonaislukuja, joista ainakin toinen on nollasta eroava. Silloin (a, b) on aina olemassa ja yksikäsitteinen.*

Lauseen 1.2.1 todistamiseksi tarvitsemme ensin seuraavan lemman.

Lemma 1.2.1. Olkoon S luonnollisten lukujen epätyhjä joukko, joka on ylhäältä rajoitettu. Tällöin joukossa S on suurin alkio, joka on yksikäsitteinen.

Todistus. Olkoon S sellainen epätyhjä luonnollisten lukujen osajoukko, jonka kaikki alkiot ovat pienempiä kuin jokin $M \in \mathbb{Z}_+$, eli S on ylhäältä luvun M rajoittama. Määritellään $S' = \{M - s \mid s \in S\}$. Myös S' on luonnollisten lukujen epätyhjä osajoukko, joten hyvinjärjestysperiaatteen mukaan se sisältää pienimmän alkion a. Siis on olemassa alkio $s \in S$ siten, että $a = M - s$ eli yhtäpitävästi $s = M - a$. Tämä s on joukon S suurin alkio, sillä jos jokin s' olisi joukon S alkio ja $s' > s$, niin $M - s' < a$, mikä tarkoittaisi, että a ei olisi joukon S' pienin alkio.

Lisäksi osoitetaan suurimman alkion yksikäsitteisyys. Oletetaan, että s_1 ja s_2 ovat kumpikin joukon S suurimpia alkioita. Tällöin $s_2 \leq s_1$ ja $s_1 \leq s_2$, joten antisymmetrisyyden nojalla $s_1 = s_2$. Siis suurin alkio on yksikäsitteinen. □

Lauseen 1.2.1 todistus. Olkoot a ja b kokonaislukuja, joista ainakin toinen on nollasta eroava. Tarkastellaan joukkoa $S = \{d \in \mathbb{Z}_+ : d \mid a, d \mid b\}$. Koska $1 \in S$, niin $S \neq \emptyset$. Joukko S on ylhäältä luvun $|a|$ (samoin kuin luvun $|b|$) rajoittama. Lemman 1.2.1 nojalla joukossa S on suurin alkio, ja se on yksikäsitteinen. Tämä alkio on (a, b). □

Huomautus. Syt:n määritelmän mukaan $(a, b) \mid a$ ja $(a, b) \mid b$. Tämän ja lauseen 1.1.2 kohdan 3 perusteella $c \mid (a, b) \Rightarrow c \mid a, c \mid b$. (Lauseen 1.3.5 (s. 12) seurauksen 1 mukaan edellinen kaava on voimassa käänteisestikin.)

Esimerkki 1.2.1. On helppo todeta, että $(6, 9) = 3$. Etsitään $(6, 16)$. Luvun 6 positiiviset tekijät ovat $1, 2, 3, 6$. Koska $2 \mid 16$, $3 \nmid 16$ ja $6 \nmid 16$, niin $(6, 16) = 2$.

Huomautus. Aliluvuissa 1.3 ja 1.7 esittelemme menetelmiä, joilla syt voidaan määrittää mekaanisesti.

Esimerkki 1.2.2. Esimerkissä 1.1.3 todettiin, että kaikki kokonaisluvut jakavat nollan. Kun $a > 0$, niin a on omista tekijöistään suurin, ja kun $a < 0$, niin $-a$ on luvun a tekijöistä suurin. Täten $(0, a) = |a|$, kun $a \neq 0$.

Koska luvulla 1 ei ole muita tekijöitä kuin 1 ja -1, niin $(1, a) = 1$ kaikilla $a \in \mathbb{Z}$.

Esimerkki 1.2.3. Osoitetaan, että $(a, a + 1) = 1$ aina, kun $a \in \mathbb{Z}$. Olkoon $b \in \mathbb{Z}$ sellainen, että $b \mid a$ ja $b \mid a + 1$. Tällöin esimerkin 1.1.4 kohdan 1 perusteella $b \mid -a + (a + 1)$ eli $b \mid 1$. On siis oltava $b = 1$ tai $b = -1$, joten 1 ja -1 ovat lukujen a ja $a + 1$ ainoat yhteiset tekijät, ja $(a, a + 1) = 1$.

Määritelmä 1.2.2. Luvut a ja b ovat *suhteellisia alkulukuja*, jos $(a, b) = 1$. Tällöin voidaan myös sanoa, että a ja b ovat *keskenään jaottomia*.

Lause 1.2.2. *Oletetaan, että $a, b > 0$. Jos $(a, b) = c$, niin a/c ja b/c ovat keskenään jaottomia.*

Todistus. Oletetaan, että $(a, b) = c$. Jos $c = 1$, väite on triviaalisti tosi. Oletetaan, että $c > 1$. Määritelmän 1.2.1 mukaan $c \mid a$ ja $c \mid b$, joten $a = ck$ ja $b = cl$ joillakin $k, l \in \mathbb{Z}$. Tällöin

$a/c = ck/c = k$ ja $b/c = cl/c = l$. Riittää siis osoittaa, että $(k, l) = 1$. Tehdään vastaoletus, että $(k, l) > 1$. Merkitään $(k, l) = d$ (> 1). Tällöin $d \mid k$ ja $d \mid l$, joten $k = dr$ ja $l = ds$ joillakin $r, s \in \mathbb{Z}$. Tällöin $a = cdr$ ja $b = cds$, mistä havaitaan, että $(a, b) \geq cd > c$. Tämä on vastoin oletusta, joten $(k, l) = 1$. □

Huomautus. Kirjallisuudessa joko määritellään erikseen $(0, 0) = 0$ tai $(0, 0)$ jätetään kokonaan määrittelemättä. Tässä esityksessä arvoa $(0, 0)$ ei tarvita.

1.3 Jakoalgoritmi

Lause 1.3.1 (Jakoalgoritmi)**.** *Jokaista lukua a ja b $(\neq 0)$ kohti on olemassa sellaiset yksikäsitteiset luvut q ja r, että*

$$a = bq + r, \text{ missä } 0 \leq r < |b|.$$

Huomautus. Lukua a sanotaan *jaettavaksi*, lukua b *jakajaksi*, lukua q *osamääräksi* ja lukua r *jakojäännökseksi*. Usein merkitään $r = a \bmod b$ (vrt. § 1.9).

Todistus. Olkoot a ja b sellaisia kokonaislukuja, että $b > 0$. (Tapaus $b < 0$ käsitellään vastaavasti.) Todistetaan ensiksi, että lauseen 1.3.1 mukaiset luvut q ja r ovat olemassa. Merkitään

$$q = \left[\frac{a}{b}\right],$$

missä $[a/b]$ on suurin kokonaisluku, joka on $\leq a/b$, ja merkitään

$$r = a - bq.$$

Koska

$$\frac{a}{b} - 1 < \left[\frac{a}{b}\right] = q \leq \frac{a}{b},$$

niin

$$a - b < bq \leq a.$$

Täten

$$0 \leq a - bq = r < b.$$

Näin olemme todistaneet, että lauseen 1.3.1 luvut q ja r ovat olemassa.

Todistamme toiseksi, että luvut q ja r ovat yksikäsitteiset. Oletamme, että

$$a = bq' + r', \quad 0 \leq r' < b.$$

Silloin

$$0 = b(q - q') + (r - r').$$

Näin ollen $b \mid (r - r')$. Koska $0 \leq r < b$ ja $0 \leq r' < b$, niin $-b < r - r' < b$ eli $|r - r'| < b$. Siis $r = r'$. Koska $b \neq 0$, niin $q = q'$. Näin olemme todistaneet lukujen q ja r yksikäsitteisyyden. Siis lause 1.3.1 on voimassa. □

Vaihtoehtoinen todistus luonnollisten lukujen hyvinjärjestyksen pohjalta. Olkoot a ja b sellaisia kokonaislukuja, että $b > 0$. (Tapaus $b < 0$ käsitellään vastaavasti.) Olkoon $S = \{a - bq' \mid q' \in \mathbb{Z}, a - bq' \geq 0\}$. Koska q' voi saada itseisarvoltaan mielivaltaisen suuria negatiivisia arvoja, niin $S \neq \emptyset$. Täten hyvinjärjestysperiaatteen nojalla joukossa S on pienin alkio $r = a - bq$. Hyvinjärjestysperiaatteen pienin alkio on yksikäsitteinen, joten r on yksikäsitteinen, ja siten myös q on yksikäsitteinen.

