TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Prof. Dr. Ulrich Thiel
Laura Voggesberger, M. Sc.

Mathematik für Informatik: Algebraische Strukturen

Sommersemester 2022 - Übungsblatt 3

Abgabetermin: 20.05.2022, 10:00 Uhr, Briefkästen Gebäude 48 Erdgeschoss oder als eine PDF mit dem Button in OLAT hochladen

Aufgabe 1 (4 Punkte)**.** Bestimmen Sie die Menge $L \subset \mathbb{Z}$ aller Lösungen x der simultanen Kongruenzen

$$\begin{aligned} x &\equiv 2 \bmod 3 \\ x &\equiv 2 \bmod 7 \\ x &\equiv 3 \bmod 10. \end{aligned}$$

Aufgabe 2 (4 Punkte)**.** Suchen Sie eine Lösung von $11x \equiv 109 \bmod 210$. Wieviele Lösungen gibt es, wenn man $0 \leq x < 210$ fordert?
Hinweis: Verwenden Sie den Chinesischen Restsatz und nutzen Sie aus, dass $210 = 2 \cdot 3 \cdot 5 \cdot 7$. *Damit können Sie* $11x \equiv 109 \bmod 210$ *in ein System von Gleichungen*

$$\begin{aligned} 11x &\equiv 109 \bmod 2 \\ 11x &\equiv 109 \bmod 3 \\ 11x &\equiv 109 \bmod 5 \\ 11x &\equiv 109 \bmod 7 \end{aligned}$$

umformen, dass Sie dann vereinfachen können.

Aufgabe 3 (4 Punkte)**.** Beweisen oder widerlegen Sie:

1. $(\mathbb{N}_0, +)$ ist eine Gruppe, wobei $N_0 := \{0, 1, 2, \ldots\}$ die natürlichen Zahlen mit 0 bezeichne.
2. Die Menge $S(X) := \{f : X \to X \mid f \text{ bijektiv}\}$ zusammen mit der Verknüpfung $\circ$ von Abbildungen ist eine Gruppe.
3. $(\mathbb{Q}, \cdot)$ ist eine Gruppe.
4. $(2\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Z}, +)$, wobei $2\mathbb{Z} = \{2x \mid x \in \mathbb{Z}\}$ die Menge der geraden Zahlen ist.

Aufgabe 4 (4 Punkte)**.** Sei G eine Menge zusammen mit einer Verknüpfung $\circ$, die folgende Axiome erfüllt:

(G1) Assoziativität: $a \circ (b \circ c) = (a \circ b) \circ c \ \forall a, b, c \in G$.

(G2') Es existiert ein linksneutrales Element, d.h. $\exists e \in G$ mit $e \circ a = a \ \forall a \in G$.

(G3') Existenz des Linksinversen, d.h. $\forall a \in G \ \exists a^{-1} \in G$ mit $a^{-1} \circ a = e$.

Zeigen Sie, dass gilt:

(a) Für a, $b \in G$ gilt: Ist $a \circ b = e$, dann auch $b \circ a = e$. (links- gleich rechtsinvers)

(b) Es ist $a \circ e = a \ \forall a \in G$.

(c) Das neutrale Element ist eindeutig.

(d) Das Inverse für ein festes $a \in G$ ist eindeutig.

(e) Für $a, b \in G$ ist $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

(f) Für $a \in G$ ist $(a^{-1})^{-1} = a$.

Zusatzaufgabe 5 (4 Punkte)**.** Schreiben Sie mit Hilfe Ihrer Implementierung von der Zusatzaufgabe auf Aufgabenblatt 2 (oder der Maple-Funktion igcdex) eine Prozedur, die die Lösungsmenge der simultanen Kongruenzen

$$x \equiv a_1 \bmod n_1$$
$$x \equiv a_2 \bmod n_2$$

für $a_1, a_2 \in \mathbb{Z}$ und $n_1, n_2 \in \mathbb{Z}_{>0}$ mit $\mathrm{ggT}(n_1, n_2) = 1$ bestimmt. Testen Sie Beispiele und drucken Sie diese mit aus.