Hochschule RheinMain
Fachbereich Design Informatik Medien
Studiengang Angewandte Informatik / Informatik Technische Systeme
Prof. Dr. Bernhard Geib

Security

Sommersemester 2022
(LV 4120 und 7240)

4. Aufgabenblatt

Ziel dieser Übung ist es, den Umgang mit algebraischen Strukturen wie Gruppen, Ringe oder Körper und hierbei insbesondere die Anwendung von mathematischen Operationen als Teil eines Kryptosystems kennen zu lernen. Bereits bei der mathematischen Formulierung einer einfachen Vigenère-Chiffre haben wir Modulo-Operationen (mod m) als Wertzuweisung benutzt und uns dabei auf den Restklassenring $\mathbf{Z}_m = \{0, 1, ..., m - 1\}$ bezogen. Von nun an werden wir dieses Konzept auch auf den Bereich von Kongruenzen anwenden. Die Berechnung und Lösung entsprechender Ausdrücke bzw. Gleichungen ist dann immer so zu verstehen, dass der zugewiesene Wert der kleinste nichtnegative Repräsentant der Restklasse ist.

Aufgabe 4.1

Lösen Sie die modulare Exponentialgleichung $x^5 \bmod 7 = 2$ auf analytischem Wege. Welchen Wert erhält man für die Unbekannte $x \in \mathbf{Z}_7$? Geben Sie den vollständigen Rechenweg an!

Aufgabe 4.2

Angenommen, Sie wissen:

i) $7^a \bmod 31 = 10$ mit $a \in \mathbf{Z}_{31}$

ii) $6^x \equiv 1 \pmod{11}$ mit $x \in \mathbf{Z}_{11}$

wobei $\mathbf{Z}_m$:= Ring mod m = $\{0, 1, 2, ..., m - 1\}$ ist. Ermitteln Sie die ganzen positiven Zahlen a und x.

Aufgabe 4.3

Wir betrachten die algebraische Struktur $<\mathbf{Z}_n, +, \cdot >$, bei der die Addition und die Multiplikation von a und b definiert sind als:

$$(a + b) \bmod n \quad \text{bzw.} \quad (a \cdot b) \bmod n$$

a) Um welche Struktur handelt es sich bei $<\mathbf{Z}_n, +, \cdot>$?

b) Ermitteln Sie für die beiden Elemente a = 1 und b = 2 in $<\mathbf{Z}_4, +, \cdot>$ die inversen Elemente

$$-a \text{ und } -b, \text{ sofern sie existieren.}$$

c) Ermitteln Sie für die beiden Elemente a = 1 und b = 2 in $<\mathbf{Z}_4, +, \cdot>$ die inversen Elemente

$$a^{-1} \text{ und } b^{-1} - \text{ sofern sie existieren.}$$

Aufgabe 4.4

Zeigen Sie, dass für a, b, c $\in$ **Z** (Menge der ganzen Zahlen) gelten:

a) Aus $b \mid a$ und $c \mid b \Rightarrow c \mid a$.

b) Aus $c \mid a$ und $c \mid b \Rightarrow c \mid (a \pm b)$.

c) Zeigen Sie ferner, dass zwei ganze Zahlen a und b bei der Division durch n genau dann restgleich sind, wenn ihre Differenz ein Vielfaches des Moduls n ist. Für a, b $\in$ **Z** also gilt:

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \mid (a - b)$$

Aufgabe 4.5

a) Bestimmen Sie alle natürlichen Zahlen n, für die $n^3 - 1$ eine Primzahl ist.

b) Bestimmen Sie alle Primzahlen p, für die $11 \cdot p + 1$ eine Quadratzahl ist (d. h., dass $11 \cdot p + 1 = n^2$ für ein n $\in$ **N** ist).