LUKUTEORIA 1

JYVÄSKYLÄN YLIOPISTO

Matemaatikot eivät ole tyytyväisiä tietäessään asioita neljästä miljoonasta tai neljästä miljardista kokonaisluvusta.

He haluavat tietää asioita jokaisesta äärettömän monesta kokonaisluvusta.

- Sir Andrew Wiles

Alkusanat

Tämä luentomateriaali on tarkoitettu kevätlukukaudella 2018 Jyväskylän yliopistossa luennoitavalle kurssille Lukuteoria 1. Kiitän kurssin aiempia luennoitsijoita, Heli Tuomista ja Päivi Lammia, ystävällisestä avusta luentojen ja harjoitustehtävien valmistelussa.

Eero Ruosteenoja

Sisältö

1. Johdanto

Lukuteoria on tasogeometrian ohella matematiikan ala, jonka perustukset luotiin antiikin Kreikassa. Pythagoras (n. 570-495 e.a.a.) salaseuroineen, Eukleides (n. 300 e.a.a.) ja Diofantos (n. 200-280) tutkivat kokonaislukujen ominaisuuksia, erityisesti jaollisuutta, ja havaitsivat alkulukujen erityisaseman kokonaislukujen joukossa. Myös Platon (n. 425-350 e.a.a.) oli hyvin kiinnostunut matematiikasta ja kirjasi muistiin joitakin kuulemiaan edistysaskelia lukuteoriassa. Seuraavien vuosisatojen aikana lukuteoriaa vietiin eteenpäin esimerkiksi Intiassa (Aryabhata n. 500) ja islamilaisessa maailmassa (Ibn al-Haytham n. 1000), kunnes Fermat (1607-1665) todenteolla käynnisti lukuteorian tutkimuksen uudelleen Euroopassa. 1700- ja 1800-luvun suurista lukuteoreetikoista mainittakoon Euler (1707-1783), Lagrange (1736-1813) ja Gauss (1777-1855).

Nykypäivänä lukuteoria on laaja ja elävä matematiikan ala, jossa työkaluina käytetään monipuolisesti modernin matematiikan työkaluja ja jolla on sovelluksia muun muassa salausmenetelmissä. Suomalaismatemaatikoista Turun yliopistossa työskentelevä Kaisa Matomäki kuuluu maailman kärkitutkijoihin lukuteorian alalla.

Tällä kurssilla opiskelemme lukuteorian perusteita. Kurssin päätuloksia ovat muun muassa Eukleideen algoritmi (jonka avulla löydetään tehokkaasti kokonaislukujen suurin yhteinen tekijä), Aritmetiikan peruslause (jonka mukaan jokaisella ykköstä suuremmalla luonnollisella luvulla on yksikäsitteinen alkutekijäesitys), sekä kongruensseihin liittyvä Fermat'n pieni lause. Opimme myös, mikä tulos raivostutti Pythagoraan ja mitkä avoimet ongelmat ovat riivanneet maailman parhaita matemaatikoita satojen vuosien ajan.

1.1. **Merkinnät ja esitiedot.**

Kurssilla käytetään tuttuja merkintöjä:

$$\begin{aligned}
&\mathbb{N} = \{0, 1, 2, ...\} \quad \text{(luonnolliset luvut)},\\
&\mathbb{Z} = \{0, \pm 1, \pm 2, ...\} \quad \text{(kokonaisluvut)},\\
&\mathbb{Q} = \{\frac{m}{n} \ : \ m, n \in \mathbb{Z}, n \neq 0\} \quad \text{(rationaaliluvut)},\\
&\mathbb{R} \quad \text{(reaaliluvut; tarkka määritelmä sivuutetaan)}.
\end{aligned}$$

Joillakin kursseilla ja joissakin kirjoissa luonnolliset luvut alkavat ykkösestä, mutta tällä kurssilla siis $0 \in \mathbb{N}$.

Kurssin tuloksia nimitetään *propositioiksi*, *lemmoiksi* ja *lauseiksi*. Proposition suomennos voisi olla "pieni huomio", lemma on usein aputulos jotain toista tulosta silmälläpitäen, ja lause on erityisen merkittävä tulos.

Kurssin ainoat esitiedot ovat joukko-opin yleisimpien merkintöjen tuntemus sekä matemaattinen induktio. Näitä voi kertailla Johdatus matematiikkaan -kurssin muistiinpanoista. Esimerkiksi yllä oleva rationaalilukujen joukon määritelmä luetaan: Rationaalilukuihin kuuluvat kaikki sellaiset luvut $\frac{m}{n}$,

missä m ja n ovat kokonaislukuja ja n eroaa nollasta. Seuraavassa esimerkissä kerrataan joitakin joukko-opin merkintöjä.

Esimerkki 1.1.1. Olkoot $A = \{1, 2, 3, 4\}$ ja $B = \{4, 5, 6\}$. Tällöin $A \subset \mathbb{N}$, $1 \in A$, $1 \notin B$, $A \cup B = \{1, 2, 3, 4, 5, 6\}$, $A \cap B = \{4\}$, $A \setminus B = \{1, 2, 3\}$, $(A \setminus B) \cap B = \emptyset$ (tyhjä joukko).

Matemaattista induktiota voi kerrata todistamalla seuraavan proposition, johon liittyy hauska tarina. Kun Gauss meni kouluun 1780-luvulla, hänen luokkansa opettaja halusi heti ottaa oppilailta luulot pois määräten heidät laskemaan yhteen luonnolliset luvut ykkösestä sataan. Opettaja luuli saaneensa ruhtinaallisen vapaa-ajan, mutta hyvin pian Gauss ilmoitti vastaukseksi 5050. Miten hän sen teki?

Propositio 1.1.2. *Olkoon $n \in \mathbb{N}$. Tällöin*

$$\sum_{j=0}^{n} j = \frac{n(n+1)}{2}.$$

Todistus. Harjoitustehtävä. □

Induktiolla voi myös todistaa tällä kurssilla erittäin hyödyllisen *luonnollisten lukujen hyvinjärjestysperiaatteen*, joka sanoo, että jokaisessa luonnollisten lukujen joukon epätyhjässä osajoukossa on pienin luku.

Lause 1.1.3. (Luonnollisten lukujen hyvinjärjestysperiaate.) *Olkoon $A \subset \mathbb{N}$, $A \neq \emptyset$. Tällöin on sellainen yksikäsitteinen luku $a \in A$, että $b \geq a$ kaikilla $b \in A$.*

Todistus. Osoitetaan, että jos $A \subset \mathbb{N}$ on joukko, jossa ei ole sellaista lukua a, että $b \geq a$ kaikilla $b \in A$, niin $A = \emptyset$. Käytetään induktiota.

Alkuaskel: Näytetään ensin, että $0 \notin A$. Koska $A \subset \mathbb{N}$, on $b \geq 0$ kaikilla $b \in A$. Koska joukossa A ei ole sellaista lukua a että $b \geq a$ kaikilla $b \in A$, on oltava $0 \notin A$.

Induktio-oletus. Oletetaan, että luvut $0, 1, 2, ..., k$ eivät kuulu joukkoon A.

Induktioväite. Osoitetaan induktio-oletuksen avulla, että luvut $0, 1, 2, ..., k, k+1$ eivät kuulu joukkoon A. Oletamme siis, että luvut $0, 1, 2, ..., k$ eivät kuulu joukkoon A. Tällöin $b \geq k + 1$ kaikilla $b \in A$, joten $k + 1 \notin A$. Induktioargumentti on valmis: mikään luonnollinen luku ei kuulu joukkoon A.

Olemme todistaneet, että jos $A \subset \mathbb{N}$ ja joukossa A ei ole pienintä lukua, joukko A on tyhjä. Tästä seuraa, että jokaisessa luonnollisten lukujen epätyhjässä joukossa on pienin luku.

Todetaan vielä pienimmän luvun yksikäsitteisyys. Jos $a, a' \in A$, $b \geq a$ kaikilla $b \in A$ ja $b \geq a'$ kaikilla $b \in A$, on $a' \geq a$ ja $a \geq a'$, eli $a = a'$. Siis pienin luku on yksikäsitteinen. □

2. Jaollisuus ja tekijät

2.1. **Jaollisuus.**

Määritelmä 2.1.1. Olkoot $a, b \in \mathbb{Z}$. Luku a *jakaa* luvun b, merkitään $a \mid b$, jos

$$b = ka \quad \text{jollakin } k \in \mathbb{Z}.$$

Tällöin sanotaan, että a on luvun b *tekijä*. Sanotaan myös, että b on *jaollinen* luvulla a.

Jos a ei jaa lukua b, merkitään $a \nmid b$.

Esimerkki 2.1.2. Pätee $3 \mid 6$, sillä $6 = 2 \cdot 3$. Sen sijaan $4 \nmid 11$, sillä yhtälöllä $11 = k \cdot 4$ ei ole kokonaislukuratkaisua.

Seuraavaksi todistetaan joitakin jaollisuuden perusominaisuuksia.

Propositio 2.1.3. *Olkoon $a \in \mathbb{Z}$. Tällöin:*

(1) $1 \mid a$.
(2) $a \mid a$.
(3) $a \mid 0$.
(4) Jos $0 \mid a$, *niin* $a = 0$.

Todistus. (1) Koska $a = a \cdot 1$ ja $a \in \mathbb{Z}$, on $1 \mid a$.
(2) Koska $a = 1 \cdot a$ ja $1 \in \mathbb{Z}$, on $a \mid a$.
(3) Koska $0 = 0 \cdot a$ ja $0 \in \mathbb{Z}$, on $a \mid 0$.
(4) Jos $0 \mid a$, on $a = k \cdot 0$ jollakin $k \in \mathbb{Z}$. Tällöin $a = 0$. □

Propositio 2.1.3 siis sanoo, että kokonaisluvulla a on ainakin kaksi luonnollisiin lukuihin kuuluvaa tekijää, luvut 1 ja a. Lisäksi a jakaa luvun 0, mutta 0 jakaa luvun a vain jos $a = 0$.

Seuraavista propositioista selviää muita jaollisuuden ominaisuuksia.

Propositio 2.1.4. *Olkoon $a, b, c, m, n \in \mathbb{Z}$. Tällöin:*

(1) Jos $a \mid b$ *ja* $b \mid c$, *niin* $a \mid c$ (transitiivisuus).
(2) Jos $a \mid b$ *ja* $a \mid c$, *niin* $a \mid (mb + nc)$ (lineaarisuus).

Todistus. Harjoitustehtävä. □

Propositio 2.1.5. *Olkoon $a, b, c \in \mathbb{Z}$. Tällöin:*

(1) Jos $b \mid c$, *niin* $ab \mid ac$ (tulo).
(2) Jos $ab \mid ac$ *ja* $a \neq 0$, *niin* $b \mid c$ (supistaminen).

Todistus. (1) Koska $b \mid c$, pätee $c = kb$ jollakin $k \in \mathbb{Z}$. Saadaan

$$ac = a(kb) = k(ab),$$

joten jaollisuuden määritelmän nojalla $ab \mid ac$.

(2) Koska $ab \mid ac$, on $ac = k(ab)$ jollakin $k \in \mathbb{Z}$. Koska $a \neq 0$, saadaan

$$c = \frac{1}{a}(ac) = \frac{1}{a}(kab) = kb,$$

joten jaollisuuden määritelmän nojalla $b \mid c$. □

Todistetaan vielä, että jos nollasta eroava luku b on jaollinen luvulla a (eli a on luvun b tekijä), niin luvun a itseisarvo on korkeintaan sama kuin luvun b itseisarvo.

Propositio 2.1.6. *Olkoot $a, b \in \mathbb{Z}$. Jos $a \mid b$ ja $b \neq 0$, niin $|a| \leq |b|$* (vertailu).

Todistus. Koska $a \mid b$, on $k \in \mathbb{Z}$, jolle $b = ka$. Koska $b \neq 0$, niin $k \neq 0$. Lisäksi koska $k \in \mathbb{Z}$, niin $|k| \geq 1$. Siten

$$|b| = |ka| = |k||a| \geq |a|.$$ □

Jos esimerkiksi halutaan tietää luvun 6 kaikki tekijät, edellisen proposition nojalla riittää tutkia kaikki kokonaisluvut joiden itseisarvo on korkeintaan 6. Luvun 6 tekijät ovat $\pm 1, \pm 2, \pm 3$ ja ± 6.

2.2. **Jakojäännöslause.** Aiemmin todettiin, että $4 \nmid 11$, eli jakolasku $\frac{11}{4}$ ei mene tasan. Voidaan kirjoittaa $11 = 2 \cdot 4 + 3$, missä lukua 3 kutsutaan *jakojäännökseksi*. Toisena esimerkkinä $3 \nmid 16$, ja voidaan kirjoittaa $16 = 5 \cdot 3 + 1$, missä 1 on jakojäännös. Yleisemmin vaikuttaisi, että jos $b \nmid a$, voidaan kirjoittaa $a = kb + r$, missä $k \in \mathbb{Z}$ ja $1 \leq r < |b|$. Tämä tulos on yksi lukuteorian kulmakivistä, kuten kurssin mittaan tulemme näkemään.

Lause 2.2.1 (Jakojäännöslause)**.** *Olkoot $a, b \in \mathbb{Z}$ ja $b \geq 1$. Tällöin on yksikäsitteiset luvut $k, r \in \mathbb{Z}$, joille*

$$a = kb + r \quad ja \quad 0 \leq r < b.$$

Jakoyhtälön luku a on *jaettava*, b *jakaja*, k *(vaillinainen) osamäärä* ja luku r on *jakojäännös*.

