

ALGEBRA I

SISÄLLYSLUETTELO

1. Relaatio ja funktio	3
1.1. Karteesinen tulo	3
1.2. Relaatio ja funktio	3
1.3. Ekvivalenssirelaatio	9
2. Lukuteoriaa	11
2.1. Jaollisuusrelaatio	11
2.2. Suurin yhteinen tekijä ja Eukleideen algoritmi	14
2.3. Alkuluvut ja aritmetiikan peruslause	17
2.4. Modulaariaritmetikkaa	21
2.5. Kongruenssiryhmistä	25
3. Ryhmäteoriaa	30
3.1. Määritelmä ja perusominaisuuksia	30
3.2. Aliryhmä ja syklinen ryhmä	34
3.3. Sivuluokat ja Lagrangen lause	37
3.4. Isomorfismi ja homomorfismi	42
3.5. Syklisten ryhmien peruslause ja vastaavuuslause	47
3.6. Suora tulo ja ryhmän \mathbb{Z}_m^* rakenne	49
Liite A. Kertausta joukko-opista ja logiikasta	55
A.1. Joukko-oppia	55
A.2. Avoin lause, kvanttorit	56
A.3. Implikaatio ja ekvivalenssi	59
A.4. Todistusmenetelmistä	60

1. RELAATIO JA FUNKTIO

1.1. **Karteesinen tulo.** Sellaista kahden alkion a, b joukkoa, jossa alkioiden järjestys on määrätty sanotaan *järjestetyksi pariksi*. Merkitään (a, b) . Järjestettyjen parien yhtäsuuruus siis määritellään näin:

$$(a, b) = (c, d) \Leftrightarrow (a = c) \wedge (b = d).$$

Yleisesti, jos alkio a_1, a_2, \dots, a_n muodostavat joukon jossa alkioiden järjestys on määrätty, sanotaan tällaista joukkoa *järjestetyksi n -jonoksi*, merkitään (a_1, \dots, a_n) .

Määritelmä 1.1. Joukkojen A_1, \dots, A_n karteesinen tulo

$$A_1 \times \dots \times A_n = \{(a_1, \dots, a_n) \mid a_1 \in A_1, \dots, a_n \in A_n\}$$

Sopimus: Merkitsemme karteesista tuloa $\underbrace{A \times \dots \times A}_n = A^n$

Esimerkki 1.1. Olkoot $A = \{x\}$, $B = \{1, 2\}$. Nyt $A \times B = \{(x, 1), (x, 2)\}$ ja $B \times A = \{(1, x), (2, x)\}$. Täten $A \times B \neq B \times A$.

Esimerkki 1.2. $\mathbb{R}^n = \{(x_1, \dots, x_n) \mid x_1, \dots, x_n \in \mathbb{R}\}$.

1.2. Relaatio ja funktio.

Määritelmä 1.2. Binäärinen relaatio joukosta A joukkoon B on karteesisen tulon $A \times B$ osajoukko R . Jos $A = B$ sanotaan, että R on *relaatio joukossa A* .

Esimerkki 1.3. Olkoon $A = \{1, 3, 5, 7\}$ ja $B = \{2, 4, 6\}$. Relaatio $R = \{(x, y) \mid x + y = 9\}$ A :sta B :hen muodostuu järjestetyistä pareista $(3, 6), (5, 4), (7, 2)$. Siis $R = \{(3, 6), (5, 4), (7, 2)\}$.

Esimerkki 1.4. Relaatio $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ joukossa \mathbb{R}^2 koostuu kaikista reaalisesta yksikköympyrän pisteistä.

Sopimus: Merkitään lyhyesti aRb jos $(a, b) \in R$.

Määritelmä 1.3. Olkoon R relaatio joukosta A joukkoon B . Relaation R *käänteisrelaatio* on relaatio

$$R^{-1} := \{(b, a) \mid (a, b) \in R\}$$

joukosta B joukkoon A .

Olkoon lisäksi S relaatio joukosta B joukkoon C . Relaatioiden R ja S *yhdistetty relaatio* on relaatio

$$S \circ R = \{(a, c) \mid (a \in A, c \in C) \wedge ((aRb) \wedge (bSc) \text{ jollakin } b \in B)\},$$

joukosta A joukkoon C .

Huomautus. $S \circ R$ muodostetaan siis seuraavasti: valitaan jokaista relaation R paria (a, b) kohti kaikki relaation S muotoa (b, c) olevat parit. Nyt $S \circ R$ on kaikkien tällaisten parien (a, c) muodostama joukko.

Esimerkki 1.5. Olkoot A, B ja $R = \{(3, 6), (5, 4), (7, 2)\}$ kuten esimerkissä 1.3. Olkoon $C = \{a, b, c\}$ ja $S = \{(2, a), (2, b), (6, c)\}$ relaatio B :stä C :hen. Nyt $S^{-1} = \{(a, 2), (b, 2), (c, 6)\}$ ja $S \circ R = \{(3, c), (7, a), (7, b)\}$.

Esimerkki 1.6. Relaation $A = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ käänteisrelaatio on A itse. Olkoon $B = \{(x, y) \in \mathbb{R}^2 \mid x \geq 0\}$. Nyt $B \circ A = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1, y \geq 0\}$.

Määritelmä 1.4. *Funktio (tai kuvaus) f joukolta A joukkoon B* on sellainen relaatio joukosta A joukkoon B jossa jokainen joukon A alkio on relaatiossa täsmälleen yhden joukon B alkion kanssa. Merkitään $f : A \rightarrow B$. Jos $(x, y) \in f$, niin merkitään $y = f(x)$.

Esimerkki 1.7. Relaatio $\{(1, 1), (2, 1), (3, 1)\}$ joukossa $A := \{1, 2, 3\}$ on funktio joukolta A joukkoon A . Relaatiot $\{(1, 1), (2, 2)\}$ ja $\{(1, 1), (2, 2), (2, 3)\}$ eivät ole funktioita joukolta A joukkoon A .

Esimerkki 1.8. Relaatio $\{(x, y) \mid x \in \mathbb{R}, y = x^2\}$ joukossa \mathbb{R}^2 on funktio. Sen käänteisrelaatio $\{(x, y) \mid x \in \mathbb{R}, x = y^2\}$ ei ole funktio, sillä esim. $(1, 1)$ ja $(1, -1)$ kuuluvat siihen.

Kertauksena funktioihin liittyvää terminologiaa:

Määritelmä 1.5. Olkoon $f : A \rightarrow B$. $f(a)$ on alkion a *kuva kuvauksessa f* (tai f :n arvo pisteessä a). A on funktion f *määrittelyjoukko* ja B on funktion f *maalijoukko*. Joukko

$$f(A) := \{f(a) \mid a \in A\} \subseteq B$$

on funktion f *kuvajoukko* (tai arvojoukko) merkitään myös $Im f = f(A)$.

Määritelmä 1.6. Olkoot $f : A \rightarrow B$ ja $A' \subseteq A, B' \subseteq B$. Joukon A' kuva on joukko

$$f(A') := \{f(a) \mid a \in A'\}.$$

Joukon B' alkukuvien joukko on joukko

$$f^{-1}(B') := \{a \in A \mid f(a) \in B'\}.$$

Huomautus. Yhden alkion joukon $\{b\}$ alkukuvien joukkoa merkitään tavallisesti $f^{-1}(b)$, ja kutakin joukon $f^{-1}(b)$ alkiota sanotaan *alkion b alkukuvaksi* (kuvauksessa f).

Esimerkki 1.9. Tarkastellaan funktiota $g = \{(a, 1), (b, 1), (c, 3)\}$ joukolta $A = \{a, b, c\}$ joukkoon $B = \{1, 2, 3\}$. Nyt a :n kuva $g(a) = 1$, g :n kuvajoukko $g(A) = \{1, 3\}$, joukon $\{1, 2\}$ alkukuvien joukko $g^{-1}(\{1, 2\}) = \{a, b\}$, alkion 1 alkukuvat ovat a ja b ja alkion 2 alkukuvien joukko $g^{-1}(2) = \emptyset$.

Määritelmä 1.7. Funktio $f : A \rightarrow B$ on *injektio* jos jokaisella joukon B alkiolla on korkeintaan yksi alkukuva kuvauksessa f . Se on *surjektio* jos jokaisella joukon B alkiolla on vähintään yksi alkukuva. Se on *bijektio* jos se on sekä injektio että surjektio ts. jokaisella joukon B alkiolla on täsmälleen yksi alkukuva.

Esimerkki 1.10. Tarkastellaan funktiota $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = 4x + 2$. Olkoon $y \in \mathbb{R}$. Yhtälöllä $y = 4x + 3$ on täsmälleen yksi ratkaisu, nimittäin $x = (y - 3)/4$. Täten f on bijektio.

Lause 1.1. Olkoon $f : A \rightarrow B$. Funktio f on injektio jos ja vain jos kaikille joukon A alkioille a, a' pätee $f(a) = f(a') \Rightarrow a = a'$.

Todistus. Oletetaan, että f on injektio. Oletetaan että joillakin $a, a' \in A$ väitteen implikaatio ei päde. Silloin $f(a) = f(a')$ ja $a \neq a'$. Nyt alkiolla $f(a)$ on kaksi alkukuvaa, mikä on vastoin injektiivisyyden määritelmää. Siispä implikaatio on tosi.

Oletetaan, että väitteen implikaatio pätee. Tällöin pätee myös sen kontrapositio $a \neq a' \Rightarrow f(a) \neq f(a')$. Täten jokaisella joukon B alkiolla on korkeintaan yksi alkukuva. □

Esimerkki 1.11. Tarkastellaan funktiota $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x^3 + x + 1$. Osoitetaan, että f on injektio. Oletetaan, että $f(a) = f(b)$. Nyt

$$\begin{aligned} a^3 + a + 1 &= b^3 + b + 1 && \Leftrightarrow \\ a^3 - b^3 &= b - a && \Leftrightarrow \\ (a - b)(a^2 + ab + b^2) &= b - a && \Leftrightarrow \\ (a - b)(a^2 + ab + b^2 + 1) &= 0. \end{aligned}$$

Täten $a - b = 0$ tai $a^2 + ab + b^2 + 1 = 0$. Näistä jälkimmäisellä yhtälöllä ei ole ratkaisua a sillä, sillä sen diskriminantti a :n suhteen $= -3b^2 - 4 < 0$. Täten $a = b$ ja f on injektio. Funktio f on myös surjektio sillä jos $a \in \mathbb{R}$, niin $f(x) - a < 0$ riittävän pienellä x :n arvolla ja $f(x) - a > 0$ riittävän suurella x :n arvolla, ja koska f on jatkuva, niin $f(x_0) = a$ jollakin $x_0 \in \mathbb{R}$. Siispä f on bijektio.

Seuraavaksi annetaan funktioiden yhdistämiseen perustuvat riittävät ehdot surjektiiivisuuden ja injektiiivisuuden toteamiseksi. Funktioiden yhdistäminen tapahtuu seuraavasti: olkoot $f : A \rightarrow B$ ja $g : B \rightarrow C$. Silloin $g \circ f$ on funktio $A \rightarrow C$, $(g \circ f)(x) = g(f(x))$. Tämä seuraa suoraan yhdistetyn relaation määritelmästä.

Lause 1.2. *Olkoot $f : A \rightarrow B$, $g : B \rightarrow A$ funktioita. Silloin pätee*

- (1) *Jos $g \circ f = id_A$ niin f on injektio,*
- (2) *Jos $f \circ g = id_B$ niin f on surjektio,*

missä id_A on A :n identiteettifunktio $A \rightarrow A$, $id_A(x) = x$ ja id_B on B :n identiteettifunktio.

Todistus. (1) $f(a) = f(a') \Rightarrow g(f(a)) = g(f(a')) \stackrel{g \circ f = id_A}{\Rightarrow} a = a'$.

(2) Olkoon $b \in B$. Nyt $f(a) = b$, kun valitaan $a = g(b)$, sillä $f \circ g = id_B$. □

Esimerkki 1.12. Olkoot f ja g funktioita $\mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$,

$$\begin{aligned} f(n) &= n + 1, \\ g(n) &= \begin{cases} 0 & \text{jos } n = 0, \\ n - 1 & \text{jos } n \geq 1. \end{cases} \end{aligned}$$

Nyt $g(f(n)) = g(n + 1) = n$, sillä $n + 1 \geq 1$. Näin ollen $g \circ f = id_{\mathbb{Z}_{\geq 0}}$ ja siispä f on injektio ja g on surjektio.

Määritelmä 1.8. Olkoon $f : A \rightarrow B$. Jos käänteisrelaatio f^{-1} joukosta B joukkoon A on funktio on se f :n käänteisfunktio.

Lause 1.3. Funktiolla f on käänteisfunktio silloin ja vain silloin kun f on bijektio.

Todistus. Olkoon $f = \{(a, b) \mid (a \in A) \wedge (b = f(a))\}$ ja $f^{-1} = \{(b, a) \mid (a \in A) \wedge (b = f(a))\}$. Nyt f^{-1} on funktio joss jokaista $b \in B$ vastaa täsmälleen yksi $a \in A$ jolle $f(a) = b$ joss f on bijektio. \square

Esimerkki 1.13. Esimerkin 1.10 käänteisfunktio $f^{-1} : \mathbb{R} \rightarrow \mathbb{R}$, $f^{-1}(x) = (x - 3)/4$. Esimerkin 1.11 funktiolla on käänteisfunktio f^{-1} , mutta sen laskeminen on hankalanpaa. Seuraavaan lauseeseen perustuen voidaan kuitenkin osoittaa, että

$$f^{-1} : \mathbb{R} \rightarrow \mathbb{R}, f^{-1}(x) = \frac{-6 + \sqrt[3]{2(27(y-1) + \sqrt{108 + 729(y-1)^2})^2}}{3\sqrt[3]{4(27(y-1) + \sqrt{108 + 729(y-1)^2})}}$$

Lause 1.4. Olkoot $f : A \rightarrow B$ ja $g : B \rightarrow A$. Silloin g on funktion f käänteisfunktio jos ja vain jos $g \circ f = id_A$ ja $f \circ g = id_B$.

Huomautus. Tarvitsemme todistuksessa seuraavaa pientä havaintoa: funktion f ja sen käänteisrelaation $g = \{(f(x), x) \mid x \in A\}$ yhdistetty relaatio $g \circ f = \{(x, x') \mid x \in A \text{ ja } x' \in f^{-1}(f(x))\}$ ja yhdistetty relaatio $f \circ g = \{(f(x), f(x)) \mid x \in A\}$.

Todistus. Oletetaan, että g on f :n käänteisfunktio. Nyt $f = \{(x, f(x)) \mid x \in A\}$ ja $g = \{(f(x), x) \mid x \in A\}$. Koska g on injektio lauseen 1.3 nojalla, niin $g \circ f = \{(x, x) \mid x \in A\} = id_A$. Koska f on surjektio lauseen 1.3 nojalla, niin $f \circ g = \{(f(x), f(x)) \mid x \in A\} \stackrel{f \text{ surjektio}}{=} \{(y, y) \mid y \in B\} = id_B$.

Oletetaan nyt, että $g \circ f = id_A$ ja $f \circ g = id_B$ ja osoitetaan että $g = f^{-1}$ eli että $\{(y, g(y)) \mid y \in B\} = \{(f(x), x) \mid x \in A\}$. Olkoon $(y, g(y)) \in g$. Koska $f \circ g = id_B$, niin $y = f(g(y))$. Täten $(y, g(y)) = (f(g(y)), g(y)) = (f(x), x) \in f^{-1}$. Olkoon $(f(x), x) \in f^{-1}$. Koska $g \circ f = id_A$, niin $x = g(f(x))$. Täten $(f(x), x) = (f(x), g(f(x))) = (y, g(y)) \in g$. \square

Esimerkki 1.14. Olkoon $g : \mathbb{R} \setminus \{1\} \rightarrow \mathbb{R}$, $g(x) = \frac{x}{x-1}$. Helposti nähdään, että $g(\mathbb{R} \setminus \{1\}) = \mathbb{R} \setminus \{1\}$. Täten f ei ole surjektio eikä sillä ole käänteisfunktiota. Olkoon nyt $f : \mathbb{R} \setminus \{1\} \rightarrow \mathbb{R} \setminus \{1\}$, $f(x) = \frac{x}{x-1}$. Koska

$$(f \circ f)(x) = \frac{f(x)}{f(x) - 1} = \frac{\frac{x}{x-1}}{\frac{x}{x-1} - 1} = x,$$

niin $f^{-1} = f$.

Esimerkki 1.15. Näimme että esimerkin 1.12 funktioille f ja g pätee $g \circ f = id_{\mathbb{Z}_{\geq 0}}$. Nyt kuitenkin $f \circ g \neq id_{\mathbb{Z}_{\geq 0}}$, sillä $f(g(0)) = f(0) = 1 \neq 0$. Täten funktiot f ja g eivät ole toistensa käänteisfunktioita.

Annetaan vielä yksi kriteeri funktion injektiivisyydelle ja surjektiivisuudelle:

Lause 1.5. *Olkoon $f : A \rightarrow B$. Silloin*

- (1) f on injektio $\Leftrightarrow f^{-1}(f(A')) = A'$ kaikilla $A' \subseteq A$,
- (2) f on surjektio $\Leftrightarrow f(f^{-1}(B')) = B'$ kaikilla $B' \subseteq B$.

Todistus. (1) Triviaalisti $A' \subseteq f^{-1}(f(A'))$ kaikilla $A' \subseteq A$.

" \Rightarrow " Jos sisältyminen $A' \subseteq f^{-1}(f(A'))$ on aito jollakin $A' \subseteq A$, niin on olemassa $a \in A \setminus A'$ jolle $f(a) \in f(A')$. Nyt $f(a') = f(a)$ jollakin $a' \in A'$ ja näin ollen alkiolla $f(a)$ on ainakin kaksi alkukuvaa ja täten f ei ole injektio.

" \Leftarrow " Olkoon $b \in f(A)$. Nyt $b = f(a)$, jollakin $a \in A$ ja $f^{-1}(b) = f^{-1}(f(a)) \stackrel{ol.}{=} a$. Täten alkiolla b on vain yksi alkukuva ja näin ollen f on injektio.

(2) Triviaalisti $f(f^{-1}(B')) \subseteq B'$ kaikilla $B' \subseteq B$.

" \Rightarrow " Jos sisältyminen $f(f^{-1}(B')) \subseteq B'$ on aito jollakin $B' \subseteq B$, niin on olemassa $b \in B'$ jolla ei ole alkukuvaa ja täten f ei ole surjektio.

" \Leftarrow " Olkoon $b \in B$. Nyt oletuksen nojalla $f(f^{-1}(b)) = b$, joten $f^{-1}(b) \neq \emptyset$ ja näin ollen f on surjektio. \square

Lopuksi äärellisten joukkojen välisiä kuvauksia koskeva tulos:

Lause 1.6. *Olkoon $f : A \rightarrow B$ ja $|A| = |B| < \infty$.*

- (1) *Jos f on injektio, niin se on bijektio.*
- (2) *Jos f on surjektio, niin se on bijektio.*

Todistus. (1) Jos f on injektio, niin $|f(A)| = |A| = |B|$. Täten f on myös surjektio.

(2) Oletetaan, että f on surjektio. Koska $A = \bigcup_{b \in B} f^{-1}(b)$, missä $f^{-1}(b) \cap f^{-1}(b') = \emptyset$ aina kun $b \neq b'$, niin $|A| = \sum_{b \in B} |f^{-1}(b)|$. Koska f on surjektio, niin $|f^{-1}(b)| \geq 1$ kaikilla $b \in B$. Mutta $|A| = |B|$ joten $|f^{-1}(b)| = 1$ kaikilla $b \in B$. Täten f on injektio. \square

1.3. Ekvivalenssirelaatio. Tarkastellaan vielä lyhyesti erästä tärkeää relaatiotyyppiä.

Määritelmä 1.9. *Ekvivalenssirelaatio joukossa A on seuraavat kolme ehtoa toteuttava relaatio R joukossa A :*

- (1) $xRx \forall x \in A$ (refleksiivisyys)
- (2) $xRy \Rightarrow yRx \forall x, y \in A$ (symmetrisyys)
- (3) $(xRy) \wedge (yRz) \Rightarrow xRz \forall x, y, z \in A$ (transitiivisuus)

Määritelmä 1.10. Olkoon $x \in A$. Alkion x määräämä relaation R *ekvivalenssiluokka* on

$$\bar{x} = \{z \in A \mid zRx\}$$

Ekvivalenssiluokan \bar{x} alkioita sanotaan sen *edustajiksi*. Sellainen A :n osajoukko, joka sisältää täsmälleen yhden edustajan kustakin ekvivalenssiluokasta on eräs *ekvivalenssiluokkien edustajisto*.

Lemma 1.1. *Olkoot \bar{x} ja \bar{y} ovat relaation R ekvivalenssiluokkia. Silloin pätevät*

- (1) $\bar{x} = \bar{y} \Leftrightarrow x \in \bar{y}$,
- (2) *joko $\bar{x} = \bar{y}$ tai $\bar{x} \cap \bar{y} = \emptyset$.*

Todistus. (1) Jos $\bar{x} = \bar{y}$, niin $x \in \bar{x} = \bar{y}$. Oletetaan sitten, että $x \in \bar{y}$. Olkoon $a \in \bar{x}$. Nyt aRx ja oletuksen nojalla xRy . Täten aRy ja näin ollen $a \in \bar{y}$. Siispä $\bar{x} \subseteq \bar{y}$. Symmetrian nojalla $\bar{y} \subseteq \bar{x}$.

(2) $z \in \bar{x} \cap \bar{y} \Rightarrow zRx \wedge zRy \Rightarrow xRz \wedge zRy \Rightarrow xRy \Rightarrow x \in \bar{y}$.

Nyt kohdan (1) nojalla $\bar{x} = \bar{y}$. □

Määritelmä 1.11. Olkoon $\mathcal{C} = \{B \mid B \subseteq A\}$ kokoelma joukon A osajoukkoja jolle pätevät seuraavat kaksi ehtoa

- (1) $A = \bigcup_{B \in \mathcal{C}} B$,
- (2) $B \cap B' = \emptyset \forall B, B' \in \mathcal{C}$.

Silloin sanotaan, että \mathcal{C} muodostaa joukon A *partition*.

