Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2023
26.06.2023

# Datensicherheit und Kryptografie

## 12. Übung

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

- bis zum 30.06.2023 um 13:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`

ab.

**1. Aufgabe:** (1+1+2+2+2+2)P
Wir betrachten Carmichael-Zahlen. Das sind Zahlen $m$ für die gilt:

$$\text{ggT}(a, m) = 1 \Rightarrow a^{m-1} \equiv 1 \pmod{m}$$

(a) Zeigen Sie, dass $1729 = 7 \cdot 13 \cdot 19$ eine Carmichael-Zahl ist.

(b) Zeigen Sie, dass $1547 = 7 \cdot 13 \cdot 17$ keine Carmichael-Zahl ist.

(c) Zeigen Sie, dass echte Potenzen von Primzahlen keine Carmichael-Zahlen sind.

(d) Zeigen Sie, dass Zahlen der Form $p^2k$ mit $p \geq 2$ keine Carmichael-Zahlen sind.

(e) Zeigen Sie, dass eine Zahl $m$ genau dann Carmichael-Zahl ist, wenn für alle Primteiler $p$ von $m$ auch $p - 1$ ein Teiler von $m - 1$ ist.

(f) Zeigen Sie, dass Carmichael-Zahlen mindestens drei Primfaktoren haben.

**2. Aufgabe:**
Sei $m = 2465 = 5 \cdot 17 \cdot 29$.

(a) Zeigen Sie, dass $\text{ggT}(a, m) = 1 \Rightarrow a^{m-1} \equiv 1 \pmod{m}$ gilt.

(b) Zeigen Sie, dass sogar $\text{ggT}(a, m) = 1 \Rightarrow a^{\frac{m-1}{2}} \equiv 1 \pmod{m}$ gilt.

(c) Zeigen Sie, dass $3^{\frac{m-1}{4}} \not\equiv 1 \pmod{m}$ gilt.

(d) Folgern Sie, dass $m$ nicht prim ist.

**3. Aufgabe:**
Eine Einheitswurzel modulo $m$ ist eine Zahl $a$, die die Gleichung

$$a^2 \equiv 1 \qquad (\text{mod } m)$$

erfüllt.

(a) Bestimmen Sie alle Einheitswurzeln modulo $m = 2$, $m = 4$, und $m = 8$.

(b) Bestimmen Sie alle Einheitswurzeln modulo $m = 2^i$ mit $i > 3$.

(c) Bestimmen Sie alle Einheitswurzeln modulo $m = p$ für ungerade Primzahlen $p$.

(d) Bestimmen Sie alle Einheitswurzeln modulo $m = p^i$ für ungerade Primzahlen $p$ und einen Exponenten $i \geq 2$.

(e) Bestimmen Sie die Anzahl der Einheitswurzeln modulo $m = 2^{i_0} \cdot p_1^{i_1} \cdot \cdots \cdot p_j^{i_j}$ wobei $i_k \geq 0$ natürliche Zahlen sind und die $p_k$ unterschiedliche Primzahlen sind.

**4. 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.