Jäännösluokka

Kongruenssi modulo m hajottaa joukon $\mathbb{Z}$ ekvivalenssiluokkiin, jotka ovat muotoa:

$$[a] = \{a + mk \mid k \in \mathbb{Z}\}.$$

Ekvivalenssiluokkaa $[a]$ sanotaan luvun *a jäännösluokaksi modulo m*. Jäännösluokasta käytetään yleensä merkintää $\overline{a}$ tai $a + m\mathbb{Z}$. Samassa jäännösluokassa olevat luvut antavat saman jakojäännöksen luvulla m jaettaessa. Kaikkien jäännösluokkien modulo m joukosta käytetään merkintää $\mathbb{Z}_m$. Jäännösluokan $\overline{a} \in \mathbb{Z}_m$ edustajaksi voidaan valita mikä tahansa luku, joka on kongruentti luvun a kanssa modulo m. Näistä luvuista voidaan jakoalgoritmin mukaan valita yksikäsitteisesti luvun *a pienin ei-negatiivinen jäännös modulo m*. Tämä jäännös r toteuttaa ehdon $0 \leq r < m$. Siis jokaisella luokalla $\overline{a} \in \mathbb{Z}_m$ on pienin ei-negatiivinen jäännös r modulo m, joka toteutaa saman ehdon. Toisaalta nämä jäännökset ovat selvästi parittain epäkongruentteja modulo m. Täten

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}.$$

Esimerkki. $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$, missä

$$\begin{array}{rcrcrcl}
\overline{0} & = & 3\mathbb{Z} & = & \{3k \mid k \in \mathbb{Z}\} & = & \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}, \\
\overline{1} & = & 1+3\mathbb{Z} & = & \{1+3k \mid k \in \mathbb{Z}\} & = & \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}, \\
\overline{2} & = & 2+3\mathbb{Z} & = & \{2+3k \mid k \in \mathbb{Z}\} & = & \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}.
\end{array}$$

Joukko $\mathbb{Z}_3$ voidaan esittää myös esimerkiksi muodossa $\{\overline{-1}, \overline{0}, \overline{1}\}$ tai $\{\overline{7}, \overline{-4}, \overline{6}\}$.

Jos $m = 1$, niin kongruenssi modulo m on triviaali: $a \equiv b \pmod 1$ kaikilla $a, b \in \mathbb{Z}$. Erityisesti siis $\mathbb{Z}_1 = \{\overline{0}\}$, missä $\overline{0} = \mathbb{Z}$.

Lause. Jäännösluokkien summa $\overline{a} + \overline{b} = \overline{a+b}$ ja tulo $\overline{a} \cdot \overline{b} = \overline{ab}$ eivät ole riippuvia jäännösluokkien edustajien valinnasta. (Sanotaan, että jäännösluokkien summa ja tulo ovat *hyvin määriteltyjä*.)

Todistus. Olkoot $\overline{a} = \overline{a'}$ ja $\overline{b} = \overline{b'}$. Silloin $a \equiv a' \pmod m$ ja $b \equiv b' \pmod m$. Sivulla Kongruenssi olevan lauseen kohdan (i) mukaan on

$$a + b \equiv a' + b' \qquad \text{ja} \qquad ab \equiv a'b' \pmod m.$$

Täten $\overline{a+b} = \overline{a'+b'}$ ja $\overline{ab} = \overline{a'b'}$, mikä todistaa väitteen. □

Linkit:
Konruenssi
Ekvivalenssiluokka
Jakoalgoritmi
Diofantoksen yhtälö