Lause 1.7. *Olkoon R ekvivalenssirelaatio joukossa A ja Q jokin ekvivalenssiluokkien edustajisto. Silloin eräs joukon A on partitiio on $\{\bar{b} \mid b \in Q\}$. Kääntäen, jokainen joukon A partitiio \mathcal{C} määrittelee ekvivalenssirelaation S joukossa A : aSb joss $a, b \in B$ jollakin $B \in \mathcal{C}$.*

Todistus. Olkoon $a \in A$. Koska Q sisältää alkion b ekvivalenssiluokasta \bar{a} , niin bRa . Nyt myös aRb joten $a \in \bar{b}$. Siispä $A \subseteq \bigcup_{b \in Q} \bar{b}$. Sisältyminen $\bigcup_{b \in Q} \bar{b} \subseteq A$ on triviaali.

Osoitetaan, että $\bar{b} \cap \bar{c} = \emptyset$ kaikilla $b, c \in Q$, $b \neq c$. Oletetaan että jokin leikkaus $\bar{b} \cap \bar{c} \neq \emptyset$. Silloin Lemman 1.1 nojalla $\bar{b} = \bar{c}$ ja nyt $b, c \in \bar{c}$. Täten Q sisältää kaksi alkioita luokasta \bar{c} , mikä on mahdotonta. Siispä ko. leikkaus on tyhjä.

Käänteisen tuloksen todistaminen jätetään (helpoksi) harjoitustehtäväksi. \square

Esimerkki 1.16. Jokainen funktio $f : A \rightarrow B$ määrittelee joukon A partition $\{f^{-1}(b) \mid b \in B\}$, jolloin siis $A = \bigcup_{b \in B} f^{-1}(b)$. Tämän partition määräämän ekvivalenssirelaation S kukin ekvivalenssiluokka muodostuu täsmälleen niistä A :n alkioista joilla on sama kuva kuvauksessa f . Esimerkiksi funktion $f : \mathbb{R}^2 \rightarrow \mathbb{R}$, $f(x, y) = \sqrt{x^2 + y^2}$ määräämät ekvivalenssiluokat ovat kaikki origokeskiset ympyrät sekä origo. Eräs näiden ekvivalenssiluokkien edustajisto on $\{(x, 0) \mid x \in \mathbb{R}_{\geq 0}\}$.

Esimerkki 1.17. Määritellään relaatio R joukossa \mathbb{R}^2 näin:

$$\mathbf{a}R\mathbf{b} \Leftrightarrow \mathbf{a} = \lambda\mathbf{b} \text{ jollakin } \lambda \in \mathbb{R} \setminus \{0\}.$$

Ts. $\mathbf{a}R\mathbf{b}$ joss \mathbf{a} ja \mathbf{b} ovat samalla origon kautta kulkevalla suoralla.

Osoitetaan, että R on ekvivalenssirelaatio:

- (1) $\mathbf{a} = 1 \cdot \mathbf{a}$, joten $\mathbf{a}R\mathbf{a} \forall \mathbf{a} \in \mathbb{R}^2$,
- (2) $\mathbf{a} = \lambda\mathbf{b} \Rightarrow \mathbf{b} = \lambda^{-1}\mathbf{a}$, joten $\mathbf{a}R\mathbf{b} \Rightarrow \mathbf{b}R\mathbf{a} \forall \mathbf{a}, \mathbf{b} \in \mathbb{R}^2$,
- (3) $(\mathbf{a} = \lambda\mathbf{b} \text{ ja } \mathbf{b} = \gamma\mathbf{c}) \Rightarrow \mathbf{a} = \lambda\gamma\mathbf{c}$, joten $(\mathbf{a}R\mathbf{b} \text{ ja } \mathbf{b}R\mathbf{c}) \Rightarrow \mathbf{a}R\mathbf{c} \forall \mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{R}^2$.

Siispä R on ekvivalenssirelaatio joukossa \mathbb{R}^2 . Nyt saamme 'partition'

$$\mathbb{R}^2 = \left(\bigcup_{k \in \mathbb{R}} \{(x, kx) \mid x \in \mathbb{R} \setminus \{0\}\} \right) \cup \{(0, y) \mid y \in \mathbb{R} \setminus \{0\}\} \cup \{(0, 0)\}.$$

Tämä voidaan ilmaista vaikkapa näin $\mathbb{R}^2/R = \mathbb{R} \cup \{\infty\} \cup \{\mathbf{0}\}$.

Joukkoa $\mathbb{R}^2 \setminus \{\mathbf{0}\}/R = \mathbb{R} \cup \{\infty\}$ sanotaan projektiiviseksi 1-avaruudeksi \mathbb{R} :n suhteen, merkitään $\mathbb{P}^1(\mathbb{R})$. Yleistys: R on ekvivalenssirelaatio myös joukossa $\mathbb{R}^{n+1} \setminus \{\mathbf{0}\}$ ja sen ekvivalenssiluokat muodostavat projektiivisen n -avaruuden

$$\mathbb{P}^n(\mathbb{R}) = \left(\bigcup_{\mathbf{k} \in \mathbb{R}^n} \{(x, k_1x, \dots, k_nx) \mid x \in \mathbb{R} \setminus \{0\}\} \right) \cup \left(\bigcup_{\mathbf{k} \in \mathbb{R}^n \setminus \{\mathbf{0}\}} \{(0, k_1x, \dots, k_nx) \mid x \in \mathbb{R} \setminus \{0\}\} \right).$$

Tämä voidaan ilmaista näin: $\mathbb{P}^n(\mathbb{R}) = \mathbb{R}^n \cup \mathbb{P}^{n-1}(\mathbb{R})$.

2. LUKUTEORIAA

2.1. Jaollisuusrelaatio.

Määritelmä 2.1. Olkoot $a, b \in \mathbb{Z}$, $a \neq 0$. Luku a jakaa luvun b , jos $b = ka$ jollakin $k \in \mathbb{Z}$. Tällöin merkitään $a \mid b$. Jos a ei jaa lukua b , niin merkitään $a \nmid b$.

Huomautus. Jos $a \mid b$, niin käytetään myös ilmaisuja b on jaollinen luvulla a , b on luvun a monikerta tai a on luvun b tekijä.

Esimerkki 2.1. $3 \mid 15$, $4 \nmid 15$.

Lause 2.1. Jaollisuusrelaatiolla \mid on seuraavat ominaisuudet:

- (1) $a \mid a \quad \forall a \in \mathbb{Z} \setminus \{0\}$.
- (2) $(a \mid b) \wedge (b \mid a) \Rightarrow a = \pm b \quad \forall a, b \in \mathbb{Z} \setminus \{0\}$.
- (3) $(a \mid b) \wedge (b \mid c) \Rightarrow a \mid c \quad \forall a, b \in \mathbb{Z} \setminus \{0\}$ ja $c \in \mathbb{Z}$.
- (4) $(c \mid a) \wedge (c \mid b) \Rightarrow c \mid (ax + by) \quad \forall a, b, x, y \in \mathbb{Z}$ ja $c \in \mathbb{Z} \setminus \{0\}$.

Todistus. Todistetaan kohta (2). Loput kohdat jätetään harjoitustehtäviksi. Koska $a \mid b$, niin $b = at$ jollakin $t \in \mathbb{Z}$, $t \neq 0$. Koska $b \mid a$, niin $a = br$ jollakin $r \in \mathbb{Z}$, $r \neq 0$. Nyt $b = at = brt$ joten $rt = 1$. Siispä $r = \pm 1$. \square

Tarkastellaan seuraavaksi ”jakokulmassa jakoa”:

Lause 2.2 (Jakoalgoritmi). Olkoot $a, d \in \mathbb{Z}$ ja $d > 0$. Silloin on olemassa yksikäsitteiset luvut $q, r \in \mathbb{Z}$ joille pätee

$$a = qd + r, \quad 0 \leq r < d.$$

Todistus. Oletetaan ensin, että $a \geq 0$. Nyt a kuuluu johonkin väleistä $[qd, (q+1)d)$, missä $q \in \mathbb{Z}_{\geq 0}$. Siispä $qd \leq a < (q+1)d$ ja näin ollen $0 \leq a - qd < d$. Siispä $a = qd + r$ jollakin ehdon $0 \leq r < d$ toteuttavalla kokonaisluvulla r .

Jos $a < 0$, niin juuri todistetun nojalla $-a - 1 = qd + r$, missä $0 \leq r < d$. Täten $a = -qd - r - 1 = -(q+1)d + (d - r - 1)$ ja $0 \leq d - r - 1 < d$.

Yksikäsitteisyys: Olkoon $a = qd + r = q'd + r'$. Nyt $(q - q')d = r - r'$, joten $d \mid |r - r'|$. Mutta $0 \leq |r - r'| < d$, joten $r - r' = 0$. Nyt välttämättä myös $q = q'$.

\square

Huomautus. Jakoalgoritmi voidaan triviaalisti yleistää myös negatiivisille jakajille d : jakoalgoritmin nojalla $a = q(-d) + r = (-q)d + r$, $0 \leq r < -d$. Täten jakoalgoritmi voidaan antaa myös seuraavassa muodossa:

Olkoot $a, d \in \mathbb{Z}$ ja $d \neq 0$. Silloin on olemassa yksikäsitteiset luvut $q, r \in \mathbb{Z}$ joille pätee

$$a = qd + r, \quad 0 \leq r < |d|.$$

Edellisessä lauseessa olevilla luvuilla a, q, d, r on vakiintuneet nimitykset:

- a on jaettava
- d on jakaja
- q on osamäärä
- r on jakojäännös

Esimerkki 2.2. Jos $a = 101$ ja $d = 11$, niin $101 = 9 \cdot 11 + 2$. Tällöin siis $q = 9$ ja $r = 2$.

Seuraus. $d \mid a \Leftrightarrow r = 0$.

Sopimus. Merkitään jakojäännöstä symbolilla $a \bmod d$.

Lause 2.3. $a \bmod d = a - [a/d]d$.

Todistus. Jakoalgoritmin nojalla $a/d = q + r/d$. Koska $q \in \mathbb{Z}$ ja $0 \leq r/d < 1$, niin on oltava $[a/d] = q$. □

Esimerkki 2.3. $101 \bmod 11 = 101 - [101/11] \cdot 11 = 101 - 9 \cdot 11 = 2$.

Tarkastellaan jakoalgoritmin sovelluksena kokonaisluvun esittämistä eri lukujärjestelmissä. Esimerkiksi luvulle kaksituhattakolmesataaviisikymmentäkaksi käytämme lyhennysmerkinä 2352. Esitämme siis kyseisen luvun antamalla sen numerot kymmenjärjestelmässä, ts.

$$2352 = 2 \cdot 10^3 + 3 \cdot 10^2 + 5 \cdot 10 + 2.$$

Lause 2.4. *Olkoon $b \in \mathbb{Z}$, $b \geq 2$. Jokainen $a \in \mathbb{N}$ voidaan esittää yksikäsitteisesti muodossa*

$$(*) \quad a = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0,$$

missä $n \in \mathbb{Z}_{\geq 0}$ ja $0 \leq a_i < b$ kaikilla $i = 0, \dots, n$.

Todistus. Sovelletaan jakoalgoritmia toistuvasti:

$$\begin{array}{lll}
 a = q_0b + a_0, & 0 \leq a_0 < b & \\
 q_0 = q_1b + a_1, & 0 \leq a_1 < b, & q_1 < q_0 \\
 q_1 = q_2b + a_2, & 0 \leq a_2 < b, & q_2 < q_1 \\
 \vdots & & \\
 q_{n-2} = q_{n-1}b + a_{n-1}, & 0 \leq a_{n-1} < b, & q_{n-1} < q_{n-2} \\
 q_{n-1} = 0 \cdot b + a_n, & 0 \leq a_n < b &
 \end{array}$$

Menettely päättyy sillä luvut q_i muodostavat aidosti vähenevän jonon positiivia kokonaislukuja. Eliminoidaan nyt luvut q_0, q_1, \dots, q_{n-1} : $a = (q_1b + a_1)b + a_0 = q_1b^2 + a_1b + a_0 = (q_2b + a_2)b^2 + a_1b + a_0 = q_2b^3 + a_2b^2 + a_1b + a_0 = \dots = a_nb^n + \dots + a_1b + a_0$.

Yksikäsitteisyyden todistaminen jätetään harjoitustehtäväksi. \square

Määritelmä 2.2. Esitys (*) on luvun a b -kantainen esitys (tai esitys b -järjestelmässä). Luvut a_i ovat a :n numerot b -kantaisessa esityksessä. Merkitään $a = (a_n a_{n-1} \dots a_0)_b$.

Esimerkki 2.4. 2-järjestelmän luku eli binääriluku $(101000110)_2$ on kymmenjärjestelmässä $1 \cdot 2^8 + 1 \cdot 2^6 + 1 \cdot 2^2 + 1 \cdot 2 = 326$.

Lauseen 2.4 todistus antaa seuraavan algoritmin luvun a esittämiseksi b -järjestelmässä:

```

Input:  $a, b \in \mathbb{N}, b \geq 2$ 
Output: Luvun  $a$  numerot  $b$ -järjestelmässä
Set  $i = 0$ 
While  $a > 0$  Do
    Set  $a_i = a \bmod b$ 
    Set  $a = \lfloor a/b \rfloor$ 
    Set  $i = i + 1$ 
EndWhile
Return  $a_0, a_1, \dots, a_{i-1}$ 

```

Esimerkki 2.5. $a = 74, b = 3$.

$$\begin{array}{ll} a_0 = 74 \bmod 3 = 2 & [74/3] = 24 \\ a_1 = 24 \bmod 3 = 0 & [24/3] = 8 \\ a_2 = 8 \bmod 3 = 2 & [8/3] = 2 \\ a_3 = 2 \bmod 3 = 2 & [2/3] = 0 \end{array}$$

Täten $74 = (2202)_3$. (Tarkistus: $2 \cdot 3^3 + 2 \cdot 3^2 + 2 = 74$)

Esimerkki 2.6. Olkoon $b = 16$ eli kyseessä ovat *heksadesimaaliluvut*. Nyt merkitään $A=10, B=11, C=12, D=13, E=14, F=15$. Muodostetaan binääriluvun $a = 1011001011101000101101111$ heksadesimaaliestys.

Tapa 1. Esitetään a ensin 10-järjestelmän lukuna $a = 2^{24} + 2^{22} + \dots + 2 + 1$ ja sovelletaan sitten eo. algoritmia 10-järjestelmän lukuihin a ja $b = 16$.

Tapa 2. (Nopeampi menetelmä) Ryhmitellään bitit neljän bitin blokkeihin lopusta lähtien:

$$\underbrace{0001}_1 \mid \underbrace{0110}_6 \mid \underbrace{0101}_5 \mid \underbrace{1101}_D \mid \underbrace{0001}_1 \mid \underbrace{0110}_6 \mid \underbrace{1111}_F$$

Siispä $a = (165D16F)_{16}$.

2.2. Suurin yhteinen tekijä ja Eukleideen algoritmi. Koska $0 = 0 \cdot a$ kaikilla $a \in \mathbb{Z}$, niin jokainen nollasta eroava kokonaisluku on 0:n tekijä. Muilla luvuilla on vain äärellinen määrä tekijöitä: jos $n \in \mathbb{Z}$, niin sen tekijät d ovat välillä $-n \leq d \leq n$.

Määritelmä 2.3. Olkoot $a, b \in \mathbb{Z}, a \neq 0$. Jos $d \mid a$ ja $d \mid b$, niin d on lukujen a ja b *yhteinen tekijä*. Lukujen a ja b *suurin yhteinen tekijä*, merkitään $\text{syt}(a, b)$, on lukujen a ja b yhteisten tekijöiden joukon suurin alkio.

Huomautus. Suurin yhteinen tekijä on aina positiivinen.

Esimerkki 2.7. Etsitään $\text{syt}(24, 32)$. Luvun 24 positiiviset tekijät ovat 1,2,3,4,6,8,12,24 ja luvun 32 positiiviset tekijät ovat 1,2,4,8,16,32. Täten lukujen 24 ja 32 yhteiset positiiviset tekijät ovat 1,2,4,8 ja näistä suurin on 8. Siispä $\text{syt}(24, 32) = 8$.

Luettelointiin perustuva menetelmä hankaloituu nopeasti lukujen kasvaessa. Sen sijaan jakoalgoritmin sovelluksena saamme erittäin tehokkaan menetelmän $\text{syt}(a, b)$:n ($b > 0$) laskemiseksi, nk. *Eukleideen algoritmin*:

$$\begin{aligned} a &= q_1 b + r_1, & 0 < r_1 < b \\ b &= q_2 r_1 + r_2, & 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3, & 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

Menettely päättyy koska jakojäännökset muodostavat aidosti vähenevän jonon positiivia kokonaislukuja. Lisäksi viimeinen nollasta eroava jakojäännös $r_n = \text{syt}(a, b)$. Tämä nähdään todeksi soveltamalla toistuvasti seuraavan lauseen Seurausta, joka lopulta antaa yhtälön $\text{syt}(a, b) = \text{syt}(r_n, 0) = r_n$.

Lause 2.5. *Olkoot $a, b \in \mathbb{Z}$, $b > 0$. Silloin*

$$\text{syt}(a, b) = \text{syt}(a + kb, b) \quad \forall k \in \mathbb{Z}.$$

Todistus. Olkoon $k \in \mathbb{Z}$. Osoitetaan, että

$$A := \{d \in \mathbb{N} \mid (d \mid a) \wedge (d \mid b)\} = \{d \in \mathbb{N} \mid (d \mid (a + kb)) \wedge (d \mid b)\} := B.$$

Jos $d \mid a$ ja $d \mid b$, niin lauseen 2.1 nojalla $d \mid (a + kb)$. Täten $A \subseteq B$.

Jos $d \mid (a + kb)$ ja $d \mid b$, niin jälleen lauseen 2.1 nojalla $d \mid ((a + kb) - kb)$. Siispä $B \subseteq A$. Täten $A = B$ ja näin ollen niillä on sama suurin alkio. \square

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

Todistus. $a \bmod b = a - [a/b]b$. \square

Esimerkki 2.8. Lasketaan jälleen $\text{syt}(24, 32)$. Nyt Eukleideen algoritmilla.

$$32 = 1 \cdot 24 + 8$$

$$24 = 3 \cdot 8$$

Siispä $\text{syt}(24, 32) = 8$.

Seuraavaksi lauseeseen 2.5 perustuva rekursiivinen algoritmi $\text{syt}(a, b)$:n laskemiseksi:

Input: $a, b \in \mathbb{Z}, b > 0$
 Output: $\text{syt}(a, b)$
 Function Eukleides(a, b)
 If $b = 0$ Then Return $|a|$
 Set $d = \text{Eukleides}(b, a \bmod b)$
 Return d

Tarkastellaan vielä esimerkkiä 2.8. Näemme, että $\text{syt}(24, 32) = 1 \cdot 32 - 1 \cdot 24$.
 Ts. luku $\text{syt}(24, 32)$ voidaan esittää lukujen 24 ja 32 \mathbb{Z} -lineaarisenä kombinaationa.
 Tämä ei ole sattumaa sillä on voimassa

Lause 2.6. *Olko $a, b \in \mathbb{Z}$. Silloin on olemassa sellaiset kokonaisluvut x ja y , että $\text{syt}(a, b) = xa + yb$.*

Todistus. Eliminoidaan Eukleideen algoritmista jakojäännökset järjestyksessä $r_{n-1}, r_{n-2}, \dots, r_1$. □

Esimerkki 2.9. Lasketaan $d := \text{syt}(78, 99)$ ja esitetään se muodossa $d = x \cdot 78 + y \cdot 99$, missä $x, y \in \mathbb{Z}$.

$$99 = 1 \cdot 78 + 21$$

$$78 = 3 \cdot 21 + 15$$

$$21 = 1 \cdot 15 + 6$$

$$15 = 2 \cdot 6 + 3$$

$$(6 = 2 \cdot 3)$$

Siispä $\text{syt}(99, 78) = 3 = 15 - 2 \cdot 6 = 15 - 2 \cdot (21 - 15) = 3 \cdot 15 - 2 \cdot 21 = 3 \cdot (78 - 3 \cdot 21) - 2 \cdot 21 = 3 \cdot 78 - 11 \cdot 21 = 3 \cdot 78 - 11 \cdot (99 - 78) = 14 \cdot 78 - 11 \cdot 99$.

Seuraavaksi *Laajennettu Eukleideen algoritmi*, joka laskee $\text{syt}(a, b)$:n lisäksi myös Lauseessa 2.6 esiintyvät luvut x ja y .

Input: $a, b \in \mathbb{Z}, b > 0$

Output: $\text{syt}(a, b), x, y$

Function LaajennettuEukleides(a, b)

If $b = 0$ Then Return $|a|, 1, 0$

Set $(d_1, x_1, y_1) = \text{LaajennettuEukleides}(b, a \bmod b)$

Set $(d, x, y) = (d_1, y_1, x_1 - [a/b]y_1)$

Return d, x, y

Lause 2.6 implikoi seuraavan karakterisoinnin syt :lle:

Seuraus. Olkoot $a, b \in \mathbb{Z}$. Olkoon d luonnollinen luku, joka toteuttaa seuraavat kaksi ehtoa

- (1) $d \mid a$ ja $d \mid b$,
- (2) $\forall c \in \mathbb{Z} : (c \mid a) \wedge (c \mid b) \Rightarrow c \mid d$.

Silloin $d = \text{syt}(a, b)$. Kääntäen, $\text{syt}(a, b)$ toteuttaa luvulle d asetetut ehdot (1) ja (2).

Todistus. Harjoitustehtävä. □

2.3. Alkuluvut ja aritmetiikan peruslause.

Määritelmä 2.4. Kokonaisluku $p > 1$ on *alkuluku* jos sillä ei ole muita positiivisia tekijöitä kuin *triviaalit tekijät* 1 ja p . Muut kokonaisluvut $n > 1$ ovat *yhdistettyjä* lukuja. Merkitään kaikkien alkulukujen joukkoa symbolilla \mathbb{P} .

Esimerkki 2.10. 2,3,5,7,11,13 ovat alkulukuja.

Alkulukuihin liittyviä kysymyksiä

- Miten testataan onko annettu luku alkuluku?
- Mitkä ovat annetun luvun alku(luku)tekijät?
- Miten alkulukuja generoidaan?