Koska $r \in S$, niin $r \geq 0$. Oletetaan, että $r \geq b$. Tällöin $a - b(q+1) = a - bq - b = r - b \geq 0$, ja koska $a - b(q+1) \in S$, niin nyt joukossa S on alkio, joka on pienempi kuin r. Tämä on mahdotonta, joten $r < b$. Näin on siis löydetty jakoalgoritmin yksikäsitteiset luvut q ja r. □

Esimerkki 1.3.1. Selvästi $7 = 2 \cdot 3 + 1$. Kun $a = -7$ ja $b = 3$, jakoalgoritmi on $-7 = 3 \cdot (-3) + 2$, sillä lauseen 1.3.1 mukaan jakojäännöksen tulee olla ei-negatiivinen.

Lause 1.3.2. *Olkoon $b \geq 2$. Jokainen luku $a \in \mathbb{Z}_+$ voidaan esittää yksikäsitteisesti muodossa*

$$a = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

missä $k \in \mathbb{Z}_0$, $0 \leq a_i < b$, $i = 0, 1, \ldots, k$ ja $a_k \neq 0$.

Todistus. Haluttu esitys saadaan soveltamalla toistuvasti jakoalgoritmia. Jaetaan ensin a luvulla b ja saadaan

$$a = bq_0 + a_0, \quad 0 \leq a_0 < b. \tag{1.1}$$

Jos $q_0 \neq 0$, jaetaan q_0 luvulla b, jolloin saadaan

$$q_0 = bq_1 + a_1, \quad 0 \leq a_1 < b. \tag{1.2}$$

Jatkamalla tähän tapaan saadaan

$$\begin{aligned}
q_1 &= bq_2 + a_2, \quad 0 \leq a_2 < b, \\
q_2 &= bq_3 + a_3, \quad 0 \leq a_3 < b, \\
&\vdots \\
q_{k-2} &= bq_{k-1} + a_{k-1}, \quad 0 \leq a_{k-1} < b, \\
q_{k-1} &= b \cdot 0 + a_k, \quad 0 \leq a_k < b.
\end{aligned}$$

Sijoittamalla q_0 yhtälöstä (1.2) yhtälöön (1.1) saadaan

$$a = b(bq_1 + a_1) + a_0 = b^2 q_1 + a_1 b + a_0.$$

Sijoittamalla tähän yksi kerrallaan yllä saadut lukujen $q_1, q_2, \ldots, q_{k-1}$ jakoyhtälöt päädytään

lopulta haluttuun esitykseen

$$\begin{aligned} a &= b^3 q_2 + a_2 b^2 + a_1 b + a_0, \\ &\vdots \\ &= b^{k-1} q_{k-2} + a_{k-2} b^{k-2} + \cdots + a_1 b + a_0, \\ &= b^k q_{k-1} + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0, \\ &= a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0. \end{aligned}$$

Osoitetaan vielä, että esitys on yksikäsitteinen. Oletetaan, että on olemassa kaksi tällaista esitystä

$$\begin{aligned} a &= a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 \\ a &= c_k b^k + c_{k-1} b^{k-1} + \cdots + c_1 b + c_0, \end{aligned}$$

missä $0 \leq a_i < b$ ja $0 \leq c_i < b, (i \in \{0, 1, \ldots, k\})$, ja missä on tarvittaessa käytetty nollakertoimia siten, että molempiin esityksiin on saatu sama määrä termejä. Kun vähennetään nämä yhtälöt puolittain toisistaan, saadaan

$$(a_k - c_k) b^k + (a_{k-1} - c_{k-1}) b^{k-1} + \cdots + (a_1 - c_1) b + (a_0 - c_0) = 0.$$

Jos esitykset eivät ole samat, on olemassa pienin kokonaisluku $j, 0 \leq j \leq k$, jolle $a_j \neq c_j$. Otetaan b^j yhteiseksi tekijäksi, jolloin saadaan

$$b^j \left((a_k - c_k) b^{k-j} + \cdots + (a_{j+1} - c_{j+1}) b + (a_j - c_j) \right) = 0,$$

ja koska $b^j \neq 0$, niin

$$(a_k - c_k) b^{k-j} + \cdots + (a_{j+1} - c_{j+1}) b + (a_j - c_j) = 0.$$

Ratkaistaan tästä $a_j - c_j$ ja saadaan

$$\begin{aligned} a_j - c_j &= (c_k - a_k) b^{k-j} + \cdots + (c_{j+1} - a_{j+1}) b \\ &= b \left((c_k - a_k) b^{k-j-1} + \cdots + (c_{j+1} - a_{j+1}) \right), \end{aligned}$$

joten $b \mid (a_j - c_j)$. Koska $0 \leq a_j < b$ ja $0 \leq c_j < b$, niin $-b < a_j - c_j < b$. Tästä seuraa, että $a_j - c_j = 0$ eli $a_j = c_j$. Tämä on ristiriita, joten esitykset ovat samat. Esityksen yksikäsitteisyys on täten todistettu. □

Huomautus. Lauseen 1.3.2 esitystä merkitään myös niin, että $a = (a_m a_{m-1} \ldots a_1 a_0)_b$. Jos $b = 10$, niin kyseessä on kymmenjärjestelmän esitys. Silloin voidaan merkitä $a = (a_m a_{m-1} \ldots a_1 a_0)_{10} = a_m a_{m-1} \ldots a_1 a_0$.

Esimerkki 1.3.2. Kymmenjärjestelmässä esitetty luku $(93)_{10}$ on 8-järjestelmässä esitettynä $(135)_8$. Nimittäin

$$93 = 8 \cdot 11 + 5 = 8(8 \cdot 1 + 3) + 5 = 1 \cdot 8^2 + 3 \cdot 8 + 5.$$

Lause 1.3.3. *Jos $a = bq + r$, niin $(a, b) = (b, r)$.*

Todistus. Merkitään $(a, b) = c$. Todistetaan, että $(b, r) = c$ eli että $(b, a - bq) = c$.

Osa 1. Todistetaan, että c on lukujen b ja $a - bq$ *yhteinen* tekijä. Koska $c \mid a$ ja $c \mid b$, niin $c \mid (-bq)$. Näin ollen lauseen 1.1.1 nojalla $c \mid (a - bq)$. Siis $c \mid b$ ja $c \mid (a - bq)$. Näin osa 1 on todistettu.

Osa 2. Todistetaan, että c on lukujen b ja $a - bq$ *suurin* yhteinen tekijä. Oletetaan, että $d \mid b$ ja $d \mid (a - bq)$. Voidaan todeta, että $d \mid a$ ja $d \mid b$. Näin ollen syt:n määritelmän nojalla $d \leq c$. Siis osa 2 on todistettu. □

Huomautus. Lauseesta 1.3.3 seuraa, että jaettavan ja jakajan syt on yhtäsuuri kuin jakajan ja jakojäännöksen syt.

Lause 1.3.4 (Eukleideen algoritmi)**.** *Olkoot a ja b sellaisia positiivisia kokonaislukuja, että $b \nmid a$. Silloin voidaan kirjoittaa*

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < b, \\
b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\
&\vdots \\
r_{k-2} &= r_{k-1} q_k + r_k, \quad 0 < r_k < r_{k-1}, \\
r_{k-1} &= r_k q_{k+1},
\end{aligned}$$

ts. prosessi päättyy niin, että jokin jakojäännös r_{k+1} ($k \geq 1$) on $= 0$. Viimeinen nollasta poikkeava jakojäännös r_k on $= (a, b)$. (Jos $b \mid a$, niin $r_1 = 0$ ja $(a, b) = b$.)

Todistus.

1) Koska jakojäännöksien jono $r_1, r_2, r_3, \ldots$ on aidosti vähenevä jono ei-negatiivisia kokonaislukuja, niin on olemassa sellainen k, että $r_{k+1} = 0$.

2) Lauseen 1.3.3 nojalla

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_k, 0) = r_k.$$

Näin olemme todistaneet lauseen 1.3.4.

□

Esimerkki 1.3.3. Sovelletaan Eukleideen algoritmia lukuihin 86 ja 8. Saadaan

$$\begin{aligned} 86 &= 8 \cdot 10 + 6, \\ 8 &= 6 \cdot 1 + 2, \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$

Eukleideen algoritmin mukaan viimeinen nollasta poikkeava jakojäännös on lukujen 86 ja 8 suurin yhteinen tekijä, joten $(86, 8) = 2$.

Lause 1.3.5. *Olkoot a ja b kokonaislukuja. Silloin*

$$\exists x, y \in \mathbb{Z} \colon (a, b) = ax + by.$$

Todistus. Kaikki Eukleideen algoritmin jakojäännökset ovat muotoa $ax + by$. Siis myös r_k eli (a, b) on tätä muotoa. Lisäksi jos $b \mid a$, niin $(a, b) = b = a \cdot 0 + b \cdot 1$. □

Esimerkki 1.3.4. Luku $(86, 8)$ voidaan kirjoittaa muodossa $(86, 8) = 86 \cdot 3 + 8 \cdot (-32)$.

