Dr. Dirk Frettlöh 25.4.2022

Übungen zur Vorlesung Kryptographie

Blatt 3

Aufgabe 9: (Quadratische Reste malen)
Finden Sie alle quadratischen Reste in Z_{15}, Z_{17} und Z_{19}. 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 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:
Zeigen Sie, dass in den Quadratische-Reste-Graphen wie in Aufgabe 9 oder Beispiel 2.4 im Skript nie ein Pfeil von einem Knoten $a \in Z_N \setminus Z_N^*$ zu einem Knoten $b \in Z_N^*$ geht, und umgekehrt auch nicht.

Aufgabe 11: (Wieviele Quadratwurzeln?)
(a) Finden Sie alle Quadratwurzeln von 4 in Z_{11}, Z_{77}, Z_{231} und Z_{1155}. Was fällt auf?

(b) Zeigen Sie: Ist p eine ungerade Primzahl, so hat ein quadratischer Rest $a \in Z_p^*$ ($a \neq 0 \mod p$) genau zwei Quadratwurzeln.

Aufgabe 12: (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, warum 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.

Aufgaben 11a und 12 lassen sich sehr viel effizienter mit `python` *oder* `sagemath` *lösen.*

Abgabe bis Montag 2.5.2022 bis 14 Uhr per Email an Ihren Tutor.
Bitte auf jeder Abgabe das Tutorium angeben. Bitte die Abgaben so nennen:
[techfakaccount]-bl$n$.pdf, also z.B. `dfrettloeh-bl2.pdf`, oder `dfrettloeh+mnebel-bl2.pdf`.

Jan-Philipp Brünger jbruenger@techfak.de
Simon Hahm shahm+krypto@techfak.de
Tim Lakämper tlakaemper+krypto@techfak.de