Kongruenssi

- Olkoon n ykköstä suurempi positiivinen kokonaisluku.
- Määritelmä: Jos kokonaislukujen a ja b erotus on jaollinen luvulla n, niin luvut a ja b ovat kongruentit modulo n.
- Merkitään $a \equiv b(mod\ n)$.
- Esim. 1. $951 \equiv 447(mod\ 24)$, koska

$$\frac{951 - 447}{24} = 21$$

Kongruenssi

- Koska $a - a = 0$, niin $a \equiv a \ (mod\ n)$.
- Esimerkkejä.

$$7 \equiv 2 \ (mod\ 5) \quad | \quad |7 - 2 = 5 \text{ ja } \frac{5}{5} = 1$$

$$12 \equiv 2 \ (mod\ 5) \quad || \ 12 - 2 = 10 \text{ ja } \frac{10}{5} = 2$$

Voi ajatella myös näin: $12 - 5 - 5 = 2$

Kongruenssi ja jakojäännös

Kokonaisluvut a ja b ovat kongruentit modulo n, jos ja vain jos (joss.) niillä on sama jakojäännös, kun luvut jaetaan luvulla n.

- Esim. 2. $12 \equiv 7 (mod\ 5)$, koska

  $12 = 2 \cdot 5 + 2$ ja $7 \equiv 1 \cdot 5 + 2$

Kongruenssi

- Esim. 3. Osoita, että $19 \equiv -37\ (mod\ 8)$.

$19 - (-37) = 56 = 7 \cdot 8$ eli erotus on jaollinen luvulla 8.

Täten $19 \equiv -37\ (mod\ 8)$.

Lisää lauseita kongruenssista

Kongruenttien lukujen summa ja tulo

- Oletetaan, että $a \equiv b (\mathrm{mod}\, n)$

  ja c $\equiv d (\mathrm{mod}\, n)$.

  Tällöin $a + b \equiv c + d \ (\mathrm{mod}\, n)$

  ja $ac \equiv bd \ (\mathrm{mod}\, n)$.

- Lisäksi: Jos $a \equiv b (\mathrm{mod}\, n)$ ja r on positiivinen kokonaisluku, niin $a^r \equiv b^r (\mathrm{mod}\, n)$

Esimerkki 4

Luvut $5^{35} + 1$ ja $21^{35} - 7$ jaetaan luvulla 8.
Osoita, että jakojäännökset ovat yhtä suuret.

- Osoitetaan, että luvut $5^{40} + 1$ ja $21^{40} - 7$ ovat kongruentteja modulo 8.

Koska $5 - 21 = -16 = -2 \cdot 8$,

niin $5 \equiv 21 \pmod 8$.

Koska $5 \equiv 21 \pmod 8$, niin
$5^{35} \equiv 21^{35} \pmod 8$.

Esimerkki 4

Koska $1 - (-7) = 8$, niin $1 \equiv -7 \pmod 8$.

Koska $5^{35} \equiv 21^{35} \pmod 8$ ja $1 \equiv -7 \pmod 8$, niin $5^{35} + 1 \equiv 21^{35} - 7 \pmod 8$.

Lisää lauseita kongruenssista

Jokainen luku on kongruentti jakojäännöksen kanssa.

- Olkoon r jakojäännös, joka jää, kun luku a jaetaan luvulla n. Tällöin $a \equiv r \pmod{n}$.
- Erityisesti siis: Jokainen luku a on kongruentti modulo n jonkin luvuista 0, 1, 2, …, $n-1$ kanssa. Luku on jakojäännös, joka jää, kun luku a jaetaan luvulla n.

Esimerkki 5

Osoita, että luku $81 + 703 \cdot 22^{18}$ on jaollinen luvulla 7.

- Koska $81 \equiv 4 \pmod 7$, $703 \equiv 3 \pmod 7$ ja $22 \equiv 1 \pmod 7$, niin

$$81 + 703 \cdot 22^{18} \equiv 4 + 3 \cdot 1^{18}$$
$$\equiv 4 + 3 \cdot 1 \equiv 7 \equiv 0 \pmod 7.$$

Siis luku $81 + 703 \cdot 22^{18}$ on jaollinen luvulla 7.

Esimerkki 6

Osoita, että jokaisella kokonaisluvulla n luku $n^3 + 2n$ on jaollinen luvulla 3.

- Voidaan tutkia tapauksia, joissa n on muotoa $3q$, $3q + 1$ tai $3q + 2$, missä q on kokonaisluku. Mutta voidaan käyttää myös kongruenssia.

Jos n on kokonaisluku, niin $n \equiv 0$ tai $n \equiv 1$ tai $n \equiv 2 \pmod 3$.

Jos $n \equiv 0 \pmod 3$, niin

$$n^3 + 2n \equiv 0^3 + 2 \cdot 0 \equiv 0 \pmod 3.$$

Jos $n \equiv 1 \pmod 3$, niin

$$n^3 + 2n \equiv 1^3 + 2 \cdot 1 \equiv 3 \equiv 0 \pmod 3.$$

Jos $n \equiv 2 \pmod 3$, niin

$$n^3 + 2n \equiv 2^3 + 2 \cdot 2 \equiv 12 \equiv 0 \pmod 3.$$

Siis aina $n^3 + 2n \equiv 0 \pmod 3$. Luku $n^3 + 2n$ on jaollinen luvulla 3 kaikilla n:n arvoilla.