Seuraus 1.3.1. *Jos $c \mid a$ ja $c \mid b$, niin $c \mid (a, b)$.*

Todistus. Lauseen 1.3.5 mukaan $(a, b) = ax + by$ joillakin $x, y \in \mathbb{Z}$. Koska $c \mid a$ ja $c \mid b$, niin $c \mid (ax + by)$ eli $c \mid (a, b)$. □

Seuraus 1.3.2. *Jos $a \mid bc$ ja $(a, b) = 1$, niin $a \mid c$.*

Todistus. Lauseen 1.3.5 mukaan $1 = ax + by$. Siis $c = axc + byc$. Koska $a \mid axc$ ja $a \mid byc$, niin $a \mid (axc + ayc)$ eli $a \mid c$. □

Seuraus 1.3.3. *Jos $a \mid c$, $b \mid c$ ja $(a, b) = 1$, niin $ab \mid c$.*

Todistus. Olettamusten ja lauseen 1.3.5 nojalla $c = ad$, $c = be$ ja $1 = ax + by$, joten

$$c = axc + byc = axbe + byad = ab(xe + yd).$$

Näin ollen $ab \mid c$. □

1.4 Lineaarinen Diofantoksen yhtälö

Määritelmä 1.4.1. *Diofantoksen yhtälö* on yhden tai usean muuttujan yhtälö, jolle etsitään kokonaislukuratkaisuja. Kahden muuttujan *lineaarinen Diofantoksen yhtälö* on muotoa

$$ax + by = c,$$

missä $a, b, c \in \mathbb{Z}$.

Lause 1.4.1. *Olkoon ainakin toinen luvuista a ja b nollasta eroava. Tällöin Diofantoksen yhtälö $ax + by = c$ on ratkeava, jos ja vain jos $(a, b) \mid c$.*

Todistus. Merkitään $(a, b) = d$. Oletetaan, että $ax + by = c$ on ratkeava. Koska $d \mid a$ ja $d \mid b$, niin $d \mid ax + by$ eli $d \mid c$. Siis $(a, b) \mid c$.

Oletetaan käänteisesti, että $(a, b) \mid c$ eli $d \mid c$. Lauseen 1.3.5 mukaan on olemassa sellaiset kokonaisluvut u ja v, että

$$d = au + bv.$$

Toisaalta on olemassa sellainen e, että

$$de = c.$$

Näin ollen

$$a(ue) + b(ve) = c,$$

joten yhtälö $ax + by = c$ on ratkeava. □

Huomautus. Yllä lause 1.4.1 antaa menetelmän, jolla voidaan tarkistaa, onko yhtälö $ax+by = c$ ratkeava.

Huomautus. Alla lause 1.4.2 antaa menetelmän, jolla ratkaisut saadaan.

Lause 1.4.2. *Olkoot a, b ja c sellaisia kokonaislukuja, että ainakin toinen luvuista a ja b on nollasta eroava. Merkitään $(a, b) = d$. Jos yhtälö $ax + by = c$ on ratkeava (ts. jos $d \mid c$), niin yhtälön kaikki ratkaisut ovat*

$$\begin{cases} x &= x_0 + bt/d, \\ y &= y_0 - at/d, \end{cases} \quad t \in \mathbb{Z}, \tag{1.3}$$

missä x_0, y_0 on yksi ratkaisu.

Huomautus. Vielä puuttuu menetelmä yksittäisen ratkaisun etsimiseksi. Yksittäinen ratkaisu saadaan esimerkiksi keksimällä tai Eukleideen algoritmilla.

Huomautus. Kaava (1.3) on luonteeltaan suoran parametriesityksen kaltainen.

Todistus.

1) Kyseessä olevat parit ovat ratkaisuja, sillä

$$a(x_0 + bt/d) + b(y_0 - at/d) = ax_0 + by_0 = c.$$

2) Todistetaan, että näin saadaan kaikki ratkaisut. Olkoon x, y mielivaltainen ratkaisu. Silloin

$$ax + by = c = ax_0 + by_0,$$

joten

$$a(x - x_0) + b(y - y_0) = 0.$$

Kun jaetaan puolittain luvulla d, saadaan

$$\frac{a}{d}(x - x_0) + \frac{b}{d}(y - y_0) = 0$$

eli

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0) \tag{1.4}$$

Näin ollen

$$\frac{b}{d} \mid \frac{a}{d}(x - x_0).$$

Lauseen 1.2.2 ja seurauksen 1.3.2 nojalla

$$\frac{b}{d} \mid x - x_0.$$

Siis

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

eli

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

Nyt yhtälön (1.4) nojalla

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

joten

$$y = y_0 - at/d.$$

Siis kaava (1.3) on voimassa.

□

Diofantoksen yhtälön $ax + by = c$ ratkaisualgoritmi

1. Tutkitaan, onko $(a, b) \mid c$ ts. onko yhtälö ratkeava (ks. lause 1.4.1).
2. Etsitään jokin yksittäinen ratkaisu x_0, y_0
   - 2.1. keksimällä (tai tietokoneella) tai
   - 2.2. Eukleideen algoritmin avulla esittämällä ensin (a, b) muodossa $(a, b) = au + bv$, missä $u, v \in \mathbb{Z}$, jolloin yksittäinen ratkaisu on $x_0 = uc/(a, b)$ ja $y_0 = vc/(a, b)$.

3. Yleinen ratkaisu on
$$\begin{cases} x &= x_0 + bt/(a,b), \\ y &= y_0 - at/(a,b), \end{cases} \quad t \in \mathbb{Z},$$
(ks. lause 1.4.2).

Esimerkki 1.4.1. Ratkaistaan yhtälö $19x + 94y = 1994$ yllä olevalla algoritmilla.

1. Koska $(19, 94) = 1$ ja $1 \mid 1994$, niin yhtälö on ratkeava.
2. Yksittäinen ratkaisu $x_0 = 100$, $y_0 = 1$ löydetään keksimällä.
3. Yleinen ratkaisu on
$$\begin{cases} x &= 100 + 94t, \\ y &= 1 - 19t, \end{cases} \quad t \in \mathbb{Z}.$$

Esimerkki 1.4.2. Ratkaistaan yhtälö $15x + 6y = 199$. Koska $(15, 6) \nmid 199$, niin yhtälö ei ole ratkeava.

Esimerkki 1.4.3. Ratkaistaan yhtälö $52x + 62y = 6$.

1. Tutkitaan, onko relaatio $(52, 62) \mid 6$ voimassa. Eukleideen algoritmilla saadaan
$$\begin{aligned} 62 &= 52 \cdot 1 + 10, \\ 52 &= 10 \cdot 5 + 2, \\ 10 &= 2 \cdot 5. \end{aligned}$$
Siis $\mathrm{syt}(52, 62) = 2$. Koska $2 \mid 6$, niin yhtälö on ratkeava.
2. Etsitään yksittäinen ratkaisu Eukleideen algoritmilla. Kohdan 1 nojalla saadaan
$$\begin{aligned} 2 &= 52 - 10 \cdot 5 = 52 - (62 - 52) \cdot 5 \\ &= 52 \cdot 6 + 62 \cdot (-5). \end{aligned}$$
Kun kerrotaan puolittain luvulla 3 (eli luvulla $c/(a,b)$), saadaan
$$6 = 52 \cdot 18 + 62 \cdot (-15).$$
Siis yksittäinen ratkaisu on $x_0 = 18$, $y_0 = -15$.
3. Kaikki ratkaisut ovat
$$\begin{cases} x &= x_0 + bt/(a,b) = 18 + 31t, \\ y &= y_0 - at/(a,b) = -15 - 26t, \end{cases} \quad t \in \mathbb{Z}.$$

Esimerkki 1.4.4. Olkoot käytössä kahden kupin vaaka ja punnuksia, joista osa painaa a ja osa b kiloa, missä $a, b \in \mathbb{Z}_+$. Punnitaan esine, jonka paino w kiloa on tuntematon. Punnitus on mahdollista silloin ja vain silloin, kun

$$\exists x, y \in \mathbb{Z}\colon\ w = ax + by$$

eli silloin ja vain silloin, kun

$$(a, b) \mid w.$$

Kaikki painot w ($\in \mathbb{Z}_+$) on mahdollista punnita silloin ja vain silloin, kun $(a, b) = 1$.

Jos siis punnukset painavat 2 ja 5 kiloa, niillä voidaan punnita mikä tahansa paino, mutta jos ne painavat 6 ja 9 kiloa, niillä voidaan punnita vain luvulla 3 jaolliset painot.

1.5 Alkuluvuista

Määritelmä 1.5.1. Luku p (> 1) on *alkuluku*, jos sen ainoat positiiviset tekijät ovat 1 ja p.