Todistus. Tarkastellaan joukkoa

$$A := \{y \geq 0 \ : \ y = a - sb \text{ jollain } s \in \mathbb{Z}\}.$$

Koska $a, b \in \mathbb{Z}$, on $y = a - sb \in \mathbb{Z}$ kaikilla $s \in \mathbb{Z}$. Siis $A \subset \mathbb{Z}$, ja koska lisäksi $y \geq 0$ kaikilla $y \in A$, on $A \subset \mathbb{N}$. Jos $a \geq 0$, niin $a = a - 0 \cdot b \in A$. Jos $a < 0$, niin $a - ab = a(1 - b) \geq 0$, joten tällöin $a - ab \in A$. Siis $A \neq \emptyset$.

Koska joukko A on luonnollisten lukujen epätyhjä osajoukko, luonnollisten lukujen hyvinjärjestysperiaatteen (Lause 1.1.3) nojalla joukossa A on pienin luku. Merkitään $r = \min A$. Tällöin $r \geq 0$ ja $r = a - kb$ jollekin yksikäsitteiselle $k \in \mathbb{Z}$. Jos olisi $r \geq b$, tiedon $b \geq 1$ nojalla pätisi

$$r = a - kb > a - (k + 1)b = r - b \geq 0,$$

jolloin olisi $a-(k+1)b \in A$ ja $a-(k+1)b < r$, mikä ei ole mahdollista. Siis $r < b$.

Olemme osoittaneet, että on sellaiset luvut $0 \leq r < b$ ja $k \in \mathbb{Z}$ että $a = kb + r$. On vielä osoitettava, että nämä luvut ovat yksikäsitteisiä. Tehdään vastaoletus: On myös luvut $0 \leq r' < b$ ja $k' \in \mathbb{Z}$ siten että $a = k'b + r'$, ja $r' \neq r$. Tällöin

$$r - r' = a - kb - a + k'b = (k' - k)b,$$

joten $b \mid (r - r')$. Koska vastaoletuksen nojalla $r - r' \neq 0$, on Proposition 2.1.6 nojalla $b \leq |r - r'|$. Mutta tämä on ristiriita, sillä tiedoista $0 \leq r < b$ ja $0 \leq r' < b$ seuraa, että $-b < r - r' < b$. Siis $r' = r$, joten olemme todistaneet lauseessa vaaditun yksikäsitteisyyden. □

Eräs yksinkertainen mutta tärkeä erikoistapaus jakojäännöslauseesta on, että mikä tahansa luku $a \in \mathbb{Z}$ voidaan esittää muodossa $a = 2k + r$, missä $k \in \mathbb{Z}$ ja $r \in \{0, 1\}$. Jos $r = 0$, luku a on *parillinen*. Jos taas $r = 1$, a on *pariton*. Seuraavassa esimerkissä mainitaan joitakin parillisuuden ja parittomuuden ominaisuuksia. Perusteluihin palataan harjoituksissa.

Esimerkki 2.2.2. (1) Kahden parillisen luvun summa on parillinen.
(2) Parillisen ja parittoman luvun summa on pariton.
(3) Kahden parittoman luvun summa on parillinen.
(4) Jos $a \in \mathbb{Z}$ ja a^2 on parillinen, niin a on parillinen.
(5) Jos $a, b \in \mathbb{Z}$ ja luku ab on pariton, niin sekä a että b ovat parittomia.

Seuraavat esimerkit havainnollistavat lisää jakojäännöslauseen käyttöä.

Esimerkki 2.2.3. Jos a^2 on jaollinen kolmella, onko a väistämättä jaollinen kolmella? Jos a ei ole jaollinen kolmella, se on jakojäännöslauseen nojalla joko muotoa $a = 3k + 1$ tai $a = 3k + 2$ jollakin $k \in \mathbb{Z}$. Saadaan

$$(3k+1)^2 = 3(3k^2 + 2k) + 1 \quad \text{(ei ole jaollinen kolmella)},$$
$$(3k+2)^2 = 3(3k^2 + 4k + 1) + 1 \quad \text{(ei ole jaollinen kolmella)}.$$

Toisaalta, jos a on jaollinen kolmella, eli $a = 3k$ jollakin $k \in \mathbb{Z}$, niin $a^2 = 3(3k^2)$ on jaollinen kolmella. Siis *jos a^2 on jaollinen kolmella, a on jaollinen kolmella.* Opimme edellisestä päättelystä myös seuraavat seikat, jotka ovat hyödyksi seuraavassa esimerkissä:

(1) Jos $a \in \mathbb{Z}$, niin $a^2 = 3k$ tai $a^2 = 3k + 1$ jollakin $k \in \mathbb{Z}$.
(2) Edellisestä kohdasta seuraa, että *minkään kokonaisluvun neliö ei voi olla muotoa $3k + 2$ jollakin $k \in \mathbb{Z}$.*

Esimerkki 2.2.4. Osoitetaan eräs Fermat'n tulos: Ei ole olemassa sellaisia lukuja $a, b, c \in \mathbb{N} \setminus \{0\}$, että

$$a^2 + b^2 = 3c^2. \tag{2.1}$$

Tehdään vastaoletus, että on yhtälön (2.1) toteuttavia lukukolmikkoja a, b, c. Asetetaan

$$A := \{c \in \mathbb{N} \setminus \{0\} \ : \ a^2 + b^2 = 3c^3 \text{ joillakin } a, b \in \mathbb{N} \setminus \{0\}\}.$$

Vastaoletuksen nojalla $A \neq \emptyset$, joten luonnollisten lukujen hyvinjärjestysperiaatteen nojalla joukossa A on pienin luku $c_0 = \min A$. Olkoot $a_0, b_0 \in \mathbb{N}$ ne luvut, joille $a_0^2 + b_0^2 = 3c_0^2$.

Tiedämme, että luku $a_0^2 + b_0^2$ on jaollinen kolmella. Jos a_0 on jaollinen kolmella, luku $b_0^2 = 3c_0^2 - a_0^2$ on jaollinen kolmella, joten edellisen esimerkin nojalla b_0 on jaollinen kolmella. Toisaalta, jos a_0 ei ole jaollinen kolmella, edellisen esimerkin nojalla $a_0^2 = 3k + 1$ jollakin $k \in \mathbb{Z}$. Tällöin

$$b_0^2 = 3c_0^2 - (3k + 1) = 3(c_0^2 - 1) + 3 - 3k - 1 = 3(c_0^2 - 1 - k) + 2,$$

mikä ei edellisen esimerkin nojalla ole mahdollista. Siis a_0 ja b_0 ovat väistämättä jaollisia kolmella. On siis $a_0 = 3a_1$ ja $b_0 = 3b_1$ joillakin $a_1, b_1 \in \mathbb{Z}$. Koska

$$3c_0^2 = a_0^2 + b_0^2 = (3a_1)^2 + (3b_1)^2 = 9(a_1^2 + b_1)^2, \tag{2.2}$$

on luku c_0^2 jaollinen kolmella, joten edellisen esimerkin nojalla c_0 on jaollinen kolmella. Siis $c_0 = 3c_1$ jollakin $c_1 \in \mathbb{Z}$. Sijoittamalla tämä yhtälöön (2.2) saadaan

$$3(3c_1)^2 = 9(a_1^2 + b_1)^2,$$

joka saadaan supistamisen jälkeen muotoon

$$a_1^2 + b_1^2 = 3c_1^2.$$

Nyt siis $c_1 \in A$ ja $c_1 = 3c_0 < c_0$, mikä on ristiriita. Siis ei ole olemassa sellaisia lukuja $a, b, c \in \mathbb{N} \setminus \{0\}$, jotka toteuttavat yhtälön (2.1).

2.3. **Suurin yhteinen tekijä.**

Esimerkki 2.3.1. Oletetaan, että sinulla on käytössä 16 ja 9 litran ämpärit. Pystytkö näiden avulla mittaamaan kolmanteen astiaan tasan litran vettä? Entä jos käytössä olisikin 12 ja 9 litran ämpärit, pystytkö mittaamaan kolmanteen astiaan tasan litran vettä?

Edeltävä esimerkki liittyy *lineaarisiin Diofantoksen yhtälöihin*, jotka puolestaan kytkeytyvät läheisesti käsitteeseen *lukujen suurin yhteinen tekijä*.

Määritelmä 2.3.2. Olkoot $a, b \in \mathbb{Z}$. Jos luvulle $c \in \mathbb{Z}$ pätee $c \mid a$ ja $c \mid b$, sanotaan että c on lukujen a ja b *yhteinen tekijä*.

Mitä tiedämme lukujen a ja b yhteisistä tekijöistä? Tapaus $a = b = 0$ ei ole kiinnostava, koska tällöin Proposition 2.1.3 nojalla kaikki kokonaisluvut ovat lukujen a ja b yhteisiä tekijöitä.

Oletetaan seuraavaksi, että vähintään toinen luvuista a ja b eroaa nollasta. Olkoon vaikka $a \neq 0$. Tällöin Proposition 2.1.6 nojalla kaikki luvun a tekijät ovat itseisarvoltaan korkeintaan luvun $|a|$ suuruisia, joten luvulla a on vain

äärellinen määrä tekijöitä. Siis tässä tapauksessa luvuilla a ja b on äärellinen määrä yhteisiä tekijöitä. Proposition 2.1.3 nojalla luku 1 on lukujen a ja b yhteinen tekijä, joten yhteisten tekijöiden joukko on epätyhjä.

Esimerkki 2.3.3. Lukujen 16 ja 9 yhteiset tekijät ovat 1 ja -1. Lukujen 12 ja 9 yhteiset tekijät ovat 3,1,-1,-3. Lukujen 18 ja 12 yhteiset tekijät ovat 6,3,2,1,-1,-2,-3,-6.

Seuraavaksi osoitamme, että *täsmälleen yksi näistä äärellisen monesta yhteisestä tekijästä on jaollinen kaikilla yhteisillä tekijöillä.*

Lause 2.3.4. *Olkoot $a, b \in \mathbb{Z}$, joista vähintään toinen eroaa nollasta. Tällöin on täsmälleen yksi luku $d \in \mathbb{Z}$, joka toteuttaa seuraavat kolme ehtoa:*

(1) $d \geq 1$.
(2) $d \mid a$ ja $d \mid b$.
(3) Jos luvulle $c \in \mathbb{Z}$ pätee $c \mid a$ ja $c \mid b$, on oltava $c \mid d$.

Todistus. Tarkastellaan joukkoa

$$A := \{c \geq 1 \ : \ c = xa + yb \text{ joillakin } x, y \in \mathbb{Z}\}.$$

Joukkoon A kuuluvat siis kaikki sellaiset luvut $c \geq 1$, jotka voidaan esittää muodossa $xa + yb$ joillakin kokonaisluvuilla $x, y \in \mathbb{Z}$. Samaan tapaan kuin Jakojäännöslauseen todistuksen alussa voidaan päätellä, että $A \subset \mathbb{N}$.

Osoitetaan seuraavaksi, että A ei ole tyhjä joukko, $A \neq \emptyset$. Lauseessa oletetaan, että vähintään toinen luvuista a ja b eroaa nollasta. Oletetaan ensin, että $a \neq 0$. Tällöin $a^2 \geq 1$ ja $a^2 = a \cdot a + 0 \cdot b$, joten luku a^2 voidaan esittää muodossa $xa + yb$ valinnalla $x = a$ ja $y = 0$. Siis $a^2 \in A$. Jos $a = 0$, on oltava $b \neq 0$, ja vastaavalla päättelyllä osoitetaan, että tällöin $b^2 \in A$. Siis $A \neq \emptyset$.

Luonnollisten lukujen hyvinjärjestysperiaatteen nojalla joukossa A on pienin luku. Merkitään tätä pienintä lukua kirjaimella d, siis

$$d = \min A,$$

. Koska $d \in A$, on sellaiset luvut $x_0, y_0 \in \mathbb{Z}$ että

$$d = x_0 a + y_0 b.$$

Osoitetaan, että d on ainoa luku joka toteuttaa lauseen kaikki kolme ehtoa.

Ehto (1). Koska kaikille $a \in A$ pätee $a \geq 1$, ja koska $d \in A$, on $d \geq 1$.

Ehto (2). Osoitetaan ensin, että $d \mid a$. Tehdään *vastaoletus*, että $d \nmid a$. Tällöin jakoyhtälön nojalla $a = kd + r$, missä $1 \leq r < d$. Käyttämällä esitystä $d = x_0 a + y_0 b$ saadaan

$$r = a - kd = a - k(x_0 a + y_0 b) = (1 - kx_0)a + (-ky_0)b.$$

Koska $(1 - kx_0) \in \mathbb{Z}$ ja $-ky_0 \in \mathbb{Z}$, on $r \in A$. Mutta $r < d$, mikä on ristiriita, sillä $d = \min A$. Koska vastaoletus $d \nmid a$ johti ristiriitaan, on $d \mid a$. Vastaavalla

tavalla osoitetaan, että $d \mid b$ (harjoitustehtävä).

Ehto (3). Olkoon $c \in \mathbb{Z}$, $c \mid a$ ja $c \mid b$. Tällöin $a = kc$ ja $b = lc$, $k, l \in \mathbb{Z}$. Saadaan

$$d = x_0 a + y_0 b = x_0(kc) + y_0(lc) = (x_0 k + y_0 l)c,$$

missä $(x_0 k + y_0 l) \in \mathbb{Z}$. Siis $c \mid d$.

