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: (Ineffzienz)
In der Kryptographie spielt die Betrachtung des Rechenaufwands eine große Rolle. Daher wird es gelegentlich Aufgaben dazu geben, z.B. diese hier.

Bemerkung 2.4 im Skript besagt, dass es im Allgemeinen schwierig ist, zu entscheiden, ob $b \in Z_N^*$ ein quadratischer Rest ist (falls N keine Primzahl ist). Bemerkung 2.5 im Skript besagt, dass ein Erzeuger von Z_N^* (also eine eine Primitivwurzel) leicht *alle* quadratischen Reste in Z_N^* liefert. Diese Aufgabe klärt diesen scheinbaren Widerspruch.

(a) Es sei $N = pq$, $p = 2^{100} + 277$, $q = 2^{100} + 331$. Beide, p und q, sind Primzahlen. Angenommen, Sie haben einen Erzeuger a von Z_N^*. Wie viel Elemente hat die Liste $a^2, a^4, a^6, \ldots, a^{\varphi(N)}$? Wieviel Speicherplatz benötigt diese Liste in etwa?

(b) Angenommen, Ihr Rechner kann eine Multiplikation in Z_N^* pro Prozessortakt ausführen, und der Prozessor ist mit 4 Ghz getaktet. Die Liste aus (a) kann mit so vielen Multiplikationen in Z_N^* erzeugt werden, wie sie lang ist (und nicht mit signifikant weniger). Wie lang würde Ihr Rechner dann in etwa brauchen, um die Liste zu erzeugen?

Abgabe bis Dienstag 25.4.2023 bis 23:59 Uhr per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben!

Jakob Niermann janiermann+krypto@techfak.de
Tim Lakämper tlakaemper+krypto@techfak.de