Merkintä. Alkulukujen joukkoa merkitään symbolilla **P**.

Määritelmä 1.5.2. Luku a (> 1) on *yhdistetty* luku, jos se ei ole alkuluku (ts. $a = bc$, missä $1 < b, c < a$).

Esimerkki 1.5.1. Luku 1 ei ole yhdistetty luku eikä alkuluku. Luvut 2, 3 ja 5 ovat alkulukuja. Luvut 4 ja 6 ovat yhdistettyjä lukuja. Lukua 20 pienemmät alkuluvut ovat 2, 3, 5, 7, 11, 13, 17 ja 19.

Esimerkki 1.5.2. Todistetaan, että $a^4 + 4$ on yhdistetty luku aina, kun $a > 1$. Kirjoitetaan $a^4 + 4$ muodossa

$$\begin{aligned} a^4 + 4 &= a^4 + 4a^2 + 4 - 4a^2 \\ &= (a^2 + 2)^2 - (2a)^2 \\ &= (a^2 + 2 - 2a)(a^2 + 2 + 2a). \end{aligned}$$

Koska $a > 1$, niin $a^2 + 2 - 2a > 1$ ja $a^2 + 2 + 2a > 1$. Siis $a^4 + 4$ on yhdistetty luku.

Esimerkki 1.5.3. Tutkitaan, milloin $a^3 - 1$ on yhdistetty luku. Selkeästi yksi sen juurista on $a = 1$, joten se voidaan kirjoittaa muodossa $a^3 - 1 = (a - 1)b$, missä b on jokin toisen asteen polynomi. Esimerkiksi geometrisen sarjan osasumman avulla saadaan

$$a^3 - 1 = (a - 1)(a^2 + a + 1).$$

Jotta kyseessä olisi yhdistetty luku, täytyy olla $a^3 - 1 > 1$, joten $a > 1$. Kun $a = 2$, niin $a^3 - 1 = 2^3 - 1 = 7 \in \mathbf{P}$. Kun $a > 2$, niin $a - 1 > 1$, joten $a^3 - 1$ on yhdistetty luku. Luku $a^3 - 1$ on siis alkuluku vain, kun $a = 2$, ja se on yhdistetty luku, kun $a > 2$.

Esimerkki 1.5.4. Todistetaan, että $(a, a+p)$ voi saada vain arvot 1 ja p, kun $p \in \mathbf{P}$. Merkitään $(a, a+p) = c$. Koska $c \mid a$ ja $c \mid a+p$, niin $a = ck$ ja $a+p = cl$ joillakin $k, l \in \mathbb{Z}$. Saadaan $p = c(l-k)$, joten $c \mid p$. Koska p on alkuluku, sen ainoat positiiviset tekijät ovat 1 ja p. Täten $(a, a+p)$ on joko 1 tai p.

Osoitetaan vielä, että $(a, a+p) = p$, jos ja vain jos $p \mid a$. Jos $(a, a+p) = p$, niin $p \mid a$. Oletetaan sitten, että $p \mid a$. Tällöin $p \mid a+p$. Koska $(a, a+p)$ voi saada vain arvot 1 ja p, niin $(a, a+p) = p$.

Lause 1.5.1. *Jokainen luku a (> 1) on alkulukujen tulo (jossa voi olla yksi tai useampia tekijöitä).*

Todistus. Sovelletaan induktiota luvun a suhteen. Jos $a = 2$, niin a on alkuluku ja väite on oikein. Oletetaan, että väite on oikein, kun $2 \leq a < k$. Silloin jos k on alkuluku, niin väite on oikein. Jos taas k on yhdistetty luku, niin $k = bc$, missä $1 < b, c < k$. Näin ollen induktio-olettamuksen nojalla b ja c ovat alkulukujen tuloja, joten bc eli k on alkulukujen tulo. □

Lause 1.5.2 (Eukleides)**.** *Alkulukuja on ääretön määrä.*

Todistus. Tehdään vastaoletus, jonka mukaan alkulukuja on äärellinen määrä. Olkoot ne p_1, p_2, …, p_n. Merkitään $N = 1 + p_1 p_2 \cdots p_n$. Lauseen 1.5.1 mukaan on olemassa sellainen $i = 1, 2, \ldots, n$, että $p_i \mid N$. Koska lisäksi $p_i \mid p_1 p_2 \cdots p_n$, niin $p_i \mid N - p_1 p_2 \cdots p_n$ eli $p_i \mid 1$. Tämä on mahdotonta, joten vastaoletus on väärin ja siis väite on oikein. □

1.6 Aritmetiikan peruslause

Esitämme aluksi apulauseita aritmetiikan peruslauseen todistamista varten.

Lemma 1.6.1. Jos p on alkuluku ja $p \mid ab$, niin $p \mid a$ tai $p \mid b$.

Todistus. Jos $p \mid a$, niin silloin ei ole mitään todistettavaa. Oletetaan, että $p \nmid a$. Silloin $(p, a) = 1$, sillä luvun p ainoat tekijät ovat 1 ja p. Nyt seurauksen 1.3.2 nojalla $p \mid b$. □

Lemma 1.6.2. Jos p on alkuluku ja $p \mid a_1 a_2 \cdots a_n$, niin on olemassa sellainen $i = 1, 2, \ldots, n$, että $p \mid a_i$.

Todistus. Todistetaan lemma induktiolla luvun n suhteen. Kun $n = 1$, oletukseksi tulee $p \mid a_1$, joten alkuaskel pätee triviaalisti. Tehdään induktio-oletus, että kun $p \mid a_1 a_2 \cdots a_k$, niin $p \mid a_i$ jollakin $i \in \{1, 2, \ldots, k\}$. Oletetaan sitten, että $p \mid a_1 a_2 \cdots a_k a_{k+1}$. Tällöin lemman 1.6.1 nojalla $p \mid a_{k+1}$ tai $p \mid a_1 a_2 \cdots a_k$. Jos $p \mid a_{k+1}$, niin todistus on valmis. Jos $p \mid a_1 a_2 \cdots a_k$, niin induktio-oletuksen mukaan $p \mid a_i$ jollakin $i \in \{1, 2, \ldots, k\}$, mikä todistaa väitteen. □

Lemma 1.6.3. Jos p_1, p_2, …, p_n ovat alkulukuja ja $p \mid p_1 p_2 \cdots p_n$, niin on olemassa sellainen $i = 1, 2, \ldots, n$, että $p = p_i$.

Todistus. Lemman 1.6.2 nojalla on olemassa sellainen $i = 1, 2, \ldots, n$, että $p \mid p_i$. Koska $p > 1$ ja alkuluvun p_i ainoat positiiviset tekijät ovat 1 ja p_i, niin $p = p_i$. □

Nyt olemme valmiit todistamaan *aritmetiikan peruslauseen*.

Lause 1.6.1 (Aritmetiikan peruslause)**.** *Jokainen kokonaisluku a (≥ 2) voidaan esittää alkulukujen tulona ja tämä tulo on yksikäsitteinen tekijöitten järjestystä lukuunottamatta.*

Todistus. Sovelletaan induktiota luvun a suhteen. Jos $a = 2$, niin väite pätee triviaalisti. Olkoon $a > 2$. Tehdään induktio-oletus, että kun $2 \leq k < a$, niin väite pätee luvulle k. Todistetaan, että väite pätee luvulle a. Jos a on alkuluku, niin silloin ei ole mitään todistettavaa. Oletetaan, että a on yhdistetty luku ja että luvulla a on kaksi alkutuloesitystä

$$a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t. \tag{1.5}$$

Todistamme, että $s = t$ ja että jonot (p_i) ja (q_i) ovat samat mahdollisesti järjestystä lukuun ottamatta. Koska $p_1 \mid q_1 q_2 \cdots q_t$, niin lemman 1.6.3 mukaan $p_1 = q_j$ jollakin $j \in \{1, 2, \ldots, t\}$. Muutetaan lukujen q_j numerointia niin, että $p_1 = q_1$. Näin ollen

$$a/p_1 = p_2 p_3 \cdots p_s = q_2 q_3 \cdots q_t.$$

Jos $s \geq 2$ tai $t \geq 2$, niin $1 < a/p_1 < a$. Induktio-olettamuksen mukaan luvun a/p_1 tuloesitykset ovat samat, joten $s = t$ ja luvun k esitykset yhtälössä (1.5) ovat samat. □

Esimerkki 1.6.1. Luvun 8750 esitys alkulukujen tulona on $8750 = 2 \cdot 5 \cdot 5 \cdot 5 \cdot 5 \cdot 7$. Tämä voidaan kirjoittaa muodossa

$$8750 = 2 \cdot 5^4 \cdot 7$$

tai

$$8750 = \prod_{p \in \mathbf{P}} p^{a(p)},$$

missä $a(2) = 1$, $a(3) = 0$, $a(5) = 4$, $a(7) = 1$, $a(p) = 0$ $(p \geq 11)$.