Olemme osoittaneet, että luku $d = \min A$ toteuttaa lauseen kaikki kolme ehtoa. Pitää vielä osoittaa, että se on ainoa luku joka toteuttaa ehdot. Olkoon $d' \in \mathbb{Z}$ luku, joka toteuttaa lauseen ehdot 1-3. Koska d' toteuttaa ehdon (2) ja d toteuttaa ehdon (3), on $d' \mid d$. Toisaalta, koska d toteuttaa ehdon (2) ja d' toteuttaa ehdon (3), on $d \mid d'$. Siis $d = kd'$ ja $d' = ld$ joillakin $k, l \in \mathbb{Z}$. Koska $d, d' \in \mathbb{N}$, on oltava $k, l \in \mathbb{N}$. Saadaan

$$d = kd' = k(ld) = (kl)d,$$

ja koska $d \geq 1$, on $kl = 1$. Koska $k, l \in \mathbb{N}$, on oltava $k = 1 = l$. Siis $d' = d$, joten luku $d = \min A$ on ainoa luku joka toteuttaa lauseen ehdot 1-3. □

Seuraus 2.3.5. *Olkoot $a, b \in \mathbb{Z}$, joista vähintään toinen eroaa nollasta, ja olkoon d se yksikäsitteinen luku, joka toteuttaa Lauseen 2.3.4 kolme ehtoa. Jos $c \in \mathbb{Z}$ on lukujen a ja b yhteinen tekijä, on $c \leq d$.*

Todistus. Jos $c \in \mathbb{Z}$ on lukujen a ja b yhteinen tekijä, Lauseen 2.3.4 nojalla on $c \mid d$. Proposition 2.1.6 nojalla $|c| \leq |d| = d$, sillä $d \geq 1$. Siis $c \leq d$. □

Määritelmä 2.3.6. Olkoot a, b, d kuten edellä. Lukua d kutsutaan *lukujen a ja b suurimmaksi yhteiseksi tekijäksi*, ja merkitään $d = \mathrm{syt}(a, b)$.

Kerrataan vielä: Olkoot $a, b \in \mathbb{Z}$, $a \neq 0$ tai $b \neq 0$, ja c jokin lukujen a ja b yhteinen tekijä. Luvulle $\mathrm{syt}(a, b) \in \mathbb{N}$ pätee:

(1) $\mathrm{syt}(a, b) \geq 1$.
(2) $\mathrm{syt}(a, b) \mid a$ ja $\mathrm{syt}(a, b) \mid b$.
(3) $c \leq \mathrm{syt}(a, b)$.
(4) $c \mid \mathrm{syt}(a, b)$.

Esimerkki 2.3.7. $\mathrm{syt}(3, 4) = 1$, $\mathrm{syt}(3, 6) = 3$ ja $\mathrm{syt}(12, 16) = 4$. Nämä voi todeta listaamalla lukujen yhteiset tekijät ja katsomalla, mikä niistä on suurin. Tämä menetelmä on hyvin työläs kun luvut ovat suuria. Mikä on $\mathrm{syt}(245, 693)$? Entä $\mathrm{syt}(1263865, 1263866)$? Seuraava propositio antaa vastauksen jälkimmäiseen.

Propositio 2.3.8. *Olkoon $a \in \mathbb{Z}$. Pätee* $\mathrm{syt}(a, a + 1) = 1$.

Todistus. Olkoon $c \in \mathbb{Z}$ lukujen a ja $a + 1$ yhteinen tekijä. Proposition 2.1.4 kohdan (2) nojalla c jakaa luvun $(a + 1) + (-1)a = 1$. Siten Proposition 2.1.6 nojalla on oltava $|c| \leq 1$. Siis lukujen a ja $a + 1$ yhteiset tekijät ovat 1 ja -1, joten $\mathrm{syt}(a, a + 1) = 1$. □

Pyrimme seuraavaksi vastaamaan seuraaviin kysymyksiin:

(1) Mitä hyötyä on tietää, mikä on kahden kokonaisluvun suurin yhteinen tekijä?
(2) Mikä olisi systemaattinen ja tehokas menetelmä suurimman yhteisen tekijän määrittämiseksi?

Eräs vastaus ensimmäiseen kysymykseen on, että $\text{syt}(a, b)$ liittyy läheisesti lineaarisiin Diofantoksen yhtälöihin.

Määritelmä 2.3.9. Olkoot $a, b, c \in \mathbb{Z}$ annettuja lukuja. Tällöin yhtälöä

$$xa + yb = c \tag{2.3}$$

sanotaan *lineaariseksi Diofantoksen yhtälöksi*. Yhtälöllä (2.3) on *kokonaislukuratkaisu*, mikäli on sellaiset kokonaisluvut $x_0, y_0 \in \mathbb{Z}$, että $x_0a + y_0b = c$.

Esimerkki 2.3.10. Onko lineaarisella Diofantoksen yhtälöllä

$$12x + 9y = 1$$

kokonaislukuratkaisuja? (Tässä siis annetut luvut a, b, c ovat 12,9,1.) Kun x ja y ovat joitakin kokonaislukuja, $12x + 9y$ on jaollinen kolmella, kun taas 1 ei ole jaollinen kolmella, joten kokonaislukuratkaisuja ei ole. Huomaa, että tämä on vastaus kappaleen alun kysymykseen 12 ja 9 litran ämpäreistä.

Entä onko yhtälöllä

$$36x + 60y = 132$$

kokonaislukuratkaisuja? Käy ilmi, että vastaus riippuu luvusta $\text{syt}(36, 60)$.

Lause 2.3.11. *Olkoot $a, b \in \mathbb{Z}$, joista vähintään toinen eroaa nollasta. Tällöin*

$$\{xa + yb \ : \ x, y \in \mathbb{Z}\} = \{k \cdot \text{syt}(a, b) \ : \ k \in \mathbb{Z}\}.$$

Todistus. Merkitään $A := \{xa+yb \ : \ x, y \in \mathbb{Z}\}$ ja $B := \{k\cdot\text{syt}(a, b) \ : \ k \in \mathbb{Z}\}$.

Todistetaan ensin, että $A \subset B$. Olkoon $e \in A$. Tällöin $e = z_1a+z_2b$ joillakin $z_1, z_2 \in \mathbb{Z}$. Koska $\text{syt}(a, b) \mid a$ ja $\text{syt}(a, b) \mid b$, on sellaiset luvut $m, n \in \mathbb{Z}$ että $a = \text{syt}(a, b)m$ ja $b = \text{syt}(a, b)n$. Saadaan

$$e = z_1a + z_2b = (z_1m + z_2n)\,\text{syt}(a, b),$$

missä $(z_1m + z_2n) \in \mathbb{Z}$. Siis $e \in B$, joten $a \subset B$.

Todistetaan seuraavaksi, että $B \subset A$. Lauseen 2.3.4 todistuksesta nähdään, että on sellaiset luvut $x_0, y_0 \in \mathbb{Z}$, että $\text{syt}(a, b) = x_0a + y_0b$. Tästä seuraa, että jos $k \in \mathbb{Z}$, niin

$$k \cdot \text{syt}(a, b) = k(x_0a + y_0b) = (kx_0)a + (ky_0)b,$$

missä $kx_0 \in \mathbb{Z}$ ja $ky_0 \in \mathbb{Z}$. Siis $B \subset A$.

Olemme osoittaneet, että $A = B$. □

Seuraus 2.3.12. *Olkoot $a, b, c \in \mathbb{Z}$ sellaisia annettuja lukuja, että vähintään toinen luvuista a ja b eroaa nollasta. Tällöin yhtälöllä*

$$xa + yb = c$$

on kokonaislukuratkaisuja täsmälleen sillä edellytyksellä, että $\text{syt}(a, b) \mid c$.

Aiemmin kysyttiin, onko yhtälöllä $36x + 60y = 132$ kokonaislukuratkaisuja. Tekijöitä listaamalla voidaan selvittää, että $\text{syt}(36, 60) = 12$. Koska $12 \mid 132$, yhtälöllä on edellisen seurauksen nojalla kokonaislukuratkaisuja. Mitä nämä ratkaisut ovat, ja miten suurin yhteinen tekijä kannattaa selvittää?

2.4. **Eukleideen algoritmi.**

Lemma 2.4.1. *Jos $a, b, q, r \in \mathbb{Z}$, $a \neq 0$ tai $b \neq 0$, ja $a = qb + r$, niin* $\text{syt}(a, b) = \text{syt}(b, r)$.

Todistus. Proposition 2.1.4 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 $\text{syt}(a, b) = \text{syt}(b, r)$. □

Esimerkki 2.4.2. Yritetään selvittää jakoyhtälön ja edellisen lemman avulla $\text{syt}(42, 30)$.

$$\begin{aligned} 42 &= 1 \cdot \underline{30} + \boxed{12} && \Rightarrow \text{syt}(42, 30) = \text{syt}(30, 12) \\ \underline{30} &= 2 \cdot \boxed{12} + \underline{\underline{6}} && \Rightarrow \text{syt}(30, 12) = \text{syt}(12, 6) \\ \boxed{12} &= 2 \cdot \underline{\underline{6}} && \Rightarrow \text{syt}(12, 6) = 6. \end{aligned}$$

Siis $\text{syt}(42, 30) = 6$. Tässä on pähkinänkuoressa Eukleideen algoritmi.

2.4.1. *Eukleideen algoritmi.* Olkoot $a, b \in \mathbb{Z}$, $a \neq 0$. Merkitään $d = \text{syt}(a, b)$. Jos $b = 0$, niin $d = |a|$. Voidaan siis olettaa, että $a, b \neq 0$.

Koska

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

niin voidaan olettaa, että $a, b \in \mathbb{N}$ ja että $a > b$.

Jakamalla a luvulla b jakoyhtälön (Lause 2.2.1) 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 $d = b$ ja voidaan 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 2.4.1 nojalla $\text{syt}(a,b) = \text{syt}(b,r_1)$. Siten, jos $r_2 = 0$, niin $d = r_1$; lopetetaan. 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 antamat jakojäännökset r_i ovat epänegatiisia ja muodostavat aidosti vähenevän jonon,

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

niin jollain n on oltava $r_n = 0$ (korkeintaan b askelta). Viimeiset kaksi vaihetta ovat

$$\begin{aligned} r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, && 0 < r_{n-1} < r_{n-2}, \\ r_{n-2} &= q_n r_{n-1} + r_n, && r_n = 0. \end{aligned} \tag{2.4}$$

Lause 2.4.3 (Eukleideen algoritmi)**.** *Olkoot a, b ja jakojäännökset r_i kuten yllä. Tällöin r_{n-1}, viimeinen positiivinen jakojäännös, on* $\text{syt}(a,b)$.

Todistus. Lemma 2.4.1 sovellettuna ylläoleviin lukujen a, b, r_1, ...,r_{n-3} yhtälöihin kertoo, että

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

Koska yhtälön (2.4) perusteella $r_{n-1} \mid r_{n-2}$, niin $\text{syt}(r_{n-2}, r_{n-1}) = r_{n-1}$. Siten $d = r_{n-1}$. □

Esimerkki 2.4.4. Lasketaan $\text{syt}(22, 60)$ ja etsitään luvut $x, y \in \mathbb{Z}$, joille $\text{syt}(a,b) = xa + yb$. Eukleideen algoritmilla saadaan (seuraa vasemman puolen yhtälöitä)

$$\begin{aligned} 60 &= 2 \cdot \underline{22} + \boxed{16} && 16 = 60 - 2 \cdot 22 \\ \underline{22} &= 1 \cdot \boxed{16} + \underline{\underline{6}} && 6 = 22 - 16 \\ \boxed{16} &= 2 \cdot \underline{\underline{6}} + 4_* && 4 = 16 - 2 \cdot 6 \\ \underline{\underline{6}} &= 1 \cdot 4_* + 2_\sharp && 2 = 6 - 4 \\ 4_* &= 2 \cdot 2_\sharp. \end{aligned}$$

Siten $\text{syt}(22, 60) = 2$. "Peruuttamalla" algoritmissa saadaan (seuraa edellisen oikeanpuoleisia yhtälöitä)

$$\begin{aligned} 2 &= 6 - 4 = 6 - (16 - 2 \cdot 6) = 3 \cdot 6 - 16 = 3(22 - 16) - 16 \\ &= 3 \cdot 22 - 4 \cdot 16 = 3 \cdot 22 - 4(60 - 2 \cdot 22) \\ &= 11 \cdot 22 - 4 \cdot 60. \end{aligned}$$

"Peruuttaminen" Eukleideen algoritmissa antaa siis keinon löytää eräät kertoimet x ja y. Nämä eivät tokikaan ole yksikäsitteiset kertoimet, sillä esimerkiksi myös

$$2 = 71 \cdot 22 - 26 \cdot 60.$$

Keksitkö lisää kertoimia?

2.5. **Diofantoksen yhtälön kaikki ratkaisut.** Oletetaan, että $a, b, c \in \mathbb{Z}$, $a > b \geq 1$. Tähän mennessä tiedämme Diofantoksen yhtälöstä seuraavaa: Yhtälöllä

$$xa + yb = c \tag{2.5}$$

on kokonaislukuratkaisuja täsmälleen sillä edellytyksellä, että $\text{syt}(a, b) \mid c$. Mikäli tämä edellytys toteutuu, eräs kokonaislukuratkaisu yhtälölle (2.5) löydetään seuraavasti: Selvitetään ensin Eukleideen algoritmilla $\text{syt}(a, b)$, ja etsitään sitten peruutusmetodilla sellaiset kokonaisluvut $z_1, z_2 \in \mathbb{Z}$, että

$$z_1 a + z_2 b = \text{syt}(a, b).$$

Koska $\text{syt}(a, b) \mid c$, on sellainen $k \in \mathbb{Z}$ että $c = k \cdot \text{syt}(a, b)$. Saadaan siis yhtälö

$$(kz_1)a + (kz_2)b = c,$$

eli eräs kokonaislukuratkaisu yhtälölle (2.5) on $x_0 = kz_1$ ja $y_0 = z_2$. Tavoitteenamme on nyt löytää tämän yhden kokonaislukuratkaisun x_0, y_0 avulla *kaikki* yhtälön (2.5) kokonaislukuratkaisut. Tarvitsemme kaksi aputulosta, jotka ovat hyödyllisiä myöhemminkin tällä kurssilla.