Suoraviivainen tapa testata onko annettu luku alkuluku on kokeilu. Seuraava lause helpottaa kokeilutyötä.

Lause 2.7. *Olkoon $a \in \mathbb{Z}$, $a > 1$. Luku a on alkuluku jos ja vain jos sillä ei ole ehdon $1 < d \leq \lfloor \sqrt{a} \rfloor$ täyttävää tekijää d .*

Todistus. Jos a on alkuluku, niin sen ainoat positiiviset tekijät ovat 1 ja p . Oletetaan sitten, että a ei ole alkuluku. Nyt $a = da'$, missä $1 < d, a' < a$. Jos sekä $d > \sqrt{a}$, että $a' > \sqrt{a}$, niin $a = da' > a$. Täten, joko $1 < d \leq \sqrt{a}$ tai $1 < a' \leq \sqrt{a}$. Koska d ja a' ovat kokonaislukuja, niin väite on todistettu. \square

Esimerkki 2.11. Onko 101 alkuluku? Koska 101 on pariton ja $\lfloor \sqrt{101} \rfloor = 10$, niin riittää tarkastella onko jokin luvuista 3, 5, 7, 9 sen tekijä. Yksikään näistä ei ole luvun 101 tekijä joten se on alkuluku. Onko 143 alkuluku? Nyt $\lfloor \sqrt{143} \rfloor = 11$ ja $11 \mid 143$, joten 143 on yhdistetty luku.

Esittämämme kokeilumenetelmä käy nopeasti liian työlääksi luvun a kasvaessa. Alkulukutestaukseen on kehitetty algoritmeja esimerkiksi *Millerin ja Rabinin alkulukuseula* joilla voidaan testata jopa 1000-numeroisten lukujen jaottomuus kohtalaisen nopeasti.

Seuraavaksi osoitamme, että jokainen kokonaisluku > 1 voidaan esittää alkulukujen tulona. Tämän tuloksen todistamiseksi tarvitsemme seuraavan lemmän.

Lemma 2.1. *Olkoon $p \in \mathbb{P}$. Jos $p \mid ab$, niin $p \mid a$ tai $p \mid b$. Yleisemmin: jos $p \mid a_1 a_2 \cdots a_m$, niin $p \mid a_i$ jollakin $i = 1, \dots, m$.*

Todistus. Jos $p \nmid b$, niin $\text{syt}(p, b) = 1$, sillä p :n ainoat tekijät ovat $\pm 1, \pm p$. Nyt lauseen 2.6 nojalla $1 = xp + yb$ ja täten $a = xap + yab$. Koska p jakaa oikean puolen, niin se jakaa myös vasemman puolen. Yleistyksen todistus jätetään harjoitustehtäväksi. \square

Lause 2.8 (Aritmetiikan peruslause). *Jokainen kokonaisluku $a > 1$ voidaan esittää alkulukujen tulona*

$$a = p_1 p_2 \cdots p_n.$$

Tämä esitys on yksikäsitteinen lukuunottamatta lukujen p_i järjestystä.

Todistus. Tarkastellaan kaikkia sellaisia kokonaislukuja > 1 joita ei voida esittää alkulukujen tulona. Jos tällaisia lukuja on olemassa, niin valitaan niistä pienin. Olkoon se b . Nyt b ei voi olla alkuluku, joten $b = uv$ joillakin $u, v \in \mathbb{Z}$, $1 < u, v <$

b. Nyt u ja v voidaan esittää alkulukujen tulona, joten myös b voidaan esittää alkulukujen tulona. Tämä ristiriita todistaa ensimmäisen väitteen.

Olkoon $a \in \mathbb{Z}$, $a > 1$ ja

$$(*) \quad a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m,$$

missä $n \leq m$ ja $p_i, q_j \in \mathbb{P}$ kaikilla $i = 1, \dots, n$, $j = 1, \dots, m$. Koska p_1 jakaa $(*)$:n jälkimmäisen yhtälön oikean puolen, niin Lemman nojalla $p_1 \mid q_j$, jollakin $j = 1, \dots, m$. Nyt $p_1 = q_j$ ja indeksointia tarvittaessa vaihtamalla voimme olettaa, että $p_1 = q_1$. Täten

$$p_2 \cdots p_n = q_2 \cdots q_m.$$

Samoin jatkamalla saadaan $p_2 = q_2, \dots, p_n = q_n$ ja $m = n$. \square

Seuraus (Eukleides). *Alkulukuja on äärettömän monta.*

Todistus. Oletetaan, että alkulukuja on vain äärellinen määrä. Olkoot ne p_1, \dots, p_n ja tarkastellaan lukua $m = p_1 p_2 \cdots p_n + 1$. Olkoon q mikä tahansa luvun m alkutekijä. Nyt $q = p_i$ jollakin $i = 1, \dots, n$. Nyt Lauseen 2.1 kohdan (4) nojalla $q \mid \underbrace{m - p_1 \cdots p_n}_{=1}$, mikä on mahdotonta. \square

Huomautus. Luvun a esitystä alkulukujen tulona sanotaan a :n *alkutekijähajoitelmaksi*. Se annetaan usein nk. *kanonisessa muodossa*

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \quad p_1 < p_2 < \cdots < p_k, \quad e_i > 0 \quad \forall i = 1, \dots, k.$$

Esimerkki 2.12. Luvun 196 kanoninen hajoitelma on: $196 = 2^2 \cdot 7^2$.

Huomautus. Vertailtaessa kahden luvun alkutekijähajoitelmia on usein mukava sallia eksponenteille e_i myös arvo 0.

Lause 2.9. *Olkoot $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ ja $b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$, $p_1 < p_2 < \cdots < p_k$ ja $e_i, f_i \geq 0$. Silloin*

$$\text{syt}(a, b) = p_1^{g_1} p_2^{g_2} \cdots p_k^{g_k},$$

missä $g_i = \min\{e_i, f_i\}$ kaikilla $i = 1, \dots, k$.

Todistus. Luvun a tekijät ovat $p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$, $0 \leq d_i \leq e_i$ kaikilla $i = 1, \dots, k$. Luvun b tekijät ovat $p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$, $0 \leq d_i \leq f_i$ kaikilla $i = 1, \dots, k$. Täten lukujen a ja b yhteiset tekijät ovat $p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$, $0 \leq d_i \leq \min\{e_i, f_i\}$ kaikilla $i = 1, \dots, k$, ja näistä suurin on juuri väitteen luku. \square

Esimerkki 2.13. $\text{synt}(35640, 7409556) = \text{synt}(2^3 \cdot 3^4 \cdot 5 \cdot 11, 2^2 \cdot 3^7 \cdot 7 \cdot 11^2) = 2^2 \cdot 3^4 \cdot 5^0 \cdot 7^0 \cdot 11^1 = 3564$.

Huomautus. Annetun kokonaislukujen tekijöihin jakoa pidetään hyvin vaikeana probleemana. Esimerkiksi RSA-salakirjoitusmenetelmän luotettavuus perustuu nykytiedon mukaan juuri tähän, ja RSA Company onkin luvannut 20000 Dollarin palkkion luvun seuraavan ”vain” 193 numeroisen luvun tekijöihin jaosta:

31074182404900437213507500358885679300373460228427
 27545720161948823206440518081504556346829671723286
 78243791627283803341547107310850191954852900733772
 4822783525742386454014691736602477652346609

Tämä luku on nimetty *RSA* – 640:ksi koska sen binääriesityksessä on 640 numeroa. Lisätietoa ja muita haastavia tekijöihinjakoprobleemoja sivulla <http://www.rsasecurity.com/rsalabs/node.asp?id=2093>.

Tarkastellaan vielä alkulukujen generointia. *Eratosteneen seula* on nopea tapa tuottaa kaikki kiinitettyä lukua n pienemmät alkuluvut, kunhan n ei ole ”liian suuri”. Periaate on sangen yksinkertainen:

Olkoon $\bar{b} = (1, 1, \dots, 1) \in \{0, 1\}^n$ ja $k = 2$. Toistetaan seuraavia askeleita kunnes $k > \lfloor \sqrt{n} \rfloor$:

- (1) Askel 1. Asetetaan $b_{ki} := 0$ kaikilla $i = 2, \dots, \lfloor n/k \rfloor$.
- (2) Askel 2. Olkoon $j > k$ ensimmäinen indeksi jolle $b_j = 1$. Asetetaan $k := j$ ja siirrytään askeleeseen 1.

Nyt täsmälleen ne indeksit $j > 1$ joilla $b_j = 1$ ovat alkulukuja.

Tämän väittämän perustelemiseksi tarvitsemme lauseen 2.7 pienen täsmennyksen.

Lause 2.10. *Olkoon $a \in \mathbb{Z}$, $a > 1$. Luku on alkuluku jos ja vain jos sillä ei ole ehdon $1 < p \leq \lfloor \sqrt{a} \rfloor$ täyttävää alkutekijää p .*

Todistus. Harjoitustehtävä. □

Nyt voimme perustella Eratosteneen seulan toimivuuden: jos $j > 1$ ja $b_j = 0$, niin j ei ole alkuluku, sillä algoritmi nolaa vain yhdistettyjä lukuja vastaavia \bar{b} :n komponentteja. Täten jokaista välin $[2, n]$ alkulukua j kohti on $b_j = 1$. Voiko olla

yhdistettyjä lukuja j joilla $b_j = 1$? Ei voi, sillä nyt Lauseen 2.10 nojalla j :llä on alkutekijä $p \leq \lfloor \sqrt{j} \rfloor \leq \lfloor \sqrt{n} \rfloor$. Täten b_j on nollattu kun $k = p$.

Esimerkki 2.14. Generoidaan kaikki lukua 100 pienemmät alkuluvut Eratosteneen seulalla.

Huomautus. Käytännössä suurten alkulukujen generointiin käytetään jotain Millerin ja Rabinin seulan tyyppistä algoritmia sekä *alkulukulausetta*, jonka mukaan

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} = 1,$$

missä $\pi(x)$ lukua x pienempien alkulukujen lukumäärä. Olkoon esimerkiksi $b = 10^{100}$. Nyt ”lähellä” b :tä noin joka $\ln b$:s luku on alkuluku. Valitaan pariton luku n , $n \approx 10^{100}$. Jos n ei ole alkuluku, niin kokeillaan olisiko $n + 2$ alkuluku jne. Nyt likimain $\ln b/2 \approx 115$ yritystä riittää.

Tällaisen menetelmän generoimat alkuluvut ovat kuitenkin vain potentiaalisia alkulukuja: ne saattavat olla yhdistettyjä, mutta tällaisten tapausten todennäköisyys saadaan riittävän pieneksi kohtuullisessa laskenta-ajassa.

2.4. Modulaariaritmetiikkaa. Seuraavaksi otamme käyttöön merkinnän joka mahdollistaa jaollisuustarkastelujen tekemisen lineaaristen yhtälöiden $ax = b$ käsittelyä muistuttavalla tavalla.

Määritelmä 2.5. Olkoot $a, b, c \in \mathbb{Z}$, $c > 0$. Luku a on kongruentti b :n kanssa modulo m , jos $m \mid (a - b)$. Tällöin merkitään

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

Huomautus. Usein käytetään myös merkintää $a \equiv b \pmod{m}$.

Esimerkki 2.15. $20 \equiv 1 \equiv -18 \pmod{19}$. Itse asiassa $20 \equiv 1 + 19t \pmod{19}$ kaikilla $t \in \mathbb{Z}$.

Lause 2.11. $a \equiv b \pmod{m} \Leftrightarrow a \bmod m = b \bmod m$.

Todistus. Jakoalgoritmin nojalla $a = q_1m + r_1$, $b = q_2m + r_2$, $0 \leq r_1, r_2 < m$.

Nyt siis $r_1 = a \bmod m$ ja $r_2 = b \bmod m$ ja

$$a \equiv b \pmod{m} \Rightarrow m \mid (a - b) \Rightarrow m \mid ((q_1 - q_2)m + (r_1 - r_2)) \stackrel{L. 2.1(4)}{\Rightarrow} m \mid (r_1 - r_2) \Rightarrow r_1 = r_2.$$

Kääntäen,

$$r_1 = r_2 \Rightarrow (a - b) = (q_1 - q_2)m \Rightarrow m \mid (a - b) \Rightarrow a \equiv b \pmod{m}.$$

□

Lause 2.12. *Olkoot $a, b, c, d, m \in \mathbb{Z}$, $m > 0$. Silloin pätevät*

- (1) $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$,
- (2) $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$,
- (3) $\text{syt}(a, m) = 1$ ja $ab \equiv ac \pmod{m} \Rightarrow b \equiv c \pmod{m}$.

Todistus. (1) Koska $a \equiv b \pmod{m}$, niin määritelmän nojalla $a - b = mk$ jollakin $k \in \mathbb{Z}$. Samoin $c - d = mt$, jollakin $t \in \mathbb{Z}$. Nyt $a + c - (b + d) = (a - b) + (c - d) = mk + mt = m(k + t)$.

(2) $ac = a(d + mt) = ad + amt = (b + mk)d + amt = bd + mkd + amt = bd + m(kd + at)$.

(3) Koska $mk = ab - ac = a(b - c)$ jollakin $k \in \mathbb{Z}$, niin $m \mid a(b - c)$. Koska $\text{syt}(a, m) = 1$, niin $m \mid (b - c)$. □

Seuraus. *Olkoon $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ polynomi jonka kertoimet $a_i \in \mathbb{Z}$ kaikilla $i = 0, \dots, n$. Silloin*

$$a \equiv b \pmod{m} \Rightarrow f(a) \equiv f(b) \pmod{m}.$$

Todistus. Valitaan lauseessa $c = a$ ja $d = b$, ja sovelletaan toistuvasti kohtaa (2) jolloin saadaan $a^i \equiv b^i \pmod{m}$ kaikilla $i = 1, \dots, n$. Nyt kohdan (2) nojalla $a_i a^i \equiv a_i b^i \pmod{m}$ kaikilla $i = 1, \dots, n$, ja väite seuraa kun nyt käytetään toistuvasti kohtaa (1). □

Esimerkki 2.16. Lasketaan luvun $9^{1531} - 1$ viimeinen numero kymmenjärjestelmässä. Olkoon $9^{1531} - 1 = a_n 10^n + \dots + a_1 10 + a_0$. Koska $10 \equiv 0 \pmod{10}$, niin Lauseen 2.12 seurauksen nojalla

$$9^{1531} - 1 \equiv a_n 0^n + \dots + a_1 0 + a_0 \equiv a_0 \pmod{10}.$$

Toisaalta

$$9 \equiv -1 \pmod{10} \stackrel{L. 2.12\text{Seur.}}{\Rightarrow} 9^{1531} \equiv (-1)^{1531} \equiv -1 \pmod{10} \stackrel{L. 2.12(1)}{\Rightarrow} 9^{1531} - 1 \equiv -1 - 1 \equiv 8 \pmod{10}.$$

Täten $a_0 \equiv 8 \pmod{10}$, ja koska $0 \leq a_0 < 10$, niin $a_0 = 8$. Nyt Lauseen 2.11 nojalla kysytty jakojäännös on 8.

Esimerkki 2.17. Osoitetaan, että luku $a = a_n 10^n + \dots + a_1 10 + a_0$ on jaollinen luvulla 3 jos ja vain jos sen numeroiden summa on jaollinen 3:lla. Koska $10 \equiv 1 \pmod{3}$,

niin Lauseen 2.12 seurauksen nojalla

$$a \equiv a_n 1^n + \cdots + a_1 1 + a_0 \equiv a_n + \cdots + a_1 + a_0 \quad (3).$$

Nyt Lauseen 2.11 nojalla $3 \mid a \Leftrightarrow 3 \mid (a_n + \cdots + a_1 + a_0)$.

Täten esimerkiksi $3 \mid 123456789$, sillä $1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 = 9 \cdot 10/2 = 45$ ja $3 \mid 45$.

Tarkastellaan seuraavaksi kongruenssin

$$ax \equiv b \quad (m)$$

ratkaisemista, kun a, b ja $m > 1$ ovat vakioita ja x on muuttuja.

Lemma 2.2. *Jos x_0 on kongruenssin $ax \equiv b \quad (m)$ ratkaisu, niin myös $x_0 + km$ on sen ratkaisu kaikilla $k \in \mathbb{Z}$.*

Todistus. $a(x_0 + km) = ax_0 + akm \stackrel{L. 2.12(1)}{\equiv} ax_0 + 0 \equiv b \quad (m)$. □

Huomautus. Jos kongruenssilla $ax \equiv b \quad (m)$ on ratkaisu x_0 , niin Lemman 2.2 nojalla sillä on myös välille $[0, m - 1]$ kuuluva ratkaisu, nimittäin $x_0 \bmod m (= x_0 - \left[\frac{x_0}{m}\right]m)$.

Lemma 2.3. (1) *Kongruenssi $ax \equiv b \quad (m)$ on ratkeava jos ja vain jos $\text{syt}(a, m) \mid b$.*
 (2) *Kongruenssilla $ax \equiv b \quad (m)$ on yksikäsitteinen välille $[0, m - 1]$ kuuluva ratkaisu jos $\text{syt}(a, m) = 1$.*

Todistus. Merkitään $d = \text{syt}(a, m)$.

(1) Jos $ax_0 \equiv b \quad (m)$ jollakin $x_0 \in \mathbb{Z}$, niin $ax_0 = b + km$ ja täten $d \mid b$.

Oletetaan sitten että $d \mid b$, ja osoitetaan että kongruenssi on ratkeava. Lauseen 2.6 nojalla $d = ax_0 + my$ joillakin $x_0, y \in \mathbb{Z}$. Kun tämä yhtälö kerrotaan puolittain kokonaisluvulla b/d niin saadaan yhtälö $b = a(x_0 b/d) + myb/d$. Täten $ax \equiv b \quad (m)$ on ratkeava.

(2) Kohdan (1) sekä huomatuksen nojalla kongruenssilla on välille $[0, m - 1]$ kuuluva ratkaisu x_0 . Olkoon myös y tälle välille kuuluva ratkaisu. Nyt $ax_0 \equiv ay \quad (m)$ ja Lauseen 2.12 (3) nojalla $x_0 \equiv y \quad (m)$. Koska $0 \leq x_0, y < m$, niin on oltava $x_0 = y$. □

Lemma 2.4. *Olkoon $d = \text{syt}(a, m)$ ja oletetaan, että $d \mid b$. Silloin*

$$ax \equiv b \quad (m) \Leftrightarrow \frac{a}{d}x \equiv \frac{b}{d} \quad \left(\frac{m}{d}\right).$$

Ts. näillä kongruensseilla on samat ratkaisujoukot.

Todistus.

$$ax_0 \equiv b \pmod{m} \Leftrightarrow ax_0 = b + km \Leftrightarrow \frac{a}{d}x_0 = \frac{b}{d} + k\frac{m}{d} \Leftrightarrow \frac{a}{d}x_0 \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

□

Lause 2.13. *Jos kongruenssi*

$$(*) \quad ax \equiv b \pmod{m}$$

on ratkeava, niin sen välille $[0, \dots, m-1]$ kuuluvat ratkaisut ovat

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \dots, x_0 + (d-1)\frac{m}{d},$$

missä $d = \text{syt}(a, m)$ ja x_0 on kongruenssin

$$(**) \quad \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

välille $[0, m/d - 1]$ kuuluva yksikäsitteinen ratkaisu.

Todistus. Koska $\text{syt}(a/d, m/d) = 1$, niin Lemman 2.3 (2) nojalla kongruenssilla (**) on yksikäsitteinen välille $[0, m/d - 1]$ kuuluva ratkaisu x_0 . Täten sen välille $[0, m-1]$ kuuluvat ratkaisut ovat $x_0 + km/d$, missä $k = 0, \dots, d-1$. Nyt Lemman 2.4 nojalla ne ovat myös kongruenssin (*) ratkaisuja.

Kongruenssilla (*) ei ole muita välille $[0, m-1]$ kuuluvia ratkaisuja, jälleen Lemman 2.4 nojalla. □

Seuraus. *Kongruenssilla $ax \equiv b \pmod{m}$ on yksikäsitteinen välille $[0, m-1]$ kuuluva ratkaisu jos ja vain jos $\text{syt}(a, m) = 1$.*

Esimerkki 2.18. Kongruenssilla $310x \equiv 21 \pmod{15}$ ei ole ratkaisua, sillä $\text{syt}(310, 15) = \text{syt}(2 \cdot 5 \cdot 31, 3 \cdot 5) = 5$ ja $5 \nmid 21$.

Määritelmä 2.6. Kongruenssin $ax \equiv b \pmod{m}$ välille $[0, m-1]$ kuuluvia ratkaisuja sanotaan sen *ratkaisuiksi modulo m* .

Huomautus. Seuraava pieni havainto helpottaa usein kongruenssien ratkaisemista: Jos $a \equiv a' \pmod{m}$ ja $b \equiv b' \pmod{m}$, niin

$$ax \equiv b \pmod{m} \Leftrightarrow a'x \equiv b' \pmod{m}.$$

Ts. eo. kongruensseilla on samat ratkaisujoukot. (Perustelu: harjoitustehtävä).

Esimerkki 2.19. Ratkaise kongruenssi $310x \equiv 20 \pmod{15}$. Koska $310 \equiv 10 \pmod{15}$ ja $20 \equiv 5 \pmod{15}$, niin ratkaistavana on kongruenssi $10x \equiv 5 \pmod{15}$. Nyt $\text{syt}(10, 15) = 5$ joten ratkaistavana on kongruenssi $2x \equiv 1 \pmod{3}$. Kokeilemalla x :n paikalle lukuja $0, 1, 2$ havaitsemme, että $2 \cdot 2 \equiv 1 \pmod{3}$. Täten alkuperäisen kongruenssin ratkaisut modulo 15 ovat $2, 2 + 1 \cdot 3, 2 + 2 \cdot 3, 2 + 3 \cdot 3$ ja $2 + 4 \cdot 3$ eli $2, 5, 8, 11$ ja 14 , ja sen ratkaisujoukko on $\{2 + 15k \mid k \in \mathbb{Z}\} \cup \{5 + 15k \mid k \in \mathbb{Z}\} \cup \{8 + 15k \mid k \in \mathbb{Z}\} \cup \{11 + 15k \mid k \in \mathbb{Z}\} \cup \{14 + 15k \mid k \in \mathbb{Z}\}$.

