Kongruensreglerna

Kongruens $a \equiv b \pmod{c}$ om differensen $a - b$ är delbar med c

Om $a_1 \equiv b_1 \pmod{c}$ och $a_2 \equiv b_2 \pmod{c}$ gäller att

1. $a_1 + a_2 \equiv b_1 + b_2 \pmod{c}$
2. $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{c}$

Om $a \equiv b \pmod{c}$ gäller att

3. $m \cdot a \equiv m \cdot b \pmod{c}$ för alla heltal m
4. $a^n \equiv b^n \pmod{c}$ för alla heltal $n \geq 0$

$a_1 \equiv b_1 \pmod{c} \Rightarrow a_1 - b_1 = c \cdot k_1 \Rightarrow a_1 = c \cdot k_1 + b_1$

$a_2 \equiv b_2 \pmod{c} \Rightarrow a_2 - b_2 = c \cdot k_2 \Rightarrow a_2 = c \cdot k_2 + b_2$

Visa 1:

$$a_1 + a_2 = c \cdot k_1 + b_1 + c \cdot k_2 + b_2 = c \cdot (k_1 + k_2) + b_1 + b_2$$

$a_1 + a_2 - (b_1 + b_2) = c \cdot (k_1 + k_2)$ delbar med $c \Rightarrow$

$a_1 + a_2 \equiv b_1 + b_2 \pmod{c}$ #

Visa 2:

$$a_1 \cdot a_2 = (c \cdot k_1 + b_1)(c \cdot k_2 + b_2) = c \cdot (c k_1 k_2 + k_1 b_2 + k_2 b_1) + b_1 \cdot b_2$$

$a_1 \cdot a_2 - b_1 \cdot b_2 = c \cdot (c k_1 k_2 + k_1 b_2 + k_2 b_1)$ delbar med $c \Rightarrow$

$a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{c}$ #

Kongruens $a \equiv b \pmod{c}$ om differensen $a - b$ är delbar med c

Om $a_1 \equiv b_1 \pmod{c}$ och $a_2 \equiv b_2 \pmod{c}$ gäller att

1. $a_1 + a_2 \equiv b_1 + b_2 \pmod{c}$
2. $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{c}$

Om $a \equiv b \pmod{c}$ gäller att

3. $m \cdot a \equiv m \cdot b \pmod{c}$ för alla heltal m
4. $a^n \equiv b^n \pmod{c}$ för alla heltal $n \geq 0$

$a \equiv b \pmod{c} \Rightarrow a - b = c \cdot k \Rightarrow a = c \cdot k + b$

Visa 3:

$m \cdot a = m(c \cdot k + b) = mck + m \cdot b$

$m \cdot a - m \cdot b = c \cdot mk$ delbar med $c \Rightarrow$

$m \cdot a \equiv m \cdot b \pmod{c}$ #

Visa 4:

$$a^n = (c \cdot k + b)^n = \sum_{q=0}^{n} \binom{n}{q} (ck)^{n-q} \cdot b^q = c \cdot (\ldots) + b^n$$

$a^n - b^n = c \cdot (\ldots)$ delbar med $c \Rightarrow$

$a^n \equiv b^n \pmod{c}$ #