Lemma 2.5.1. *Olkoot $a, b, c \in \mathbb{Z}$. Jos pätee $a \mid bc$ ja $\text{syt}(a, b) = 1$, niin $a \mid c$.*

Todistus. Koska $\text{syt}(a, b) = 1$, Seurauksen 2.3.12 nojalla on sellaiset kokonaisluvut z_1, z_2 että

$$z_1 a + z_2 b = 1.$$

Kerrotaan puolittain luvulla c, jolloin saadaan

$$(z_1 c)a + z_2(bc) = c.$$

Koska $a \mid bc$, on $bc = ka$ jollakin $k \in \mathbb{Z}$. Saadaan

$$c = (z_1 c)a + z_2(bc) = (z_1 c)a + (z_2 k)a = (z_1 c + z_2 k)a,$$

joten $a \mid c$. □

Lemma 2.5.2. *Olkoot $a, b \in \mathbb{Z}$, vähintään toinen eroaa nollasta. Tällöin*

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

Todistus. Merkitään notaation keventämiseksi $d = \text{syt}(a, b)$ ja

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

On siis osoitettava, että $c = 1$. Koska $\frac{a}{d} \neq 0$ tai $\frac{b}{d} \neq 0$, tiedetään että $c \geq 1$. Riittää siis osoittaa, että $c \leq 1$. Koska c on lukujen $\frac{a}{d} \neq 0$ ja $\frac{b}{d} \neq 0$ yhteinen tekijä, on sellaiset luvut $z_1, z_2 \in \mathbb{Z}$ että

$$\frac{a}{d} = z_1 c, \quad \frac{b}{d} = z_2 c.$$

Siis $a = z_1(cd)$ ja $b = z_2(cd)$. Siis luku cd on lukujen a ja b yhteinen tekijä. Koska $d = \text{syt}(a, b)$, on

$$cd \leq d.$$

Koska $d \geq 1$, voidaan supistaa ja saadaan $c \leq 1$. Siis $c = 1$. □

Lause 2.5.3. *Olkoot $a, b, c \in \mathbb{Z}$, $a \neq 0$ tai $b \neq 0$. Oletetaan, että Diofantoksen yhtälöllä*

$$xa + yb = c \tag{2.6}$$

on kokonaislukuratkaisu x_0, y_0. Tällöin kokonaislukupari z, w on Diofantoksen yhtälön (2.6) *ratkaisu täsmälleen sillä ehdolla, että*

$$z = x_0 + \frac{kb}{\text{syt}(a,b)}, \quad w = y_0 - \frac{ka}{\text{syt}(a,b)} \quad \text{jollakin } k \in \mathbb{Z}. \tag{2.7}$$

Todistus. Oletetaan ensin, että kokonaislukupari z, w toteuttaa ehdon (2.7) jollakin $k \in \mathbb{Z}$. Suoralla laskulla saadaan

$$\begin{aligned} za + wb &= \left(x_0 + \frac{kb}{syt(a,b)}\right) a + \left(y_0 - \frac{ka}{syt(a,b)}\right) b \\ &= x_0 a + y_0 b + \left(\frac{kba}{syt(a,b)} - \frac{kab}{syt(a,b)}\right) \\ &= x_0 a + y_0 b = c, \end{aligned}$$

sillä x_0, y_0 on eräs kokonaislukuratkaisu. Siis jos z, w toteuttaa ehdon (2.7), se on Diofantoksen yhtälön (2.6) eräs ratkaisu.

Oletetaan seuraavaksi, että z, w on Diofantoksen yhtälön (2.6) eräs kokonaislukuratkaisu. Pitää osoittaa, että pari z, w toteuttaa ehdon (2.7) jollakin $k \in \mathbb{Z}$. Koska parit x_0, y_0 ja z, w ovat kokonaislukuratkaisuja, pätee

$$(x_0 - z)a + (y_0 - w)b = x_0 a + y_0 b - (za + wb) = c - c = 0.$$

Siirtämällä termi $(x_0 - z)a$ yhtälön toiselle puolelle ja jakamalla puolittain luvulla $\text{syt}(a, b)$, saadaan

$$(y_0 - w)\frac{b}{\text{syt}(a,b)} = -(x_0 - z)\frac{a}{\text{syt}(a,b)}, \tag{2.8}$$

joten $\frac{b}{\text{syt}(a,b)} \mid -(x_0 - z)\frac{a}{\text{syt}(a,b)}$. Lemmojen 2.5.2 ja 2.5.1 nojalla on $\frac{b}{\text{syt}(a,b)} \mid -(x_0 - z)$. Siis on sellainen $k \in \mathbb{Z}$, että

$$-(x_0 - z) = k\frac{b}{\text{syt}(a,b)},$$

joten

$$z = x_0 + \frac{kb}{\text{syt}(a,b)}.$$

Sijoittamalla tämä yhtälöön (2.8) saadaan ratkaistua

$$w = y_0 - \frac{ka}{\text{syt}(a,b)}.$$

Todistus on valmis. □

3. Alkuluvut

3.1. **Aritmetiikan peruslause.**

Määritelmä 3.1.1. Luonnollinen luku $a \geq 2$ on *alkuluku* (*prime*), jos sen ainoat positiiviset tekijät ovat 1 ja a. Luonnollista lukua $b \geq 2$, joka ei ole alkuluku, sanotaan *yhdistetyksi luvuksi* (*composite*).

Yleensä mielivaltaisesti valittua alkulukua merkitään kirjaimella p, ja jos valitaan n kappaletta alkulukuja, ne nimetään useimmiten $p_1, p_2, ..., p_n$.

Huomautus 1.

(1) Luku 1 ei ole alkuluku eikä yhdistetty luku, vaan se on kokonaan tämän jaottelun ulkopuolella.
(2) Edellisen määritelmän nojalla joukko $\mathbb{N}\backslash\{0,1\}$ on yhdiste kahdesta keskenään pistevieraasta joukosta: kaikkien alkulukujen joukosta ja kaikkien yhdistettyjen lukujen joukosta.
(3) 2 on ainoa parillinen alkuluku. (Mieti miksi!)

Esimerkki 3.1.2.

(a) Kymmenen esimmäistä alkulukua ovat $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.
(b) Luku 4 ei ole alkuluku, sillä $2 \mid 4$. Luku 9 ei ole alkuluku, sillä $3 \mid 9$.

Esimerkki 3.1.3. Tarkastellaan seuraavaa lemmaa silmälläpitäen paria yhdistettyä lukua. Heuristisesti puhuen puramme ne osiin vähän kuin purkaisimme legorakennelman yksittäisiin legopalikoihin asti.

Luku 20 on yhdistetty luku, koska se on jaollinen esimerkiksi kakkosella, $20 = 2 \cdot 10$. Luku 2 on alkuluku, mutta luku 10 on edelleen yhdistetty luku, $10 = 2 \cdot 5$. Siis

$$20 = 2^2 \cdot 5,$$

joten luku 20 voidaan esittää alkulukujen tulona.

Luku 504 on yhdistetty luku, koska se on jaollinen esimerkiksi kakkosella,

$$504 = 2 \cdot 252 = 2^2 \cdot 126 = 2^3 \cdot 63.$$

Luku 63 ei ole enää jaollinen kakkosella, mutta se on jaollinen kolmosella,

$$2^3 \cdot 63 = 2^3 \cdot 3 \cdot 21 = 2^3 \cdot 3^2 \cdot 7.$$

Siis luku 504 voidaan esittää alkulukujen tulona.

Lemma 3.1.4. *Olkoon $n \geq 2$ luonnollinen luku. Tällöin n on alkuluku tai alkulukujen tulo.*

Todistus. Todistetaan väite induktiolla. (Koska väite koskee lukua 2 suurempia luonnollisia lukuja, niin induktiotodistuksen ensimmäisessä vaiheessa tarkastetaan, että väite on totta luvulle $n = 2$.)

(1) Koska 2 on alkuluku, niin väite on totta kun $n = 2$.

(2) Olkoon $k \in \mathbb{N}$, $k \geq 2$. Oletetaan, väite on totta luvuille $2, \ldots, k$. Pitää näyttää, että väite on totta luvulle $k+1$. Jos $k+1$ on alkuluku, asia on selvä. Jos $k+1$ ei ole alkuluku, niin sillä on positiivinen tekijä $d \in \mathbb{N}$, $d \neq 1$, $d \neq (k+1)$. Proposition 2.1.6 nojalla on oltava $1 < d < k+1$, ja on luonnollinen luku $1 < m < k+1$ siten että

$$k + 1 = md.$$

Induktio-oletuksen nojalla m ja d voidaan esittää alkulukujen tulona (tai ne ovat alkulukuja). Siten myös $k + 1$ on alkulukujen tulo.

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

Onko jokaisella yhdistetyllä luvulla järjestystä vaille *yksikäsitteinen* esitys alkulukujen tulona? Termillä "järjestystä vaille"tarkoittaa, että esimerkiksi $2^2 \cdot 5$ on järjestystä vaille sama alkulukujen tulo kuin $5 \cdot 2^2$.

Oletetaan, että yhdistetty luku a voidaan ilmaista keskenään erisuurten alkulukujen $p_1, ..., p_n$ tulona,

$$a = p_1^{c_1} \cdots p_n^{c_n}, \quad c_1, ..., c_n \in \mathbb{N} \setminus \{0\}.$$

Oletetaan myös, että sama luku a voidaan esittää keskenään erisuurten alkulukujen $q_1, ..., q_m$ tulona,

$$a = q_1^{d_1} \cdots q_m^{d_m}, \quad d_1, ..., d_m \in \mathbb{N} \setminus \{0\}.$$

Lihavoitu kysymyksemme kuuluu: Päteekö väistämättä $n = m$ ja

$$p_1^{c_1} = q_{j_1}^{d_{j_1}},\ p_2^{c_2} = q_{j_2}^{d_{j_2}}, ...,\ p_n^{c_n} = q_{j_n}^{d_{j_n}}, \quad \text{missä} \quad \{j_1, j_2, ..., j_n\} = \{1, 2, ..., n\}?$$

Siis, ovatko luvun a kaksi esitystä alkulukujen tuloina järjestystä vaille sama esitys? Vastaus on kyllä. Tämä on aritmetiikan peruslause. Enne sitä tarvitsemme lemman.

Lemma 3.1.5 (Eukleideen lemma)**.** *Olkoon p alkuluku ja olkoot $a, b \in \mathbb{Z}$. Jos $p \mid (ab)$, niin $p \mid a$ tai $p \mid b$. Yleisemmin, jos $p \mid (a_1 \cdots a_n)$, missä $a_i \in \mathbb{Z}$ kaikilla $i = 1, \ldots, n$, niin $p \mid a_i$ jollain i. Lisäksi, jos $p, p_1, p_2, \ldots, p_n$ ovat alkulukuja siten, että $p \mid (p_1 \cdots p_n)$, niin $p = p_i$ jollain $i = 1, \ldots, n$.*

Todistus. Jos $p \mid (ab)$ ja $p \nmid a$, on $\text{syt}(p, a) = 1$, ja Lemman 2.5.1 nojalla $a \mid b$.

Todistetaan seuraavaksi induktiolla, että jos $p \mid (a_1 \cdots a_n)$, niin $p \mid a_i$ jollain i. Alkuaskel $n = 1$ on selvä. Tehdään induktio-oletus, että jos $p \mid (a_1 \cdots a_k)$, niin $p \mid a_i$ jollakin $i = 1, ..., k$. Induktioväite on, että jos $p \mid (a_1 \cdots a_{k+1})$, niin $p \mid a_i$ jollakin $i = 1, ..., k+1$. Oletetaan siis, että $p \mid (a_1 \cdots a_{k+1})$. Merkitään $a = a_1 \cdots a_k$ ja $b = a_{k+1}$. Tällöin aiemman nojalla joko $p \mid b$, jolloin asia on selvä, tai $p \mid a$, jolloin induktioväite seuraa induktio-oletuksesta.

Oletetaan lopuksi, että $p \mid (p_1 \cdots p_n)$. Tällöin edellisen nojalla $p \mid p_i$ jollain $i = 1, ..., n$. Siis eräs luvun p_i tekijä on p, ja koska luvun p_i ainoat positiiviset tekijät ovat 1 ja p_i, on oltava $p = p_i$.

□

Lause 3.1.6 (Aritmetiikan peruslause)**.** *Jokainen luonnollinen luku $n \geq 2$ on joko alkuluku tai voidaan esittää alkulukujen tulona. Tämä esitys on tekijöiden järjestystä vaille yksikäsitteinen.*

Todistus. Olkoon $n \in \mathbb{N}$, $n \geq 2$. Lemman 3.1.4 perusteella n on alkuluku tai alkulukujen tulo. Näytetään, että n voidaan esittää yksikäsitteisellä tavalla tulona

$$n = p_1^{e_1} \cdots p_r^{e_r},$$

missä $p_1, \ldots p_r$ ovat alkulukuja, $p_i \neq p_j$ kun $i \neq j$ ja $e_i \in \mathbb{N} \setminus \{0\}$ kaikilla $i = 1, \ldots r$. Todistetaan esityksen yksikäsitteisyys induktiolla luvun n suhteen.

(1) Koska luku $n = 2$ on alkuluku, väite on totta kun $n = 2$.

