Übungsblatt 6

Technische Hochschule Mittelhessen, Fachbereich MNI, Diskrete Mathematik, Prof. Dr. B. Just

Aufgabe 1

a.) Bitte wenden Sie den Euklidischen Algorithmus an auf die Zahlen 20 und 12.

b.) Bitte bestimmen Sie $x, y \in \mathbb{Z}$ mit $20x + 12y = \text{ggT}(20, 12)$.

c.) Bitte wenden Sie den Euklidischen Algorithmus an auf die Zahlen 53 und 41.

d.) Bitte bestimmen Sie $x, y \in \mathbb{Z}$ mit $53x + 41y = \text{ggT}(53, 41)$.

e.) Bitte beweisen Sie: Für $a, m \in \mathbb{N}$ ist $a \cdot a^{-1} + q \cdot m = 1$ lösbar mit $a^{-1}, q \in \mathbb{Z} \Longleftrightarrow \text{ggT}(a, m) = 1$.

Aufgabe 2

Bitte bestimmen Sie die multiplikativen Inversen zu den folgenden Zahlen und Modulen. Z.B. ist $5^{-1} \equiv 2 \mod 9$, denn es ist $5 \cdot 2 \equiv 1 \mod 9$.

a.) $2^{-1} \mod 11$ b.) $7^{-1} \mod 15$ c.) $101^{-1} \mod 111$

Bitte entscheiden Sie (mit Begründung), ob es multiplikative Inverse für die folgenden Reste gibt:

d.) $3 \mod 11$ e.) $14 \mod 21$ f.) $100 \mod 200$

Aufgabe 3

Bitte entscheiden Sie, wer Gruppe oder Körper oder keines von beiden ist (jeweils mit Begründung):

a.) $(\mathbb{Z}/m\mathbb{Z}, +)$ mit der Addition mod m

b.) (gerade Zahlen in $\mathbb{Z}, +$) mit der Addidion in $\mathbb{Z}$

c.) $(G, \circ)$, wobei G die Menge aller (sinnvollen oder sinnlosen) Wörter ist, die aus den Buchstaben a, b und c bestehen, inclusive dem leeren Wort, und $\circ$ das Hintereinanderhängen bedeutet. So ist z.B. aabac $\circ$ bac = aabacbac.

d.) $(G, \circ)$ wie in c., jedoch zusätzlich mit der Berechnungsvorschrift aa=bb=cc=leeres Wort.

e.) $(\mathbb{C}, +, \cdot)$ mit der komplexen Addition und Multiplikation.

f.) $(\{0, 1, 2\}, +, \cdot)$ mit der Addition und Multiplikation mod 3.

Aufgabe 4

Ein Satz aus der Gruppentheorie besagt: Für jede endliche Gruppe $(G, \circ)$ und jedes $x \in G$ ist

$$\underbrace{x \circ x \circ .... \circ x \circ x}_{\text{Anzahl Gruppenelemente mal}} = \text{neutrales Element}.$$

Dieser Satz ist die mathematische Basis für viele Verschlüsselungsalgorithmen, z.B. das RSA-System.

Bitte prüfen Sie diese Aussage anhand der folgenden Gruppen und Elemente x nach:

a.) $(\mathbb{Z}/12\mathbb{Z}, +)$ mit der Addition mod 12 und $x = 3$.

b.) $(\mathbb{Z}/5\mathbb{Z}^*, \cdot)$ mit der Multiplikation mod 5 und $x = 4$.

c.) $(\mathbb{Z}/17\mathbb{Z}^*, \cdot)$ mit der Multiplikation mod 17 und $x = 13$

d.) $(\mathbb{Z}/21\mathbb{Z}^*, \cdot)$ mit der Multiplikation mod 21 und $x = 5$

e.) $(G, \circ)$, wobei ein Quadrat mit Mittelpunkt M gegeben sei, und G aus den Drehungen gegen den Uhrzeigersinn um M um $0°, 90°, 180°, 270°$ besteht, die das Quadrat in sich selbst überführen. $\circ$ bezeichne die Hintereinanderausführung von Drehungen. x sei die Drehung um 270°.

Viel Spass und Erfolg!