Huomautus. Edellisessä esimerkissä kokeilu voidaan korvata Laajennetulla Eukleideen algoritmilla. Tarkastellaan kongruenssia $ax \equiv b \pmod{m}$ ja oletetaan että $\text{syt}(a, m) = 1$. Lauseen 2.6 nojalla $at + my = 1$ joillakin $t, y \in \mathbb{Z}$. Siispä $at \equiv 1 \pmod{m}$. Kun nyt kerrotaan kongruenssi $ax \equiv b \pmod{m}$ puolittain luvulla t , saadaan $x \equiv bt \pmod{m}$ ja täten kongruenssin yksikäsitteinen ratkaisu modulo m on jakojäännös $bt \pmod{m}$.

Määritelmä 2.7. Olkoot $a, m \in \mathbb{Z}, m > 1$. Oletetaan, että $\text{syt}(a, m) = 1$. Kongruenssin $ax \equiv 1 \pmod{m}$ yksikäsitteistä ratkaisua modulo m sanotaan a :n *käänteisalkkioksi modulo m* . Merkitään $a^{-1} \pmod{m}$.

Esimerkki 2.20. Ratkaistaan kongruenssi $13x \equiv 25 \pmod{29}$. Nyt $\text{syt}(13, 29) = 1$ ja $1 = 13 \cdot 9 + 29 \cdot (-4)$. Täten $13^{-1} \pmod{29} = 9$ ja $x \equiv 9 \cdot 25 \equiv 22 \pmod{29}$. Täten kongruenssin $13x \equiv 25 \pmod{29}$ yksikäsitteinen välille $[0, 28]$ kuuluva ratkaisu on 22 ja sen ratkaisujoukko on $\{22 + 29k \mid k \in \mathbb{Z}\}$.

2.5. Kongruenssiryhmistä. Tarkastellaan seuraavaksi kongruenssiparin

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

ratkaisemista. Etsittävänä on siis näiden kongruenssien yhteiset ratkaisut.

Lause 2.14. *Olkoot $m, n \in \mathbb{N}, \text{syt}(m, n) = 1$. Silloin eo. kongruenssiparilla on ratkaisu $x = a + (b - a)mm'$, missä $mm' \equiv 1 \pmod{n}$. Lisäksi jakojäännös $x_0 := x \pmod{mn}$ on parin yksikäsitteinen ratkaisu modulo mn , ja sen ratkaisujoukko on $\{x_0 + kmn \mid k \in \mathbb{Z}\}$.*

Todistus. Koska $\text{syt}(m, n) = 1$, niin kongruenssilla $mx \equiv 1 \pmod{n}$ on ratkaisu m' . Olkoon $x = a + (b - a)mm'$. Nyt $x \equiv a \pmod{m}$ ja $x \equiv a + (b - a) \cdot 1 \equiv b \pmod{n}$.

Merkitään $x_0 = x \pmod{mn}$. Nyt $x_0 = x + tmn$ jollakin $t \in \mathbb{Z}$ joten $x_0 \equiv x \pmod{m}$ ja $x_0 \equiv x \pmod{n}$. Siispä x_0 on eräs välille $[0, mn - 1]$ kuuluva kongruenssiparin ratkaisu.

Olkoon y mikä tahansa parin ratkaisu jolloin siis $y_0 := y \pmod{mn}$ on välille $[0, mn - 1]$ kuuluva ratkaisu. Nyt $x_0 \equiv y_0 \pmod{m}$ ja $x_0 \equiv y_0 \pmod{n}$, joten $m \mid (x_0 - y_0)$ ja $n \mid (x_0 - y_0)$. Koska $\text{syt}(m, n) = 1$, niin myös $mn \mid (x_0 - y_0)$ ja näin ollen $x_0 = y_0$. \square

Esimerkki 2.21. Ratkaistaan kongruenssipari

$$x \equiv 3 \pmod{5} \quad (5)$$

$$x \equiv 1 \pmod{7} \quad (7)$$

Koska $\text{syt}(5, 7) = 1$, niin tällä parilla on ratkaisu $x = 3 + (1 - 3)5 \cdot m'$, missä $5m' \equiv 1 \pmod{7}$. Nyt $m' \equiv 3 \pmod{7}$, joten $x = 3 - 2 \cdot 5 \cdot 3 = -27 \equiv 8 \pmod{35}$. Täten parin yksikäsitteinen välille $[0, 34]$ kuuluva ratkaisu on 8 ja sen ratkaisujoukko on $\{8 + 35k \mid k \in \mathbb{Z}\}$. (Tarkistus: $8 \equiv 3 \pmod{5}$ ja $8 \equiv 1 \pmod{7}$.)

Edellinen lause yleistyy seuraavasti:

Lause 2.15 (Kiinalainen jäännöslause). *Olkoot $m_1, m_2, \dots, m_r \in \mathbb{N}$. Oletetaan, että $\text{syt}(m_i, m_j) = 1$ aina kun $i \neq j$ ja merkitään $m = m_1 m_2 \dots m_r$. Silloin kongruenssiryhmällä*

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_r \pmod{m_r}$$

on ratkaisu

$$x = a_1 u_1 v_1 + a_2 u_2 v_2 + \dots + a_r u_r v_r,$$

missä $u_i = m/m_i$ ja $u_i v_i \equiv 1 \pmod{m_i}$ kaikilla $i = 1, \dots, r$. Lisäksi jakojäännös $x \pmod{m}$ on ryhmän yksikäsitteinen ratkaisu modulo m .

Todistus. Ensiksi havaitsemme, että kongruenssi $u_i y \equiv 1 \pmod{m_i}$ on ratkeava kaikilla $i = 1, \dots, r$ sillä oletuksesta $\text{syt}(m_i, m_j) = 1$ kaikilla $j \neq i$, seuraa $\text{syt}(u_i, m_i) = 1$. Koska $u_j v_j \equiv 0 \pmod{m_i}$ kaikilla $j \neq i$, niin saamme $x \equiv a_i u_i v_i \equiv a_i \pmod{m_i}$ kaikilla $i = 1, \dots, r$. Täten x on kongruenssiryhmän ratkaisu. Yksikäsitteisyyden todistaminen jätetään harjotustehtäväksi. \square

Esimerkki 2.22. Ratkaistaan kongruenssiryhmä

$$x \equiv 1 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

$$x \equiv 3 \pmod{8}$$

Kongruenssiryhmä on ratkeava sillä $\text{syt}(5, 7) = 1$, $\text{syt}(5, 8) = 1$ ja $\text{syt}(7, 8) = 1$. Kiinalaisen jäännöslauseen merkinnöin $m = 5 \cdot 7 \cdot 8$ ja

i	m_i	$u_i = \frac{m}{m_i}$	$u_i v_i \equiv 1 \pmod{m_i}$
1	5	$7 \cdot 8$	$56v_1 \equiv 1 \pmod{5}$
2	7	$5 \cdot 8$	$40v_2 \equiv 1 \pmod{7}$
3	8	$5 \cdot 7$	$35v_3 \equiv 1 \pmod{8}$

Ratkaistaan taulukon kongruenssit: $56v_1 \equiv v_1 \equiv 1 \pmod{5}$, $40v_2 \equiv 5v_2 \equiv 1 \pmod{7} \Rightarrow v_2 \equiv 3 \pmod{7}$, $35v_3 \equiv 3v_3 \equiv 1 \pmod{8} \Rightarrow v_3 \equiv 3 \pmod{8}$. Nyt siis kongruenssiryhmän eräs ratkaisu on $x = 1 \cdot 56 \cdot 1 + 2 \cdot 40 \cdot 3 + 3 \cdot 35 \cdot 3 = 611$. Sen yksikäsiteinen välille $[0, 5 \cdot 7 \cdot 8 - 1] = [0, 279]$ kuuluva ratkaisu on $x \pmod{280} = 51$ ja ratkaisujoukko on $\{51 + 280k \mid k \in \mathbb{Z}\}$.

Huomautus. Edellisen esimerkin kongruenssiryhmä voidaan tietysti ratkaista myös käyttämällä toistuvasti lausetta 2.14: ratkaistaan ensin pari

$$x \equiv 2 \pmod{7}$$

$$x \equiv 3 \pmod{8}$$

Tämän parin ratkaisut ovat $x \equiv 51 \pmod{56}$. Sitten ratkaistaan pari

$$x \equiv 1 \pmod{5}$$

$$x \equiv 51 \pmod{56}$$

josta saamme ratkaisut $x \equiv 51 \pmod{280}$.

Tämän idean yleistykseenä saamme seuraavan algoritmin joka ratkaisee Lauseessa 2.15 esiintyvän kongruenssiryhmän:

Input: $a = (a_1, a_2, \dots, a_r), m = (m_1, m_2, \dots, m_r), \text{syt}(m_i, m_j) = 1$

Output: ko. ryhmän eräs ratkaisu

While $r > 1$ Do

 Set $t = m^{-1}(a_r - a_{r-1}) \bmod m_r$

 Set $a_{r-1} = a_{r-1} + tm_{r-1}$

 Set $m_{r-1} = m_{r-1}m_r$

 Set $r = r - 1$

EndWhile

Return a_r

Tässä luvun m käänteisluvun modulo $m (=m^{-1} \bmod m_r)$ laskentaan käytetään esimerkiksi Laajennettua Eukleideen algoritmia.

Sovellus: *Laajennetun tarkkuuden aritmetiikka.* Käytännön salaussovelluksissa on tietokoneen kyettävä laskemaan hyvin suurilla kokonaisluvuilla. Olkoot k ja n kokonaislukuja joiden tulo $\approx 10^{100}$. Oletetaan, että 65535 on suurin koneen tuntema kokonaisluku. Mikä neuvoksi kun k ja n pitäisi kertoa keskenään?

Tapa 1. Olkoon $b = 256$ ($b^2 = 65536$) ja esitetään k ja n b -kantaisina lukuina

$$k = \sum_{i=0}^{20} k_i b^i, \quad 0 \leq k_i < 256,$$

$$n = \sum_{i=0}^{20} n_i b^i, \quad 0 \leq n_i < 256,$$

ja lasketaan tulo kn kertomalla kaikki termit keskenään, summataan ja tehdään tarvittavat siirrot. Kertolaskuja tulee $21 * 21 = 441$ kpl ja muita em. operaatioita runsaasti.

Tapa 2. 54:n ensimmäisen alkuluvun tulo $p_1 p_2 \cdots p_{54} > 10^{100}$. Esitetään k ja n modulaarikannan $(p_1, p_2, \dots, p_{54})$ avulla:

$$k = (k \bmod p_1, k \bmod p_2, \dots, k \bmod p_{54})$$

$$n = (n \bmod p_1, n \bmod p_2, \dots, n \bmod p_{54})$$

Merkitään $k_i = k \bmod p_i$ ja $n_i = n \bmod p_i$. Nyt tulon kn esitys ko. modulaarikannassa on

$$kn = (k_1 n_1 \bmod p_1, k_2 n_2 \bmod p_2, \dots, k_{54} n_{54} \bmod p_{54}),$$

sillä $k \equiv k_i \pmod{p_i}$ ja $n \equiv n_i \pmod{p_i}$ ja näin ollen $kn \equiv k_i n_i \pmod{p_i}$. Siispä $kn \bmod p_i = k_i n_i \bmod p_i$.

Nyt kertolaskuja (ja jakolaskuja) tarvitaan vain 54 kpl. Menetelmän (2) hankaluutena on siirtyminen modulaarikannasta takaisin kymmenjärjestelmään. Tämä voidaan tehdä Kiinalaisen jäännöslauseen avulla ratkaisemalla kongruenssiryhmä

$$x \equiv k_1 n_1 \pmod{p_1}$$

$$x \equiv k_2 n_2 \pmod{p_2}$$

$$\vdots$$

$$x \equiv k_{54} n_{54} \pmod{p_{54}}$$

jonka ainoa välille $[0, p_1 \cdots p_{54}]$ ratkaisu on juuri kn , mutta algoritmissa m_r on lopulta niin suuri, että jossain vaiheessa laskennassa tarvitaan menetelmää (1). Menetelmä (2) on kuitenkin tehokas sellaisissa sovelluksissa, joissa on paljon suurten lukujen laskentaa ”välivaiheina”. Tällöin Kiinalaista jäännöslauseetta tarvitaan vain ehkä kerran, lopullisen vastauksen antamiseen.

3. RYHMÄTEORIAA

3.1. Määritelmä ja perusominaisuuksia. Tarkastellaan seuraavaksi kongruenssia modulo m relaationa R joukossa \mathbb{Z} :

$$\forall a, b \in \mathbb{Z} : aRb \Leftrightarrow a \equiv b \pmod{m}.$$

Lause 3.1. (1) *Relaatio \equiv on ekvivalenssirelaatio joukossa \mathbb{Z} .*

(2) *Relaation \equiv ekvivalenssiluokat ovat $\bar{a} = \{a + km \mid k \in \mathbb{Z}\}$ kaikilla $a \in \mathbb{Z}$.*

(3) *Eräs näiden ekvivalenssiluokkien edustajisto on $\{0, 1, \dots, m-1\}$.*

Todistus. (1) Refleksiivisyys: $a \equiv a \pmod{m}$ kaikilla $a \in \mathbb{Z}$, sillä $m \mid (a - a)$.

Symmetria: Jos $a \equiv b \pmod{m}$, niin $m \mid (a - b)$ ja täten $m \mid -(a - b)$. Siispä $b \equiv a \pmod{m}$.

Transitiivisuus: Jos $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m}$, niin $m \mid ((a - b) + (b - c))$. Siispä $a \equiv c \pmod{m}$.

(2) Olkoon $a \in \mathbb{Z}$. Nyt $b \equiv a \pmod{m}$ joss $m \mid (b - a)$ joss $b = a + km$ jollakin $k \in \mathbb{Z}$.

(3) Olkoon $a \in \mathbb{Z}$. Nyt jakoalgoritmin nojalla $a = mq + r$, $0 \leq r < m$. Täten $a \equiv r \pmod{m}$ ja näin ollen $a \in \bar{r}$. Jos lisäksi $a \in \bar{t}$ missä $0 \leq t < m$, niin $ms + t = a = mq + r$.

Nyt $m \mid (r - t)$ joten $r = t$. □

Esimerkki 3.1. Tarkastellaan kongruenssia modulo 3. Nyt saamme \mathbb{Z} :n partition $\{\bar{0}, \bar{1}, \bar{2}\}$, ts.

$$(1) \mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2}$$

$$(2) \bar{0} \cap \bar{1} = \emptyset, \bar{0} \cap \bar{2} = \emptyset \text{ ja } \bar{1} \cap \bar{2} = \emptyset.$$

Jatkossa \mathbb{Z} :n partitiota relaation \equiv ekvivalenssiluokkiin merkitään symbolilla \mathbb{Z}_m .
Ts.

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$$

Joukon \mathbb{Z}_m alkoita kutsutaan *jäännösluokiksi modulo m* .

Huomautus. Olkoot $\bar{a}, \bar{b} \in \mathbb{Z}_m$. Koska \equiv on ekvivalenssirelaatio, niin

$$\bar{a} = \bar{b} \Leftrightarrow a \equiv b \pmod{m}.$$

Esimerkki 3.2. Joukossa \mathbb{Z}_4 on $\bar{5} = \bar{1}$, $\bar{7} = \bar{3}$ ja $\bar{5} \neq \bar{7}$. Täten myös $\{0, 2, 5, 7\}$ on eräs jäännösluokkien modulo 4 edustajisto ja $\mathbb{Z}_4 = \{\bar{0}, \bar{2}, \bar{5}, \bar{7}\}$

Määritelmä 3.1. Olkoot $\bar{a}, \bar{b} \in \mathbb{Z}_m$. Jäännösluokkien \bar{a} ja \bar{b} summa ja tulo, merkitään $+$ ja \cdot määritellään seuraavasti:

$$\bar{a} + \bar{b} = \overline{a + b}, \quad \bar{a} \cdot \bar{b} = \overline{ab}.$$

Lause 3.2. Jäännösluokkien tulo ja summa ovat hyvin määriteltyjä, ts. niiden arvot eivät riipu jäännösluokkien edustajien valinnasta.

Todistus. Olkoot $\bar{a} = \bar{a}'$ ja $\bar{b} = \bar{b}'$. Nyt $a \equiv a' \pmod{m}$ ja $b \equiv b' \pmod{m}$, joten Lauseen 2.12 kohtien (1) ja (2) nojalla $a + b \equiv a' + b' \pmod{m}$ ja $ab \equiv a'b' \pmod{m}$. Täten $\bar{a} + \bar{b} = \overline{a + b} = \overline{a' + b'} = \bar{a}' + \bar{b}'$ ja $\bar{a} \cdot \bar{b} = \overline{ab} = \overline{a'b'} = \bar{a}' \cdot \bar{b}'$. \square

Seuraavassa näemme, että jäännösluokkien yhteenlasku toteuttaa samoja laskulakeja kuin esimerkiksi reaalityöjen yhteenlasku tai matriisien yhteenlasku:

- (1) Assosiativisuus: $(\bar{a} + \bar{b}) + \bar{c} = \overline{(a + b) + c} = \overline{a + (b + c)} = \bar{a} + \overline{(b + c)} = \bar{a} + (\bar{b} + \bar{c}), \forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$.
- (2) On olemassa neutraalialkio $\bar{0}$: $\bar{0} + \bar{a} = \overline{0 + a} = \bar{a}$, ja $\bar{a} + \bar{0} = \bar{a} \forall \bar{a} \in \mathbb{Z}_m$
- (3) Jokaisella alkiolla $\bar{a} \in \mathbb{Z}_m$ on olemassa käänteisalkio (vasta-alkio) $-\bar{a}$: valitaan $-\bar{a} = \overline{-a}$, jolloin $\bar{a} + (-\bar{a}) = \bar{a} + \overline{-a} = \overline{a - a} = \bar{0}$. Samoin $-\bar{a} + \bar{a} = \bar{0}$.

Näiden lisäksi pätee vielä kommutatiivisuus jonka perustelu jätetään harjoitustehtäväksi:

$$\bar{a} + \bar{b} = \bar{b} + \bar{a} \quad \forall \bar{a}, \bar{b} \in \mathbb{Z}_m.$$

Seuraavaksi abstrahoidaan: otetaan nämä reaalityöjen, matriisien ja jäännösluokkien yhteenlaskun ominaisuudet aksiomiksi ja katsotaan mitä voidaan päätellä puhtaasti tältä pohjalta. Näin saamme tuloksia, jotka koskevat samanaikaisesti kaikkia edellä mainittuja algebrallisia systeemejä, ja yleisemmin kaikkia sellaisia algebrallisia systeemejä joissa nämä aksiomat toteutuvat.

Määritelmä 3.2. Olkoon G epätyhjä joukko jossa on määritelty binäärinen operaatio \circ , ts. kuvaus $\circ : G \times G \rightarrow G$. Pari (G, \circ) on *ryhmä* jos seuraavat kolme ehtoa ovat voimassa.

- (1) Assosiativisuus: $(a \circ b) \circ c = a \circ (b \circ c) \forall a, b, c \in G$,
- (2) Neutraalialkion olemassaolo: $(\exists e \in G)(\forall a \in G) a \circ e = e \circ a = a$,
- (3) Käänteisalkion olemassaolo: $(\forall a \in G)(\exists a' \in G) a \circ a' = a' \circ a = e$.

Ryhmä (G, \circ) on *Abelin ryhmä*, jos kaikille $a, b \in G$ pätee

- (4) kommutatiivisuus: $a \circ b = b \circ a$.

Määritelmä 3.3. Ehdon (2) täyttävä alkio e on ryhmän (G, \circ) *neutraalialkio*. Ehdon (3) täyttävä alkio a' on alkion a *käänteisalkio* (tai *vasta-alkio*).

Huomautus. Jatkossa ryhmästä (G, \circ) käytetään usein myös ilmaisua *ryhmä G operaation \circ suhteen*. Käytämme usein myös tulomerkintää ab merkinnän $a \circ b$ asemesta.

Esimerkki 3.3. Tuttuja ryhmiä: $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(Mat(n, \mathbb{R}), +)$ eli reaaliset $n \times n$ -matriisit, $(GL(n, \mathbb{R}), \cdot)$ eli kääntyvät $n \times n$ -matriisit, $(C[0, 1], +)$ eli välillä $[0, 1]$ määritellyt jatkuvat reaalfunktiot, operaationa funktioiden arvojen yhteenlasku. Näistä Abelin ryhmiä ovat kaikki muut paitsi $(GL(n, \mathbb{R}), \cdot)$.

Esimerkki 3.4. Olkoon X epätyhjä joukko ja S_X kaikkien joukon X permutaatioiden eli bijektiivisten kuvausten $X \rightarrow X$ muodostama joukko. Nyt (S_X, \circ) on ryhmä kun operaationa \circ on kuvausten yhdistäminen, neutraalialkiona identiteetikuvaus id_X , ja alkion f käänteisalkiona käänteiskuvaus f^{-1} . (Perustelu: harjoitustehtävä). (S_X, \circ) on *joukon X permutaatioryhmä*.

Esimerkki 3.5. $(\mathbb{Z}_m, +)$ on ryhmä. Tämä nähtiin juuri ennen ryhmän määritelmää. Ryhmää $(\mathbb{Z}_m, +)$ sanotaan *additiiviseksi jäännösluokkaryhmäksi modulo m* .

Esimerkki 3.6. Etsitään joukosta \mathbb{Z}_m mahdollisimman suuri osajoukko, joka on ryhmä jäännösluokkien kertolaskun suhteen. Koska $\bar{1} \cdot \bar{a} = \bar{a} = \bar{a} \cdot \bar{1}$ kaikilla $\bar{a} \neq \bar{0}$, niin luonnollinen valinta neutraalialkioksi on $\bar{1}$. Millä \mathbb{Z}_m :n alkiolla on käänteisalkio? Vastauksen antaa Lemma 2.3 (1): yhtälö

$$\bar{a} \cdot x = \bar{1}$$

on ratkeava joukossa \mathbb{Z}_m jos ja vain jos $\text{syt}(a, m) = 1$. Koska jäännösluokkien kertolasku on kommutatiivista, niin käänteisalkio on olemassa täsmälleen niillä jäännösluokilla \bar{a} joilla $\text{syt}(a, m) = 1$.

