TECHNISCHE UNIVERSITÄT DRESDEN

Fachrichtung Mathematik • Institut für Algebra • Prof. Bodirsky, Dr. Noack

Einführung in die Mathematik für Informatiker: Diskrete Strukturen INF 110
Wintersemester 2019/20

6. Übungsblatt

für die Woche 25.11. - 01.12.2019

Rechnen mod n, Gruppen

Ü31 Ein Fahrzeug kann durch zwei Befehle gesteuert werden: Auf den Befehl **V** hin fährt es genau 143 cm vorwärts, auf den Befehl **R** hin fährt es genau 210 cm rückwärts. Das Fahrzeug soll durch eine Kombination dieser Befehle um genau 1 cm vorwärts bewegt werden. Wie viele der Befehle **V** bzw. **R** könnten kombiniert werden, um dies zu erreichen?
Ist es auch möglich, wenn das Fahrzeug beim Befehl **R** genau 231 cm rückwärts fährt?

Ü32 (a) Welche der Elemente $z_1 = 7,\ z_2 = 8,\ z_3 = 13$ und $z_4 = 15$ aus $\mathbb{Z}_{24}$ sind Nullteiler, welche sind Einheiten? Bestimmen Sie für diese Elemente, wenn möglich, das multiplikative Inverse in $\mathbb{Z}_{24}$. Verwenden Sie dazu den erweiterten euklidischen Algorithmus.

(b) Bestimmen Sie alle $x \in \mathbb{Z}_{24}$, die die Gleichung $253 \cdot x + 21 \equiv 3 \pmod{24}$ erfüllen.

Ü33 (a) Es sei R die Menge aller Symmetrieabbildungen eines Rechtecks, das kein Quadrat ist.

(1) Geben Sie alle diese Symmetrieabbildungen als Permutationen der Eckpunkte des Rechtecks an (die Eckpunkte seien gegen den Uhrzeigersinn mit $1, 2, 3, 4$ bezeichnet).

(2) Zeigen Sie, dass $(R, \circ)$ mit der Hintereinanderausführung $\circ$ von Abbildungen eine Gruppe bildet. Stellen Sie dazu die Verknüpfungstafel auf und verwenden Sie diese für Ihre Argumentation.

(3) Ist $(R, \circ)$ abelsch?

(b) Zeigen Sie, dass $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ mit der komponentenweisen Addition mod 2 eine Gruppe bildet. Stellen Sie die Verknüpfungstafel auf.

H34 $\boxed{\textbf{A}}$

(a) Ermitteln Sie das multiplikativ Inverse von m in $\mathbb{Z}_n$ für

(i) $m = 21, n = 101$ (ii) $m = 3, n = 13$ (iii) $m = 144, n = 3003$,

mit dem erweiterten euklidischen Algorithmus, wenn es existiert. Begründen Sie, wenn das multiplikative Inverse nicht existiert, warum das der Fall ist.

(b) Bestimmen Sie alle $x \in \mathbb{Z}_{42}$, die die Gleichung $13 \cdot x \equiv 40^8 \pmod{42}$ erfüllen.

(c) $\boxed{\text{Zusatz}}$ Bestimmen Sie alle $x \in \mathbb{Z}_{42}$, die die Gleichung $15 \cdot x \equiv 24 \pmod{42}$ erfüllen.

H35 (a) Es sei $(G;\circ)$ eine Gruppe mit neutralem Element e. Beweisen Sie die Kürzungsregeln:

$$\forall\ a,b,c \in G:\ a \circ b = a \circ c\ \Rightarrow\ b = c \quad \text{und} \quad b \circ a = c \circ a\ \Rightarrow\ b = c.$$

(b) Zeigen Sie, dass für jede endliche Gruppe $(G;\circ)$ gilt: In der Verknüpfungstafel tritt in jeder Zeile und in jeder Spalte jedes Element der Gruppe genau einmal auf.

H36 Zeigen Sie, dass die Menge $G = \{x \in \mathbb{R} \mid x > 1\}$ mit der Operation

$$a \circ b := a^{\ln b}$$

eine abelsche Gruppe bildet.