Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2022
17.06.2022

Datensicherheit und Kryptografie

9. Übung

Abgabe: Lösen Sie die Aufgabe **4**. Ihre Lösungen geben Sie bitte entweder

- bis zum 22.06.2022 um 20:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`
  mit *Betreff:* `DuK Hausaufgaben` oder
- nach der Vorlesung am 21.06.2022

ab.

1. Aufgabe:
Vergleichen Sie die Funktionswerte der Funktionen
$\log_2(\log_2(x))$, $\log_2(x)$, $log_2(x)^2$, $log_2(x)^3$, $log_2(x)^4$, $log_2(x)^5$, $log_2(x)^6$, x und $x\log(x)$
für die Funktionswerte
$x = 10$, $x = 10^3$, $x = 10^6$, $x = 10^9$ und $x = 10^{12}$.

2. Aufgabe:

(a) Zeigen Sie, dass aus $\text{ggT}(a, m) > 1$ folgt, dass $a^{m-1} \not\equiv 1 \pmod{m}$ gilt.

(b) Zeigen Sie, dass für gerade m die Ungleichung $(m-1)^{m-1} \not\equiv 1 \pmod{m}$ gilt.

(c) Zeigen Sie, dass für ungerade a die Äquivalenz $a^2 \equiv 1 \pmod{8}$ gilt.

3. Aufgabe:
Wir betrachten Untergruppen.

(a) 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. Berechnen Sie U_m für $m = 8$, $m = 15$ und $m = 561$ und zeigen Sie, dass U_m wirklich eine Untergruppe von $\mathbb{Z}_m^*$ ist.

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

(c) Sei G eine Gruppe mit Untergruppe U. Zeigen Sie, dass für $b \in G \setminus U$ und $u, u' \in U$ mit $u \neq u'$ gilt, dass bu und bu' auch verschieden sind.

4. 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) $1729 = 7 \cdot 13 \cdot 19$ ist eine Carmichael-Zahl.

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

(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.