(2) Oletetaan, että esitys on yksikäsitteinen luonnollisilla luvuilla $2, 3, \ldots, k$. Pitää näyttää, että tällöin myös luvulla $k + 1$ on yksikäsitteinen esitys. Jos $k + 1$ on alkuluku, asia on kunnossa

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

$$k + 1 = p_1^{e_1} \cdots p_r^{e_r} = q_1^{f_1} \cdots q_s^{f_s}. \tag{3.1}$$

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

Numeroimalla luvut q_j tarvittaessa uudelleen voidaan olettaa, että $p_1 \mid q_1$. Koska p_1 ja q_1 ovat alkulukuja, niin on $p_1 = q_1$. Jakamalla (3.1) luvulla p_1 saadaan

$$\tfrac{k+1}{p_1} = p_1^{e_1 - 1} \cdots p_r^{e_r} = q_1^{f_1 - 1} \cdots q_s^{f_s}.$$

Koska $p_1 \geq 2$, on $\frac{k+1}{p_1} \leq k$. Induktio-oletuksen mukaan luvulla $(k + 1)/p_1$ on (järjestystä vailla) yksikäsitteinen esitys alkulukujen tulona. Järjestämällä tarvittaessa luvut p_i ja q_j suuruusjärjestykseen saadaan, että $r = s$, $p_i = q_i$ ja $e_i = f_i$ kaikilla $i = 1, \ldots, r$.

Siten myös esitys (3.1) on yksikäsitteinen. Väite seuraa induktioperiaatteesta. □

Huomautus 2. Äskeisessä todistuksessa käytettiin epäyhtälöä:

$$\tfrac{k+1}{p} \leq \tfrac{k+1}{2} \leq k,$$

missä p on alkuluku ja $k \in \mathbb{N}$, $k \geq 2$. Todistus on helppo harjoitustehtävä.

Määritelmä 3.1.7. Aritmetiikan peruslauseen antamaa yhdistetyn luvun $n \in \mathbb{N}$, $n \geq 2$ yksikäsitteistä esitystä alkulukujen tulona sanotaan luvun n *alkutekijäesitykseksi*. Esityksessä olevat alkuluvut ovat luvun n *alkutekijöitä*.

Huomautus 3. Alkutekijäesityksen yksikäsitteisyys on syy siihen, että lukua 1 ei kutsuta alkuluvuksi.

Alkutekijäesityksen löytäminen isoille luvuille voi olla hankalaa. Seuraava tulos helpottaa tekijöiden löytämistä.

Lemma 3.1.8. *Olkoon $n \in \mathbb{N}$, $n \geq 2$. Luku n on yhdistetty luku täsmälleen sillä ehdolla että 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 on $p \leq \sqrt{n}$. □

Alkutekijäesityksen avulla voidaan helposti todistaa esimerkikisi luvun $\sqrt{2}$ irrationaalisuus. Muista, että luku x on rationaaliluku jos $x = n/m$ jollain $n, m \in \mathbb{Z}$, $m \neq 0$.

Seuraus 3.1.9. *Olkoot $n, a \in \mathbb{N} \setminus \{0\}$. Jos $\sqrt[n]{a}$ on rationaaliluku, niin $\sqrt[n]{a}$ on luonnollinen luku, erityisesti $a = r^n$ jollain $r \in \mathbb{N} \setminus \{0\}$.*

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

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

Voidaan olettaa, että $\text{syt}(r, s) = 1$ (jos ei, niin supistetaan). Näytetään, että $s = 1$. Jos olisi $s > 1$, niin olisi alkuluku p, jolle $p \mid s$. Tällöin p jakaisi tulon $as^n = r^n$. Siten Eukleideen lemman perusteella $p \mid r$. Tämä on mahdotonta, sillä $\text{syt}(r, s) = 1$ ja p on alkuluku. On siis $s = 1$ ja siten $\sqrt[n]{a} = r$. □

Alkuluvut tarjoavat uuden tavan nähdä kahden luvun suurin yhteinen tekijä.

Lause 3.1.10. *Olkoot $a, b \geq 2$ kokonaislukuja,*

$$a = \prod_{i=1}^{n} p_i^{e_i} \quad ja \quad b = \prod_{i=1}^{n} p_i^{f_i}$$

missä luvut $p_1, ..., p_n$ ovat eri alkulukuja ja $e_i, f_i \geq 0$ ovat kokonaislukuja. Tällöin

$$\text{syt}(a, b) = \prod_{i=1}^{n} p_i^{u_i}, \quad \text{missä } u_i = \min\{e_i, f_i\} \text{ kaikilla } i = 1, 2, \ldots, n$$

Katsotaan ennen todistusta esimerkkiä.

Esimerkki 3.1.11. Olkoot

$$a = 30 = 2 \cdot 3 \cdot 5 = 2 \cdot 3 \cdot 5 \cdot 7^0 \quad \text{ja}$$
$$b = 140 = 2^2 \cdot 5 \cdot 7 = 2^2 \cdot 3^0 \cdot 5 \cdot 7.$$

Nyt

$$\text{syt}(a, b) = 2^1 \cdot 3^0 \cdot 5^1 \cdot 7^0 = 10.$$

Lauseen 3.1.10 todistus. Olkoon $d = \prod_{i=1}^{n} p_i^{u_i}$, missä $u_i = \min\{e_i, f_i\}$ kaikilla $i = 1, 2, \ldots, n$. Koska $u_i \leq e_i$ ja $u_i \leq f_i$ kaikilla $i = 1, 2, \ldots, n$, niin $d \mid a$ ja $d \mid b$. Siispä d on lukujen a ja b yhteinen tekijä.

Jos myös f on yhteinen tekijä, eli $f \mid a$ ja $f \mid b$, niin on $|f| = \prod_{i=1}^{n} p_i^{c_i}$, missä $c_i \leq e_i$ ja $c_i \leq f_i$ kaikilla $i = 1, 2, \ldots, n$. Mutta nyt $u_i = \min\{e_i, f_i\} \geq c_i$ kaikilla $i = 1, 2, \ldots, n$, joten $|f| \mid d$ eli $f \mid d$. Näin ollen $f \leq d$, ja siis d on yhteisistä tekijöistä suurin: $d = \text{syt}(a, b)$.

□

3.2. **Alkulukujen esiintymistiheydestä.** Tässä luvussa tutkitaan, kuinka paljon alkulukuja on ja kuinka ne sijoittuvat luonnollisten lukujen joukkoon.

Lause 3.2.1 (Eukleides)**.** *Alkulukuja on äärettömän monta.*

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

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

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

Nyt $N \in \mathbb{N}$ ja $N > 2$, joten se on Lemman 3.1.4 mukaan joko alkuluku tai alkulukujen tulo. Jos N on alkuluku, on löydetty alkuluku, joka on kaikkia lukuja $p_1, p_2, \ldots, p_n$ aidosti suurempi.

Jos N ei ole alkuluku, niin sillä on alkulukutekijä q. Jos $q = p_i$ jollain i, niin Proposition 2.1.4 perusteella q jakaisi luvun $N - p_1 \cdots p_n = 1$, mikä on mahdotonta. Siten $q \neq p_i$ kaikilla $i = 1, \ldots, n$. □

Huomautus 4. Luku $N = p_1 \cdots p_n + 1$ **ei** välttämättä ole alkuluku. Esimerkiksi jos $p_1 = 3$ 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.

Huomaa, että jos luku 2 ei ole alkulukujen $p_1, p_2, \ldots p_n$ joukossa, niin tulo $p_1 \cdots p_n$ on pariton (harjoitustehtävä). Tällöin $N = p_1 \cdots p_n + 1$ on parillinen eikä siten ole alkuluku.

Esimerkki 3.2.2. Lauseen 3.2.1 todistusmenetelmä toimii muissakin tilanteissa. Näytetään seuraavaksi, että muotoa

$$4n + 3, \quad n \in \mathbb{N} \setminus \{0\},$$

olevia alkulukuja on äärettömän monta. Olkoot $p_1, \ldots, p_k$ muotoa $4n+3$ olevia alkulukuja. Määritellään

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

Luku N on muotoa $4n + 3$. Se ei ole jaollinen millään luvuista p_i, $i = 1, \ldots, k$, eikä luvuilla $2, 3$. (Miksi ei?)

Lauseen 3.1.6 nojalla $N = q_1 \cdots q_s$, missä luvut q_i ovat alkulukuja. Näytetään, että jokin luvun N alkutekijöistä q_i on muotoa $4n + 3$.

Jakoyhtälön perusteella kaikilla $i = 1, \ldots, s$ on $n_i, r_i \in \mathbb{Z}$, joille

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

Koska N ei ole jaollinen luvulla 2, niin r_i ei voi olla 0 eikä 2. Jos olisi $r_i = 1$ kaikilla $i = 1, \ldots s$, niin N olisi muotoa $4n + 1$ olevien lukujen tulona myös muotoa $4n + 1$ (harjoitustehtävä).

Siten on oltava $q_i = 4n_i + 3$ jollain $i = 1, \ldots s$. Koska luvut $p_1, \ldots p_k$ eivät ole luvun N tekijöitä, niin q_i ei ole mikään luvuista p_i.

Olkoot n ensimmäistä alkulukua $p_1, p_2, \ldots, p_n$. Seuraava tulos antaa karkean ylärajan luvulle p_n.

Seuraus 3.2.3. *Olkoon $n \in \mathbb{N} \setminus \{0\}$. Tällöin $p_n \leq 2^{2^{n-1}}$.*

Todistus. Todistetaan induktiolla luvun n suhteen.
(1) Kun $n = 1$, niin $p_1 = 2 = 2^{2^0}$.
(2) Oletetaan, että arvio on totta luvuille $p_1, \ldots, p_n$. Kuten Lauseen 3.2.1 todistuksessa, huomataan, että luvulla

$$p_1 \cdots p_n + 1$$

on alkutekijä p ja että $p \neq p_i$ kaikilla $i = 1, \ldots, n$. Koska alkuluku p ei ole n:n ensimmäisen alkuluvun joukossa, niin $p_{n+1} \leq p$. Induktio-oletusta ja geometrisen sarjan osasummaa käyttämällä saadaan

$$\begin{aligned} p_{n+1} \leq p \leq p_1 \cdots p_n + 1 &\leq 2^{2^0} \cdot 2^{2^1} \cdots 2^{2^{n-1}} + 1 \\ &= 2^{1+2+4+\cdots+2^{n-1}} + 1 = 2^{2^n - 1} + 1 \\ &= \frac{1}{2} \cdot 2^{2^n} + 1 \leq 2^{2^n}. \end{aligned}$$

Siten väite on totta kaikille $n \in \mathbb{N} \setminus \{0\}$. □

Seuraavaksi tarkastellaan luonnollisten lukujen joukossa esiintyviä reikiä alkulujen välillä ja alkulukujen esiintymistiheyttä. Huomataan, että alkulukujen välissä on sekä pieniä että suuria aukkoja.

Lause 3.2.4. *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

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

on $n-1$ kappaletta. Nyt

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

on jaollinen luvulla 2,

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

on jaollinen luvulla 3, ja yleisesti

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

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

3.3. **Harrastemateriaalia.** Määritellään funktio $\pi : [0, \infty) \to \mathbb{N} \cup \{0\}$,

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

missä $\sharp$ tarkoittaa lukumäärää. Annetulle luvulle x, $\pi(x)$ kertoo siis välillä $[0, x]$ olevien alkulukujen lukumäärän (prime counting function). Tällä funktiolla ei ole mitään tekemistä vakion π kanssa.

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

Huomautus 5. Jos p_n on n. alkuluku, niin $\pi(p_n) = n$. Toisaalta $p_{\pi(n)} = n$ jos ja vain jos n on alkuluku.

Jos jaetaan $\pi(x)$ eli alkulukujen määrä välillä $[0, x]$ välin pituudella x, niin saadaan alkulukujen esiintymistiheys tällä välillä.

Esimerkki 3.3.1.

x	2	7	25	100	500	5000
$\pi(x)$	1	4	9	25	95	669
$\frac{\pi(x)}{x}$	$0,5$	$\sim 0,57$	$0,36$	$0,25$	$0,19$	$\sim 0,13$

Huomaa, että

$$\pi(101)/101 = 26/101 \sim 0,257 > 0,25 = \pi(100)/100.$$

Koska alkulukuja on äärettömän monta, niin $\pi(x) \to \infty$ kun $x \to \infty$. Alkulukujen tiheys $\pi(x)/x$ lähestyy nollaa kun x lähestyy ääretöntä. Seuraava lause kertoo, että tiheyden lasku on hidasta; $\pi(x)/x$ lähestyy nollaa yhtä hitaasti kuin $1/\log(x)$.

Lause 3.3.2 (Alkulukulause (prime number theorem))**.**

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

Todistus. Vaikea. □

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

(1) Kirjoitetaan luonnolliset luvut (> 1), jotka ovat pienempiä tai yhtäsuuria kuin x.
(2) Poistetaan ensimmäisen alkuluvun eli luvun 2 monikerrat.
(3) Poistetaan toisen alkuluvun eli luvun 3 monikerrat.
(4) Poistetaan kolmannen alkuluvun eli luvun 5 monikerrat.
(5) Jatketaan ... jäljelle jääneet luvut ovat lukua x pienemmät alkuluvut.

Huomaa, että Lemman 3.1.8 nojalla riittää käydä läpi lukua $\sqrt{x}$ pienemmät alkuluvut.

Esimerkki 3.3.3. Etsitään alkuluvut p, joille $p \leq 37$. Riittää käydä läpi alkuluvut $p < 7$, sillä $6^2 = 36 < 37 < 49 = 7^2$.

	2	3	$\boxed{4}$	5	$\boxed{\bar{6}}$	7	$\boxed{8}$	$\bar{9}$	$\boxed{10}$
11	$\boxed{\bar{12}}$	13	$\boxed{14}$	$\bar{15}_*$	$\boxed{16}$	17	$\boxed{\bar{18}}$	19	$\boxed{20_*}$
$\bar{21}$	$\boxed{22}$	23	$\boxed{\bar{24}}$	25_*	$\boxed{26}$	$\bar{27}$	$\boxed{28}$	29	$\boxed{\bar{30}_*}$
31	$\boxed{32}$	$\bar{33}$	$\boxed{34}$	35_*	$\boxed{\bar{36}}$	37			

4. Kongruenssi

Kongruenssi mahdollistaa jaollisuuteen liittyvien asioiden käsittelyn tavalla, joka muistuttaa yhtälöiden käsittelyä. Kongruenssiaritmetiikkaa kutsutaan joskus myös "kellotauluaritmetiikaksi".