Esimerkki 1.6.2. Luku 600 voidaan kirjoittaa muodossa

$$600 = 2^3 \cdot 3 \cdot 5^2$$

tai

$$600 = \prod_{p \in \mathbf{P}} p^{a(p)},$$

missä $a(2) = 3$, $a(3) = 1$, $a(5) = 2$, $a(p) = 0$ $(p \geq 7)$.

Määritelmä 1.6.1. Luvun a (> 1) *kanoninen alkutekijäesitys* on muotoa

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \tag{1.6}$$

missä $p_1, p_2, \ldots, p_n$ ($p_1 < p_2 < \cdots < p_n$) ovat luvun a alkutekijät (eli alkulukutekijät) ja $a_1, a_2, \ldots, a_n > 0$. Kanoniseksi alkutekijäesitykseksi sanotaan myös esitystä

$$a = \prod_{p \in \mathbf{P}} p^{a(p)}, \tag{1.7}$$

missä $a(p) \geq 0$. Usein (1.7) kirjoitetaan lyhyesti $a = \prod_p p^{a(p)}$ eli merkintä $\in \mathbf{P}$ jätetään pois.

Huomautus. Kaavassa (1.7) $a(p) > 0$, jos ja vain jos $p \mid a$, ts. p on luvun a alkutekijä. Edelleen kaavassa (1.7) tulo on äärellinen, ts. $a(p) > 0$ vain äärellisellä määrällä alkulukuja p. Kaava (1.7) on hyödyllinen monissa teoreettisissa tarkasteluissa.

Huomautus. Kanonista alkutekijäesitystä sanotaan usein lyhyesti *kanoniseksi esitykseksi*.

Esimerkki 1.6.3. Esimerkeissä 1.6.1 ja 1.6.2 on lukujen 8750 ja 600 kanoniset esitykset.

Esimerkki 1.6.4. Luku a on parillinen, jos ja vain jos $a(2)$ on > 0 sen kanonisessa esityksessä.

Huomautus. Olkoot lukujen $a, b > 1$ kanoniset alkutekijäesitykset

$$a = \prod_{p \in \mathbf{P}} p^{a(p)} \text{ ja } b = \prod_{p \in \mathbf{P}} p^{b(p)},$$

missä $a(p), b(p) \geq 0$. Tällöin

$$ab = \left(\prod_{p \in \mathbf{P}} p^{a(p)} \right) \left(\prod_{p \in \mathbf{P}} p^{b(p)} \right) = \prod_{p \in \mathbf{P}} p^{a(p)+b(p)},$$

joten $(ab)(p) = a(p) + b(p)$.

1.7 Aritmetiikan peruslauseen sovelluksia

Aritmetiikan peruslause on erittäin käyttökelpoinen työväline monissa sellaisissa tehtävissä, jotka käsittelevät luvun tekijöitä, lukujen syt:tä ja lukujen tuloja. Esitämme tässä joitakin esimerkkejä. *Koko tässä aliluvussa tarkastelemme positiivisia kokonaislukuja* ja merkitsemme

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \quad a_1, a_2, \ldots, a_n > 0$$

tai

$$a = \prod_p p^{a(p)}, \quad a(p) \geq 0,$$

jossa p käy läpi kaikki alkuluvut.

Lause 1.7.1. *Luku d on luvun a tekijä (eli $d \mid a$), jos ja vain jos d on muotoa*

$$d = \prod_p p^{d(p)}, \tag{1.8}$$

missä $0 \leq d(p) \leq a(p)$, $p \in \mathbf{P}$.

Todistus. Oletetaan, että $d \mid a$. Silloin $a = db$, missä $b \in \mathbb{Z}_+$. Merkitään $b = \prod_p p^{b(p)}$, missä $b(p) \geq 0$. Silloin

$$a(p) = d(p) + b(p), \quad p \in \mathbf{P},$$

missä $a(p)$, $d(p)$, $b(p) \geq 0$, $p \in \mathbf{P}$. Näin ollen $0 \leq d(p) \leq a(p)$, $p \in \mathbf{P}$, eli d on muotoa (1.8).

Oletetaan käänteisesti, että d on muotoa (1.8). Merkitään $b = \prod_p p^{a(p)-d(p)}$. Silloin $a(p) - d(p) \geq 0$, $p \in \mathbf{P}$, joten $b \in \mathbb{Z}_+$. Siis

$$bd = \left(\prod_p p^{a(p)-d(p)}\right)\left(\prod_p p^{d(p)}\right) = \prod_p p^{a(p)} = a,$$

joten $d \mid a$. □

Seuraus 1.7.1. *Luvun a positiivisten tekijöiden lukumäärä on*

$$\prod_p (a(p) + 1).$$

Esimerkki 1.7.1. Luvun 200 kanoninen esitys on $2^3 \cdot 5^2$. Siis luvun 200 positiiviset tekijät ovat

$$\begin{array}{lll} 1, & 5, & 5^2, \\ 2, & 2 \cdot 5, & 2 \cdot 5^2, \\ 2^2, & 2^2 \cdot 5, & 2^2 \cdot 5^2, \\ 2^3, & 2^3 \cdot 5, & 2^3 \cdot 5^2. \end{array}$$

Luvun 200 tekijöiden lukumäärä on $(3 + 1)(2 + 1)$ eli 12.

Lause 1.7.2. *Lukujen a ja b* syt *on*

$$(a, b) = \prod_p p^{c(p)},$$

missä $c(p) = \min\{a(p), b(p)\}$.

Todistus. Merkitään kirjaimella c yhtälön oikean puolen lukua, ts. $c = \prod_p p^{c(p)}$, missä $c(p) = \min\{a(p), b(p)\}$. Silloin $c(p) \leq a(p)$ ja $c(p) \leq b(p)$, joten lauseen 1.7.1 nojalla

$$c \mid a, \quad c \mid b. \tag{1.9}$$

Oletetaan, että $d \mid a$, $d \mid b$. Silloin lauseen 1.7.1 mukaan $d(p) \leq a(p)$ ja $d(p) \leq b(p)$, joten $d(p) \leq \min\{a(p), b(p)\}$ eli $d(p) \leq c(p)$. Näin ollen $d \mid c$. Siis

$$d \leq c. \tag{1.10}$$

Kaavojen (1.9) ja (1.10) nojalla $c = (a, b)$. □

Esimerkki 1.7.2. Lauseen 1.7.2 nojalla saadaan

$$(60, 18) = (2^2 \cdot 3 \cdot 5, 2 \cdot 3^2) = 2^1 \cdot 3^1 \cdot 5^0 = 6.$$

Esimerkki 1.7.3. Todistetaan, että $(ac, bc) = (a, b)c$, kun $c > 0$. Lauseen 1.7.2 nojalla

$$(a, b)c = \left(\prod_p p^{d(p)}\right)\left(\prod_p p^{c(p)}\right) = \prod_p p^{d(p)+c(p)},$$

missä $d(p) = \min\{a(p), b(p)\}$. Lauseen 1.7.2 nojalla

$$(ac, bc) = \prod_p p^{e(p)}$$

missä $e(p) = \min\{(ac)(p), (bc)(p)\}$. Riittää siis osoittaa, että $d(p) + c(p) = e(p)$. Koska minimin ominaisuuksien nojalla

$$\begin{aligned} d(p) + c(p) &= \min\{a(p), b(p)\} + c(p) \\ &= \min\{a(p) + c(p), b(p) + c(p)\} \\ &= \min\{(ac)(p), (bc)(p)\} \\ &= e(p), \end{aligned}$$

niin väite on todistettu.

Määritelmä 1.7.1. Luku c on lukujen a ja b *pienin yhteinen monikerta* (pym), jos

1) $c > 0$,

2) $a \mid c$, $b \mid c$,

3) $a \mid d$, $b \mid d$, $d > 0 \Rightarrow c \leq d$.

Merkintä. Lukujen *a* ja *b pienintä yhteistä monikertaa* merkitään symbolilla $[a, b]$, pym$[a, b]$ tai lcm$[a, b]$.

Lause 1.7.3. *Kun $a, b \in \mathbb{Z}$, niin $[a, b]$ on aina olemassa ja yksikäsitteinen.*

Todistus. Olkoot $a, b \in \mathbb{Z}$. Tarkastellaan joukkoa $S = \left\{ d \in \mathbb{Z}_+ \,\middle|\, a \mid d, b \mid d \right\}$. Koska $ab \in S$, niin $S \neq \emptyset$. Hyvinjärjestysperiaatteen nojalla joukossa S on pienin alkio. Tämä alkio on $[a, b]$ ja se on yksikäsitteinen. □

Esimerkki 1.7.4. Luettelemalla kasvavassa järjestyksessä luvun 6 monikertoja havaitaan, että niistä ensimmäinen, joka on jaollinen luvulla 9, on 18. Siis $[6, 9] = 18$.

