Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2022
24.06.2022

Datensicherheit und Kryptografie

10. Übung

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

- bis zum 29.06.2022 um 20:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`
  mit *Betreff:* `DuK Hausaufgaben` oder
- nach der Vorlesung am 28.06.2022

ab.

1. Aufgabe: (2+3+2+3)P
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.

2. Aufgabe:
Eine Einheitswurzel modulo m ist eine Zahl a, die die Gleichung

$$a^2 \equiv 1 \pmod{m}$$

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.

3. 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

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

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.