Kongruenzen

Kongruenzen – Begriff

Wdh: Division mit Rest ($a \in \mathbb{Z}$ durch $b \in \mathbb{N}$): $a = qb + r$, $0 \leq r < b$

Es ist $\boxed{a \bmod b := r}$.

$27 \bmod 8 = 3$, da $27 = 3 \cdot 8 + 3$

$-29 \bmod 8 = 3$, da $-29 = -4 \cdot 8 + 3$

Def. Sei $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$.

a heißt **kongruent** zu b **modulo** m $:\Leftrightarrow$ $\boxed{a \bmod m = b \bmod m}$

Man schreibt $\mathbf{a \equiv b \bmod m}$.

Bsp. $27 \equiv -29 \bmod 8$

Kongruenzen – Kongruenz-Kriterium

Satz. $\boxed{a \equiv b \mod m \iff m \mid a-b}$

ü Zeigen oder widerlegen Sie:

✓ a) $128 \equiv 5 \mod 3$ $\quad 5 = 1 \cdot 3 + 2;\ 128 = 42 \cdot 3 + 2$

✓ b) $5 \equiv 2 \mod 3$ $\quad 5 = 1 \cdot 3 + 2;\ 2 = 0 \cdot 3 + 2$

✗ c) $134 \equiv 38 \mod 71$ $\quad 134 = 1 \cdot 71 + 63;\ 38 = 0 \cdot 71 + 38$

Kongruenzen – Rechenregeln

Wie rechnet man mit Kongruenzen?

Satz. Seien $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{N}$ mit

$$a \equiv b \bmod m \quad \wedge \quad c \equiv d \bmod m.$$

Dann gilt:

1) $a + c \equiv b + d \bmod m$

2) $a - c \equiv b - d \bmod m$

3) $a \cdot c \equiv b \cdot d \bmod m$

ü Berechnen Sie unter Verwendung von

$$115 \equiv 5 \bmod 5 \quad \wedge \quad 238 \equiv 3 \bmod 5$$

a) $115 + 238 \equiv 5 + 3 = 353 \equiv 8 \bmod 5$

b) $115 - 238 \equiv 5 - 3 = -123 \equiv 2 \bmod 5$

c) $115 \cdot 238 \equiv 5 \cdot 3 = 27.370 \equiv 15 \bmod 5$