Lause 1.7.4. *Lukujen a ja b* pym *on*

$$[a, b] = \prod_p p^{c(p)},$$

missä $c(p) = \max\{a(p), b(p)\}$.

Todistus. Merkitään $c = \prod_p p^{c(p)}$. Koska $p > 1$ kaikilla $p \in \mathbf{P}$, niin $c > 0$. Koska $c(p) = \max\{a(p), b(p)\}$, niin $c(p) \geq a(p)$ ja $c(p) \geq b(p)$. Täten lauseen 1.7.1 nojalla $a \mid c$ ja $b \mid c$.

Olkoon $d \in \mathbb{Z}$ ja oletetaan, että $a \mid d, b \mid d$ ja $d > 0$. Silloin lauseen 1.7.1 mukaan $d(p) \geq a(p)$ ja $d(p) \geq b(p)$, joten $d(p) \geq \max\{a(p), b(p)\}$ eli $d(p) \geq c(p)$. Näin ollen $c \mid d$. Siis $c \leq d$.

Yllä olevan perusteella $c = [a, b]$. □

Esimerkki 1.7.5. Lauseen 1.7.4 nojalla

$$[60, 18] = [2^2 \cdot 3 \cdot 5, 2 \cdot 3^2] = 2^2 \cdot 3^2 \cdot 5 = 180.$$

Lause 1.7.5. *Lukujen a ja b* syt *ja* pym *toteuttavat yhtälön*

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

Todistus. Lauseiden 1.7.2 ja 1.7.4 nojalla

$$(a, b)[a, b] = \left(\prod_p p^{c(p)} \right) \left(\prod_p p^{d(p)} \right) = \prod_p p^{c(p)+d(p)},$$

missä $c(p) = \min\{a(p), b(p)\}$ ja $d(p) = \max\{a(p), b(p)\}$. Koska

$$\min\{a(p), b(p)\} + \max\{a(p), b(p)\} = a(p) + b(p),$$

niin aritmetiikan peruslauseen nojalla

$$\prod_p p^{c(p)+d(p)} = \prod_p p^{a(p)+b(p)} = \left(\prod_p p^{a(p)}\right)\left(\prod_p p^{b(p)}\right) = ab,$$

mikä todistaa väitteen. □

Esimerkki 1.7.6. Esimerkin 1.2.3 perusteella $(a, a+1) = 1$. Näin ollen lauseen 1.7.5 perusteella

$$[a, a+1] = a(a+1).$$

1.8 Kongruenssi

Määritelmä 1.8.1. Olkoon $m \in \mathbb{Z}_+$. Silloin sanotaan, että luku a on *kongruentti* luvun b kanssa *modulo* m, jos

$$m \mid (a-b).$$

Merkintä. Jos luku a on kongruentti luvun b kanssa modulo m, niin merkitään

$$a \equiv b \pmod{m}.$$

Esimerkki 1.8.1. Koska $2 \mid (7-5)$, niin $5 \equiv 7 \pmod 2$, mutta $6 \not\equiv 7 \pmod 2$, koska $2 \nmid (7-6)$.

Lause 1.8.1. *$a \equiv b \pmod m$, jos ja vain jos*

$$\exists k \in \mathbb{Z}\colon a = b + km.$$

Todistus. Määritelmien 1.8.1 ja 1.1.1 mukaan

$$\begin{aligned} a \equiv b \pmod m &\Leftrightarrow m \mid (a-b) \\ &\Leftrightarrow \exists k \in \mathbb{Z}\colon a - b = mk \\ &\Leftrightarrow \exists k \in \mathbb{Z}\colon a = b + km. \end{aligned}$$

□

Lause 1.8.2. *Kongruenssi $\equiv$ on ekvivalenssirelaatio, ts.*

1) $a \equiv a \pmod m$, *(refleksiivisyys)*

2) $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$, *(symmetrisyys)*

3) $a \equiv b \pmod m$, $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$, *(transitiivisuus).*

Todistus.

1) Esimerkin 1.1.3 nojalla $m \mid 0$, joten $m \mid (a - a)$.

2) Oletetaan, että $a \equiv b \pmod{m}$. Silloin $m \mid (a - b)$, joten $a - b = mk$ jollakin $k \in \mathbb{Z}$. Tällöin $b - a = m(-k)$, joten $m \mid (b - a)$. Täten $b \equiv a \pmod{m}$.

3) Oletetaan, että $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m}$, jolloin $m \mid (a - b)$ ja $m \mid (b - c)$. Koska $a - c = (a - b) + (b - c)$, niin lauseen 1.1.1 kohdan 1 mukaan $m \mid (a - c)$. Täten $a \equiv c \pmod{m}$.

□

Lause 1.8.3. *Oletetaan, että $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m}$. Silloin*

1) $ax + cy \equiv bx + dy \pmod{m}$ *aina, kun* $x, y \in \mathbb{Z}$,

2) $ac \equiv bd \pmod{m}$,

3) *kun* $a_i \equiv b_i \pmod{m}$, $(i = 1, 2, 3, \ldots, n)$, *niin* $a_1 a_2 \cdots a_n \equiv b_1 b_2 \cdots b_n \pmod{m}$,

4) $f(a) \equiv f(b)$ *aina, kun* f *on kokonaislukukertoiminen polynomi.*

Todistus.

1) Koska $m \mid (a - b)$ ja $m \mid (c - d)$, niin esimerkin 1.1.4 kohdan 1 nojalla

$$m \mid (a - b)x + (c - d)y$$

eli

$$m \mid (ax + cy) - (bx + dy),$$

mikä todistaa väitteen.

2) Koska $m \mid (a - b)$ ja $m \mid (c - d)$, niin on olemassa sellaiset $k, l \in \mathbb{Z}$, että $a - b = mk$ ja $c - d = ml$. Saadaan $ac - bd = (mk + b)c - b(c - ml) = m(kc + bl)$. Täten $m \mid (ac - bd)$, mistä väite seuraa.

3) Todistetaan väite induktiolla luvun n suhteen. Kun $n = 1$, niin väite pätee suoraan oletuksen nojalla. Tehdään induktio-oletus, että väite pätee, kun $n = k \geq 1$. Tällöin induktio-oletuksen nojalla $b_1 b_2 \cdots b_k \equiv c_1 c_2 \cdots c_k \pmod{m}$ ja oletuksen nojalla $b_{k+1} \equiv c_{k+1} \pmod{m}$, joten kohdan 2 perusteella $b_1 b_2 \cdots b_k b_{k+1} \equiv c_1 c_2 \cdots c_k c_{k+1} \pmod{m}$, mikä päättää induktion.

4) Todistetaan väite induktiolla polynomin asteen $\deg(f)$ suhteen. Kun $\deg(f) = 0$, niin f on vakiopolynomi ja siten $f(a) = f(b)$. Näin ollen alkuaskel pätee. Tehdään induktio-oletus, että kun $\deg(f) \leq k$, $(k \in \mathbb{Z}_0)$, niin $f(a) \equiv f(b)$. Tarkastellaan sitten $(k+1)$-asteista polynomia $f(x) = c_{k+1}x^{k+1} + c_k x^k + \cdots + c_1 x + c_0$. Merkitään $g(x) = c_k x^k + \cdots + c_1 x + c_0$. Koska $\deg(g) \leq k$, niin induktio-oletuksen mukaan $g(a) \equiv g(b)$. Koska $a \equiv b$, niin kohdan 3 mukaan $c_{k+1}a^{k+1} \equiv c_{k+1}b^{k+1}$. Tällöin kohdan 1 mukaan $c_{k+1}a^{k+1} + g(a) \equiv c_{k+1}b^{k+1} + g(b)$ eli $f(a) \equiv f(b)$, mikä päättää induktion.

□

Esimerkki 1.8.2. Olkoon luvun a esitys 10-järjestelmässä $a = (a_n a_{n-1} \ldots a_1 a_0)_{10}$. Todistetaan, että tällöin

$$3 \mid a \Leftrightarrow 3 \mid a_n + a_{n-1} + \cdots + a_1 + a_0.$$

Merkitään $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Koska $10 \equiv 1 \pmod 3$, niin $f(10) \equiv f(1) \pmod 3$ eli

$$a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 3.$$

Näin ollen lauseen 1.8.2 nojalla

$$\begin{aligned} 3 \mid a &\Leftrightarrow a \equiv 0 \pmod 3 \\ &\Leftrightarrow a_n + a_{n-1} + \cdots + a_1 + a_0 \equiv 0 \pmod 3 \\ &\Leftrightarrow 3 \mid a_n + a_{n-1} + \cdots + a_1 + a_0. \end{aligned}$$

Huomautus. Edellinen esimerkki pitää paikkansa, kun luku 3 korvataan luvulla 9.

