Dr. Dirk Frettlöh 23.4.2025

Übungen zur Vorlesung Kryptographie

Blatt 3

Aufgabe 9: (Quadratwurzeln mod N)
Finden Sie alle quadratischen Reste in Z_{17}, Z_{19} und Z_{21}. Visualisieren Sie die Quadrat-Wurzel-Beziehung jeweils in einem Graphen wie in Beispiel 2.4 der Vorlesung. (Überprüfen Sie für sich Ihr Ergebnis, ob es zu Satz 2.6. passt.)
Für die Abgabe reicht der korrekte Graph. Die quadratischen Reste sind ja genau die, auf die ein Pfeil zeigt.

Aufgabe 10: (Quadratwurzeln und Primitivwurzeln)
(a) Finden Sie die kleinste Primitivwurzel in Z_{23}^*. Zeigen Sie, dass das wirklich eine Primitivwurzel ist.

(b) Bestimmen Sie alle quadratischen Reste in Z_{23}^*, einmal mittels des Eulerkriteriums im Skript; einmal mit Bemerkung 2.5 im Skript.

(c) Bestimmen Sie beide Quadratwurzeln von 18 in Z_{23}^* mittels Satz 2.8. Können Sie so auch die Quadratwurzel von 17 bestimmen?

Aufgabe 11: (Wieviele Quadratwurzeln?)
(a) Finden Sie alle Quadratwurzeln von 4 in Z_{11}, Z_{55}, Z_{385} und Z_{1155}. Wie passt das zu Satz 2.6 im Skript?

(b) Zeigen Sie: Ist p eine ungerade Primzahl, so hat ein quadratischer Rest $a \in Z_p^*$ genau zwei Quadratwurzeln.

Aufgabe 12: (Primitivwurzelmagie)
(a) Sei a eine Primitivwurzel in Z_N^*. Zeigen Sie, dass $a^{-1} \neq a$ für $N \notin \{2, 3, 4, 6\}$.

(b) Seien $a_1, a_2, \ldots, a_k$ alle Primitivwurzeln in Z_N^*, wobei $N \notin \{2, 3, 4, 6\}$. Zeigen Sie, dass $a_1 \cdot a_2 \cdots a_k \equiv 1 \bmod N$.

Abgabe bis Mittwoch 30.4.2025 bis 14 Uhr per Email an die Tutorin.
Bitte auf jeder Abgabe das Tutorium angeben!

Lisa Harms lharms+krypto@techfak.de
Lisa Henetmayr lhenetmayr+krypto@techfak.de