Vorlesung LinADi
Wintersemester 2022/23
Prof. Dr. Bastian von Harrach
M. Sc. Andrej Brojatsch
M. Sc. Stephan Gardoll

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

---

4. Übungsblatt (Ausgabe am 10.11.2022, Abgabe am 16.11.2022 bis 12:00 Uhr)

Aufgabe 4.1 (Modulare Arithmetik I)[4 Punkte]

(a) Zeigen Sie, dass zu $a, c \in \mathbb{N}$ und $1 \leq a \leq c-1$ ein $b \in \mathbb{N}$ mit $1 \leq b \leq c-1$ und $a+b \mod c = 0$ existiert.

(b) Bestimmen Sie für alle $a \in \{1, ...6\}$ ein $b \in \{1, ..., 6\}$, sodass $a \cdot b \mod 7 = 1$ gilt.

(c) Zeigen oder widerlegen Sie, dass es für alle $a, c \in \mathbb{N}$ mit $1 \leq a \leq c-1$ ein $b \in \mathbb{N}$ mit $a \cdot b \mod c = 1$ gibt.

Aufgabe 4.2 (Modulare Arithmetik II)[4 Punkte]
Bestimmen Sie die Reste der nachstehenden Ausdrücke. Bitte geben Sie nur die Ergebnisse an.

(a) $8729 + 4596 + 4860 + 2947 \mod 100$, (b) $11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \mod 10$.

Aufgabe 4.3 (Multiple Choice - Teilbarkeit ganzer Zahlen)[4 Punkte]
Kreuzen Sie unter den folgenden Aussagen diejenigen an, die korrekt sind. Korrekte Kreuze bringen 1 Punkt. Falsche Kreuze bringen -1 Punkt. Sie bekommen auf diese Aufgabe mindestens 0 Punkte.

◯ Es gilt $x - \lfloor x \rfloor < 0$ für alle $x \in \mathbb{R}$.
◯ Es gilt $\lceil x \rceil - \lfloor x \rfloor = 1$ für alle $x \in \mathbb{R}$.
◯ Es gilt $\lceil x \rceil - \lfloor x \rfloor = 1$ für alle $x \in \mathbb{R} \setminus \mathbb{Z}$.
◯ Für alle $a \in \mathbb{N},\ a > 1$ gilt $17 \mod a = 17$.
◯ Für alle $a \in \mathbb{N}$ gilt $a \mod 18 < 18$.
◯ Es gilt $(20 \mod 3) \mod 3 = (5 \mod 3) \cdot (4 \mod 3)$.
◯ Für alle $a, b, c \in \mathbb{N}$ gilt $a \cdot b \mod c = (a \mod c) \cdot (b \mod c)$.
◯ Für alle $a, b, c \in \mathbb{N}$ gilt $a + b \mod c = (a \mod c) + (b \mod c)$.
◯ Es seien $a \in \mathbb{Z}$ und $b \in \mathbb{N}$. Existieren nun $(q_1, r_1), (q_2, r_2) \in \mathbb{Z}^2$ mit $a = bq_1 + r_1,\ a = bq_2 + r_2$ sowie $0 \leq r_1, r_2 \leq b - 1$, dann folgt $(q_1, r_1) = (q_2, r_2)$.

Aufgabe 4.4 (Beweise zur modularen Arithmetik)[4 Punkte]
Es seien $a, b, c, d \in \mathbb{Z}$ sowie $k, m \in \mathbb{N}$. Zeigen Sie die folgenden Aussagen.

(a) $a^k \mod m = (a \mod m)^k \mod m$.
(b) $a \mod m = b \mod m \Rightarrow c \cdot a \mod m = c \cdot b \mod m$.
(c) $a \mod m = b \mod m,\ c \mod m = d \mod m \Rightarrow a + c \mod m = b + d \mod m$.