Esimerkki 1.8.3. Relaatio $9 \mid 819$ on voimassa, koska $9 \mid (8 + 1 + 9)$.

Lause 1.8.4. *Merkitään $(a, m) = d$. Silloin*

$$ab \equiv ac \pmod m \Leftrightarrow b \equiv c \pmod{m/d}.$$

Todistus. Selvästi

$$\begin{aligned} ab \equiv ac \pmod m &\Leftrightarrow m \mid a(b-c) \\ &\Leftrightarrow \frac{m}{d} \,\Big|\, \frac{a}{d}(b-c) \\ &\Leftrightarrow \frac{m}{d} \,\Big|\, b - c \quad \text{(seuraus 1.3.2)} \\ &\Leftrightarrow b \equiv c \pmod{m/d}. \end{aligned}$$

□

Esimerkki 1.8.4. Lauseen 1.8.4 avulla saadaan

$$4x \equiv 20 \pmod 6 \Leftrightarrow x \equiv 5 \pmod 3.$$

Siis $x \equiv 2 \pmod 3$.

Huomautus. Jos $a \equiv b \pmod m$, niin $(a, m) = (b, m)$. (Tämä on sisällöltään sama kuin lause 1.3.3.)

1.9 Jäännös ja kongruenssi

Kun luku a jaetaan jakoalgoritmin mukaisesti luvulla m (> 0), niin saadaan

$$a = qm + r,$$

missä $0 \leq r < m$. Lukua r sanotaan *jäännökseksi*. Tässä yhteydessä puhutaan tarkemmin *jäännöksestä modulo m* ja merkitään $r = a \bmod m$. Jäännöksellä on selkeä yhteys kongruenssiin, joka todetaan tässä aliluvussa.

Lause 1.9.1.

1) Jos $r = a \bmod m$, *niin* $a \equiv r \pmod{m}$.

2) Jos $a \equiv r \pmod{m}$ *ja* $0 \leq r < m$, *niin* $r = a \bmod m$.

Todistus. Jakoalgoritmin ja lauseen 1.8.1 nojalla

$$\begin{aligned} r = a \bmod m &\Leftrightarrow a = qm + r \text{ jollakin } q \in \mathbb{Z}, 0 \leq r < m \\ &\Leftrightarrow a - r = qm \text{ jollakin } q \in \mathbb{Z}, 0 \leq r < m \\ &\Leftrightarrow m \mid (a - r), 0 \leq r < m \\ &\Leftrightarrow a \equiv r \pmod{m}, 0 \leq r < m. \end{aligned}$$

□

Seuraus 1.9.1. *Jokaista kokonaislukua a kohti on olemassa yksikäsitteinen* $r \in \{0, 1, \ldots, m - 1\}$ *niin, että* $a \equiv r \pmod{m}$. *Tämä yksikäsitteinen r on luvun a jäännös modulo m.*

Todistus. Seuraa suoraan jakojäännöksen yksikäsitteisyydestä ja lauseesta 1.9.1. □

Huomautus. Lauseista 1.8.2 ja 1.8.3 seuraa, että kun tuloja ja summia sisältävässä kokonaislukulausekkeessa jokin yhteenlaskettava tai tulontekijä korvataan sen kanssa kongruentin luvun kanssa $\pmod{m}$, niin saatu uusi lauseke on kongruentti alkuperäisen lausekkeen kanssa $\pmod{m}$.

Esimerkki 1.9.1. Määritetään $32^{2001} \bmod 3$ eli luvun 32^{2001} jäännös modulo 3. Etsitään sellainen $r \in \{0, 1, 2\}$, että $32^{2001} \equiv r \pmod{3}$. Yllä olevan huomautuksen periaatteella saadaan

$$32^{2001} \equiv (-1)^{2001} = -1 \equiv 2 \pmod{3}$$

eli jäännös on 2.

Esimerkki 1.9.2. Määritetään luvun $2^{71} + 17 \cdot 6^{833}$ jäännös modulo 5. Saadaan

$$\begin{aligned} 2^{71} + 17 \cdot 6^{833} &= 4^{35} \cdot 2 + 17 \cdot 6^{833} \\ &\equiv (-1)^{35} \cdot 2 + 17 \cdot 1^{833} = -2 + 17 \\ &= 15 \equiv 0 \pmod 5. \end{aligned}$$

Näin ollen $5 \mid 2^{71} + 17 \cdot 6^{833}$ eli jäännös on 0.

Esimerkki 1.9.3. Määritetään lukujen 7835714 ja $\sum_{i=1}^{100} i!$ jäännökset modulo 4. Saadaan

$$\begin{aligned} 7835714 &= 78357 \cdot 100 + 14 \\ &\equiv 78357 \cdot 0 + 14 \equiv 2 \pmod 4 \end{aligned}$$

ja

$$\begin{aligned} \sum_{i=1}^{100} i! &= 1! + 2! + 3! + 4! + \cdots + 100! \\ &\equiv 1 + 2 + 2 + 0 + \cdots + 0 \equiv 1 \pmod 4. \end{aligned}$$

Siis jäännökset ovat 2 ja 1.

Lause 1.9.2. *$a \equiv b \pmod m$, jos ja vain jos $a \bmod m = b \bmod m$.*

Todistus. Oletetaan, että $a \equiv b \pmod m$. Todistetaan, että $a \bmod m = b \bmod m$. Kirjoitetaan

$$a = qm + r, \quad 0 \leq r < m. \tag{1.11}$$

Silloin

$$r = a \bmod m. \tag{1.12}$$

Oletuksen ja lauseen 1.8.1 mukaan on olemassa sellainen k, että

$$a = b + km. \tag{1.13}$$

Kaavojen (1.11) ja (1.13) perusteella

$$b + km = qm + r, \quad 0 \leq r < m$$

eli

$$b = (q - k)m + r, \quad 0 \leq r < m.$$

Näin ollen

$$b \bmod m = r. \tag{1.14}$$

Kaavojen (1.12) ja (1.14) perusteella $a \bmod m = b \bmod m$.

Oletetaan käänteisesti, että $a \bmod m = b \bmod m$. Todistetaan, että $a \equiv b \pmod{m}$. Kirjoitetaan

$$\begin{aligned} a &= qm + r, \quad 0 \leq r < m, \\ b &= q'm + r', \quad 0 \leq r' < m. \end{aligned}$$

Oletuksen mukaan $r = r'$. Näin ollen

$$a - b = (q - q')m,$$

joten

$$m \mid a - b.$$

Siis

$$a \equiv b \pmod{m}.$$

□

1.10 Jäännösluokat

Olkoon $m \in \mathbb{Z}_+$ kiinteä. Lauseessa 1.8.2 on todistettu, että kongruenssi $\equiv \pmod{m}$ on ekvivalenssirelaatio joukossa $\mathbb{Z}$. Tämä antaa oikeutuksen seuraavalle määritelmälle.

Määritelmä 1.10.1. Olkoon $m \in \mathbb{Z}_+$ kiinteä. Silloin ekvivalenssirelaation $\equiv \pmod{m}$ ekvivalenssiluokkia sanotaan *jäännösluokiksi* modulo m.

Merkintä. Merkitään lyhyesti $\overline{a} = (a/\equiv \pmod{m})$, ts.

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}.$$

Siis $\overline{a}$ on luvun a jäännösluokka modulo m. (Tarvittaessa ks. Merikoski, Virtanen, Koivisto, Johdatus diskreettiin matematiikkaan, 2018, luku 4.4, `https://matematiikkalehtisolmu.fi/2018/jdm-2017-12-19.pdf`.)

Huomautus. Jäännösluokka $\overline{a}$ riippuu luvusta m, vaikka se ei merkinnästä $\overline{a}$ ilmenekään. Jos modulo m ei selviä asiayhteydestä, niin se on syytä mainita erikseen. Termin jäännösluokka luontevuus tulee selväksi alla olevista ominaisuuksista.

Merkintä. Merkitään lyhyesti

$$\mathbb{Z}_m = (\mathbb{Z}/\equiv \pmod{m})$$

ts.

$$\mathbb{Z}_m = \{\overline{a} \mid a \in \mathbb{Z}\}.$$

Siis $\mathbb{Z}_m$ on kaikkien jäännösluokkien joukko modulo m.