4.1. Kongruenssin perusominaisuuksia.

Määritelmä 4.1.1. Olkoon $n \in \mathbb{N} \setminus \{0\}$ ja olkoot $a, b \in \mathbb{Z}$. Luku a on *kongruentti luvun b kanssa modulo n*, merkitään

$$a \equiv b \pmod{n},$$

jos $n \mid (a-b)$. Jos $n \nmid (a-b)$, niin merkitään $a \not\equiv b \pmod{n}$. Lukua n sanotaan *moduliksi*.

Merkintä $a \equiv b \pmod{n}$ tarkoittaa siis, että $a - b = kn$ jollain $k \in \mathbb{Z}$.

Seuraava propositio on hyvä lämmittely-harjoitustehtävä kongruenssista. Se sanoo, että a on kongruentti luvun b kanssa modulo n täsmälleen sillä ehdolla, että luvuilla a ja b on sama jakojäännöslauseen antama jakojäännös $0 \leq r < n$ jaettaessa luvulla n.

Propositio 4.1.2. *Olkoon $n \in \mathbb{N}\backslash\{0\}$ ja $a, b \in \mathbb{Z}$. Tällöin $a \equiv b \pmod{n} \iff$ On luvut $k, l, r \in \mathbb{Z}$, $0 \leq r < n$, joille $a = kn + r$ ja $b = ln + r$.*

Todistus. Harjoitustehtävä. □

Esimerkki 4.1.3.

(a) $19 \equiv 7 \pmod{12}$, $1 \equiv -1 \pmod{2}$, $8 \equiv 1 \pmod{7}$.
(b) $n \in \mathbb{Z}$ on parillinen jos ja vain jos $n \equiv 0 \pmod{2}$.
(c) $n \in \mathbb{Z}$ on pariton jos ja vain jos $n \equiv 1 \pmod{2}$.
(d) $a \equiv b \pmod{1}$ kaikilla $a, b \in \mathbb{Z}$,
(e) Olkoon $n \in \mathbb{N} \setminus \{0\}$ ja $a, b \in \mathbb{Z}$. Jos $a \equiv b \pmod{n}$ ja $d \in \mathbb{N}$ on luvun n tekijä, niin $a \equiv b \pmod{d}$ (Harjoitustehtävä).
(f) Kello; minuutit modulo 60 ja tunnit modulo 12 tai 24, esimerkiksi $40 + 35 \equiv 15 \pmod{60}$, $19 + 7 \equiv 2 \pmod{24}$ ja $10 + 5 \equiv 3 \pmod{12}$.

Lause 4.1.4. *Olkoon $n \in \mathbb{N} \setminus \{0\}$ ja $a, b, c \in \mathbb{Z}$. Tällöin pätee:*

(1) $a \equiv a \pmod{n}$ (refleksiivisyys),
(2) jos $a \equiv b \pmod{n}$, niin $b \equiv a \pmod{n}$ (symmetrisyys),
(3) jos $a \equiv b \pmod{n}$ ja $b \equiv c \pmod{n}$, niin $a \equiv c \pmod{n}$ (transitiivisuus).

Näiden ominaisuuksien vuoksi sanotaan, että kongruenssi on joukon $\mathbb{Z}$ *ekvivalenssirelaatio.*

Todistus. Kohdat 1-3 seuraavat jaollisuuden ominaisuuksista (katso Propositiot 2.1.3 ja 2.1.4).

(1) $n \mid 0$,
(2) jos $n \mid (a - b)$, niin $n \mid (b - a)$,
(3) jos $n \mid (a - b)$ ja $n \mid (b - c)$, niin n jakaa luvun $(a - b) + (b - c) = a - c$.

□

Seuraava lause kertoo, kuinka **saman modulin** kongruensseja voidaan laskea yhteen ja kertoa.

Lause 4.1.5 (Laskusäännöt)**.** *Olkoon $n \in \mathbb{N} \setminus \{0\}$ 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. Jaollisuuslauseen 2.1.4 perusteella saadaan:

(1) Koska $n \mid (a - b)$ ja $n \mid (c - d)$, niin n jakaa luvun

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

(2) ja luvun

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

(3) Induktiolla: jos $m = 0$, niin OK. Oletetaan, että $a^m \equiv b^m \pmod{n}$. Valitsemalla kohdassa (2) $c = a$ ja $d = b$, saadaan

$$a^m a \equiv b^m b \pmod{n} \text{ eli } a^{m+1} \equiv b^{m+1} \pmod{n}.$$

Induktioperiaatteen nojalla väite on totta kaikilla $m \in \mathbb{N}$.

□

Huomautus 4.1.6. *Lauseesta 4.1.5 seuraa, että*

(1) (induktiolla)

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

jos $a_i \equiv b_i \pmod{n}$ *kaikilla* $i = 1, \ldots, k$.

(2) kongruenssin molemmille puolille voi lisätä minkä tahansa kokonaisluvun. Siis jos $a, b, a_0 \in \mathbb{Z}$ *ja* $n \in \mathbb{N}$, *niin* $a \equiv b \pmod{n}$ *jos ja vain jos* $a + a_0 \equiv b + a_0 \pmod{n}$. *(Muista refleksiivisyys: Lause 4.1.4* (1)*).*

Esimerkki 4.1.7.

(a) Koska $2 \equiv 5 \pmod{3}$, niin Lauseen 4.1.5 perusteella $2^{100} \equiv 5^{100} \pmod{3}$. Edelleen, Lauseista 4.1.4 ja 4.1.5 seuraa, että

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

(b) Mikä on luvun 2011^{2001} viimeinen numero 10–järjestelmässä? Nyt

$$2011 \equiv 1 \pmod{10},$$

joten

$$(2011)^{2001} \equiv 1^{2001} \equiv 1 \pmod{10}.$$

Niinpä viimeinen numero on 1.

(c) Olkoon $n \in \mathbb{N}$, olkoot $a, b \in \mathbb{Z}$ ja olkoon P kokonaislukukertoiminen polynomi,

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

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

Perustelu: Koska $a \equiv b \pmod{n}$, niin Lauseen 4.1.5 perusteella $a^i \equiv b^i \pmod{n}$ kaikilla $i \in \mathbb{N}$. Edelleen, Lauseesta 4.1.5 seuraa, että $c_i a^i \equiv c_i b^i \pmod{n}$ kaikilla i ja että $\sum_{i=0}^{k} c_i a^i \equiv \sum_{i=0}^{k} c_i b^i \pmod{n}$. Siten $P(a) \equiv P(b) \pmod{n}$. Jos kokonaislukukertoimisella polynomilla P on juuri $a \in \mathbb{Z}$, niin $P(a) \equiv 0 \pmod{n}$ kaikilla $n \in \mathbb{N}$.

(d) Kongruensseja **ei** yleensä voi jakaa: $14 \equiv 8 \pmod{6}$, mutta $7 \not\equiv 4 \pmod{6}$. Lukua 2 ei siis voi supistaa pois.

Seuraava tulos kertoo, miten kongruensseja voi/saa jakaa.

Lause 4.1.8 (Supistussääntö)**.** *Olkoon $n \in \mathbb{N} \setminus \{0\}$ ja olkoot $a, b, c \in \mathbb{Z}$ lukuja, joille $ac \equiv bc \pmod{n}$. Jos $\text{syt}(n, c) = 1$, niin $a \equiv b \pmod{n}$. Yleisemmin, jos $d = \text{syt}(n, c)$, niin*

$$a \equiv b \pmod{\tfrac{n}{d}}.$$

Todistus. Todistetaan tapaus $d = 1$ (yleinen tapaus on harjoitustehtävä). Pitää siis näyttää, että $n \mid (a - b)$. Oletuksen mukaan $ac \equiv bc \pmod{n}$, joten $n \mid c(a - b)$. Koska $\text{syt}(n, c) = 1$, niin Lemman 2.5.1 perusteella $n \mid (a - b)$. On siis $a \equiv b \pmod{n}$. □

4.2. **Jaollisuussääntöjä kongruenssien avulla.** Onko luku $n \in \mathbb{N}$,

$$n = a_s 10^s + a_{s-1} 10^{s-1} + \cdots + a_1 10 + a_0,$$

jaollinen luvulla $t \in \mathbb{N}$?

Esimerkki 4.2.1. Kolmella jaollisuus perustellaan seuraavasti: Koska $10 \equiv 1 \pmod{3}$, niin Lauseen 4.1.5 (3) perusteella $10^k \equiv 1 \pmod{3}$ kaikilla $k \in \mathbb{N}$. Koska Lauseen 4.1.5 ja Huomautuksen 4.1.6 perusteella on

$$a_s 10^s + \cdots + a_1 10 + a_0 \equiv a_s + \cdots + a_1 + a_0 \pmod{3},$$

niin n on jaollinen luvulla 3 jos ja vain jos sen numerosumma on jaollinen luvulla 3. Siis esimerkiksi 2018 ei ole jaollinen kolmella, sillä $2 + 0 + 1 + 8 = 11$ ei ole jaollinen kolmella. Vastaava perustelu toimii luvulla 9 jaollisuudelle, sillä $10 \equiv 1 \pmod{9}$.

Esimerkki 4.2.2. Neljällä jaollisuus: Koska $10^k \equiv 0 \pmod{4}$ kaikilla $k \in \mathbb{N}$, $k \geq 2$, niin Lauseen 4.1.5 ja Huomautuksen 4.1.6 perusteella on

$$a_s 10^s + \cdots + a_2 10^2 + a_1 a_0 \equiv (a_s + \cdots + a_2) \cdot 0 + (a_1 10 + a_0) \pmod{4},$$

eli $n \equiv a_1 10 + a_0 \pmod{4}$. Siten $4 \mid n$ jos ja vain jos 4 jakaa luvun $10a_1 + a_0$.

Toisaalta koska $10 \equiv 2 \pmod{4}$, niin

$$a_s 10^s + \cdots + a_1 10 + a_0 \equiv (a_s + \cdots + a_2) \cdot 0 + (a_1 2 + a_0) \pmod{4},$$

eli $n \equiv 2a_1 + a_0 \pmod{4}$. Siten $n \mid 4$ jos ja vain jos 4 jakaa luvun $2a_1 + a_0$. Näin saatiin toinen sääntö luvulla 4 jaollisuudelle.

4.3. **Kongruenssiluokista.** Lauseen 4.1.4 perusteella kongruenssi on ekvivalenssirelaatio joukossa $\mathbb{Z}$. Ekvivalenssirelaatio jakaa joukon $\mathbb{Z}$ erillisiin ekvivalenssiluokkiin, joita kongruenssin tapauksessa kutsutaan *kongruenssiluokiksi* tai *jäännösluokiksi modulo n.*

Määritelmä 4.3.1. Olkoon $n \in \mathbb{N} \setminus \{0\}$ ja olkoon $a \in \mathbb{Z}$. Joukko

$$[a]_n = \left\{ b \in \mathbb{Z} \mid a \equiv b \pmod{n} \right\}$$

on luvun *a määräämä kongruenssiluokka modulo n* (tai *jäännösluokka modulo n*).

Luokka $[a]_n$ koostuu siis muotoa $a + kn$, $k \in \mathbb{Z}$, olevista kokonaisluvuista, esimerkiksi

$$[\,4\,]_3 = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}.$$

Lemma 4.3.2. *Olkoon $n \in \mathbb{N} \setminus \{0\}$ ja olkoot $a, b \in \mathbb{Z}$. Tällöin*

(1) $a \in [a]_n$,
(2) $a \equiv b \pmod{n}$ jos ja vain jos $[a]_n = [\,b\,]_n$,
(3) joko $[a]_n = [\,b\,]_n$ tai $[a]_n \cap [\,b\,]_n = \emptyset$.

Todistus.

(1) Koska $a \equiv a \pmod{n}$ (Lauseen 4.1.4 kohta (1)), ensimmäinen kohta seuraa.

(2) Oletetaan ensin, että $a \equiv b \pmod{n}$. Olkoon $c \in [a]_n$. Koska $c \equiv a \pmod{n}$ ja $a \equiv b \pmod{n}$, Lauseen 4.1.4 nojalla on $c \equiv b \pmod{n}$ eli $c \in [b]_n$. Siis $[a]_n \subset [b]_n$. Täysin vastaavalla tavalla päätellään $[b]_n \subset [a]_n$ ja saadaan siis $[a]_n = [b]_n$.

Oletetaan seuraavaksi, että $[a]_n = [b]_n$. Kohdan (1) nojalla $b \in [b]_n$, joten oletuksen nojalla myös $b \in [a]_n$. Siis $a \equiv b \pmod{n}$.

(3) Riittää näyttää, että jos $[a]_n \cap [\,b\,]_n \neq \emptyset$, niin $[a]_n = [\,b\,]_n$. Oletetaan, että on $c \in [a]_n \cap [\,b\,]_n$ eli $a \equiv c \pmod{n}$ ja $b \equiv c \pmod{n}$. Lauseen 4.1.4 (2)–(3) perusteella on $a \equiv b \pmod{n}$. Väite seuraa kohdasta (2).

□

Seuraava lause kertoo, että jokainen kongruenssiluokka vastaa yhtä luvulla n jaettaessa jäävää jakojäännöstä $0, 1, \ldots, n-1$. Lauseen virke "Kongruenssiluokat $[\,0\,]_n, [\,1\,]_n, \ldots, [n-1]_n$ ovat erillisiä" tarkoittaa, että jos $i, j \in \{0, 1, ..., n-1\}$ ja $i \neq j$, niin $[i]_n \cap [j]_n = \emptyset$.

