RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Enrico Thomae, Philipp Wagner, Vera Knüppels

Präsenzübungen zur Vorlesung

Zahlentheorie

Sommersemester 2012

Blatt 11

AUFGABE 1:
Zeigen Sie mit dem Lucas-Lehmer Primzahltest, dass $n = 2^7 - 1 = 127$ eine Primzahl und $n = 2^{11} - 1 = 2047$ keine Primzahl ist.

AUFGABE 2:
Betrachten Sie den zum Solovay-Strassen Primzahltest gehörenden Algorithmus für $n = 23$ und $l = 3$. Angenommen der Algorithmus generiert $a_1 = 3$, $a_2 = 5$ und $a_3 = 7$. Wie lautet dann die Ausgabe? Ist die Ausgabe korrekt?

AUFGABE 3:
Sei $A := \{a \in \mathcal{U}_n | a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)\}$ die Menge der Eulerzeugen. Zeigen Sie, dass A eine Untergruppe von $\mathcal{U}_n$ ist.

AUFGABE 4:
Betrachten Sie den zum Miller-Rabin Primzahltest gehörenden Algorithmus für $n = 29$ und $l = 2$. Angenommen der Algorithmus generiert $a_1 = 2$ und $a_2 = 3$. Wie lautet dann die Ausgabe? Ist die Ausgabe korrekt?