Zahlenmengen

Modulares Rechnen

- Einleitendes Beispiel.
- Sei a eine ganze Zahl, $a \in \mathbb{Z}$, und m eine positive ganze Zahl, $m \in \mathbb{N}$; dann gibt es eindeutig bestimmte ganze Zahlen q und r mit $0 \leq r < m$, so daß

$$a = qm + r.$$

- Schreibweise für den Rest r: $\quad r = a \bmod m$.
- Beispiele
- Definition

  Wir schreiben

$$a \equiv b \mod m \qquad \text{(gelesen: „}a \text{ kongruent } b \text{ modulo } m\text{“)},$$

  wenn $a \bmod m = b \bmod m$, d.h. wenn a und b bei Division durch m den selben Rest lassen.
- Anmerkung: Die Schreibweise mit Klammern $a \equiv b \pmod{m}$ wird gleichwertig verwendet.
- Beispiele
- Satz

$$a \equiv b \mod m \qquad \Leftrightarrow \qquad m \mid (a - b)$$

- Beweis
- Satz

$$a \equiv b \mod m \qquad \Leftrightarrow \qquad a = b + qm \quad \text{mit } q \in \mathbb{Z}.$$

- Beweis und Beispiel.
- Satz

  Die Relation $\sim$ auf $\mathbb{Z}$ mit

$$a \sim b \qquad \Leftrightarrow \qquad a \equiv b \mod m$$

  ist eine Äquivalenzrelation.

- Beweis und Beispiel.
- Satz

  Wenn $a \equiv x \pmod{m}$ und $b \equiv y \pmod{m}$, dann ist $a + b \equiv x + y \pmod{m}$ und $ab \equiv xy \pmod{m}$.
- Beweis
- Anmerkung: Aufgrund dieser Eigenschaften kann ein Rechnen mit Äquivalenzklassen definiert werden, bei dem $[a] + [b] = [a + b]$ und $[a] \cdot [b] = [ab]$ gilt. Der Satz garantiert, daß diese Operationen wohldefiniert sind, d.h. nicht von den Repräsentanten der Äquivalenzklassen abhängen.
- Beispiel