Lause 4.3.3. *Olkoon $n \in \mathbb{N} \setminus \{0\}$. Kongruenssiluokat $[\,0\,]_n, [\,1\,]_n, \ldots, [n-1]_n$ ovat erillisiä ja niiden yhdiste on $\mathbb{Z}$. Toisin sanoen jokainen kokonaisluku on kongruentti modulo n täsmälleen yhden kokonaisluvun $0, 1, \ldots, n-1$ kanssa.*

Todistus. Huomataan ensin, että mitkään kaksi eri lukua joukosta $\{0, 1, \ldots, n-1\}$ eivät ole kongruentteja keskenään modulo n: Jos eri luvut ovat i, j ja on $i > j$, niin $1 \leq i - j \leq n - 1$, ja jos taas $j > i$, on $1 \leq j - i \leq n - 1$. Siten Lemman 4.3.2 nojalla kongruenssiluokat $[\,0\,]_n, [\,1\,]_n, \ldots, [n-1]_n$ ovat erillisiä.

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 $k \in [r]_n$.

Koska toisaalta jokainen kongruenssiluokka $[\,i\,]_n$, $i = 0, 1, \ldots, n-1$, on joukon $\mathbb{Z}$ osajoukko, niin

$$\mathbb{Z} = \bigcup_{i=0}^{n-1} [\,i\,]_n.$$

□

Usein merkitään

$$\mathbb{Z}_n = \big\{ [\, i \,]_n : i = 0, 1 \ldots, n-1 \big\} = \big\{ [\, i \,]_n : i \in \mathbb{Z} \big\}$$

ja kutsutaan joukkoa $\mathbb{Z}_n$ *kokonaisluvuiksi modulo n* (tai *jäännösluokkarenkaaksi modulo n*.)

Esimerkki 4.3.4. Koska kaikki kokonaisluvut ovat kongruentteja keskenään modulo 1, niin kongruenssiluokkia modulo 1 on vain yksi; $\mathbb{Z}_1 = [0]_1 = \mathbb{Z}$.

Kongruenssiluokkia modulo 2 on kaksi ja $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$. Luokista $[0]_2$ ja $[1]_2$ edellinen koostuu parillisista ja jälkimmäinen parittomista luvuista.

Kongruenssiluokilla voidaan laskea yhteen-, vähennys- ja kertolaskuja.

Määritelmä 4.3.5. Olkoon $n \in \mathbb{N} \setminus \{0\}$ ja olkoot $a, b \in \mathbb{Z}$. Määritellään laskutoimitukset joukossa $\mathbb{Z}_n$ seuraavasti:

$$\begin{aligned} [a]_n + [\, b \,]_n &= [a+b]_n, \\ [a]_n - [\, b \,]_n &= [a-b]_n, \\ [a]_n [\, b \,]_n &= [ab]_n. \end{aligned} \tag{4.1}$$

Jotta laskutoimitukset olisivat hyvin määriteltyjä, kohdan (4.1) kaavojen oikeat puolet saavat riippua vain ekvivalenssiluokista $[a]_n$ ja $[\, b \,]_n$, eivät ekvivalenssiluokkien edustajista a ja b.

Näytetään, että yhteenlasku on hyvin määritelty: Pitää näyttää, että jos on $a^*, b^* \in \mathbb{Z}$, joille $[a]_n = [a^*]_n$ ja $[\, b \,]_n = [b^*]_n$, niin $[a+b]_n = [a^*+b^*]_n$. Lemman 4.3.2 (2) nojalla on $a \equiv a^* \pmod{n}$ ja $b \equiv b^* \pmod{n}$, joten Lauseen 4.1.5 (1) perusteella on $a + b \equiv a^* + b^* \pmod{n}$. Lemma 4.3.2 (2) toiseen suuntaan kertoo, että $[a+b]_n = [a^*+b^*]_n$.

Esimerkki 4.3.6. Esimerkkejä kongruessiluokkien yhteen- ja kertolaskusta:

$$\begin{aligned} [\, 1 \,]_3 + [\, 2 \,]_3 &= [1+2]_3 = [\, 3 \,]_3 = [\, 0 \,]_3 \\ [\, 2 \,]_5 [\, 4 \,]_5 &= [\, 2 \cdot 4 \,]_5 = [\, 8 \,]_5 = [\, 3 \,]_5. \end{aligned}$$

Esimerkki 4.3.7. Olkoon $a \in \mathbb{Z}$. Osoita, että a^2 ei voi olla muotoa $7k+3$ millään $k \in \mathbb{Z}$.

Tiedetään, että $a \in [r]_7$ jollakin $0 \leq r < 7$. Kongruenssiluokkien kertolaskusäännön nojalla $[r]_7^2 = [r]_7 [r]_7 = [r^2]_7$. Saadaan:

$$\begin{aligned} &[0]_7^2 = [0]_7, \quad [1]_7^2 = [1]_7, \quad [2]_7^2 = [4]_7, \\ &[3]_7^2 = [9]_7 = [2]_7, \quad [4]_7^2 = [16]_7 = [2]_7, \\ &[5]_7^2 = [25]_7 = [4]_7, \quad [6]_7^2 = [36]_7 = [1]_7. \end{aligned}$$

Huomataan, että tulokseksi tulee aina $[0]_7, [1]_7, [2]_7, [4]_7$. Esimerkiksi, jos korotamme toiseen jonkin luvun $b \in [3]_7$ (eli luvun jonka jakojäännös jaettuna seitsemällä on 3), tulokseksi tulee jokin luku, jonka jakojäännös jaettaessa seitsemällä on 2. (Tämän kertoo lasku $[3]_7^2 = [2]_7$). Huomataan, että luvun a^2 jakojäännös jaettaessa seitsemällä on oltava $0, 1, 2$, tai 4.

4.4. **Lineaarinen kongruenssi.**

Määritelmä 4.4.1. Olkoon $n \in \mathbb{N} \setminus \{0\}$ ja olkoot $a, b \in \mathbb{Z}$. Kongruenssia

$$ax \equiv b \pmod{n} \tag{4.2}$$

sanotaan (yhden muuttujan) *lineaariseksi kongruenssiyhtälöksi*. Sellaista lukua $x_0 \in \mathbb{Z}$ jolle pätee $ax_0 = b$ sanotaan kongruenssiyhtälön (4.2) (erääksi) *ratkaisuksi*.

Huomautus 4.4.2.

(1) Jos x_0 on yhtälön (4.2) eräs ratkaisu ja $x_0 \equiv y_0 \pmod{n}$, niin Lauseen 4.1.5 mukaan

$$ay_0 \equiv ax_0 \equiv b \pmod{n},$$

joten myös y_0 on yhtälön (4.2) ratkaisu. Siispä, jos $z \in \mathbb{Z}$, niin **joko kongruenssiluokan $[z]_n$ kaikki luvut** *ovat lineaarisen kongruenssiyhtälön (4.2) ratkaisuja* **tai mikään luku joukosta $[z]_n$ ei** *ole ratkaisu.*

(2) Koska jokaisen luvun $x \in \mathbb{Z}$ jakojäännökselle r modulo n pätee $x \equiv r \pmod{n}$, niin yhtälöön (4.2) ratkaisua haettaessa riittää kohdan (1) perusteella tutkia luvut $0, 1, \ldots, n-1$.

(3) Pätee

$$\begin{aligned} ax \equiv b \pmod{n} &\iff n \mid (ax - b) \\ &\iff ax - b = yn \quad \textit{jollekin } y \in \mathbb{Z} \\ &\iff ax - ny = b \quad \textit{jollekin } y \in \mathbb{Z}. \end{aligned}$$

Lineaarisen kongruenssiyhtälön ratkaisujen etsintä palautuu siis Diofantoksen yhtälöihin.

Esimerkki 4.4.3. Tarkastellaan lineaarista kongruenssiyhtälöä

(a) $2x \equiv 6 \pmod{12}$.
Etsitään siis kokonaislukuja x, joille $2x - 12y = 6$. jollakin $y \in \mathbb{Z}$. Eräs ratkaisu on $x = 3$ (kun $y = 0$). Onko muita ratkaisuja?

Muistetaan Lause 2.5.3: Lineaarisen Diofantoksen yhtälön

$$ax + by = c$$

kaikki ratkaisut ovat muotoa

$$x = x_0 + \frac{bm}{\mathrm{syt}(a,b)}, \quad y = y_0 - \frac{am}{\mathrm{syt}(a,b)}, \quad m \in \mathbb{Z},$$

missä $x_0, y_0 \in \mathbb{Z}$ ovat yhtälön eräs ratkaisupari. Nyt $\mathrm{syt}(2, 12) = 2$ ja eräs ratkaisupari $(x_0, y_0) = (3, 0)$. Siispä ratkaisut ovat muotoa

$$x = 3 - \frac{12m}{2} = 3 - 6m \quad (\text{ja } y = -\frac{2m}{m} = -m), \quad m \in \mathbb{Z}.$$

Nyt siis $x = 3 = 3 - 6 \cdot 0$ (kun $y = 0$) ja $x = 3 - 6 \cdot (-1) = 9$ (kun $y = 1$) ovat ratkaisuja. Siis ainakin kongruenssiluokat $[3]_{12}$ ja $[9]_{12}$ ovat ratkaisuja. Osoitetaan seuraavaksi, että olipa $m \in \mathbb{Z}$ mikä vain, niin joko $3 - 6m \in [3]_{12}$ tai $3 - 6m \in [9]_{12}$.

Kun $m = 2k$, $k \in \mathbb{Z}$, niin $3 - 6m = 3 - 12j \in [3]_{12}$, ja kun $m = 2k+1$, $k \in \mathbb{Z}$, niin $3-6m = -3-12k \in [9]_{12}$. Näin ollen $[\,3\,]_{12}$ ja $[\,9\,]_{12}$ ovat ainoat kongruessiyhtälön $2x \equiv 6 \pmod{12}$ ratkaisut.

(b) Tarkastellaan kongruenssiyhtälöä $2x \equiv 3 \pmod 4$. On monta tapaa nähdä, että ratkaisuja ei ole:
   (i) Riittää tutkia, toteuttavatko luvut $0, 1, 2, 3$ tämän yhtälön. Tutki! Huomataan, että tällä kongruenssiyhtälöllä ei ole ratkaisuja.
   (ii) Koska $2x - 3 = 2(x - 2) + 1$ on pariton kaikilla $x \in \mathbb{Z}$, niin $4 \nmid (2x - 3)$ kaikilla $x \in \mathbb{Z}$. Siispä kongruenssiyhtälöllä ei ole ratkaisua.
   (iii) Mille $x \in \mathbb{Z}$ on $2x + 4y = 3$?
   Tiedetään, että vain $\text{syt}(4, 2)$:n moninkerrat voidaan esittää tällaisena summana. Nyt $\text{syt}(4, 2) = 2$ ja $2 \nmid 3$, joten summalla ei ole ratkaisuja ja siis kongruenssiyhtälöllä $2x \equiv 3 \pmod 4$ ei ole ratkaisuja.

Yleisesti saadaan:

Lause 4.4.4 (Lineaarisen kongruenssin lause)**.** *Olkoon $n \in \mathbb{N} \setminus \{0\}$, olkoot $a, b \in \mathbb{Z}$ ja $d = \text{syt}(a, n)$.*

(1) Jos $d \nmid b$, niin lineaarisella kongruenssilla $ax \equiv b \pmod n$ ei ole ratkaisua $x \in \mathbb{Z}$.

(2) Jos $d \mid b$, niin lineaarisella kongruenssilla $ax \equiv b \pmod n$ on d ratkaisua (kongruenssiluokkaa modulo n). Ratkaisut saadaan kaavalla

$$x \equiv x_0 + i\,\frac{n}{d} \pmod n, \quad i = 0, 1, \ldots, d-1,$$

missä x_0 on eräs kongruenssin ratkaisu.

Todistus. Haetaan siis lukua $x \in \mathbb{Z}$, jolle

$$ax + ny = b \quad \text{jollakin} \quad y \in \mathbb{Z}.$$

(Huomaa, että tämä yhtälö antaa samat ratkaisut muuttujan x suhteen kuin aiemmassa esimerkissä ollut muoto $ax - ny = b$.)

Jos $d \nmid b$, niin Seurauksen 2.3.12 nojalla tällaista lukua ei löydy.

Jos $d \mid b$, niin Lauseen 2.3.11 nojalla on olemassa $k_0, l_0 \in \mathbb{Z}$ siten, että

$$ak_0 + nl_0 = d,$$

jolloin

$$a \cdot \underbrace{\frac{b}{d}k_o}_{\in\mathbb{Z}} + n \cdot \underbrace{\frac{b}{d}l_o}_{\in\mathbb{Z}} = b$$

ja siis

$$x_0 = \frac{b}{d}k_0$$

on eräs ratkaisu. Loput seuraa lineaarisen Diofantoksen yhtälön ratkaisuista (Lause 2.5.3) sekä jakoyhtälöstä, jonka mukaan on $q, i \in \mathbb{Z}$ siten, että $m = qd+i$ ja $0 \leq i \leq d-1$:

$$x = x_0 + m\frac{n}{d} = x_0 + (qd+i)\frac{n}{d} \equiv x_0 + i\frac{n}{d} \pmod{n}, \quad i = 0, 1, \ldots, d-1.$$

□

Seuraus 4.4.5. *Jos $n \in \mathbb{N} \setminus \{0\}$, $a \in \mathbb{Z}$ ja $\mathrm{syt}(a, n) = 1$, niin lineaarisella kongruenssilla $ax \equiv b \pmod{n}$ on ratkaisu kaikilla $b \in \mathbb{Z}$. Ratkaisu on yksikäsitteinen kongruenssiluokkana.*

Todistus. Lause 4.4.4. □

Esimerkki 4.4.6. Ratkaise yhtälö

(a) $9x \equiv 6 \pmod{12}$
Koska $\mathrm{syt}(9, 12) = 3$ ja $3 \mid 6$, niin Lauseen 4.4.4 nojalla yhtälöllä on kolme ratkaisua. Nyt

$$9 \cdot (-1) + 12 \cdot 1 = 3,$$

joten $x_0 = \frac{6}{3} \cdot (-1) = -2 \equiv 10 \pmod{12}$ on ratkaisu.
Toinen ratkaisu on $x_1 \equiv x_0 + 1 \cdot \frac{12}{3} \pmod{n}$ eli $x_1 \equiv 2 \pmod{12}$, ja kolmas ratkaisu on $x_2 \equiv x_0 + 2 \cdot \frac{12}{3} \pmod{n}$ eli $x_2 \equiv 6 \pmod{12}$. Ratkaisut ovat siis kongruenssiluokat $[\,2\,]_{12}$, $[\,6\,]_{12}$ ja $[\,10\,]_{12}$.

