

§ 3. Division mit Rest

(3.1) SATZ: Division mit Rest

Sei $n \in \mathbb{N}$ eine beliebige natürliche Zahl. Dann gibt es zu jeder ganzen Zahl a zwei Zahlen $q, r \in \mathbb{Z}$ mit folgenden Eigenschaften:

$$a = qn + r \quad \text{und} \quad 0 \leq r < n.$$

Die beiden Zahlen q und r sind eindeutig bestimmt.

q heißt der **Quotient** bei Division von a durch n

r heißt der **Rest** bei Division von a durch n

Bezeichnungen: $r = a \bmod n$.

Die Menge der möglichen Reste bei Division durch n wird mit $\mathcal{R}_n$ bezeichnet. Es ist $\mathcal{R}_n = \{0, 1, 2, 3, \dots, n-1\}$.

(3.2) SATZ: Rechenregeln für die Restbildung

Seien $n \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Dann gilt:

a) $a \bmod n = 0 \iff n \mid a$ (d.h. n ist ein Teiler von a)

b) $(a + kn) \bmod n = a \bmod n$ für alle $k \in \mathbb{Z}$

c) $(a \bmod n) \bmod n = a \bmod n$

d) $a \bmod n = b \bmod n \iff n \mid (a - b)$

e) $((a \bmod n) + (b \bmod n)) \bmod n = (a + b) \bmod n$

f) $((a \bmod n) \cdot (b \bmod n)) \bmod n = (a \cdot b) \bmod n$

g) $((a \bmod n)^m) \bmod n = a^m \bmod n$ für alle $m \in \mathbb{N}_0$.