

Kongruenslagarna

Om $a \equiv b \pmod{n}$ och $c \equiv d \pmod{n}$, $n \geq 2 \Rightarrow$

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

2. $a \cdot c \equiv b \cdot d \pmod{n}$

3. $k \cdot a \equiv k \cdot b \pmod{n}$

4. $a^m \equiv b^m \pmod{n}$

exempel: $(a, b, c, d) = (7, 12, 17, 22)$, $n = 5$

1:a lagen: $7 + 12 \equiv 17 + 22 \pmod{5}$

$$7 \pmod{5} + 12 \pmod{5} = 17 \pmod{5} + 22 \pmod{5}$$

$$2 + 2 = 2 + 2$$

2:a lagen: $7 \cdot 17 \equiv 12 \cdot 22 \pmod{5}$

$$7 \pmod{5} \cdot 17 \pmod{5} = 12 \pmod{5} \cdot 22 \pmod{5}$$

$$2 \cdot 2 = 2 \cdot 2$$

3:e lagen: $k = 6 \Rightarrow 6 \cdot 7 \equiv 6 \cdot 12 \pmod{5}$

$$6 \pmod{5} \cdot 7 \pmod{5} = 6 \pmod{5} \cdot 12 \pmod{5}$$

$$1 \cdot 2 = 1 \cdot 2$$

4:e lagen: $m = 6 \Rightarrow 7^6 \equiv 12^6 \pmod{5}$

$$(7 \pmod{5})^6 = (12 \pmod{5})^6$$

$$2^6 = 2^6$$