Kongruenssi

Kongruenssin käsite mahdollistaa jaollisuuteen liittyvien asioiden käsittelyn tavalla, joka muistuttaa yhtälöiden käsittelyä.

Määritelmä. Olkoon m positiivinen kokonaisluku. Jos $a, b \in \mathbb{Z}$ ja $a-b$ on jaollinen luvulla m sanotaan, että luku a on *kongruentti* luvun b kanssa *modulo* m, ja merkitään

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

Tätä joukon $\mathbb{Z}$ relaatiota nimitetään *kongruenssiksi* ja luku m on sen *moduli*.

Edellisen vastakohta on, että luku a on *epäkongruentti* luvun b kanssa *modulo* m. Tätä merkitään $a \not\equiv b \pmod{m}$.

Esimerkki. $27 \equiv 2 \pmod{5}$, $12 \equiv -8 \pmod{10}$, $30 \not\equiv 1 \pmod{7}$.

Määritelmän mukaan $a \equiv b \pmod{m}$ jos ja vain jos a on luvun m monikertaa vaille yhtä suuri kuin b. Toisin sanoen

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad a = b + mq, \text{ jollekin } q \in \mathbb{Z}.$$

Tästä nähdään helposti (tarkistamalla ekvivalenssirelaation ehdot E1-E3), että kongruenssi modulo m on joukon $\mathbb{Z}$ ekvivalenssirelaatio.

Lause. (i) Jos $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m}$, niin

$$a + c \equiv b + d \pmod{m} \qquad \text{ja} \qquad ac \equiv bd \pmod{m}.$$

(ii) Jos $ca \equiv cb \pmod{m}$ ja $\text{syt}(c, m) = 1$, niin $a \equiv b \pmod{m}$.
(iii) Jos $a \equiv b \pmod{km}$, missä k on positiivinen kokonaisluku, niin $a \equiv b \pmod{m}$.

Todistus. (i) Luku $(a+c)-(b+d) = (a-b)+(c-d)$ on jaollinen luvulla m, koska $m \mid (a-b)$ ja $m \mid (c-d)$. Samoin luku $ac - bd = (a-b)c + (c-d)b$ on luvun m monikerta.

(ii) Koska c ja m ovat parittain suhteellisia alkulukuja ja $m \mid (ca - cb) = c(a-b)$, niin $m \mid (a-b)$ (katso aritmetiikan peruslausetta edeltävä lause).

(iii) Koska luku $a-b$ on luvun km monikerta on se myös luvun m monikerta. □

Lauseen kohdan (i) mukaan kongruensseja modulo m voi laskea yhteen ja kertoa puolittain, samoin voidaan myös vähentää ja korottaa potenssiin puolittain. Erityisesti, jos $P(x)$ on kokonaiskertoiminen polynomi eli

$$P(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_t x^t, \quad \text{missä } c_i \in \mathbb{Z} \text{ kaikilla arvoilla } i.$$

niin kongruenssista $a \equiv b \pmod{m}$ seuraa, että $P(a) \equiv P(b) \pmod{m}$.

Linkit:
Ekvivalenssirelaatio

Aritmetiikan peruslause

Jäännösluokka