Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2023
03.07.2022

Datensicherheit und Kryptografie

13. Übung

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

- bis zum 07.07.2023 um 13:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`

ab.

1. Aufgabe:
Für eine gegebene Zahl m mit der Zerlegung $m-1 = 2^t l$ mit $l \equiv 1 \pmod 2$ haben wir für den Miller-Rabin-Primzahltest die Zahl s durch

$$\exists a : a^{2^s l} \equiv -1 \pmod m \text{ und}$$

$$\forall a : a^{2^{s+1} l} \not\equiv -1 \pmod m$$

definiert.
Wir definieren außerdem s durch

$$\exists a : a^{2^{s'} l} \not\equiv 1 \pmod m \text{ und}$$

$$\forall a : a^{2^{s'+1} l} \equiv 1 \pmod m.$$

Bestimmen Sie die Zahlen s und s' für die folgenden Carmichael-Zahlen aus den vorherigen Übungszetteln:

- $m = 561 = 3 \cdot 11 \cdot 17$,
- $m = 1729 = 7 \cdot 13 \cdot 19$,
- $m = 2465 = 5 \cdot 17 \cdot 29$,
- $m = 8911 = 7 \cdot 19 \cdot 67$,

Bestimmen Sie außerdem, wie s und s' für Primzahlen aussehen.

2. Aufgabe:
Zeigen Sie, dass die Menge

$$E_{k,m} = \{a \in 0, 1, 2, \ldots, m-1 | a^k \equiv 1 \pmod m\}$$

der k-ten Einheitswurzeln modulo m und die Menge

$$P_{k,m} = \{a^k \bmod m | a \in 0, 1, 2, \ldots, m-1\}$$

der k-ten Potenzen modulo m Untergruppen von $\mathbb{Z}_m^*$ sind.
Zeigen Sie außerdem, dass $|E_{k,m}| \cdot |P_{k,m}| = |\mathbb{Z}_m^*|$ gilt.

3. Aufgabe:
Sei G eine endliche kommutative Gruppe mit Untergruppe U.

(a) Zeigen Sie, dass $|G|$ ein Vielfaches von $|U|$ ist.

(b) Sei G' eine weitere endliche kommutative Gruppe mit Homomorphismen $f : G \to G'$ und $g : G' \to G$. Zeigen Sie, dass das Bild von U bezüglich f und das Urbild von U bezüglich g Untergruppen von G' sind.