Merkitään

$$\mathbb{Z}_m^* = \{\bar{a} \in \mathbb{Z}_m \mid \text{syt}(a, m) = 1\},$$

ja osoitetaan, että (\mathbb{Z}_m^*, \cdot) on ryhmä kun neutraalialkiona $e = \bar{1}$.

(0) Operaatio \cdot on binäärinen operaatio joukossa \mathbb{Z}_m^* :

$$\bar{a}, \bar{b} \in \mathbb{Z}_m^* \Rightarrow \text{syt}(a, m) = \text{syt}(b, m) = 1 \Rightarrow \text{syt}(ab, m) = 1 \Rightarrow \bar{a} \cdot \bar{b} = \overline{ab} \in \mathbb{Z}_m^*.$$

- (1) Assosiatiivisuus: harjoitustehtävä.
 (2) $\bar{1}$ toteuttaa neutraalialkioehdon (perustelu: harjoitustehtävä).
 (3) Käänteisalkio: olkoon $\bar{a} \in \mathbb{Z}_m^*$. Koska $\text{syta}(a, m) = 1$, niin kongruenssi $ax \equiv 1 \pmod{m}$ on ratkeava Lemman 2.3 (1) nojalla. Olkoon a' sen ratkaisu. Nyt

$$\bar{a}' \cdot \bar{a} = \overline{a'a} = \bar{1} = \overline{aa'} = \bar{a} \cdot \bar{a}',$$

ja näin ollen \bar{a}' on alkion \bar{a} käänteisalkio. Siispä (\mathbb{Z}_m^*, \cdot) on ryhmä, vieläpä Abelin ryhmä.

Ryhmää (\mathbb{Z}_m^*, \cdot) sanotaan *multiplikatiiviseksi jäännösluokkaryhmäksi modulo m* ja sen alkioita *alkuluokiksi modulo m* .

Määritelmä 3.4. Eulerin φ -funktio on kuvaus $\varphi : \mathbb{N} \rightarrow \mathbb{N}$, $\varphi(m) = |\mathbb{Z}_m^*|$.

Esimerkki 3.7. $\mathbb{Z}_{15}^* = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}$ ja $\varphi(15) = 8$.

Esimerkki 3.8. Muodostetaan ryhmien $(\mathbb{Z}_4, +)$ ja (\mathbb{Z}_4^*, \cdot) ryhmätaulut.

$$\begin{array}{c|cccc} + & \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \hline \bar{0} & \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{1} & \bar{1} & \bar{2} & \bar{3} & \bar{0} \\ \bar{2} & \bar{2} & \bar{3} & \bar{0} & \bar{1} \\ \bar{3} & \bar{3} & \bar{0} & \bar{1} & \bar{2} \end{array} \qquad \begin{array}{c|cc} \cdot & \bar{1} & \bar{3} \\ \hline \bar{1} & \bar{1} & \bar{3} \\ \bar{3} & \bar{3} & \bar{1} \end{array}$$

Näemme, että kummassakin ryhmätaulussa jokainen ryhmän alkio esiintyy täsmälleen kerran jokaisella rivillä ja sarakkeella. Tämä ei ole sattumaa sillä on voimassa seuraava tulos.

Lause 3.3. Olkoon (G, \circ) ryhmä ja olkoot $a, b \in G$. Silloin yhtälöillä

$$a \circ x = b \qquad y \circ a = b$$

on yksikäsitteiset ratkaisut; nimittäin $x = a^{-1} \circ b$ ja $y = b \circ a^{-1}$. Erityisesti, kuvaukset $x \mapsto a \circ x$ ja $y \mapsto y \circ a$ ovat joukon G permutaatioita.

Todistus. Olkoon x_0 ensimmäisen yhtälön mikä tahansa ratkaisu. Nyt $b = a \circ x_0$, joten

$$a^{-1} \circ b = a^{-1} \circ (a \circ x_0) = (a^{-1} \circ a) \circ x_0 = e \circ x_0 = x_0.$$

Toinen yhtälö käsitellään samoin. □

Seuraus. Ryhmän neutraalialkio on yksikäsitteinen; samoin kunkin alkion käänteisalkio.

Todistus. Jos e ja e' ovat ryhmän neutraalialkioita, niin ne ovat yhtälön $ex = e$ ratkaisuja. Täten $e = e'$.

Jos b ja c ovat alkion a käänteisalkioita, niin ne ovat yhtälön $ax = e$ ratkaisuja. Täten $b = c$. \square

3.2. Aliryhmä ja syklinen ryhmä.

Määritelmä 3.5. Olkoon (G, \circ) ryhmä ja $H \subseteq G$. Jos (H, \circ) on ryhmä, niin se on ryhmän (G, \circ) *aliryhmä*. Merkitään $(H, \circ) \leq (G, \circ)$ tai lyhyemmin $H \leq G$.

Esimerkki 3.9. $(\mathbb{Z}, +) \leq (\mathbb{R}, +)$, $(\mathbb{Z}_m^*, \cdot) \not\leq (\mathbb{Z}_m, +)$.

Huomautus. Ryhmällä G on ainakin *triviaalit aliryhmät*: $\{e\}$ ja G .

Seuraavaa lemmaa käytetään jatkossa toistuvasti viittamatta siihen eksplisiittisesti.

Lemma 3.1. *Olkoon $H \leq G$.*

(1) *Olkoot e_G ja e_H ryhmien G ja H neutraalialkiot. Silloin $e_G = e_H$.*

(2) *Olkoon $a \in H$ ja olkoot a_G^{-1} ja a_H^{-1} alkion a käänteisalkiot ryhmässä G ja H . Silloin $a_G^{-1} = a_H^{-1}$.*

Todistus. (1) Koska $e_G e_H \stackrel{G:ssä}{=} e_H \stackrel{H:ssä}{=} e_H e_H$, niin $e_G = e_H$.

(2) Koska $aa_H^{-1} = e_H = a_H^{-1}a$ ja $e_G = e_H$, niin käänteisalkion yksikäsitteisyyden (G :ssä) nojalla $a_G^{-1} = a_H^{-1}$. \square

Lause 3.4 (Aliryhmäkriteeri). *Olkoon G ryhmä ja olkoon $H \subseteq G$. Silloin H on G :n aliryhmä jos ja vain jos seuraavat kaksi ehtoa pätevät*

(i) $H \neq \emptyset$,

(ii) $ab^{-1} \in H \forall a, b$.

Todistus. Oletetaan ensin, että $H \leq G$. Ryhmän määritelmän nojalla $H \neq \emptyset$. Olkoot $a, b \in H$. Nyt $b^{-1} \in H$ jälleen ryhmän määritelmän nojalla. Koska \cdot on binäärinen operaatio H :ssa, niin $ab^{-1} \in H$.

Oletetaan sitten, että ehdot (i) ja (ii) pätevät. Nyt

(1) assosiatiivisuus pätee koko G :ssä siis myös H :ssa.

(2) Osoitetaan, että G :n neutraalialkio e on neutraalialkio H :ssa. Ehdon (i) nojalla H :ssa on alkio h . Sovelletaan ehtoa (ii) alkioihin $a = h$ ja $b = h$,

jolloin saamme $e = hh^{-1} \in H$. Koska $H \subseteq G$, niin $eh = h = he$ kaikilla $h \in H$.

- (3) Käänteisalkio: olkoon $h \in H$. Sovelletaan ehtoa (ii) alkioihin $a = e$ ja $b = h$, jolloin $h^{-1} = ab^{-1} \in H$.

Lisäksi \circ on binäärinen operaatio H :ssa: jos $h', h \in H$, niin kohdan (3) nojalla $h^{-1} \in H$. Sovelletaan nyt ehtoa (ii) alkioihin $a = h'$ ja $b = h^{-1}$. Koska $b^{-1} = (h^{-1})^{-1} = h$, niin $h'h = ab^{-1} \in H$.

□

Esimerkki 3.10. Merkitään $SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) \mid \det(A) = 1\}$. Osoitetaan, että $(SL(n, \mathbb{R}), \cdot) \leq (GL(n, \mathbb{R}), \cdot)$. Ensinnäkin $SL(n, \mathbb{R})$ on epätyhjä sillä $I_{n \times n}$ kuuluu siihen. Olkoot sitten $A, B \in SL(n, \mathbb{R})$. Nyt

$$\det(AB^{-1}) = \det(A) \det(B^{-1}) = \det(A) \det(B)^{-1} = 1 \cdot 1 = 1,$$

joten $AB^{-1} \in SL(n, \mathbb{R})$. Siispä $(SL(n, \mathbb{R}), \cdot) \leq (GL(n, \mathbb{R}), \cdot)$.

Esimerkki 3.11. Olkoon $m \in \mathbb{Z}$. Merkitään $m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}$. Osoitetaan, että $(m\mathbb{Z}, +) \leq (\mathbb{Z}, +)$. Olkoot $a, b \in m\mathbb{Z}$ ($\neq \emptyset$). Nyt $a = mk$ ja $b = mt$ joillakin $k, t \in \mathbb{Z}$, ja täten $a - b = m(k - t) \in m\mathbb{Z}$. Siispä $(m\mathbb{Z}, +) \leq (\mathbb{Z}, +)$.

Aliryhmä $m\mathbb{Z}$ on esimerkki nk. syklistä ryhmästä: se koostuu yhden alkion ($= m$) monikerroista. Tämä havainto antaa aiheen seuraavaan abstrahointiin.

Olkoon G ryhmä ja $a \in G$. Merkitään $\langle a \rangle := \{a^k \mid k \in \mathbb{Z}\}$, missä alkion a *potenssit* (tai *monikerrat*) määritellään näin:

$$\begin{aligned} a^0 &= e, \\ a^k &= \underbrace{a \cdot a \cdots a}_{k \text{ kertaa}} \text{ jos } k > 0, \\ a^k &= (a^{-1})^{-k} \text{ jos } k < 0. \end{aligned}$$

Lemma 3.2. *Olkoon G ryhmä ja $a \in G$. Silloin*

- (1) $(a^k)^l = a^{kl} \quad \forall k, l \in \mathbb{Z}$,
- (2) $a^k a^l = a^{k+l} \quad \forall k, l \in \mathbb{Z}$.

Todistus. Harjoitustehtävä. □

Lause 3.5. *Olkoon G ryhmä ja $a \in G$. Silloin $\langle a \rangle$ on ryhmän G aliryhmä.*

Todistus. Ensinnäkin $\langle a \rangle$ on epätyhjä, sillä $e = a^0 \in \langle a \rangle$. Olkoot $a^k, a^l \in \langle a \rangle$. Nyt $a^k(a^l)^{-1} = a^k a^{-l} = a^{k-l} \in \langle a \rangle$. \square

Määritelmä 3.6. Ryhmän G aliryhmä $\langle a \rangle$ on *syklinen*, ja a on sen (eräs) *generoija*. Jos $G = \langle a \rangle$, niin G on *syklinen ryhmä*.

Esimerkki 3.12. $(\mathbb{Z}, +)$ on syklinen ryhmä sillä $\mathbb{Z} = \langle 1 \rangle = \{k \cdot 1 \mid k \in \mathbb{Z}\}$. Samoin \mathbb{Z}_m on syklinen: $\mathbb{Z}_m = \{\bar{0}, 1 \cdot \bar{1}, 2 \cdot \bar{1}, \dots, (m-1) \cdot \bar{1}\} \subseteq \langle \bar{1} \rangle \subseteq \mathbb{Z}_m$. Sen sijaan $(\mathbb{R}, +)$ ei ole syklinen ryhmä.

Esimerkki 3.13. Osoitetaan, että $\mathbb{Z}_5^* = \langle \bar{2} \rangle$. Koska $\bar{2}^0 = \bar{1}$, $\bar{2}^1 = \bar{2}$, $\bar{2}^2 = \bar{4}$, $\bar{2}^3 = \bar{3}$, niin $\mathbb{Z}_5^* \subseteq \langle \bar{2} \rangle \subseteq \mathbb{Z}_5^*$.

Määritelmä 3.7. Olkoon G ryhmä. Alkion $a \in G$ *kertaluku* $\text{ord}(a)$ on syklisen ryhmän $\langle a \rangle$ kertaluku.

Lause 3.6. *Olkoon $G = \langle a \rangle$ syklinen ryhmä.*

(1) *Jos $|G| = n$, niin*

$$G = \{e, a, \dots, a^{n-1}\},$$

ja n on pienin ehdon $a^n = e$ täyttävistä positiivista luvuista.

(2) *Jos G on ääretön ryhmä, niin*

$$G = \{a^k \mid k \in \mathbb{Z}\},$$

ja sen alkio a^k ovat pareittain erisuuria.

Todistus. (1) Koska G on äärellinen, niin kaikki potenssit a^k , $k \geq 0$, eivät voi olla erisuuria. Siispä $a^s = a^m$ joillakin $0 \leq m < s$. Nyt $a^{s-m} = e$ ja $s-m > 0$. Olkoon n pienin positiivinen kokonaisluku jolla $a^n = e$. Sisältyminen $\{e, a, \dots, a^{n-1}\} \subseteq \langle a \rangle$ on triviaali. Olkoon $a^k \in \langle a \rangle$. Nyt jakoalgoritmin nojalla $k = nq + r$, $0 \leq r < n$, joten $a^k = (a^n)^q a^r = a^r \in \{e, a, \dots, a^{n-1}\}$.

(2) Jos $a^k = a^t$, joillakin $k \neq t$, niin päädyimme äärelliseen ryhmään kuten edellä. \square

Seuraus. *Olkoon G äärellinen ryhmä ja $a \in G$. Silloin $\text{ord}(a)$ on pienin ehdon $a^n = e$ täyttävistä positiivisista kokonaisluvuista n .*

Esimerkki 3.14. Muodostetaan ryhmän \mathbb{Z}_6 aliryhmä $\langle \bar{2} \rangle$: $0 \cdot \bar{2} = \bar{0}$, $1 \cdot \bar{2} = \bar{2}$, $2 \cdot \bar{2} = \bar{4}$, $(3 \cdot \bar{2} = \bar{0})$. Siispä $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}\}$ ja $\text{ord}(\bar{2}) = 3$.

3.3. Sivuluokat ja Lagrangen lause.

Esimerkki 3.15. Tarkastellaan jälleen syklistä ryhmää $m\mathbb{Z}$. Määritellään nyt relaatio R joukossa \mathbb{Z} seuraavasti:

$$aRb \Leftrightarrow a \in b + m\mathbb{Z} := \{b + mk \mid k \in \mathbb{Z}\}.$$

Selvästi R on ekvivalenssirelaatio, jos $m = 0$. Jos taas $m \neq 0$, niin aRb joss $a \equiv b \pmod{|m|}$. Täten R on ekvivalenssirelaatio kaikilla $m \in \mathbb{Z}$. Jos siis $m \neq 0$, niin R :n ekvivalenssiluokat ovat jäännösluokat modulo $|m|$ eli $\{0 + mk \mid k \in \mathbb{Z}\}, \{1 + mk \mid k \in \mathbb{Z}\}, \dots, \{(m-1) + mk \mid k \in \mathbb{Z}\}$.

Tämä konstruktio yleistetään seuraavassa lauseessa.

Lause 3.7. *Olkoon G ryhmä ja H sen aliryhmä. Määritellään relaatiot L ja R joukossa G seuraavasti:*

$$aLb \Leftrightarrow a \in bH := \{bh \mid h \in H\},$$

$$aRb \Leftrightarrow a \in Hb := \{hb \mid h \in H\},$$

Silloin L ja R ovat ekvivalenssirelaatioita. Alkion $a \in G$ ekvivalenssiluokat relaatioiden L ja R suhteen ovat aH ja Ha .

Todistus. Harjoitustehtävä. □

Määritelmä 3.8. Relaation L (vast. R) ekvivalenssiluokat ovat ryhmän H vasemmat (vast. oikeat) sivuluokat G :ssä. Aliryhmän H kaikkien vasempien (vast. oikeiden) sivuluokkien joukko on G :n vasen (vast. oikea) tekijäjoukko aliryhmän H suhteen, merkitään G/H_L (vast. G/H_R).

Esimerkki 3.16. Tarkastellaan kaikkia joukon $X := \{1, 2, 3\}$ permutaatioita eli permutaatioryhmää (S_X, \circ) . Sen alkiot ovat seuraavat kuvaukset

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, x = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, y = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$z = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, u = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, v = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

missä esimerkiksi e on kuvaus $e(1) = 1, e(2) = 2$ ja $e(3) = 3$; ts. se on ryhmän S_X neutraalialkio. Olkoon nyt $H = \langle y \rangle = \{e, y\}$. Nyt H :n vasemmat sivuluokat ovat

$$\begin{aligned} H &= \{e, y\}, \\ xH &= \{x, x \circ y\} = \{x, u\}, \\ zH &= \{z, z \circ y\} = \{z, v\}, \end{aligned}$$

ja oikeat sivuluokat ovat

$$\begin{aligned} H &= \{e, y\}, \\ Hx &= \{x, y \circ x\} = \{x, z\}, \\ Hu &= \{u, y \circ u\} = \{u, v\}. \end{aligned}$$

Siispä

$$S_X/H_L = \{H, xH, zH\}, \quad S_X/H_R = \{H, Hx, Hu\}.$$

Huomaa, että $xH \neq Hx$ ja $zH \neq Hz (=Hx)$. Permutaatioryhmiä ei käsitellä tarkemmin tällä kurssilla vaan kurssilla Algebra II.

Huomautus. Jatkossa käsitellään lähinnä vasempia sivuluokkia sillä oikeat sivuluokat käyttäytyvät samoin. Jos G on Abelin ryhmä, niin $aH = Ha$ kaikilla $a \in G$ joten puhutaan lyhyesti *sivuluokista* ja *tekijäjoukosta aliryhmän H suhteen*, merkitään G/H .

Esimerkki 3.17. Jos $m \in \mathbb{N}$, niin $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.

Määritelmä 3.9. Ryhmän G aliryhmän H vasempien sivuluokkien lukumäärä G :ssä on H :n *indeksi* G :ssä, merkitään $[G : H]$.

Esimerkki 3.18. $[\mathbb{Z} : m\mathbb{Z}] = m$.

Esimerkki 3.19. Tarkastellaan ryhmiä $(\mathbb{R}, +)$ ja $(\mathbb{C}, +)$. Alkion $z_0 = x_0 + iy_0 \in \mathbb{C}$ määrämä \mathbb{R} :n sivuluokka on

$$z_0 + \mathbb{R} = \{x_0 + iy_0 + x \mid x \in \mathbb{R}\} = \{x + iy_0 \mid x \in \mathbb{R}\},$$

jonka geomerinen vastine tasossa \mathbb{R}^2 on pisteen $(0, y_0)$ kautta kulkeva x -akselin suuntainen suora. Nyt

$$\mathbb{C}/\mathbb{R} = \bigcup_{y \in \mathbb{R}} \{x + iy \mid x \in \mathbb{R}\},$$

ja täten $[\mathbb{C} : \mathbb{R}] = \infty$.

Seuraavan lemmän nojalla jokaisessa sivuluokassa on ”yhtä monta” alkioita.

Lemma 3.3. *Olkoon G ryhmä ja H sen aliryhmä. Olkoon $a \in G$, silloin kuvaus*

$$f : H \rightarrow aH, f(h) = ah$$

on bijektio.

Todistus. Harjoitustehtävä. □

Lause 3.8 (Lagrange). *Jos G on äärellinen ryhmä ja H sen aliryhmä, niin*

$$[G : H] = \frac{|G|}{|H|}.$$

Erityisesti siis äärellisen ryhmän G aliryhmän kertaluku on G :n kertaluvun tekijä.

Todistus. Koska H :n sivuluokat H, a_2H, \dots, a_kH , $k = [G : H]$, muodostavat G :n partition joillakin $a_2, \dots, a_k \in G$, niin $|G| = |H| + |a_2H| + \dots + |a_kH|$. Koska jokaisessa sivuluokassa on yhtä monta alkioita, niin $|G| = k|H|$. □

Seuraus. *Olkoon G äärellinen ryhmä ja $a \in G$. Silloin $\text{ord}(a)$ on G :n kertaluvun $|G|$ tekijä.*

Todistus. Koska $\text{ord}(a) = |\langle a \rangle|$, niin väite seuraa välittömästi Lagrangen lauseesta. □

Esimerkki 3.20. Osoitetaan, että $\mathbb{Z}_{19}^* = \langle \bar{2} \rangle$. Koska $\varphi(19) = 18 = 2 \cdot 3^2$, niin $\text{ord}(\bar{2}) = 1, 2, 3, 6, 9$ tai 18 . Nyt $\bar{2}^1 \neq \bar{1}$, $\bar{2}^2 \neq \bar{1}$ ja $\bar{2}^3 \neq \bar{1}$. Lisäksi $\bar{2}^6 = \bar{7} \neq \bar{1}$ ja $\bar{2}^9 = \bar{2}^6 \cdot \bar{2}^3 = \bar{7} \cdot \bar{8} = \bar{56} = \bar{18} \neq \bar{1}$. Täten $\text{ord}(\bar{2}) = 18$.

Lause 3.9. *Olkoon G äärellinen ryhmä jonka kertaluku on m . Silloin*

$$a^m = e \quad \forall a \in G.$$

Todistus. Olkoon $a \in G$ ja merkitään $n = \text{ord}(a)$. Lauseen 3.6 Seurauksen nojalla $a^n = e$. Toisaalta Lagrangen lauseen Seurauksen nojalla $n \mid m$. Nyt $a^m = (a^n)^{\frac{m}{n}} = e$. □

Seuraus (Euler). *Olkoon $m \in \mathbb{N}$ ja $a \in \mathbb{Z}$. Silloin pätee*

$$\text{syt}(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Todistus. Jos $\text{syt}(a, m) = 1$, niin $\bar{a} \in \mathbb{Z}_m^*$. Nyt Lauseen 3.9 nojalla $\bar{a}^{\varphi(m)} = \bar{1}$; ekvivalentisti $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Huomautus. Jos $m = p \in \mathbb{P}$, niin $\phi(m) = p - 1$, ja saamme *Fermat'n pienen lauseen*:

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

Huomautus. Eulerin lause voidaan todistaa helposti myös ilman ryhmäteoriaa: jos $a_1, a_2, \dots, a_{\phi(m)}$ on jokin alkuluokkien modulo m edustajisto, niin myös $aa_1, aa_2, aa_3, \dots, aa_{m-1}$ on sitä mikäli $\text{synt}(a, m) = 1$. Nyt

$$a^{\phi(m)} a_1 a_2 \cdots a_{\phi(m)} = aa_1 \cdot aa_2 \cdots aa_{\phi(m)} \equiv a_1 a_2 \cdots a_{\phi(m)} \pmod{m}.$$

Koska $\text{synt}(a_1 \cdots a_{\phi(m)}, m) = 1$, niin nyt Lauseen 2.12 (3) nojalla

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Ilman ryhmäteoriaa Eulerin lause olisi kuitenkin jäänyt vain lukuteoreettiseksi kuriositeetiksi ilman selitystä sille *miksi* Eulerin lause pätee.

