Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2023
19.06.2023

Datensicherheit und Kryptografie

11. Übung

Abgabe: Lösen Sie die Aufgabe **3**. Ihre Lösungen geben Sie bitte

- bis zum 23.06.2023 um 13:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`

ab.

1. Aufgabe:
Für teilerfremde Zahlen m, n können wir mit dem erweiterten Euklidischen Algorithmus Zahlen a, b bestimmen, sodass $1 = am + bn$ gilt.
Zeigen Sie, dass das Gleichungssystem aus

$$x \equiv k \pmod{m}$$

und

$$x \equiv l \pmod{n}$$

durch

$$x \equiv lam + kbn \pmod{mn}$$

gelöst wird.

2. Aufgabe: (5+5)P
Nutzen Sie den Chinesischen Restsatz (bzw. die Formeln aus Aufgabe 1), um alle Zahlen x zu finden, $0 \leq x < 15$ und $x^2 \equiv 1 \pmod{15}$ erfüllen.
Finden Sie außerdem alle Zahlen x, die $0 \leq x < 187 = 11 \cdot 17$ und $x^2 \equiv 1 \pmod{187}$ erfüllen.

3. Aufgabe:
Geben Sie für die Funktion

$$\begin{aligned} \mathbb{Z}/15\mathbb{Z} &\to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ x &\mapsto (x \mod 3, x \mod 5) \end{aligned}$$

für $0 \leq x < 15$ alle Funktionswerte an.

4. Aufgabe:
Zeigen Sie, dass für alle $0 \leq a < 561 = 3 \cdot 11 \cdot 17$ die Äquivalenz $a^{561} \equiv a \pmod{561}$ gilt.
Hinweis: Benutzen Sie zwei mal den Chinesischen Restsatz und verwenden Sie, dass die Abbildung aus dem Chinesischen Restsatz die Gleichung $f(h \cdot jh') = f(h) \cdot f(h')$ erfüllt.

5. Aufgabe:
Seien p, q und q' Primzahlen. Geben Sie an, wann die simultane Kongruenz

$$\begin{aligned} x &\equiv a \pmod{pq} \\ x &\equiv b \pmod{pq'} \end{aligned}$$

eine Lösung hat und beschreiben Sie, wie Sie die Lösung algorithmisch ermitteln können.