

6. Kongruenssi

Kongruenssi (määritelmä)

Olkoon n lukua yksi suurempi kokonaisluku. Kokonaisluvut a ja b ovat kongruentit modulo n , jos niiden erotus on jaollinen luvulla n .

Jos luvut a ja b ovat kongruentit modulo n , niin merkitään

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

Esim1.

a) $14 \equiv 2 \pmod{6}$, koska erotus $14 - 2 = 12$ on jaollinen luvulla 6.

b) $25 \equiv 7 \pmod{3}$, koska erotus $25 - 7 = 18$ on jaollinen luvulla 3.

Kongruenttien lukujen jakojäännökset (lause)

Positiiviset kokonaisluvut a ja b ovat kongruentit modulo n , jos ja vain jos luvuilla a ja b on sama jakojäännös, kun ne jaetaan luvulla n .

Esim2. Käytetään esimerkin 1 lukuja

a) $14 = 6 \cdot 2 + 2$

$$2 = 6 \cdot 0 + 2$$

b) $25 = 3 \cdot 8 + 1$

$$7 = 3 \cdot 2 + 1$$

Jakojäännöksen kongruenssi (lause)

Jos jakolaskun $a : n$ jakojäännös on r , niin

$$a \equiv r \pmod{n}$$

Esim3. Osoita, että

a) $18 \equiv 6 \pmod{3}$

b) $29 \equiv -6 \pmod{5}$

c) Mikä on pienin luonnollinen luku, jonka kanssa 29 on kongruentti modulo 5?

Ratk.

a) Osoitetaan, että lukujen 18 ja 6 erotus on jaollinen luvulla 3

$$18 - 6 = 12 = 3 \cdot 4$$

Siis $18 \equiv 6 \pmod{3}$.

b) Osoitetaan, että lukujen 29 ja -6 erotus on jaollinen luvulla 5

$$29 - (-6) = 35 = 5 \cdot 7$$

Siis $29 \equiv -6 \pmod{5}$.

c) $29 = 5 \cdot 5 + 4$

Joten

$$29 \equiv 4 \pmod{5}$$

V: 4

Summan, tulon ja potenssin kongruenssi (lause)

Olkoon $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$ ja $k \in \mathbb{Z}_+$

1) Kongruenttien summat ovat kongruentteja

$$a + c \equiv b + d \pmod{n}$$

2) Kongruenttien lukujen tulot ovat kongruentteja

$$ac \equiv bd \pmod{n}$$

3) Kongruenttien lukujen potenssit ovat kongruentteja

$$a^k \equiv b^k \pmod{n}$$

Esim4.

Määritä kongruenssia käyttäen jakojäännös, kun luku $52 \cdot 14 + 7^4$ jaetaan luvulla 5.

Ratkaisu

Lasketaan jokaiselle luvulle erikseen kongruenssi modulo 5

$$52 \equiv 2 \pmod{5}$$

$$14 \equiv 4 \pmod{5}$$

$$7 \equiv 2 \pmod{5}$$

Korvataan laskutoimituksen luvut kongruenteilla luvuilla modulo 5

$$52 \cdot 14 + 7^4$$

$$\equiv 2 \cdot 4 + 2^4$$

$$\equiv 8 + 16$$

$$\equiv 24$$

$$\equiv 4 \pmod{5}$$

V: Jakojäännös on 4

Esim5.

Määritä luvun 2^{99} viimeinen numero.

Ratk.

Kun luku 2^{99} jaetaan luvulla 10, niin jakojäännös on luvun viimeinen numero.

Huomataan

$$2^5 = 32 \equiv 2 \pmod{10}$$

$$\begin{aligned} 2^{99} &= 2^{5 \cdot 19 + 4} \\ &= (2^5)^{19} \cdot 2^4 \\ &\equiv 2^{19} \cdot 2^4 \\ &\equiv 2^{23} \\ &\equiv 2^{5 \cdot 4 + 3} \\ &\equiv 2^4 \cdot 2^3 \\ &\equiv 2^5 \cdot 2^2 \\ &\equiv 2 \cdot 4 \\ &\equiv 8 \pmod{10} \end{aligned}$$

Joten viimeinen numero luvussa 2^{99} on 8

V: Viimeinen numero on 8

Laskimen komento: remain

Tehtävät: 1, 4, 5, 6, 18, 22