Esimerkki 3.21. Lasketaan luvun $3^{1203} - 2$ jakojäännös jaettaessa luvulla 13. Koska $\phi(13) = 12$ ja $1203 = 12 \cdot 100 + 3$, niin

$$3^{1203} - 2 = (3^{12})^{100} 3^3 - 2 \equiv 1 \cdot 27 - 2 \equiv 25 \equiv 12 \pmod{13}.$$

Sovellus: *RSA-salakirjoitus.* RSA-salakirjoitus on esimerkki *julkisen avaimen* salausjärjestelmästä: tietoverkon käyttäjä A voi paljastaa muille verkon käyttäjille oman salausavaimensa, jonka jälkeen tätä avainta käyttäen voidaan lähettää A :lle salattuja viestejä. Henkilö A pitää tulkinta-avaimen visusti omana tietonaan ja sen määräminen salausavaimen nojalla on äärimmäisen hidasta ellei mahdotonta.

RSA-salauksessa henkilön A salausavain on pari $(e, m) \in \mathbb{N}^2$, missä $m = pq$ ja p, q ovat alkulukuja $\approx 10^{50}$ (low risk application) tai jopa $\approx 10^{1000}$ (high risk application). Lisäksi $e > 1$ ja $\text{synt}(e, \phi(m)) = 1$ (nyt $\phi(m) = (p-1)(q-1)$). Tulkinta-avain on pari (d, m) missä d on kongruenssin $ex \equiv 1 \pmod{\phi(m)}$ välillä $[0, \phi(m) - 1]$ kuuluva ratkaisu.

SALAUUS (eli kryptaus): Koodataan lähetettävä viesti jollain standardimenetelmällä kokonaisluvuksi $x < m$. Jos $p, q \approx 10^{50}$, niin voidaan käyttää esim. 20-numeroisia 256-järjestelmän lukuja vastaamaan 20 merkin merkkijonoja missä kukin numero on vastaavan merkin ASCII-arvo. Esimerkiksi viestiä *hei hei* vastaa luku $x =$

$104 \cdot 256^{19} + 101 \cdot 256^{18} + 105 \cdot 256^{17} + 32 \cdot 256^{16} + 104 \cdot 256^{15} + 101 \cdot 256^{14} + 105 \cdot 256^{13} = 59599657324855574295082244897183469353225418752$.

Salattu viesti on jakojäännös $y = x^e \pmod m$ ja lähetetään y tietoverkkoon henkilölle A .

TULKINTA (eli dekrytaus): Nyt $y = x^e \pmod m$ on henkilön A vastaanottama viesti. Lasketaan jakojäännös $r := y^d \pmod m$. Seuraavassa näytetään, että lähetetty viesti $x = r$.

Koska $de = 1 + k\varphi(m)$, niin

$$y^d \equiv x^{ed} = x^{1+k\varphi(m)} = x(x^{\varphi(m)})^k \pmod m$$

- (1) Jos $\text{syt}(x, m) = 1$, niin Eulerin lauseen nojalla $x^{\varphi(m)} \equiv 1 \pmod m$, joten $y^d \equiv x \pmod m$ ja näin ollen $y^d \pmod m = x$, joka on lähetetty viesti koodattuna.
- (2) Jos $\text{syt}(x, m) = p$, niin Fermat'n pienen lauseen nojalla

$$x^{\varphi(m)} = x^{(p-1)(q-1)} = (x^{q-1})^{p-1} \equiv 1^{p-1} = 1 \pmod q,$$

joten $x(x^{\varphi(m)})^k \equiv x \pmod q$. Lisäksi triviaalisti $x(x^{\varphi(m)})^k \equiv x \pmod p$, joten $pq \mid x(x^{\varphi(m)})^k - x$ eli $x(x^{\varphi(m)})^k \equiv x \pmod{pq}$ eli $y^d \equiv x \pmod m$. Tässäkin tapauksessa saamme siis lähetetyn viestin. Jos koodaus suoritettiin käyttämällä 256-järjestelmän lukuja, voidaan se nyt purkaa esittämällä x 256-järjestelmän lukuna.

Miksi RSA-salaus on turvallinen? Tulkinta-avain (d, m) voidaan periaatteessa laskea salausavaimen (e, m) avulla: d on kongruenssin $ex \equiv 1 \pmod{\varphi(m)}$ ratkaisu. Mutta $\varphi(m)$:n laskeminen on hankalaa m :n avulla. Se voidaan tehdä, jos m onnistetaan hajoittamaan tekijöihin $m = pq$. Silloin $\varphi(m) = (p-1)(q-1)$. Mutta kuten aikaisemmin todettiin, on tekijöihin jako hyvin hidasta jos p ja q ovat suuria.

Sovellus: *Elektroninen allekirjoitus.* Elektronisella allekirjoituksella tarkoitetaan menetelmää jolla voidaan varmistaa tietoverkkoon lähetetyn viestin lähettäjä.

MENETELMÄ: Verkon käyttäjät julkaisevat tulkinta-avaimensa (d, m) mutta pitävät salausavaimen (e, m) omana tietonaan. Jos henkilö A haluaa lähettää viestin x , niin hän lähettää verkkoon viestin $x^e \pmod m$. Nyt kuka tahansa verkon

käyttäjä voi varmistaa, että ko. viestin on todellakin lähettänyt henkilö A : laskeetaan $(x^e)^d \pmod m$ ja jos koodauksen purkamisen jälkeen saadaan järkevää tekstiä, on viestin lähettäjä todellakin ollut henkilö A .

Sovellus: *Salaus ja elektroninen allekirjoitus.* Kukin verkon käyttäjä generoi neljä suurta alkulukua p, q, p', q' , muodostaa luvut $m = pq$ ja $m' = p'q'$, valitsee luvut e ja e' joille $\text{syte}(e, \varphi(m)) = 1 = \text{syte}(e', \varphi(m'))$, laskee käänteisalkiot $d = e^{-1} \pmod{\varphi(m)}$ ja $d' = e'^{-1} \pmod{\varphi(m')}$, ja julkaisee parit (e, m) ja (d', m') .

Jos henkilö A haluaa lähettää viestin x henkilölle B , hän (esimerkiksi) ensin allekirjoittaa sen avaimellaan e'_A : $y = x^{e'_A} \pmod{m'_A}$ ja sitten salaa sen henkilön B avaimella e_B : $z = y^{e_B} \pmod{m_B}$.

Henkilö B tulkitsee saamansa viestin laskemalla ensin $z^{d_B} \pmod{m_B} = y$ ja sitten $y^{d'_A} \pmod{m'_A} = x$.

Huomautus. Mikäli $m'_A > m_B$, niin informaatiota saattaa kadota jakojäännöksen modulo m_B laskemisessa. Tämän vuoksi sovitaan että jokaisen käyttäjän salausmodulit m ovat esimerkiksi välillä $10^{51} < m < 10^{52}$ ja allekirjoitusmodulit m' välillä $10^{50} < m' < 10^{51}$.

3.4. Isomorfismi ja homomorfismi. Tarkastellaan ryhmien \mathbb{Z}_4 ja \mathbb{Z}_5^* ryhmättauluja

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	\cdot	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
0	0	1	2	3	1	1	2	3	4
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	2	2	4	$\bar{1}$	$\bar{3}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	3	3	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	4	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Ensi silmäyksellä tauluissa on melko vähän yhtäläisyyttä. Nimetäänpä kummasakin taulussa alkiot uudelleen:

$$\begin{aligned} \mathbb{Z}_4\text{:ssa: } \bar{0} &\leftrightarrow e, \bar{1} \leftrightarrow a, \bar{2} \leftrightarrow b, \bar{3} \leftrightarrow c, \\ \mathbb{Z}_5^*\text{:ssa: } \bar{1} &\leftrightarrow e, \bar{2} \leftrightarrow a, \bar{3} \leftrightarrow c, \bar{4} \leftrightarrow b. \end{aligned}$$

Nimetään vielä kummankin ryhmän operaatiot uudelleen: $+$ \leftrightarrow \circ ja \cdot \leftrightarrow \circ . Nyt molemmilla ryhmillä on ryhmättaulu

\circ	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Ryhmäteoriassa äärellisiä ryhmiä, joilla on alkioiden permutointia ja uudelleen nimeämistä vaille samat ryhmätaulut, pidetään olennaisesti samanlaisina eli *isomorfisina*. Seuraavaksi täsmennetään tämä käsite. Olkoot (G, \circ) ja (G', \bullet) äärellisiä ryhmiä ja olkoon $f : G \rightarrow G'$ bijektio. Muodostetaan näiden ryhmätaulut:

\circ	e_G	g_1	\dots	g_n	\bullet	$e_{G'}$	$f(g_1)$	\dots	$f(g_n)$
e_G	e_G	g_1	\dots	g_n	$e_{G'}$	$e_{G'}$	$f(g_1)$	\dots	$f(g_n)$
g_1	g_1	$g_1 \circ g_1$	\dots	$g_1 \circ g_n$	$f(g_1)$	$f(g_1)$	$f(g_1) \bullet f(g_1)$	\dots	$f(g_1) \bullet f(g_n)$
\vdots	\vdots	\vdots	\dots	\vdots	\vdots	\vdots	\vdots	\dots	\vdots
g_n	g_n	$g_n \circ g_1$	\dots	$g_n \circ g_n$	$f(g_n)$	$f(g_n)$	$f(g_n) \bullet f(g_1)$	\dots	$f(g_n) \bullet f(g_n)$

Nyt näemme, että ryhmällä on alkioiden uudelleen nimeämistä vaille samat ryhmätaulut jos f toteuttaa seuraavat kaksi ehtoa

- (1) $e_{G'} = f(e_G)$
- (2) $f(g_i) \bullet f(g_j) = f(g_i \circ g_j), \forall i, j = 1, \dots, n$

Näistä ehdoista ensimmäinen seuraa jälkimmäisestä:

$$(2) \Rightarrow f(e_G) = f(e_G \circ e_G) = f(e_G) \bullet f(e_G) \xrightarrow{|\bullet f(e_G)^{-1}|} e_{G'} = f(e_G).$$

Määritelmä 3.10. Olkoot (G, \circ) ja (G', \bullet) ryhmiä. Jos on olemassa bijektio $f : G \rightarrow G'$ jolle pätee

$$f(a \circ b) = f(a) \bullet f(b) \quad \forall a, b \in G,$$

niin kuvaus f on *isomorfismi* ja ryhmät (G, \circ) ja (G', \bullet) ovat *isomorfitset*, merkitään $G \simeq G'$.

Esimerkki 3.22. $\mathbb{Z}_4 \simeq \mathbb{Z}_5^*$. Isomorfismina esimerkiksi kuvaus:

$$f : \mathbb{Z}_4 \rightarrow \mathbb{Z}_5^*, f(n \cdot \bar{1}) = \bar{2}^n, \forall n \in \mathbb{Z}.$$

Esimerkki 3.23. $(\mathbb{R}, +) \simeq (\mathbb{R}_{>0}, \cdot)$; nimittäin eksponenttifunktio

$$\mathbb{R} \rightarrow \mathbb{R}_{>0}, f(x) = e^x$$

on tunnetusti bijektio, ja $f(x + y) = e^{x+y} = e^x e^y = f(x)f(y)$.

Isomorfismin käsitettä voidaan yleistää luopumalla bijektiivisyys-vaatimuksesta.

Määritelmä 3.11. Olkoot (G, \circ) ja (G', \bullet) ryhmiä. Jos on olemassa kuvaus $f : G \rightarrow G'$ jolle pätee

$$f(a \circ b) = f(a) \bullet f(b) \quad \forall a, b \in G,$$

niin kuvaus f on *homomorfismi*.

Huomautus. Isomorfismin yleistäminen homomorfismin käsitteeksi ei ole mitenkään keinotekoinen: jatkossa näemme, että jokaiseen homomorfismiin voidaan liittää isomorfismi. Homomorfismit osoittautuvat myös käteviksi työkaluiksi tutkittaessa abstraktien ryhmien rakennetta: niiden avulla abstrakteja ryhmiä voidaan usein verrata joihinkin hyvin tunnettuihin ryhmiin.

Jatkossa käytämme ryhmän G operaatiolle multiplikaatiivista merkintätapaa ts. merkitään ab merkinnän $a \circ b$ asemesta.

Määritelmä 3.12. Homomorfismin $f : G \rightarrow G'$ ydin on G' :n neutraalialkion alkukuva kuvauksessa f . Ts.

$$\text{Ker}(f) = f^{-1}(e_{G'}) = \{a \in G \mid f(a) = e_{G'}\}.$$

Lemma 3.4. *Olkoon $f : G \rightarrow G'$ homomorfismi. Silloin*

- (1) $e_G \in \text{Ker}(f)$,
- (2) $f(a)^{-1} = f(a^{-1}) \quad \forall a \in G$.

Todistus. (1) $f(e_G) = f(e_G e_G) = f(e_G) f(e_G) \Rightarrow e_{G'} = f(e_G)$. (Deja vu?)

(2) $e_{G'} \stackrel{(1)}{=} f(e_G) = f(a a^{-1}) = f(a) f(a^{-1})$. □

Lause 3.10. $\text{Ker}(f) \leq G$.

Todistus. Väite seuraa lähes välittömästi edellisestä Lemmasta ja aliryhmäkriteeristä: $\text{Ker}(f)$ on epätyhjä, ja jos $a, b \in \text{Ker}(f)$, niin $f(ab^{-1}) = f(a) f(b^{-1}) = f(a) f(b)^{-1} = e_{G'} e_{G'} = e_{G'}$. Täten $ab^{-1} \in \text{Ker}(f)$. □

Homomorfismin ydin on kunkin alkion alkukuvien lukumäärän mittari:

Lause 3.11. *Olkoot $f : G \rightarrow G'$ homomorfismi ja $a \in G$. Merkitään $b = f(a)$. Silloin*

$$f^{-1}(b) = a \text{Ker}(f).$$

Todistus. Olkoon $a' \in G$. Silloin

$$f(a') = f(a) \Leftrightarrow f(a'a^{-1}) = f(a')f(a)^{-1} = e_{G'} \Leftrightarrow a'a^{-1} \in \text{Ker}(f) \Leftrightarrow a' \in a\text{Ker}(f).$$

Täten a' on alkion b alkukuva jos ja vain jos $a' \in a\text{Ker}(f)$. \square

Seuraus. *Homomorfismi $f : G \rightarrow H$ on injektio jos ja vain jos sen ydin on $\{e_G\}$.*

Todistus. Jos f on injektio, niin jokaisella alkiolla $b \in f(G)$ on täsmälleen yksi alkukuva $a \in G$. Täten sivuluokassa $a\text{Ker}(f)$ on vain yksi alkio ($= a$) ja näin ollen $\text{Ker}(f) = \{e_G\}$. Jos taas $\text{Ker}(f) = \{e_G\}$, niin jokaisessa sen sivuluokassa on täsmälleen yksi alkio. \square

Seuraavaksi tarkastelemme jäännösluokkaryhmän konstruktion yleistämistä. Olkoon $G \rightarrow G'$ homomorfismi ja $a \in G$. Merkitään $\bar{a} = a\text{Ker}(f)$ ja määritellään tekijäjoukossa $G/\text{Ker}(f)$ binäärinen operaatio \cdot :

$$\bar{a} \cdot \bar{b} = \overline{ab}.$$

Pian näemme että operaatio on hyvin määritelty. Tämä seuraa olennaisesti seuraavasta lemmasta.

Lemma 3.5. $a\text{Ker}(f) = \text{Ker}(f)a$ kaikilla $a \in G$.

Todistus. Jos $a' \in a\text{Ker}(f)$, niin $a' = ab$ jollakin $b \in \text{Ker}(f)$. Nyt $a' = (aba^{-1})a$ ja koska $f(aba^{-1}) = f(a)f(b)f(a^{-1}) = f(a)e_{G'}f(a)^{-1}$, niin $aba^{-1} \in \text{Ker}(f)$.

Käänteinen sisältyminen osoitetaan samoin. \square

Lause 3.12. $(G/\text{Ker}(f), \cdot)$ on ryhmä.

Todistus. Operaatio on hyvin määritelty: jos $\bar{a} = \bar{a}'$ ja $\bar{b} = \bar{b}'$, niin $a = a'h_1$ ja $b = b'h_2$ joillakin $h_1, h_2 \in \text{Ker}(f)$. Nyt $ab = a'h_1b'h_2$ ja Lemma 3.5 sovellettuna alkioon b' antaa $h_1b' = b'h'$ jollakin $h' \in \text{Ker}(f)$. Siispä $ab = a'b'h'h_2 \in a'b'\text{Ker}(f)$. Täten $\bar{a} \cdot \bar{b} = \overline{ab} = \overline{a'b'} = \bar{a}' \cdot \bar{b}'$.

Ryhmäaksioomien tarkistaminen jätetään harjoitustehtäväksi (vihje: neutraali-alkio on \bar{e}_G ja käänteisalkio $\bar{a}^{-1} = \overline{a^{-1}}$). \square

Huomautus. Olkoon G ryhmä ja H sen aliryhmä. Näimme edellä, että ehto $aH = Ha$ kaikilla $a \in G$, on riittävä sille, että operaatio $aH \cdot bH = abH$ on hyvin määritelty tekijäjoukossa G/H . Helposti nähdään, että se on myös välttämätön. Abstrahoidaan tämä aliryhmän ominaisuus:

Määritelmä 3.13. Olkoon G ryhmä ja H sen aliryhmä jolle pätee

$$aH = Ha \quad \forall a \in G.$$

Silloin H on *normaali* G :ssä ja merkitään $H \trianglelefteq G$.

Lause 3.12'. Jos $H \trianglelefteq G$, niin $(G/H, \cdot)$ on ryhmä.

Huomautus. Jos G on Abelin ryhmä, niin sen jokainen aliryhmä on normaali ja täten tekijäryhmä G/H on olemassa kaikilla $H \leq G$.

Huomautus. Jokaisella ryhmällä on ainakin kaksi normaalia aliryhmää nimittäin sen triviaalit aliryhmät. Jos ryhmällä ei ole muita normaaleja aliryhmiä, on se *yksinkertainen*. Yksinkertaisista ryhmistä lisää kurssilla Algebra II.

Esimerkki 3.24. Koska \mathbb{Z}_7^* on Abelin ryhmä, niin voidaan muodostaa esimerkiksi tekijäryhmä $\mathbb{Z}_7^*/\langle \bar{6} \rangle$. Aliryhmän $\langle \bar{6} \rangle$ sivuluokat ovat

$$\bar{1} = \langle \bar{6} \rangle = \{\bar{1}, \bar{6}\}, \quad \bar{2} = \bar{2} \langle \bar{6} \rangle = \{\bar{2}, \bar{5}\}, \quad \bar{3} = \bar{3} \langle \bar{6} \rangle = \{\bar{3}, \bar{4}\},$$

ja tekijäryhmän $\mathbb{Z}_7^*/\langle \bar{6} \rangle$ ryhmätaulu on

$$\begin{array}{c|ccc} \cdot & \bar{1} & \bar{2} & \bar{3} \\ \hline \bar{1} & \bar{1} & \bar{2} & \bar{3} \\ \bar{2} & \bar{2} & \bar{3} & \bar{1} \\ \bar{3} & \bar{3} & \bar{1} & \bar{2} \end{array}$$

Osoitetaan seuraavaksi, että jokainen homomorfismi voidaan hajoittaa tekijöihin: surjektiiviseen ja injektiiviseen tekijään, joista kumpikin on homomorfismi. Ensimmäinen pieni aputuloks:

Lemma 3.6. Olkoon $f : G \rightarrow G'$ homomorfismi.

- (1) Jos $H \leq G$, niin $f(H) \leq G'$.
- (2) Jos $H' \leq G'$, niin $f^{-1}(H') \leq G$.

Todistus. Harjoitustehtävä. (Vihje: aliryhmäkriteeri) □

Olkoon $f : G \rightarrow G'$ homomorfismi. Määritellään kuvaukset π ja F seuraavasti

$$\begin{aligned} \pi : G &\rightarrow G/\text{Ker}(f), \pi(a) = \bar{a}, \\ F : G/\text{Ker}(f) &\rightarrow G', F(\bar{a}) = f(a). \end{aligned}$$

Lause 3.13. π on surjektiivinen homomorfismi, F on injektiivinen homomorfismi ja $f = F \circ \pi$.

Todistus. Selvästi π on surjektio. Se on myös homomorfismi: $\pi(ab) = \overline{ab} = \bar{a} \cdot \bar{b} = \pi(a) \cdot \pi(b)$.

F on hyvin määritelty: jos $\bar{a} = \bar{b}$, niin $a = bh$ jollakin $b \in \text{Ker}(f)$. Nyt $f(a) = f(bh) = f(b)f(h) = f(b)$, joten $F(\bar{a}) = F(\bar{b})$. Injektiivisyys: Koska

$$F(\bar{a}) = e_{G'} \Leftrightarrow f(a) = e_{G'} \Leftrightarrow a \in \text{Ker}(f) \Leftrightarrow \bar{a} = \bar{e}_G,$$

niin Lauseen 3.11 seurauksen nojalla F on injektio. Se on myös homomorfismi: $F(\bar{a} \cdot \bar{b}) = F(\overline{ab}) = f(ab) = f(a)f(b) = F(\bar{a})F(\bar{b})$.

Olkoon $a \in G$. Nyt $(F \circ \pi)(a) = F(\pi(a)) = F(\bar{a}) = f(a)$. Täten $F \circ \pi = f$.

□

Seuraus (Ensimmäinen isomorfialause). $G/\text{Ker}(f) \simeq f(G)$.