Lause 1.10.1. *Kokoelma* $\overline{0}$, $\overline{1}$, $\overline{2}$, ..., $\overline{m-1}$ *käsittää kaikki jäännösluokat modulo m täsmälleen kerran, ts.*

$$\mathbb{Z}_m = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\right\}, \tag{1.15}$$

missä jäännösluokat $\overline{0}$, $\overline{1}$, $\overline{2}$, ..., $\overline{m-1}$ *ovat erisuuret.*

Todistus. Todistetaan ensiksi kaava (1.15). Selvästi $\left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\right\} \subseteq \mathbb{Z}_m$. Todistetaan, että $\mathbb{Z}_m \subseteq \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\right\}$. Olkoon $\overline{a} \in \mathbb{Z}_m$ mielivaltainen jäännösluokka. Merkitään $r = a \bmod m$. Silloin $a \equiv r \pmod{m}$ ja $0 \leq r < m$. Ekvivalenssirelaation ominaisuuksien nojalla $\overline{a} = \overline{r}$ ja $0 \leq r < m$. Siis $\overline{a} \in \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\right\}$.

Todistetaan toiseksi, että jäännösluokat $\overline{0}$, $\overline{1}$, $\overline{2}$, ..., $\overline{m-1}$ ovat erisuuret. Oletetaan, että $\overline{u} = \overline{v}$, missä $0 \leq u, v < m$. Silloin ekvivalenssiluokkien yleisten ominaisuuksien nojalla

$$u \equiv v \pmod{m},$$

joten

$$m \mid u - v.$$

Koska $0 \leq |u - v| < m$, niin $u - v = 0$ eli $u = v$. □

Lause 1.10.2. *Joukko* $\mathbb{Z}_m$ *muodostaa joukon* $\mathbb{Z}$ *osituksen, ts. sen alkiot ovat erilliset ja niiden unioni on* $\mathbb{Z}$.

Todistus. Lauseen 1.8.2 mukaan kongruenssi on ekvivalenssirelaatio. Väite seuraa suoraan ekvivalenssirelaation ominaisuuksista (ks. Merikoski, Virtanen, Koivisto, Johdatus diskreettiin matematiikkaan, 2018, luku 4.4). □

Huomautus. Seuraavat ominaisuudet ovat voimassa jäännösluokille:

1) $\overline{r} = \{x \in \mathbb{Z} \mid x \bmod m = r\}$, kun $0 \leq r < m$,

2) $\overline{a} = \overline{r}$, missä $r = a \bmod m$,

3) x ja y kuuluvat samaan jäännösluokkaan $\Leftrightarrow x \equiv y \pmod{m} \Leftrightarrow x \bmod m = y \bmod m$,

4) $\overline{a} = \overline{b} \Leftrightarrow a \equiv b \pmod{m} \Leftrightarrow a \bmod m = b \bmod m$,

5) $\overline{a} = \{x \in \mathbb{Z} \mid x \bmod m = a \bmod m\}$,

6) $r \in \overline{a}$, missä $r = a \bmod m$.

Näiden todistukset jätetään harjoitustehtäviksi.

1.11 Fermat'n pieni lause

Tässä aliluvussa todistamme Fermat'n pienen lauseen, jonka avulla voidaan laskea suurten kokonaislukupotenssien jakojäännöksiä modulo p.

Lause 1.11.1. *(Fermat'n pieni lause). Jos p on alkuluku, $a \in \mathbb{Z}_+$ ja $(a, p) = 1$, niin $a^{p-1} \equiv 1 \pmod{p}$.*

Esimerkki 1.11.1. Koska $2+3+4+5+6+7+8 = 35$ ja $3 \nmid 35$, niin esimerkin 1.8.2 nojalla $3 \nmid 2345678$. Tällöin $(2345678, 3) = 1$, koska 3 on alkuluku. Täten Fermat'n pienen lauseen mukaan $2345678^2 \equiv 1 \pmod{3}$, joten $3 \mid 2345678^2 - 1$.

Esimerkki 1.11.2. Jos p on alkuluku ja $a \in \mathbb{Z}_+$, niin $a^p \equiv a \pmod{p}$. Nimittäin jos $p \mid a$, niin $p \mid a(a^{p-1} - 1)$ eli $p \mid (a^p - a)$, jolloin kongruenssin määritelmän 1.8.1 mukaan $a^p \equiv a \pmod{p}$. Jos taas $p \nmid a$, niin $(a, p) = 1$, koska p on alkuluku. Tällöin Fermat'n pienen lauseen perusteella $a^{p-1} \equiv 1 \pmod{p}$. Kertomalla molemmat puolet luvulla a saadaan $a^p \equiv a \pmod{p}$.

Esimerkki 1.11.3. (Käänteisalkio kertolaskun suhteen modulo p.) Jos p on alkuluku ja $p \nmid a$, niin yhtälön $a \cdot x \equiv 1 \pmod{p}$ eräs ratkaisu on $x = a^{p-2}$, sillä $a \cdot a^{p-2} = a^{p-1}$, jolloin tulos seuraa suoraan Fermat'n pienestä lauseesta.

Fermat'n pienen lauseen todistamiseksi tarvitaan seuraavat lemmat. Tästä eteenpäin tässä aliluvussa merkitään $P = \{1, 2, \ldots, p-1\}$, missä p on alkuluku. Lisäksi koko aliluvun ajan oletetaan, että $a \in \mathbb{Z}_+$ ja $(a, p) = 1$.

Lemma 1.11.1. Kun $k \in P$, niin $p \nmid ka$.

Todistus. Koska $k \in P$, niin $k < p$, joten $p \nmid k$. Tehdään vastaoletus, että $p \mid ka$ jollakin $k \in P$. Koska $(a, p) = 1$, niin seurauksen 1.3.2 mukaan $p \mid k$. Tämä on ristiriita, joten $p \nmid ka$. □

Lemma 1.11.2. Kun $1 \leq i < j \leq p-1$, niin $ia \not\equiv ja \pmod{p}$.

Todistus. Tehdään vastaoletus, että $ia \equiv ja \pmod{p}$, jolloin $p \mid (ja - ia) = a(j - i)$. Koska $j - i \in P$, niin lemman 1.11.1 mukaan $p \nmid a(j - i)$. Tämä on ristiriita, joten $ia \not\equiv ja \pmod{p}$. □

Lemma 1.11.3. Kun $k \in P$, niin $(ka \bmod p) \in P$.

Todistus. Jakoalgoritmin mukaan on olemassa sellaiset $q, r \in \mathbb{Z}, 0 \leq r < p$, että $ka = pq + r$. Koska lemman 1.11.1 perusteella $p \nmid ka$, niin $r \neq 0$, joten $r \in P$. Koska $r = ka - pq$ ja $0 \leq r < p$, niin $r = ka \bmod p$, joten $(ka \bmod p) \in P$. □

Lemma 1.11.4. Kun p on alkuluku, niin $(p, (p-1)!) = 1$.

Todistus. Merkitään $d = (p, (p-1)!)$. Koska $d \mid p$ ja p on alkuluku, niin $d \in \{1, p\}$. Oletetaan, että $d = p$. Tällöin $p \mid (p-1)!$, joten lemman 1.6.2 nojalla p jakaa jonkin alkion joukosta P. Tämä on mahdotonta, joten $d = 1$. □

Lemma 1.11.5. Kun $(d, m) = 1$ ja $bd \equiv cd \pmod{m}$, niin $b \equiv c \pmod{m}$.

Todistus. Oletetaan, että $(d, m) = 1$ ja $bd \equiv cd \pmod{m}$. Tällöin $m \mid bd - cd = (b-c)d$, joten seurauksen 1.3.2 nojalla $m \mid (b-c)$. Täten $b \equiv c \pmod{m}$. □

Nyt olemme valmiit todistamaan Fermat'n pienen lauseen.

Fermat'n pienen lauseen todistus. Merkitään $A = \{ka \bmod p \mid k \in P\}$. Olkoon $x \in A$. Tällöin $x = ka \bmod p$ jollakin $k \in P$, joten lemman 1.11.3 mukaan $x \in P$. Täten $A \subseteq P$. Lauseen 1.9.2 ja lemman 1.11.2 perusteella $k_1 a \bmod p \neq k_2 a \bmod p$, kun $k_1, k_2 \in P$ ja $k_1 \neq k_2$. Joukossa A on siis $p-1$ alkiota, joten täytyy olla $A = P$.

Koska $A = P$, niin lauseen 1.8.3 kohdan 3 perusteella

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

Täten $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Lemman 1.11.4 nojalla tähän voidaan soveltaa lemmaa 1.11.5, mistä seuraa

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

□

2 Kirjallisuutta

D. M. Burton, Elementary Number Theory, 5th ed., McGraw-Hill, 2002.

K. H. Rosen, Elementary Number Theory and Its Applications, 5th ed., Pearson/Addison-Wesley, 2005.