

§ 7. Restklassen modulo n

(7.1) DEF: Sei $n \in \mathbb{N}$. Dann heißt für $a \in \mathbb{Z}$ die Menge

$$[a]_n := \{a + kn \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$$

die **Restklasse von a modulo n** .

Die Menge aller Restklassen modulo n wird mit \mathbb{Z}_n bezeichnet.

$$\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{Z}\}$$

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

- a) $a \in [a]_n$
- b) $b \in [a]_n \iff b \equiv a \pmod{n}$
- c) $[a]_n = [b]_n \iff a \equiv b \pmod{n}$
- d) $[a]_n \neq [b]_n \iff [a]_n \cap [b]_n = \emptyset$
- e) \mathbb{Z} ist die Vereinigung aller Restklassen modulo n .

(7.3) BEM: a) Es gilt $[4]_6 = [-2]_6 = [28]_6 = [-14]_6$. Jede der Zahlen $r \in \mathbb{Z}$ mit $[r]_6 = [4]_6$ heißt ein **Repräsentant** der Restklasse $[4]_6$.

b) Es gilt $[a]_n = \{b \mid b \in \mathbb{Z}, b \equiv a \pmod{n}\}$, d.h., $[a]_n$ ist nichts anderes als die Äquivalenzklasse von a bzgl. der Kongruenzrelation modulo n .

(7.4) SATZ: Für jedes $n \in \mathbb{N}$ gilt:

- a) $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}$
- b) $|\mathbb{Z}_n| = n$.

(7.5) DEF: Für $n \in \mathbb{N}$ bezeichne

$$\mathcal{R}_n = \{0, 1, 2, \dots, n-1\} \subseteq \mathbb{Z}$$

die Menge der Reste bei Division durch n .

(7.6) BEM: a) $\mathbb{Z}_n = \{[r]_n \mid r \in \mathcal{R}_n\}$

b) $\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\} = \{[-2]_4, [-1]_4, [0]_4, [1]_4\} = \{[-24]_4, [33]_4, [14]_4, [-49]_4\}$

(7.7) SATZ: Auf der Menge \mathbb{Z}_n lassen sich eine Addition und eine Multiplikation definieren, so dass die entsprechenden Rechenregeln wie in (1.1) gültig sind.

Addition:

$$[a]_n \oplus [b]_n := [a + b]_n \quad (a, b \in \mathbb{Z})$$

Multiplikation:

$$[a]_n \odot [b]_n := [a \cdot b]_n \quad (a, b \in \mathbb{Z})$$

Man sagt: Die Rechenoperationen auf \mathbb{Z}_n sind **repräsentantenweise** definiert.

Gezeigt werden muss, dass die Definition der Rechenoperationen unabhängig von der Auswahl der Repräsentanten der einzelnen Restklassen ist, d.h.

$$[a]_n = [a']_n \text{ und } [b]_n = [b']_n \implies [a + b]_n = [a' + b']_n$$

$$[a]_n = [a']_n \text{ und } [b]_n = [b']_n \implies [a \cdot b]_n = [a' \cdot b']_n$$

(7.8) FOLGERUNG: $(\mathbb{Z}_n, \oplus, \odot)$ ist ein kommutativer Ring.

(7.9) BEM: Ein wesentlicher Unterschied zwischen den Rechenregeln, die für \mathbb{Z} bzw. \mathbb{Z}_n gültig sind, besteht darin, dass in \mathbb{Z}_n ein Produkt zweier von Null verschiedener Restklassen Null sein kann, während in \mathbb{Z} das Produkt zweier von Null verschiedener Zahlen immer ungleich Null ist (s. (1.8b)). Beispiel:

$$[2]_6 \odot [3]_6 = [2 \cdot 3]_6 = [6]_6 = [0]_6$$

Beispiele: a) $[3]_{10} \odot [7]_{10} = [3 \cdot 7]_{10} = [21]_{10} = [1]_{10}$

b) $[4]_{10} \odot [x]_{10} = [4 \cdot x]_{10} \neq [1]_{10}$ für alle $[x]_{10} \in \mathbb{Z}_{10}$.

(7.10) DEF: Eine Restklasse $[a]_n \in \mathbb{Z}_n$ heißt **invertierbar**, wenn es eine Restklasse $[b]_n \in \mathbb{Z}_n$ gibt mit

$$[a]_n \odot [b]_n = [1]_n.$$

$[b]_n$ heißt dann die zu $[a]_n$ **inverse Restklasse modulo n** .

(7.11) SATZ: Eine Restklasse $[a]_n$ ist genau dann invertierbar, wenn a und n teilerfremd sind.

(7.12) BEM: a) Die Restklasse $[1]_n$ ist für alle $n \in \mathbb{N}$ invertierbar.

b) Die Restklasse $[0]_n$ ist nur für $n = 1$ invertierbar.

c) Ist die Restklasse $[a]_n$ invertierbar, so läßt sich ein Repräsentant der inversen Restklasse mit Hilfe des EEA berechnen.

(7.13) SATZ: Für $n \in \mathbb{N}$, $n \geq 2$ sind folgende Aussagen äquivalent:

a) Jede Restklasse $\neq [0]_n$ ist invertierbar b) n ist eine Primzahl.