Todistus. Lemman 3.6 (1) ja Lauseen 3.13 nojalla $F : G/\text{Ker}(f) \rightarrow \text{Im}(F)$ on bijektiivinen homomorfismi. Mutta $\text{Im}(F) = \text{Im}(f)$. □

Esimerkki 3.25. Olkoon $f : \mathbb{C}^* \rightarrow \mathbb{R}^*$, $f(z) = |z|$. Nyt $f(zw) = |zw| = |z||w| = f(z)f(w)$, joten f on homomorfismi. Selvästi $f(\mathbb{C}^*) = \mathbb{R}_{>0}$. Ydin $\text{Ker}(f) = \{z \in \mathbb{C}^* \mid |z| = 1\}$ on kompleksitason yksikköympyrä S^1 ja $\mathbb{C}^*/S^1 \simeq \mathbb{R}_{>0}$.

3.5. Syklisten ryhmien peruslause ja vastaavuuslause. Olkoon $\langle a \rangle$ syklinen ryhmä. Tarkastellaan kuvausta

$$f : \mathbb{Z} \rightarrow \langle a \rangle, f(k) = a^k.$$

Nyt $f(k+m) = a^{k+m} = a^k a^m = f(k)f(m)$, joten f on homomorfismi. Selvästi f on surjektio. Määrätään sen ydin: jos $\text{Ker}(f) = \{0\}$, niin f on injektio ja $\mathbb{Z} \simeq \langle a \rangle$.

Oletetaan, että $\text{Ker}(f) \neq \{0\}$. Jos $k \in \text{Ker}(f)$, niin myös $-k \in \text{Ker}(f)$. Olkoon n pienin positiivinen luku joka kuuluu ytimeen ja olkoon $k \in \text{Ker}(f)$. Jakoalgoritmin nojalla $k = nq + r$, $0 \leq r < n$, ja näin ollen $e = f(k) = f(nq + r) = (a^n)^q a^r = e a^r = a^r$. Siispä $r \in \text{Ker}(f)$. Mutta $0 \leq r < n$, joten n :n minimaalisuuden nojalla $r = 0$. Siispä $\text{Ker}(f) = n\mathbb{Z}$ ja näin ollen $\mathbb{Z}/n\mathbb{Z} \simeq \langle a \rangle$. Näin saimme Lauseen 3.6 täsmennyksen:

Lause 3.14. Olkoon G syklinen ryhmä. Tällöin joko $G \simeq \mathbb{Z}$ tai $G \simeq \mathbb{Z}_n$, jollakin $n \in \mathbb{N}$.

Etsitään seuraavaksi kaikki ryhmien \mathbb{Z} ja \mathbb{Z}_n aliryhmät.

Olkoon $\pi : \mathbb{Z} \rightarrow \mathbb{Z}_n, \pi(a) = \bar{a}$ ja $H' \leq \mathbb{Z}_n$. Lemman 3.6 nojalla $H := \pi^{-1}(H')$ on \mathbb{Z} :n aliryhmä. Selvästi $\pi(H) \subseteq H'$ ja koska π on surjektio, niin $\pi(H) = H'$. Nyt Lemman 3.6 nojalla

$$\Psi : \{H \mid H \leq \mathbb{Z}\} \rightarrow \{H' \mid H' \leq \mathbb{Z}_n\}, \Psi(H) = \pi(H)$$

on surjektio. Rajoitetaan nyt kuvauksen Ψ määrittelyjoukkoa siten, että saamme bijektion Ψ' .

Jos $\Psi(H) = \Psi(S)$, niin $\pi(H) = \pi(S)$. Jos nyt $\pi^{-1}(\pi(H)) = H$ kaikilla $H \in Mj(\Psi)$, niin Ψ on injektio. Selvästi $H \subseteq \pi^{-1}(\pi(H))$. Tutkitaan millä ehdolla pätee käänteinen sisältyminen.

Jos $a \in \pi^{-1}(\pi(H))$, niin $\pi(a) \in \pi(H)$ eli $\pi(a) = \pi(h)$ jollakin $h \in H$. Nyt

$$\pi(a) = \pi(h) \Leftrightarrow \pi(a - h) = \bar{0} \Leftrightarrow a - h \in Ker(\pi) \Leftrightarrow a \in h + Ker(\pi).$$

Täten $a \in H$ jos $Ker(\pi) \subseteq H$.

Lause 3.15. *Kuvaus*

$$\Psi' : \{H \mid H \leq \mathbb{Z} \text{ ja } H \supseteq n\mathbb{Z}\} \rightarrow \{H' \mid H' \leq \mathbb{Z}_n\}, \Psi'(H) = H/n\mathbb{Z},$$

missä $H/n\mathbb{Z} = \{h + nk \mid h \in H, k \in \mathbb{Z}\}$, on bijektio.

Todistus. Koska $H/n\mathbb{Z} = \pi(H)$ ja $Ker(\pi) = n\mathbb{Z}$, niin Ψ' on injektio kuten juuri todettiin. Se on myös surjektio sillä Ψ on surjektio ja $\Psi^{-1}(H') = \pi^{-1}(H') \supseteq Ker(\pi)$. \square

Etsitään nyt ehdon $n\mathbb{Z} \subseteq H$ täyttävät $(\mathbb{Z}, +)$:n aliryhmät H .

Lemma 3.7. *Ryhmän $(\mathbb{Z}, +)$ aliryhmät ovat täsmälleen sykkliset ryhmät $\langle m \rangle = m\mathbb{Z}$, missä $m \in \mathbb{Z}_{\geq 0}$. Lisäksi $\langle m \rangle \neq \langle s \rangle$, jos $m \neq s \geq 0$.*

Todistus. Ensinnäkin jokainen \mathbb{Z} :n aliryhmä H on syklinen: $H = \langle b \rangle$, missä b on H :n pienin positiivinen alkio, tai $H = \langle 0 \rangle$. Tämä nähdään kuten Lauseen 3.14 todistuksessa.

Jos $\langle b \rangle = \langle c \rangle \neq \langle 0 \rangle$, niin $b = ct = bkt$, joillakin $k, t \in \mathbb{Z}$. Siispä $kt = 1$ ja $b = \pm c$. \square

Koska $n\mathbb{Z} \subseteq m\mathbb{Z}$ jos ja vain jos $m \mid n$, niin on voimassa

Lemma 3.8. *Jäännösluokkaryhmän \mathbb{Z}_n aliryhmät ovat täsmälleen sykliset ryhmät*

$$\begin{aligned} m\mathbb{Z}/n\mathbb{Z} &= \{\bar{0}, \bar{m}, \bar{2m}, \dots, \overline{\left(\frac{n}{m} - 1\right)m}\} \\ &= \langle \bar{m} \rangle, \end{aligned}$$

missä m on mikä tahansa luvun n tekijä.

Lause 3.16 (Syklisten ryhmien peruslause). *Olkoon $G = \langle a \rangle$ syklinen ryhmä.*

- (1) *Jos G on ääretön, niin G :n aliryhmät ovat täsmälleen sykliset ryhmät $\langle a^m \rangle$, missä $m = 0, 1, \dots$. Lisäksi $\langle a^m \rangle \neq \langle a^s \rangle$ jos $m \neq s \geq 0$.*
- (2) *Jos $|G| = n$, niin G :llä on jokaista luvun n tekijää k kohti täsmälleen yksi aliryhmä jonka kertaluku on k , nimittäin*

$$\langle a^m \rangle = \{e, a^m, a^{2m}, \dots, a^{(k-1)m}\},$$

missä $k = n/m$. Ryhmällä G ei ole muita aliryhmiä.

Todistus. Väitteet seuraavat välittömästi Lauseesta 3.14 sekä Lemmoista 3.7 ja 3.8. □

Esimerkki 3.26. Etsitään kaikki ryhmän \mathbb{Z}_7^* aliryhmät. Koska $|\mathbb{Z}_7^*| = 6 = 2 \cdot 3$, niin ryhmällä \mathbb{Z}_7^* on täsmälleen 4 aliryhmää ja niiden kertaluvut ovat 1, 2, 3 ja 6.

Koska $\bar{3}^2 = \bar{2}$ ja $\bar{3}^3 = \bar{6}$, niin $\text{ord}(\bar{3}) = 6$ ts. $\mathbb{Z}_7^* = \langle \bar{3} \rangle$. Täten ryhmän \mathbb{Z}_7^* aliryhmät ovat $\langle \bar{1} \rangle$, $\langle \bar{3} \rangle$, $\langle \bar{3}^2 \rangle = \langle \bar{2} \rangle$ ja $\langle \bar{3}^3 \rangle = \langle \bar{6} \rangle$.

Huomautus. Syklisten ryhmien peruslause voidaan todistaa myös ilman vertailua \mathbb{Z} :n aliryhmiin. Käyttämämme vertailu ryhmien \mathbb{Z} ja \mathbb{Z}_n välillä kuitenkin yleistyy välittömästi nk. *vastaavuuslauseeksi* joka on tehokas työkalu ryhmäteoriassa.

Lause 3.17 (Vastaavuuslause). *Olkoon $H \trianglelefteq G$. Silloin kuvaus*

$$\Psi : \{S \mid S \leq G \text{ ja } S \supseteq H\} \rightarrow \{S' \mid S' \leq G/H\}, \Psi(S) = S/H$$

on bijektio.

Todistus. Katso Lauseen 3.15 todistus. □

3.6. Suora tulo ja ryhmän \mathbb{Z}_m^* rakenne. Vektoriavaruus $(\mathbb{R}^2, +)$ on ryhmä kun operaationa on \mathbb{R} :n yhteenlasku komponenteittain ts. $(a, b) + (a', b') = (a + a', b + b')$ kaikilla $(a, b), (a', b') \in \mathbb{R}^2$. Tarkastellaan tämän konstruktion yleistämistä.

Olkoot (G_1, \circ) ja (G_2, \bullet) ryhmiä. Määritellään karteesisessa tulossa $G_1 \times G_2$ binäärinen operaatio \cdot seuraavasti:

$$(a, b) \cdot (a', b') = (a \circ a', b \bullet b') \quad \forall (a, b), (a', b') \in G_1 \times G_2.$$

Lause 3.18. $(G_1 \times G_2, \cdot)$ on ryhmä.

Todistus. Neutraalialkio: (e_{G_1}, e_{G_2}) ; käänteisalkio: $(a, b)^{-1} = (a^{-1}, b^{-1})$ kaikilla $(a, b) \in G_1 \times G_2$; assoatiivisuus palautuu ryhmien G_1 ja G_2 assosiatiivisuuteen. Yksityiskohdat harjoitustehtävänä. \square

Määritelmä 3.14. Ryhmä $(G_1 \times G_2, \cdot)$ on ryhmien G_1 ja G_2 suora tulo. Jos G_1 ja G_2 ovat Abelin ryhmiä, niin käytetään myös termiä *(ulkoinen) suora summa*.

Esimerkki 3.27. Muodostetaan suoran tulon $\mathbb{Z}_3^* \times \mathbb{Z}_2 = \{(\bar{1}, \bar{0}), (\bar{2}, \bar{0}), (\bar{1}, \bar{1}), (\bar{2}, \bar{1})\}$ ryhmätaulu. Merkitään $e = (\bar{1}, \bar{0})$, $a = (\bar{2}, \bar{0})$, $b = (\bar{1}, \bar{1})$ ja $c = (\bar{2}, \bar{1})$. Nyt esimerkiksi $a \cdot b = (\bar{2} \cdot \bar{1}, \bar{0} + \bar{1}) = c$, $a \cdot c = (\bar{2} \cdot \bar{2}, \bar{0} + \bar{1}) = b$, $b \cdot c = (\bar{1} \cdot \bar{2}, \bar{1} + \bar{1}) = a$, ja saamme ryhmätaulun

\circ	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Näemme, että jokaisen alkion kertaluku on 2. Kysessä on siis ei-syklinen kertalukua 4 oleva ryhmä, nk. *Kleinin neliryhmä* K_4 . Täten olemme löytäneet kaksi epäisomorfista kertalukua 4 olevaa ryhmää: \mathbb{Z}_4 ja K_4 . Helposti nähdään, että jokainen kertalukua 4 oleva ryhmä $G \simeq \mathbb{Z}_4$ tai $\simeq K_4$: jos $G = \{e, x, y, z\}$, niin taulu

\circ	e	x	y	z
e	e	x	y	z
x	x			
y	y			
z	z			

voidaan täydentää ryhmätauluksi vain kahdella olennaisesti eri tavalla.

Huomautus. Suora tulo voidaan välittömästi yleistää useammalle kuin kahdelle ryhmälle.

Olkoon $m \in \mathbb{Z}$. Seuraavassa hajoitamme ryhmät \mathbb{Z}_m ja \mathbb{Z}_m^* ”tekijöihin”. Olkoon $m = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ luvun m kanoninen alkutekijähajoitelma.

Lause 3.19.

$$(1) \quad \mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_t^{a_t}},$$

$$(2) \quad \mathbb{Z}_m^* \simeq \mathbb{Z}_{p_1^{a_1}}^* \times \cdots \times \mathbb{Z}_{p_t^{a_t}}^*.$$

Todistus. Osoitetaan, että kuvaus

$$\phi : \mathbb{Z}_m \rightarrow \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_t^{a_t}}, \phi(\bar{a}) = (\bar{a}_1, \dots, \bar{a}_t)$$

on isomorfismi. Se on hyvin määritelty, sillä jos $\bar{a} = \bar{b} \in \mathbb{Z}_m$, niin $a \equiv b \pmod{m}$. Täten $a \equiv b \pmod{p_i^{a_i}}$ kaikilla $i = 1, \dots, t$, ja näin ollen $\bar{a} = \bar{b} \in \mathbb{Z}_{p_i^{a_i}}$ kaikilla $i = 1, \dots, t$.

Osoitetaan, että ϕ on surjektio. Olkoon $(\bar{a}_1, \dots, \bar{a}_t) \in \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_t^{a_t}}$. Nyt kiinalaisen jäännöslauseen nojalla kongruenssiryhmällä

$$\begin{aligned} x &\equiv a_1 \pmod{p_1^{a_1}} \\ &\vdots \\ x &\equiv a_t \pmod{p_t^{a_t}} \end{aligned}$$

on ratkaisu $x \equiv a \pmod{m}$. Koska $a \equiv a_i \pmod{p_i^{a_i}}$ kaikilla $i = 1, \dots, t$, niin $\bar{a} = \bar{a}_i \in \mathbb{Z}_{p_i^{a_i}}$ kaikilla $i = 1, \dots, t$ ja näin ollen $\phi(\bar{a}) = (\bar{a}_1, \dots, \bar{a}_t) = (\bar{a}_1, \dots, \bar{a}_t)$.

Koska ϕ on surjektio ja $|\mathbb{Z}_m| = m = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t} = |\mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_t^{a_t}}|$, niin ϕ on myös injektio.

Kuvaus ϕ on myös homomorfismi:

$$\begin{aligned} \phi(\bar{a} + \bar{b}) &= \phi(\overline{a+b}) = (\overline{a+b}, \dots, \overline{a+b}) = (\bar{a} + \bar{b}, \dots, \bar{a} + \bar{b}) = (\bar{a}, \dots, \bar{a}) + (\bar{b}, \dots, \bar{b}) \\ &= \phi(\bar{a}) + \phi(\bar{b}). \end{aligned}$$

Näin todistettu isomorfia (1).

Isomorfian (2) todistamiseksi näytetään ensin, että kuvauksen ϕ rajoittuma ϕ' alkuluokille on surjektio joukkoon $\mathbb{Z}_{p_1^{a_1}}^* \times \cdots \times \mathbb{Z}_{p_t^{a_t}}^*$.

Jos $(\bar{a}_1, \dots, \bar{a}_t) \in \mathbb{Z}_{p_1^{a_1}}^* \times \cdots \times \mathbb{Z}_{p_t^{a_t}}^*$ ja $x \equiv a \pmod{m}$ on ylläolevan kongruenssiryhmän ratkaisu, niin $a \equiv a_i \pmod{p_i^{a_i}}$ kaikilla $i = 1, \dots, t$. Koska $\text{syt}(p_i, a_i) = 1$, niin $\text{syt}(p_i, a) = 1$ kaikilla $i = 1, \dots, t$. Täten $a \in \mathbb{Z}_m^*$ ja ϕ' on surjektio.

Kuvaus ϕ' on myös injektio sillä ϕ on sitä. Homomorfisuuden

$$\phi'(\bar{a} \cdot \bar{b}) = \phi'(\bar{a}) \cdot \phi'(\bar{b})$$

todistaminen jätetään harjoitustehtäväksi. \square

Seuraus. Eulerin φ -funktiolle pätee

$$\varphi(m) = p_1^{a_1-1}(p_1-1)p_2^{a_2-1}(p_2-1) \cdots p_t^{a_t-1}(p_t-1),$$

jos $m = p_1^{a_1}p_2^{a_2} \cdots p_t^{a_t}$ on luvun m kanoninen alkutekijähajoitelma.

Todistus. Lauseen 3.19 nojalla $\varphi(m) = |\mathbb{Z}_m^*| = |\mathbb{Z}_{p_1^{a_1}}^*| \cdots |\mathbb{Z}_{p_t^{a_t}}^*| = \varphi(p_1^{a_1}) \cdots \varphi(p_t^{a_t})$, joten riittää osoittaa, että $\varphi(p_i^{a_i}) = p_i^{a_i-1}(p_i-1)$.

Luvuista $1, 2, \dots, p_i^{a_i}$ ovat p_i :llä jaollisia luvut $p_i, 2p_i, \dots, p_i^{a_i-1}p_i$. Siispä $|\mathbb{Z}_{p_i^{a_i}}^*| = p_i^{a_i} - p_i^{a_i-1} = p_i^{a_i-1}(p_i-1)$. \square

Esimerkki 3.28. $|\mathbb{Z}_{12250}^*| = \varphi(12250) = \varphi(2 \cdot 5^3 \cdot 7^2) = (2-1)5^2(5-1)7(7-1) = 4200$.

Ryhmän \mathbb{Z}_m^* rakenteen selvittämiseksi on selvitettävä ryhmien $\mathbb{Z}_{p^l}^*$ rakenteet kun $p \in \mathbb{P}$.

Lause 3.20. Jos $p = 2$ ja $l \geq 3$, niin $\mathbb{Z}_{p^l}^*$ ei ole syklinen ja $\mathbb{Z}_{p^l}^* \simeq \langle -1 \rangle \times \langle \bar{5} \rangle$, $\bar{1}, \bar{5} \in \mathbb{Z}_{p^l}^*$. Muulloin $\mathbb{Z}_{p^l}^*$ on syklinen.

Emme todista tätä lausetta.

Lause 3.21. \mathbb{Z}_m^* on syklinen jos ja vain jos $m = 2, 4, p^a$ tai $2p^a$, missä $p > 2$ on mikä tahansa alkuluku ja a on mikä tahansa luonnollinen luku.

Todistus. Todistetaan ensin pieni aputulos:

Lemma 3.9. Olkoot G_1 ja G_2 syklisiä ryhmiä. Silloin $G_1 \times G_2$ on syklinen jos ja vain jos $\text{sy}(m_1, m_2) = 1$, missä $m_i = |G_i|$.

Lemman todistus. Olkoon $G := G_1 \times G_2 = \langle (a, b) \rangle$, jolloin siis $\text{ord}((a, b)) = m_1 m_2$. Jos $d := \text{sy}(m_1, m_2) > 1$ ja $k = m_1 m_2 / d$, niin $(a, b)^k = (a^k, b^k) = e_G$ mikä on mahdotonta sillä $\text{ord}((a, b)) > k$.

Oletetaan, että $d = 1$. Olkoot a ja b ryhmien G_1 ja G_2 generoijat. Nyt

$$e_G = (a, b)^n = (a^n, b^n) \Leftrightarrow a^n = e_{G_1} \text{ ja } b^n = e_{G_2} \Leftrightarrow m_1 \mid n \text{ ja } m_2 \mid n \stackrel{d=1}{\Leftrightarrow} m_1 m_2 \mid n.$$

Täten pienin positiivinen luku n jolla $(a, b)^n = e_G$ on $m_1 m_2$, ja näin ollen $\text{ord}((a, b)) = m_1 m_2$. Siispä $\langle (a, b) \rangle = G$.

Lauseen todistus. Lauseen 3.20 nojalla voidaan olettaa, että $m \neq 2^l, l \geq 3$. Jos nyt m ei ole väitteen muotoa, niin $m = uv$, missä $u, v > 2$ ja $\text{syt}(u, v) = 1$. Nyt $\mathbb{Z}_m \simeq \mathbb{Z}_u \times \mathbb{Z}_v$ ja edelleen $\mathbb{Z}_m^* \simeq \mathbb{Z}_u^* \times \mathbb{Z}_v^*$ (ks. Lauseen 3.19 todistus). Koska 2 on tekijänä kertaluvuissa $|\mathbb{Z}_u^*|$ ja $|\mathbb{Z}_v^*|$ Lauseen 3.19 Seurauksen nojalla, niin Lemman 3.9 nojalla \mathbb{Z}_m^* ei ole syklinen.

Jos $m = 2, 4$ tai p^a , niin Lauseen 3.20 nojalla \mathbb{Z}_m^* on syklinen. Jos $m = 2p^a$, niin $\mathbb{Z}_m^* \simeq \mathbb{Z}_2^* \times \mathbb{Z}_{p^a}^* \simeq \mathbb{Z}_{p^a}^*$ on syklinen. \square

Seuraava tulos on välitön seuraus Lauseista 3.19 ja 3.20.

Lause 3.22. \mathbb{Z}_m^* on isomorfinen syklisten ryhmien suoran tulon kanssa.

