# Kongruenz- (Modulo) Rechnung

## Definition

Zwei Zahlen $a, b \in \mathbb{Z}$ heißen kongruent, wenn gilt (modulo $m$)

$a = t_a \cdot m + r_a \quad 0 \leq r_a \leq m-1$

$b = t_b \, m + r_b \quad 0 \leq r_b \leq m-1$

und $r_a = r_b$

Schreibweise: $a \equiv b \bmod m$

Beispiel: $m = 7$

$a = 30 \quad b = 51$

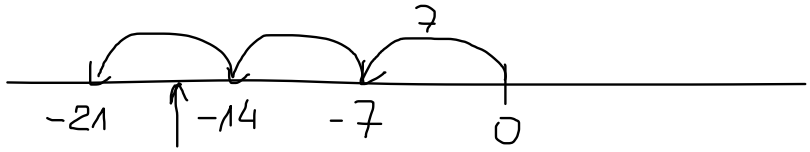
$30 = 4 \cdot 7 + 2$

$51 = 7 \cdot 7 + 2$

also $30 \equiv 51 \bmod 7$

$30 \not\equiv 51 \bmod 10$

$-3 = (-1) \cdot 7 + 4 \quad (m=7) \qquad -3 \equiv 4 \bmod 7$




$-16 = (-3)\,7 + 5 \quad (-16) \qquad -16 \equiv 5 \bmod 7$

$\equiv 12 \bmod 7$

$-12 = (-2)\,7 + 2 \qquad 5 = 0 \cdot 7 + 5$

## Satz 1

$a \equiv b \bmod m \iff a - b$ ist ohne Rest durch $m$ teilbar

Beispiel:

$m = 11 \quad a = 26 \quad b = 26 + 44 = 70$

$26 \equiv 70 \bmod 11$ (Rest 4)

Beweis „⇒"

Voraus. $a \equiv b \bmod m$

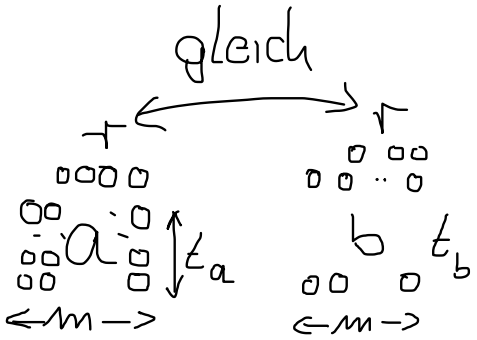
$a = t_a m + r$

$b = t_b m + r$

---

$a - b = t_a m - t_b m + r - r$

$= \underbrace{(t_a - t_b)}_{\in \mathbb{Z}} \cdot m$ also ist $a-b$ durch $m$ teilbar




$m = 4$

$\{ -8, -4, 0, 4, 8, 12, \ldots \}$ Rest 0 mod 4

$\{ -7, -3, 1, 5, 9, 13, \ldots \}$ Rest 1 mod 4

$\{ -6, -2, 2, 6, 10, 14, \ldots \}$ Rest 2 mod 4

$\{ -5, -1, 3, 7, 11, 15, \}$ Rest 3 mod 4

$m = 2$ $\{ -4, -2, 0, 2, 4, 6, \}$ gerade Zahl

$\{ -3, -1, 1, 3, 5, 7, \}$ ungerade Z

Satz 2

$a \equiv b \bmod m$ und $c \equiv d \bmod m$

$\Rightarrow a \left\{ \begin{matrix} + \\ \cdot \end{matrix} \right\} c \equiv b \left\{ \begin{matrix} + \\ \cdot \end{matrix} \right\} d \bmod m$

Anwendung

Welchen Rest lässt 1000 000 beim Teilen durch 19?

$10 \equiv 10 \equiv -9 \bmod 19$

$100 \equiv 5 \bmod 19$

$1000 \equiv 50 \equiv 12 \equiv -7 \bmod 19$

$1000000 \equiv 49 \equiv 11 \bmod 19$