(b) $7x \equiv 3 \pmod{12}$.
Koska $7 \cdot 9 = 63 \equiv 3 \pmod{12}$, niin kongruenssiluokka $[\,9\,]_{12}$ on ratkaisu. Koska $\mathrm{syt}(7, 12) = 1$, niin Lauseen 4.4.4 nojalla tämä on ainoa ratkaisu.

(c) $4x \equiv 5 \pmod{12}$.
Koska $\mathrm{syt}(4, 12) = 4$ ja $4 \nmid 5$, niin ratkaisua ei ole.

(d) Onko jokaisella $[\,a\,]_{12} \in \mathbb{Z}_{12}$ olemassa kongruenssiluokka $[\,b\,]_{12} \in \mathbb{Z}_{12}$ siten, että

$$[\,a\,]_{12}[\,b\,]_{12} = [\,1\,]_{12}?$$

Eli onko lineaarisella kongruenssilla

$$ab \equiv 1 \pmod{12}$$

olemassa ratkaisu jokaisella $a = 0, 1, 2, \ldots, 11$?

Nyt $0 \cdot b \equiv 0 \pmod{12}$ kaikilla $[\,b\,]_{12} \in \mathbb{Z}_{12}$. Ratkaisua ei siis ole olemassa ainakaan kun $a = 0$.

Lauseen 4.4.4 mukaan, jos $\text{syt}(a, 12) \nmid 1$, niin ratkaisua ei ole olemassa. Toisin sanoen, kun $\text{syt}(a, 12) > 1$ eli kun $a = 2, 3, 4, 6, 8, 9, 10$, niin ratkaisua ei myöskään ole.

Kun $\text{syt}(a, 12) = 1$ eli kun $a = 1, 5, 7, 11$, niin Seurauksen 4.4.5 nojalla ratkaisu on olemassa ja se on yksikäsitteinen (kongruenssiluokkana). Mikä ratkaisu on kussakin tapauksessa?

Määritelmä 4.4.7. Olkoot $n \in \mathbb{N} \setminus \{0\}$ ja $a, b \in \mathbb{Z}$. Joukossa $\mathbb{Z}_n$ alkio $[\,b\,]_n$ on alkion $[\,a\,]_n$ *käänteisalkio,* jos $[\,a\,]_n[\,b\,]_n = [\,1\,]_n$. Alkiota $[\,a\,]_n$ sanotaan tällöin myös *kääntyväksi alkioksi.*

Lemman 4.3.2 mukaan on $[\,a\,]_n[\,b\,]_n = [\,ab\,]_n = [\,1\,]_n$ jos ja vain jos $ab \equiv 1 \pmod{n}$. Joskus jätetään myös hakasulut merkitsemättä, jolloin $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ ja $b \in \mathbb{Z}_n$ on alkion $a \in \mathbb{Z}_n$ käänteisalkio, merk. $b = a^{-1}$, jos $ab \equiv 1 \pmod{n}$. Tällä kurssilla käytämme kuitenkin selvyyden vuoksi aina hakasulkuja puhuessamme kongruenssiluokista.

Lause 4.4.8. *Olkoon $n \in \mathbb{N} \setminus \{0\}$. Alkiolla $[\,a\,]_n \in \mathbb{Z}_n$ on yksikäsitteinen käänteisalkio täsmälleen sillä ehdolla että* $\text{syt}(a, n) = 1$.

Todistus. Olkoon $[\,b\,]_n \in \mathbb{Z}_n$ alkion $[\,a\,]_n \in \mathbb{Z}_n$ käänteisalkio. Tällöin saadaan

$$\begin{aligned}
[\,a\,]_n[\,b\,]_n = [\,ab\,]_n = [\,1\,]_n &\iff ab \equiv 1 \pmod{n} \\
&\iff ab - 1 = kn \quad \text{jollekin } k \in \mathbb{Z} \\
&\iff ab - nk = 1 \quad \text{jollekin } k \in \mathbb{Z} \\
&\implies \text{syt}(a, n) = 1.
\end{aligned}$$

Toinen suunta seuraa Seurauksesta 4.4.5. □

Tästä saadaan seuraavat seurakset:

Seuraus 4.4.9. *Kun p on alkuluku, niin joukon $\mathbb{Z}_p$ jokaisella nollasta eroavalla alkiolla on käänteisalkio.*

Seuraus 4.4.10. *Jos alkiolla $[\,a\,]_n$ on joukossa $\mathbb{Z}_n$ käänteisalkio $[\,b\,]_n$, niin kongruenssiyhtälöllä $ax \equiv c \pmod{n}$ on jokaisella $c \in \mathbb{Z}$ yksikäsitteinen ratkaisu (kongruenssiluokkana) $x \equiv bc \pmod{n}$.*

Käänteisalkioiden avulla voidaan osoittaa *Fermat'n pieni lause.*

Lause 4.4.11 (Fermat'n pieni lause)**.** *Kun p on alkuluku, pätee*

$$a^p \equiv a \pmod{p} \quad \textit{kaikilla } a \in \mathbb{Z}.$$

Todistus. Koska $0^p \equiv 0 \pmod{p}$, niin riittää osoittaa, että

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{kaikille } a = 1, 2, \ldots, p-1,$$

koska tällöin $a^p = a \cdot a^{p-1} \equiv a \cdot 1 = a \pmod{p}$.

Seurauksen 4.4.9 mukaan jokaisella tällaisella a on käänteisalkio b joukossa $\mathbb{Z}_p$. Jos nyt $xa \equiv ya \pmod{p}$, niin $x(ab) \equiv y(ab) \pmod{p}$ eli $x \equiv y \pmod{p}$. Siispä alkiot $a, 2a, \ldots, (p-1)a$ kuuluvat eri luokkiin joukossa $\mathbb{Z}_p$, eli ne ovat kongruentteja alkioiden $1, 2, \ldots, p-1$ kanssa modulo p tosin mahdollisesti eri järjestyksessä. Näin ollen

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

eli

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

Koska syt $(p, (p-1)!) = 1$, supistussäännön (Lause 4.1.8) nojalla

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

□

Seuraus 4.4.12 (Fermat'n pieni lause)**.** *Kun p on alkuluku, $a \in \mathbb{Z}$ ja $p \nmid a$* (tai yhtäpitävästi syt$(a, p) = 1$)*, pätee*

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

Monissa yhteyksissä Fermat'n pieni lause annetaan Seurauksen 4.4.12 muodossa. Siis jos kysytään, mikä on Fermat'n pieni lause, voi antaa jomman kumman kahdesta muotoilusta. On kuitenkin tärkeää muistaa, että seurauksen versiota voi käyttää vain kun lisäehto $p \nmid a$ on voimassa. Huomaa, että koska p on alkuluku, niin jos tiedämme että $p \nmid a$, on $p \nmid a^j$ kaikilla $j \in \mathbb{N}$. Tämä on kätevää kun halutaan käyttää seurauksen versiota Fermat'n pienestä lauseesta.

Fermat'n pieni lause on monesti käyttökelpoinen kongruenssitarkasteluissa:

Esimerkki 4.4.13. (1) Osoitetaan, että $8^{40} = 5k + 1$ jollakin $k \in \mathbb{Z}$. On siis osoitettava, että $8^{40} \equiv 1 \pmod{5}$. Koska 5 on alkuluku ja $5 \nmid 8$, on $5 \nmid 8^j$ kaikilla $j \in \mathbb{N}$. Käyttämällä Fermat'n pienen lauseen jälkimmäistä (Seuraus 4.4.12) versiota saadaan

$$8^{40} \equiv (8^{10})^{5-1} \equiv 1 \pmod{5}.$$

(2) Osoitetaan, että $6^{122} \equiv 3 \pmod{11}$. Koska 11 on alkuluku ja $11 \nmid 6$, molemmat Fermat'n pienen lauseen versiot ovat taas käytössä. Huomataan ensin, että $122 = 11 \cdot 11 + 1$. Fermat'n pienen lauseen molempia versioita käyttämällä saadaan

$$6^{122} \equiv 6^{11 \cdot 11 + 1} \equiv (6^{11})^{11} \cdot 6 \equiv 6^{11} \cdot 6 \equiv 6^{11-1} \cdot 6^2 \equiv 6^2 \equiv 3 \pmod{11}.$$

Kiinalainen jäännöslause. Kiinalainen munkki Sun Zi esitti aikoinaan seuravan arvoituksen

> *Meillä on jokin määrä esineitä, mutta emme tarkkaan tiedä, montako. Jos esineet jakaa kolmen ryhmiin, jää kaksi yli. Jos ne jaetaan viiden ryhmiin, jää kolme yli. Jos ne taas jaetaan seitsemän ryhmiin, jää kaksi yli. Montako esinettä meillä on?*

Arvoitus voidaan kurssin merkinnöillä muotoilla seuraavanlaiseksi kysymykseksi: Onko lukua $x \in \mathbb{Z}$, jolle lineaariset kongruenssiyhtälöt

$$(*) \qquad \begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

ovat totta? Huomaa, että jos $x_0 \in \mathbb{Z}$ on yhtälöryhmän ratkaisu, niin myös luku

$$x_0 + 3 \cdot 5 \cdot 7t$$

on ratkaisu kaikilla $t \in \mathbb{Z}$. Kaikki kongruenssiluokan $[x_0]_{105}$ luvut ovat siis ratkaisuja. Se, että muita ratkaisuja ei ole, seuraa Lauseesta 4.4.15.

Esimerkki 4.4.14. Onko lukua $x \in \mathbb{Z}$, jolle lineaariset kongruenssiyhtälöt

$$x \equiv 3 \pmod 9 \quad \text{ja} \quad x \equiv 2 \pmod 6$$

ovat totta?

Jos $x \equiv 3 \pmod 9$, niin $3 \mid (x-3)$ ja siten 3 jakaa luvun $x - 3 + 3 = x$. Jos $x \equiv 2 \pmod 6$, niin $3 \mid (x-2)$. Jos $3 \mid x$, niin 3 jakaisi luvun $x - (x-2) = 2$, mikä ei ole totta. Siis $3 \nmid x$, eikä yhtälöillä ole yhteistä ratkaisua.

Lause 4.4.15 (Kiinalainen jäännöslause)**.** *Olkoot $n_1, \ldots, n_k \in \mathbb{N} \setminus \{0\}$ lukuja, joille $\operatorname{syt}(n_i, n_j) = 1$ aina, kun $i \neq j$. Olkoot $b_1, \ldots, b_k \in \mathbb{Z}$. Tällöin kongruenssiyhtälöryhmällä*

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

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

Todistus. (Ei käsitellä luennolla.) Olkoon

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

Koska $\operatorname{syt}(n_i, n_j) = 1$ aina, kun $i \neq j$, niin $\operatorname{syt}(c_i, n_i) = 1$ kaikilla $i = 1, 2, \ldots, k$. Seurauksen 4.4.5 perusteella yhtälöllä

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

on yksikäsitteinen ratkaisu kongruenssiluokkana modulo n_i. Olkoon se $[d_i]_{n_i}$

Näytetään, että luku

$$x_0 = b_1c_1d_1 + b_2c_2d_2 + \cdots + b_kc_kd_k$$

on yhtälöryhmän ratkaisu.

Jos $i \neq j$, niin $n_i \mid c_j$ ja siten $b_jc_jd_j \equiv 0 \pmod{n_i}$. Luvun x_0 määritelmän mukaan on siis $x_0 \equiv b_ic_id_i \pmod{n_i}$. Koska $c_id_i \equiv 1 \pmod{n_i}$, niin on

$$x_0 \equiv b_i \pmod{n_i}$$

eli x_0 on kaikkien ryhmän kongruenssiyhtälöiden ratkaisu. Jaollisuuslauseen avulla nähdään helposti, että kongruenssiluokka $[x_0]_n$ on yhtälöryhmän ratkaisu.

Näytetään seuraavaksi, että muita ratkaisuja ei ole. Olkoon $x \in \mathbb{Z}$ yhtälöryhmän ratkaisu. Koska tällöin on $x \equiv b_i \pmod{n_i}$ ja $x_0 \equiv b_i \pmod{n_i}$, niin Lauseen 4.1.4 perusteella $x_0 \equiv x \pmod{n_i}$ ja siten $n_i \mid (x - x_0)$ kaikilla $i = 1, 2, \ldots, k$. Koska $\text{syt}(n_i, n_j) = 1$, niin luku $n = n_1 \cdots n_k$ jakaa luvun $x - x_0$ eli $x \equiv x_0 \pmod{n}$ (harjoitustehtävä). Siis ainoa ratkaisu on $[x_0]_n$. □