Huomautus. Tätä tulosta voidaan täsmentää seuraavasti. Olkoon $m = 2^a p_2^{a_2} \cdots p_t^{a_t}$, kanoninen alkutekijähajoitelma jossa $a \geq 0$. Lauseen 3.20 nojalla

$$\mathbb{Z}_{2^a}^* \simeq \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_{2^{a-2}}, & \text{jos } a \geq 3, \\ \mathbb{Z}_2^{a-1}, & \text{jos } a = 1, 2, \end{cases} \quad \text{ja} \quad \mathbb{Z}_{p_i^{a_i}}^* \simeq \mathbb{Z}_{\varphi(p_i^{a_i})}.$$

Hajoitetaan nyt kukin tekijä Lauseen 3.19 hajoitelmassa (2) hajoitelman (1) mukaiseksi esitykseksi. Järjestämällä sitten tekijät uudelleen saamme hajoitelman

$$\mathbb{Z}_m^* \simeq G_{q_1} \times \cdots \times G_{q_s}$$

missä luvut q_1, \dots, q_s ovat kertaluvun $|\mathbb{Z}_m^*|$ erisuuret alkutekijät ja kukin tekijä

$$G_{q_i} \simeq \mathbb{Z}_{q_i^{b_1}} \times \cdots \times \mathbb{Z}_{q_i^{b_l}}, \quad 1 \leq b_1 \leq \cdots \leq b_l,$$

missä $q_i^{b_1 + \cdots + b_l}$ on korkein luvun q_i potenssi joka on tekijänä kertaluvussa $|\mathbb{Z}_m^*|$.

Tämä yleistyy nk. *äärellisten Abelin ryhmien peruslauseeksi*, jonka mukaan jokainen kertalukua n oleva Abelin ryhmä G on isomorfinen syklisten ryhmien suoran tulon kanssa. Tarkemmin: olkoon $n = q_1^{a_1} \cdots q_s^{a_s}$ kanoninen alkutekijähajoitelma. Silloin

$$G \simeq G_{q_1} \times \cdots \times G_{q_s},$$

missä kukin tekijä

$$G_{q_i} \simeq \mathbb{Z}_{q_i^{b_1}} \times \cdots \times \mathbb{Z}_{q_i^{b_l}}, \quad 1 \leq b_1 \leq \cdots \leq b_l \quad \text{ja} \quad q_i^{b_1 + \cdots + b_l} = q_i^{a_i}.$$

Jokaisen äärellisen Abelin ryhmän ”alkutekijät” ovat siis muotoa \mathbb{Z}_{p^a} , $p \in \mathbb{P}$, $a \in \mathbb{N}$, olevat sykliset ryhmät.

Esimerkki 3.29. $|\mathbb{Z}_{35}^*| = 2^3 \cdot 3$ ja

$$\mathbb{Z}_{35}^* \simeq \mathbb{Z}_5^* \times \mathbb{Z}_7^* \simeq \mathbb{Z}_4 \times \mathbb{Z}_6 \simeq \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3.$$

LIITE A. KERTAUSTA JOUKKO-OPISTA JA LOGIIKASTA

A.1. **Joukko-oppia.** Joukko-opin peruskäsitteitä ovat *joukko* ja *alkio* sekä niiden välillä vallitseva suhde: alkion *kuuluminen joukkoon*.

Tarkastelemme nk. naivia joukko-oppia eli emme määrittele joukkoa aksiomaattisesti, sen sijaan luonnehdimme joukon olevan *kokoelma toisistaan erotettavissa olevia objekteja*. Näitä olioita kutsumme kyseisen joukon alkioiksi.

Jos A on joukko ja a sen alkio merkitään $a \in A$ (a kuuluu joukkoon A). Jos a ei ole joukon A alkio merkitsemme $a \notin A$ (a ei kuulu joukkoon A).

Joukkoja tarkastellessamme rajoitumme tietyn tyyppisiin alkioihin; ne muodostavat *perusjoukon* E ja joukko A muodostuu E :n alkioista.

Esitämme usein joukot muodossa $\{x \mid P(x)\}$, joka on joukko, jonka alkioina ovat kaikki ne perusjoukon E alkio x jotka toteuttavat ehdon $P(x)$. Toinen yleinen tapa esittää joukko on sen alkioiden luetteloiminen aaltosulkeiden välissä.

Esimerkki A.1. $E = \{x \mid x \text{ on Suomen kaupunki}\}$ ja $A = \{x \mid x \in E \text{ ja } x\text{:n väkiluku} \leq 60000\}$. Eräs joukon A alkio on Vaasa.

Eräitä perusjoukkoja

- $\mathbb{N} = \{1, 2, \dots\}$ on luonnollisten lukujen joukko
- $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ on kokonaislukujen joukko
- $\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z}, q \neq 0\}$ on rationaalilukujen joukko
- $\mathbb{R} = \{x \mid x \text{ on rationaalinen tai irrationaalinen}\}$ on reaalilukujen joukko eli kaikkien desimaalilukujen joukko

Määritelmä A.1. Joukko A on joukon B *osajoukko* jos jokainen joukon A alkio on joukon B alkio. Tällöin merkitään $A \subseteq B$.

Esimerkki A.2. Parilliset luvut $2\mathbb{Z} := \{2m \mid m \in \mathbb{Z}\} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$. Parittomat luvut $2\mathbb{Z}+1 := \{2m+1 \mid m \in \mathbb{Z}\} \subseteq \mathbb{Z}$. \mathbb{Z} ei ole joukon $2\mathbb{Z}$ osajoukko sillä esimerkiksi $1 \in \mathbb{Z}$ mutta $1 \notin 2\mathbb{Z}$

Huomautus. Tyhjä joukko \emptyset , eli joukko jossa ei ole yhtään alkioita, on osajoukkona jokaisessa joukossa.

Määritelmä A.2. Joukot A ja B ovat *yhtäsuuret* jos $A \subseteq B$ ja $B \subseteq A$. Tällöin merkitään $A = B$.

Esimerkki A.3. Olkoon $A = \{n + 3 \mid n \in \mathbb{Z}\}$ ja $B = \mathbb{Z}$. Osoitetaan, että $A = B$. On siis näytettävä, että *jokainen* joukon A alkio on joukon B alkio, ja että *jokainen* joukon B alkio on joukon A alkio.

(1) Olkoon a mikä tahansa joukon A alkio jolloin siis $a = n + 3$, missä n on jokin kokonaisluku. Täten a on kokonaisluku ja niinpä $a \in B$. Täten jokainen jokainen joukon A alkio on joukon B alkio eli $A \subseteq B$.

(2) Olkoon b mikä tahansa joukon B alkio. Valitsemalla $n = b - 3 \in \mathbb{Z}$, saadaan $b = n + 3 \in A$. Täten $B \subseteq A$.

Siispä joukkojen yhtäsuuruuden määritelmän mukaan $A = B$.

Määritelmä A.3. Joukon $A \subseteq E$ *komplementti* perusjoukon E suhteen on joukko

$$A^c = \{x \mid x \notin A\}$$

Joukkojen A ja B *leikkaus* on joukko

$$A \cap B = \{x \mid x \in A \text{ ja } x \in B\}$$

Joukkojen A ja B *yhdiste* (*unioni*) on joukko

$$A \cup B = \{x \mid x \in A \text{ tai } x \in B\}$$

Joukkojen A ja B *erotus* on joukko

$$A \setminus B = \{x \mid x \in A \text{ ja } x \notin B\}$$

A.2. Avoin lause, kvanttorit. Logiikan eräs peruskäsite on *lause*. Se on ilmaisu jolla on *totuusarvo*: lause on joko *tos*i tai *epätosi* muttei kumpaakin yhtäaikaan. Esimerkiksi lause $p : 2 + 1 = 3$ on tosi ja lause $q : 2 + 1 = 4$ on epätosi. Merkinnällä $2 + 1$ ei ole totuusarvoa. Se ei ole lause vaan *lauseke*.

Lauseke $p(x) : x < 3, x \in \mathbb{N}$ on *avoin lause eli predikaatti*, jonka määrittelyjoukko M_j on \mathbb{N} . Siitä saadaan lause sijoitettiinpa muuttujan x paikalle mikä tahansa määrittelyjoukon alkio. Esim. muuttujan arvoa $x = 4$ vastaa epätosi lause $p(4) :$

$4 < 3$. Avoimen lauseen $p(x)$ ratkaisujoukko $R_j(p)$ koostuu kaikista niistä muuttujan x arvoista $a \in M_j$ joilla $p(a)$ on tosi. Siispä $R_j(p) = \{1, 2\}$.

Määritelmä A.4. Olkoon $q(x)$ mikä tahansa avoin lause. Lauseen $q(x)$ määrittelyjoukko on muuttujan x saamien arvojen perusjoukko E . Lauseen $q(x)$ ratkaisujoukko on täsmälleen niiden muuttujan x saamien arvojen $a \in E$ joukko joilla $q(x)$ on tosi. Siispä

$$R_j(q) = \{a \in E \mid q(a) \text{ on tosi}\}$$

Jos $R_j(q) = E$ on $q(x)$ identtisesti tosi joukossa E . Jos taas $R_j(q) = \emptyset$ on $q(x)$ identtisesti epätosi joukossa E .

Esimerkki A.4. Avoin lause $\sin^2 x + \cos^2 x = 1, x \in \mathbb{R}$ on identtisesti tosi joukossa \mathbb{R} . Avoin lause $\sin^2 x + \cos^2 x = 2, x \in \mathbb{R}$ on identtisesti epätosi joukossa \mathbb{R} .

Jos avoimen lauseen $q(x)$ ratkaisujoukko $R_j(q) \neq \emptyset$, niin on olemassa ainakin yksi x :n arvo jolla $q(x)$ toteutuu. Tämä ilmaistaan *olemassaolo-kvanttorin* \exists avulla:

$$\exists x \in E : q(x),$$

joka luetaan: on olemassa x :n arvo jolla $q(x)$ on tosi.

Jos $R_j(q) = E$, eli $q(x)$ on identtisesti tosi E :ssä, niin tämä ilmaistaan *kaikki-kvanttorin* \forall avulla

$$\forall x \in E : q(x),$$

joka luetaan: $q(x)$ on tosi kaikilla x :n arvoilla.

Kvanttorien avulla avoimista lauseista saadaan lauseita, kun niiden totuusarvot määritellään seuraavasti:

- lause $\exists x \in E : q(x)$ on tosi täsmälleen silloin kun $R_j(q) \neq \emptyset$
- lause $\forall x \in E : q(x)$ on tosi täsmälleen silloin kun $R_j(q) = E$

Esimerkki A.5. Avoimesta lauseesta $q(x) : 2x + 1 > 0, x \in \mathbb{Z}$ saamme lauseen $\exists x \in \mathbb{Z} : 2x + 1 > 0$ joka on tosi sillä sen ratkaisujoukko on epätyhjä: esim. $1 \in R_j(q)$. Sen sijaan lause $\forall x \in \mathbb{Z} : 2x + 1 > 0$ on epätosi, sillä esim. $-1 \in \mathbb{Z}$ mutta $2(-1) + 1 < 0$, joten $R_j(q) \neq \mathbb{Z}$.

Määritelmä A.5. Olkoot $p(x)$ ja $q(x)$ avoimia lauseita, joiden määrittelyjoukko on E . Silloin

- $p(x)$:n *negaatio* $\sim p(x)$ on avoin lause jonka määrittelyjoukko on E ja ratkaisujoukko on $E \setminus R_j(p)$.
- $p(x)$:n ja $q(x)$:n *konjunktio* $p(x) \wedge q(x)$ on avoin lause jonka määrittelyjoukko on E ja ratkaisujoukko on $R_j(p) \cap R_j(q)$.
- $p(x)$:n ja $q(x)$:n *disjunktio* $p(x) \vee q(x)$ on avoin lause jonka määrittelyjoukko on E ja ratkaisujoukko on $R_j(p) \cup R_j(q)$.

Huomautus. Edellisen määritelmän nojalla saamme kaikilla muuttujan x arvoilla $a \in E$ seuraavat totuustaulut konnektiiveille \sim , \wedge ja \vee (perustelu jätetään harjoitustehtäväksi):

$p(a)$	$\sim p(a)$	$p(a)$	$q(a)$	$p(a) \wedge q(a)$	$p(a)$	$q(a)$	$p(a) \vee q(a)$
F	T	F	F	F	F	F	F
F	T	F	T	F	F	T	T
T	F	T	F	F	T	F	T
T	T	T	T	T	T	T	T

missä F on epätosi ja T on tosi.

Esimerkki A.6. Olkoot $p(x) : x > 1, x \in \mathbb{R}$ ja $q(x) : x < 3, x \in \mathbb{R}$. Silloin lauseen $p(x) \wedge q(x)$ ratkaisujoukko $R_j(p) \cap R_j(q) = (1, \infty) \cap (-\infty, 3) = (1, 3)$.

Avoimessa lauseessa voi olla myös kaksi tai useampia muuttujia. Olkoon $p(x, y)$ avoin lause missä muuttujan x määrittelyjoukko on A ja muuttujan y määrittelyjoukko on B . Jotta saisimme tästä lauseen, on jokaiselle muuttujalle annettava arvo. Usein vastaantulevat tapaukset:

Määrittelemme lauseen $\forall x \exists y : p(x, y)$ olevan tosi täsmälleen silloin kun jokaista $a \in A$ kohti voidaan valita $b \in B$ siten, että $p(a, b)$ on tosi.

Määrittelemme lauseen $\exists x \forall y : p(x, y)$ olevan tosi täsmälleen silloin jos joukosta A voidaan valita sellainen alkio a , että $p(a, b)$ on tosi jokaisella $b \in B$.

Esimerkki A.7. Avoimesta lauseesta $p(x, y) : x = y^2, x \in \mathbb{R}_{\geq 0}, y \in \mathbb{R}$ saadaan esimerkiksi lause $\forall x \in \mathbb{R}_{\geq 0} \exists y \in \mathbb{R} : x = y^2$, missä $\mathbb{R}_{\geq 0}$ on ei-negatiivisten reaalilukujen joukko. Tämä luetaan näin: jokaista ei-negatiivista reaalilukua x kohti on olemassa

reaaliluku y jolle pätee $x = y^2$. Lause on tosi, sillä annettua x :ää kohti alkioiksi y voidaan valita \sqrt{x} . Lause $\exists x \in \mathbb{R}_{\geq 0} \forall y \in \mathbb{R} : x = y^2$ on epätosi sillä esim. $1^2 \neq 2^2$, ja näin ollen lauseessa esiintyvää x :ää ei ole olemassa.

A.3. Implikaatio ja ekvivalenssi.

Määritelmä A.6. Olkoot $p(x)$ ja $q(x)$ joukossa E määriteltyjä avoimia lauseita. Niiden

- *implikaatio* $p(x) \Rightarrow q(x)$ on avoin lause jonka ratkaisujoukko koostuu täsmälleen niistä muuttujan x arvoista a joille pätee: sekä $p(a)$ että $q(a)$ ovat tosia tai $p(a)$ on epätosi,
- *ekvivalenssi* $p(x) \Leftrightarrow q(x)$ on avoin lause jonka ratkaisujoukko koostuu täsmälleen niistä muuttujan x arvoista a joille pätee: $p(a)$ on tosi ja $q(a)$ on tosi, tai $p(a)$ on epätosi ja $q(a)$ on epätosi.

Huomautus. Edellisen määritelmän nojalla saamme kaikilla muuttujan x arvoilla $a \in E$ seuraavat totuustaulut konnektiiveille \Rightarrow ja \Leftrightarrow :

$p(a)$	$q(a)$	$p(a) \Rightarrow q(a)$
F	F	T
F	T	T
T	F	F
T	T	T

$p(a)$	$q(a)$	$p(a) \Leftrightarrow q(a)$
F	F	T
F	T	F
T	F	F
T	T	T

Lause A.1. *Implikaatio* $p(x) \Rightarrow q(x)$ on tosi täsmälleen silloin kun $R_j(p) \subseteq R_j(q)$ ja *ekvivalenssi* $p(x) \Leftrightarrow q(x)$ on tosi täsmälleen silloin kun $R_j(p) = R_j(q)$.

Todistus. Harjoitustehtävä. □

Seuraus. *Ekvivalenssi* $p(x) \Leftrightarrow q(x)$ on tosi täsmälleen silloin kun sekä *implikaatio* $p(x) \Rightarrow q(x)$ että $q(x) \Rightarrow p(x)$ on tosi.

Todistus. Harjoitustehtävä. □

Huomautus. Jos implikaatiossa $p(x) \Rightarrow q(x)$ avoin lause $p(x)$ on identtisesti epätosi, niin implikaatio on identtisesti tosi sillä tyhjä joukko on jokaisen joukon osajoukko.

Esimerkki A.8. Olkoot $p(x) : x < 2, x \in \mathbb{R}$ ja $q(x) : x^2 < 4, x \in \mathbb{R}$. Nyt $R_j(p) = (-\infty, 2)$ ja $R_j(q) = (-2, 2)$. Täten implikaatio $p(x) \Rightarrow q(x)$ on epätosi ja implikaatio $q(x) \Rightarrow p(x)$ on tosi. Täten myös ekvivalenssi $p(x) \Leftrightarrow q(x)$ on epätosi.

A.4. Todistusmenetelmistä. Matemaattisen teorian *peruskäsitteet* ovat käsitteitä joita ei voida määritellä ”yksinkertaisempien” käsitteiden avulla. Peruskäsitteitä ja niiden välisiä suhteita luonnehtivat *peruslauseet* eli *aksiomat*. Nämä lauseet oletetaan tosiksi. Matemaattinen teoria rakentuu peruskäsitteiden ja aksiomien varaan ja niihin nojautuen

- määritellään uusia käsitteitä
- todistetaan lauseita eli teoreemoja

Todistamisella tarkoitetaan seuraavaa prosessia: on olemassa joukko *päätelysääntöjä*, joiden avulla voimme johtaa määritelmien, aksiomien sekä aikaisemmin todistettujen teoreemojen avulla *johtopäätöksiä*. Päätelysäännöt valitaan niin, että johtopäätökset ovat identtisesti tosia.

Tarkastellaan seuraavassa muotoa $p \Rightarrow q$ olevien lauseiden todistamista. Tässä lause p on *oletus* ja q on *väitös*.

- (1) *Suora todistus (modus ponens)*. Nojautuen lauseisiin p_1, p_2, \dots, p_k , jotka voivat olla määritelmiä, aksiomia tai aikaisemmin todistettuja teoreemoja, osoitamme että väitös q on tosi kaikilla niillä muuttujien arvoilla joilla oletus p on tosi, ja teemme johtopäätöksen että $p \Rightarrow q$ on identtisesti tosi.

Esimerkki A.9. Todistetaan, että kahden parittoman kokonaisluvun tulo on pariton. Olkoot a ja b mitkä tahansa kaksi paritonta lukua. On siis osoitettava, että lause $p \Rightarrow q$ on tosi, missä $p : a \text{ pariton ja } b \text{ pariton}$ ja $q : ab \text{ pariton}$. Koska oletus on tosi, niin parittoman luvun määritelmän nojalla $a = 2m + 1$ ja $b = 2n + 1$ joillakin $m, n \in \mathbb{Z}$. Nyt osittelulakien nojalla $ab = (2m + 1)(2n + 1) = 4mn + 2(m + n) + 1 = 2(2mn + m + n) + 1$. Koska $mn + m + n \in \mathbb{Z}$, niin parittoman luvun määritelmän nojalla ab on pariton. Siispä q on tosi ja olemme todistaneet lauseen $p \Rightarrow q$.

- (2) *Epäsuora todistus (kontrapositio)*. Tarkastelemme lauseen $p \Rightarrow q$ asemesta sen kanssa yhtäpitävää (eli loogisesti ekvivalenttia) lausetta $\sim q \Rightarrow \sim p$. Tämä lause todistetaan oikeaksi esim. suoraa todistusta käyttäen.

Esimerkki A.10. Kolmen kokonaisluvun summa = 10. Todistetaan, että ainakin yksi summattavista on suurempi kuin 3. Olkoot $a, b, c \in \mathbb{Z}$. Nyt $p : a + b + c = 10$ ja $q : (a > 3) \vee (b > 3) \vee (c > 3)$. Oletetaan, että väitteen q negaatio $\sim q : (a \leq 3) \wedge (b \leq 3) \wedge (c \leq 3)$ on tosi. Nyt $a + b + c \leq 3 + 3 + 3 =$

$9 \neq 10$, joten $\sim p$ on tosi. Täten lause $\sim q \Rightarrow \sim p$ on identtisesti tosi, joten myös sen kanssa yhtäpitävä lause $p \Rightarrow q$ on identtisesti tosi.

- (3) *Todistus ristiriidan avulla (reduktio ad absurdum)*. Oletamme todeksi väitteen negaation $\sim q$ ja johdamme epätoden lauseen eli ristiriidan. Tällöin päättelemme, että $\sim q$ on epätosi ja edelleen, että q on tosi.

Esimerkki A.11. Todistetaan, että $\sqrt{2}$ on irrationaalinen. Oletetaan väitteen negaatio $\sim q$: $\sqrt{2}$ ei ole irrationaalinen todeksi. Koska jokainen reaaliluku on joko rationaalinen tai irrationaalinen ja $\sqrt{2}$ ei ole irrationaalinen on sen oltava rationaalinen. Täten $\sqrt{2} = a/b$ joillakin $a, b \in \mathbb{Z}$, $b \neq 0$, missä joko a tai b on pariton. Nyt $a^2 = 2b^2$, joten a^2 on parillinen. Tällöin myös a on parillinen eli $a = 2n$ joillakin $n \in \mathbb{Z}$. Nyt $4n^2 = 2b^2$ joten $b^2 = 2n^2$. Siispä b^2 on parillinen ja täten myös b on parillinen. Nyt päädyimme ristiriitaan sen kanssa, että joko a tai b on pariton. Siispä väitteen q on oltava tosi.

Kerrataan vielä miten kvanttoireita tai implikaation sisältävän lauseen negaatio muodostetaan

$$\begin{aligned} \sim ((\forall x)P(x)) &\Leftrightarrow (\exists x) \sim P(x) \\ \sim ((\exists x)P(x)) &\Leftrightarrow (\forall x) \sim P(x) \\ \sim (P(x) \Rightarrow Q(x)) &\Leftrightarrow P(x) \wedge \sim Q(x) \end{aligned}$$

Esimerkki A.12. Olkoon f reaalifunktio. Määritelmän mukaan f on jatkuva pisteessä $a \in \mathbb{R}$ jos

$$(\forall \epsilon > 0)(\exists \delta > 0)(\forall x \in \mathbb{R}) : |x - a| < \delta \Rightarrow |f(x) - f(a)| < \epsilon.$$

Täten f on epäjatkuva pisteessä a jos

$$(\exists \epsilon > 0)(\forall \delta > 0)(\exists x \in \mathbb{R}) : |x - a| < \delta \wedge |f(x) - f(a)| \geq \epsilon.$$