Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2023
10.06.2023

Datensicherheit und Kryptografie

10. Übung

Abgabe: Lösen Sie die Aufgabe **1**. Ihre Lösungen geben Sie bitte

- bis zum 16.06.2023 um 13:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`

ab.

1. Aufgabe: (7+3)P
Schreiben Sie in einer Programmiersprache Ihrer Wahl ein möglichst effizientes Programm, das (echte) Potenzen erkennt. Wenn eine natürliche Zahl m eingegeben wird, soll also genau dann True ausgegeben werden, wenn es natürliche Zahlen b, e mit $e \geq 2$ gibt, sodass $m = b^e$ gilt.
Geben Sie auch die Laufzeit des Programms an.

2. Aufgabe:
Sei a eine Einheitswurzel modulo m und e eine ungerade Zahl. Zeigen Sie die Gleichung $a^e \equiv a \pmod{m}$.

3. Aufgabe:
In der Vorlesung haben wir die Untergruppen

$$U_m = \{a | a \in \mathbb{Z}_m^*, \quad a^{m-1} \equiv 1 \pmod{m}\}$$

von $\mathbb{Z}_m^*$ eingeführt.

(a) Berechnen Sie U_m für $m = 8$ und $m = 15$.

(b) Zeigen Sie, dass eine multiplikativ abgeschlossene Teilmenge einer endlichen Gruppe auch unter Inversen abgeschlossen ist.

(c) Zeigen Sie, dass U_m wirklich eine Untergruppe von $\mathbb{Z}_m^*$ ist.

(d) Sei G eine Gruppe mit Untergruppe U. Zeigen Sie, dass für $b, b' \in G$ die beiden Mengen

$$bU = \{bu | u \in U\}$$

und

$$b'U = \{b'u | u \in U\}$$

entweder disjunkt oder gleich sind.

(e) Zeigen Sie, dass für jede Gruppe G mit Untergruppe U, die Zahl $\frac{|G|}{|U|}$ in $\mathcal{N}_{\geq 1}$ liegt.

(f) Welche Folgerung ergibt sich dadurch für die Anzahl der Fermat-Zeugen a, die durch

$$a^{m-1} \not\equiv 1 \pmod{m}$$

zeigen, dass m nicht prim ist?