Dr. Dirk Frettlöh 29.4.2026

Übungen zur Vorlesung Kryptographie

Blatt 3

Aufgabe 9: (Primitivwurzeln)
(a) Finden Sie alle Primitivwurzeln in Z_{10}^*. Zeigen Sie, dass das wirklich Primitivwurzeln sind.

(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.

(Diese Aufgabe lässt sich prima in `sagemath` *lösen.)*

Aufgabe 10: (Quadratische Reste malen)
Finden Sie alle quadratischen Reste in Z_{15}, Z_{17} und Z_{19}. (Das ist hier also immer zu lesen als $(Z_{15}, + \bmod 15, \cdot \bmod 15)$ usw.) 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 11: (Von Hand rechnen)
Lösen Sie folgende Aufgaben vollständig von Hand und geben Sie Ihren gesamten Rechenweg an. *(Gesucht ist natürlich die kleinste Lösung, die hat jeweils nur zwei Dezimalstellen.)*

(a) $5^{1355} \mod 124$
(b) $29^{161^{19}} \mod 150$
(c) Was sind die letzten beiden Dezimalziffern von $23^{1\,000\,005}$?

Aufgabe 12: (Quadratwurzeln mod p)
Sei p eine ungerade Primzahl und sei g ein Erzeuger von $\mathbb{Z}_p^*$. Zeigen Sie

$$-1 \text{ ist quadratischer Rest} \quad \Leftrightarrow \quad p \equiv 1 \mod 4.$$

Bestimmen Sie anschließend alle Quadratwurzeln von -1 in ihrer Darstellung durch g, angenommen es gilt $p \equiv 1 \mod 4$.

Abgabe bis Mittwoch 6.5.2026 bis 12:00 Uhr per Email an die Tutorin.
Bitte auf jeder Abgabe das Tutorium angeben!

Lisa Henetmayr Mi 12 Uhr in S0-115 lhenetmayr+krypto@techfak.de
Lisa Henetmayr Mi 16 Uhr in U2-147 lhenetmayr+krypto@techfak.de