Dr. Dirk Frettlöh 17.4.2019

Übungen zur Vorlesung Kryptographie

Blatt 3

Aufgabe 9: (Schnelles Potenzieren mod N)
(a) Berechnen Sie $3^{1\,000\,003}$ mod 101 von Hand.

(b) Berechnen Sie die letzten beiden Dezimalziffern von $23^{1\,000\,005}$ von Hand.

Aufgabe 10: (Quadratwurzeln mod N)
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 2.5 passt.)

(Für die Abgabe reicht der korrekte Graph. Die quadratischen Reste sind ja genau die, auf die ein Pfeil zeigt.)

Aufgabe 11: (Wieviele Quadratwurzeln?)
Zeigen Sie:
(a) Ist p eine ungerade Primzahl, so hat ein quadratischer Rest $a \in Z_p$ ($a \neq 0 \bmod p$) genau zwei Quadratwurzeln.

(b) Ist $n = pq$, wobei p und q zwei verschiedene ungerade Primzahlen sind, so hat ein quadratischer Rest $a \in Z_n$ ($a \neq 0 \bmod n$) genau zwei oder genau vier Quadratwurzeln.

Aufgabe 12: (Primitivwurzeln)
(a) Finden Sie eine Primitivwurzel in Z_7^*. Zeigen Sie, warum das wirklich eine Primitivwurzel ist.

(b) Finden Sie die kleinste Primitivwurzel in Z_{13}^*. Zeigen Sie, warum das wirklich eine Primitivwurzel ist.

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

Alle Aufgaben außer 9 dürfen auch mit dem Computer gelöst werden; bei Aufgabe 12 sollte man es tun. Falls Sie Programmcode abgeben, beschreiben Sie auf jeden Fall auch, wie Sie vorgingen.

Abgabe: Mittwoch 24.4.2019 bis 14 Uhr in Postfach 2183 in V3, oder per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben! (Di oder Do)

Philipp Braukmann pbraukmann@techfak.uni-bielefeld.de
Oliver Tautz otautz@techfak.uni-bielefeld.de