Kongruenssien laskusääntöjä

- Olkoot $a \equiv b \pmod{n}$ ja $c \equiv d \pmod{n}$ ja $p \in \mathbb{Z}_+$. Tällöin pätee
  1. $a + c \equiv b + d \pmod{n}$
  2. $ac \equiv bd \pmod{n}$
  3. $a^p \equiv b^p \pmod{n}$
- Todistus s. 77 oppikirjassa.

t. 332, s. 82

$a \equiv b \pmod{n}$

a) Koska luvuilla a ja b on sama jakojäännös, niin myös luvuilla $a + 7$ ja $b + 7$ on keskenään sama jakojäännös lauseen 1. perusteella.

$(c = d = 7, 7 \equiv 7 \pmod{n})$

Siis $a + 7 \equiv b + 7 \pmod{n}$.

Kongruenssiyhtälöön voidaan siis lisätä (tai vähentää) sama luku puolittain kuten tavallisessakin yhtälössä.

b) Nyt ($c = d = 3$, $3 \equiv 3 \pmod n$), joten kongruenssi $3a \equiv 3b \pmod n$ pitää paikkansa lauseen 2. perusteella.
Luvuilla $3a$ ja $3b$ on siis sama jakojäännös n:llä jaettaessa.

Kongruenssiyhtälön voi siis kertoa puolittain kokonaisluvulla, kuten tavallisenkin yhtälön.

c) Väite voidaan kirjoittaa muotoon $a \cdot a \equiv b \cdot b \pmod n$.
Tämä kongruenssi pitää myös paikkansa lauseen 2. perusteella.

Huomaa, että kongruenssiyhtälöä ei välttämättä voi jakaa puolittain samalla kokonaisluvulla:

Esimerkiksi kongruenssi $6 \equiv 16 \pmod{10}$ on tosi, mutta puolittain kahdella jaettu muoto $3 \equiv 8 \pmod{10}$ on epätosi.

Yleisesti, jos $ka \equiv kb \pmod n$, ja $syt(n, k) = 1$, niin $a \equiv b \pmod n$.

Esimerkiksi $4 \equiv 14 \pmod 5$ ja puolittain kahdella jaettu muoto $2 \equiv 7 \pmod 5$ on myös tosi, sillä $\mathrm{syt}(5, 2) = 1$.