Kongruenssi

Esimerkki Erään koneen koekäyttö aloitettiin klo 8. Mihin kellonaikaan koe päättyi, kun koe kesti 110 tuntia?

Koska 24 tunnin lisääminen kuluneeseen aikaan ei muuta kellonaikaa, lasketaan, kuinka monta ”täyttä vuorokautta” koe kesti ja lisätään ”ylimääräiset” tunnit aloitusaikaan 8. Tarkemmin sanottuna muodostetaan jakolasku $110:24$ ja katsotaan mikä on jakojäännös, eli

$$110 = 24 \cdot 4 + 14.$$

Jakojäännös 14 ilmoittaa ”ylimääräiset tunnit” → koe päättyi siis klo $8 + 14 = 22$.

Yleisesti jaollisuutta koskevissa laskuissa/ilmiön tarkasteluissa *jakoyhtälöllä* ja erityisesti *jakojäännöksellä* on ratkaisevan tärkeä rooli. Nimittäin joskus on syytä pitää ”samanlaisina” niitä kokonaislukuja, joiden erotus on jaollinen annetulla kokonaisluvulla.

Määritelmä, kongruenssi:
Olkoon $n \geq 1$. Sanotaan, että luku a on luvun b kanssa *kongruentti modulo* n, jos erotus $a - b$ on jaollinen luvulla n. Tällöin merkitään

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

Siis $a \equiv b \pmod{n} \iff n|(a-b)$.
Jos luku a ei ole luvun b kanssa kongruentti modulo n, niin merkitään

$$a \not\equiv b \pmod{n}.$$

Lukua n sanotaan *moduliksi*.

Esimerkkejä

a) $18 \equiv 6 \pmod{4}$, sillä $18 - 6 = 12$ ja $4|12$ (eli $12 = 4 \cdot 3$).
b) $-4 \equiv 16 \pmod{5}$, sillä $-4 - 16 = -20$ ja $5|-20$.
c) $15 \not\equiv 3 \pmod{7}$, sillä $15 - 3 = 12$ ja $7 \nmid 12$.
d) $a \equiv 0 \pmod{k}$, vain silloin, kun $k|a$. Eli vain tällöin jakojäännös on nolla.

Lause, kongruenssi ja jakojäännös:
Lukujen a ja b kongruenssi modulo n tarkoittaa samaa kuin se, että jaettaessa luvut a ja b luvulla n saadaan sama jakojäännös r, eli

$$a \equiv b \pmod{n} \iff \begin{matrix} a = pn + r \\ b = qn + r \end{matrix}, \qquad p, q, r \in \mathbb{Z}.$$

Lauseen tulos on *jos ja vain jos* tulos, joten pitää osoittaa molemmat suunnat. Osoitetaan ensin "$\Longrightarrow$" suunta ja sitten "$\Longleftarrow$" suunta.

Oletus: $a \equiv b \pmod{n}$

Väite: Jakolaskuissa $\frac{a}{n}$ ja $\frac{b}{n}$ on sama jakojäännös.

Todistus: Oletuksen mukaan $a - b = pn$ eli $a = pn + b$ jollakin $p \in \mathbb{Z}$. Olkoon q osamäärän kokonaisosa ja jakojäännös r jakolaskussa $\frac{b}{n}$, jolloin voidaan kirjoittaa $b = qn + r$. Näin ollen

$$a = pn + \overbrace{b}^{qn+r} = pn + qn + r = \overbrace{(p+q)}^{s} \cdot n + r =: sn + r\,.$$

Tämä tarkoittaa sitä, että jakolaskussa $\frac{a}{n}$ osamäärän kokonaisosa on s ja jakojäännös on r. Jakojäännökset ovat siis samat, mikä piti osoittaa.

Oletus: Jakolaskuissa $\frac{a}{n}$ ja $\frac{b}{n}$ on sama jakojäännös.

Väite: $a \equiv b \pmod{n}$

Todistus: Oletuksen mukaan on olemassa sellaiset kokonaisluvut p, q ja r, että $a = pn + r$ ja $b = qn + r$. Koska $a - b = pn - qn = (p - q)n$, niin pätee $n|(a - b)$ mistä väite $a \equiv b \pmod{n}$ seuraa.

Lause, kongruenssin perusominaisuudet:

Kongruenssi on *refleksiivinen*:	Aina	$a \equiv a \pmod{n}$.
Kongruenssi on *symmetrinen*:	Jos	$a \equiv b \pmod{n}$,
	niin	$b \equiv a \pmod{n}$.
Kongruenssi on *transitiivinen*:	Jos	$a \equiv b \pmod{n}$,
	ja	$b \equiv c \pmod{n}$,
	niin	$a \equiv c \pmod{n}$,

Huomautus Kyseessä on niin sanotun ekvivalenssirelaation ehdot; *refleksiivisyys, symmetrisyys ja transitiivisuus*. Lyhyesti sanottuna tämä tarkoittaa sitä, että luvut a ja b ovat "samoja" eli edustavat samaa joukkoa (jäännösluokkaa) luvun n suhteen.

Todistus: Seuraava dia.

Kongruenssi

$a \equiv b \pmod{n}$	$\Leftrightarrow$	Luvuilla a ja b sama jakojäännös, kun jaetaan luvulla n.
$a \equiv b \pmod{n}$	$\Leftrightarrow$	$n\|(a - b)$
$a \equiv b \pmod{n}$	$\Leftrightarrow$	$a = kn + b$

Todistus:
1) Refleksiivisyys, eli $a \equiv a \pmod{n}$
Koska $a - a = 0$ ja kaikille $n \neq 0$ pätee $n|0$, eli $n|(a - a)$.

2) Symmetrisyys, eli jos $a \equiv b \pmod{n}$, niin $b \equiv a \pmod{n}$.
Jos $a \equiv b \pmod{n}$, niin $n|(a - b)$. Tulon jaollisuussäännön nojalla pätee, että kaikille $p \in \mathbb{Z}$ on voimassa $n|p \cdot (a - b)$. Valitsemalla nyt $p = -1$, saadaan

$$n| -1 \cdot (a - b) \implies n|(b - a)$$

Siis $b \equiv a \pmod{n}$.

3) Transitiivisuus, eli jos $a \equiv b \pmod{n}$ ja $b \equiv c \pmod{n}$, niin $a \equiv c \pmod{n}$.
Oletuksista saadaan $n|(a - b)$ ja $n|(b - c)$. Näin ollen yhteenlaskun jaollisuussäännön nojalla pätee

$$n|(a - b + b - c) \implies n|(a - c)$$

Siis $a \equiv c \pmod{n}$.