

Übungen zur Vorlesung Kryptographie

Blatt 3

Aufgabe 9: (Quadratische Reste malen)

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 Aufgabe 11(b) bzw 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: (Primitivwurzeln finden)

(a) Finden Sie eine Primitivwurzel in Z_{17}^* . Zeigen Sie, dass das wirklich eine Primitivwurzel ist.

(b) Finden Sie die kleinste Primitivwurzel in Z_{26}^* . Zeigen Sie, dass das wirklich eine Primitivwurzel ist.

(c) Finden Sie das kleinste $N \in \mathbb{N}$ ($N > 1$), so dass es keine Primitivwurzel in Z_N^* gibt. Begründen Sie, warum dies wirklich das kleinste solche N ist.

Aufgabe 11: (Wieviele Quadratwurzeln?)

(a) Finden Sie alle Quadratwurzeln von 1 in Z_5 , Z_{15} , Z_{105} und Z_{1155} . Was fällt auf?

(b) Zeigen Sie: Ist p eine ungerade Primzahl, so hat ein quadratischer Rest $a \in Z_p$ ($a \neq 0 \pmod p$) 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 $a_1, a_2, \dots, a_k$ alle Primitivwurzeln in Z_N^* , wobei $N \notin \{2, 3, 4, 6\}$. Zeigen Sie, dass $a_1 \cdot a_2 \cdots a_k \equiv 1 \pmod N$.

Abgabe bis Mittwoch 29.4.2020 bis 14 Uhr per Email an den Tutor.

Philipp Braukmann pbraukmann@techfak.de
Jonas Friemel jfriemel+krypto@techfak.de