RUHR
UNIVERSITÄT
BOCHUM

RUB

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

Hausübungen zur Vorlesung

Zahlentheorie

Sommersemester 2012

Blatt 12

Abgabe bis 02. Juli 2012, 12 Uhr (vor der Vorlesung)

AUFGABE 1 F1 (4 Punkte)**:**
Sei $n \in \mathbb{N}$ ungerade, zusammengesetzt und keine Primzahlpotenz. Zeigen Sie, dass dann mindestens die Hälfte aller Paare (x, y) mit $0 \leq x, y < n$ und $x^2 \equiv y^2 \mod n$ die Ungleichung $1 < \text{ggT}(x - y, n) \leq n$ erfüllt.

AUFGABE 2 F1 (4 Punkte)**:**
Faktorisieren Sie die zusammengesetzte Zahl $n = 13199$ mit der Fermat Faktorisierung.

AUFGABE 3 F2 (4 Punkte)**:**
Faktorisieren Sie die zusammengesetzte Zahl $n = 7729$ mit der Kettenbruch Faktorisierung von Morrison-Brillhart.

AUFGABE 4 F2 (4 Punkte)**:**
Faktorisieren Sie die zusammengesetzte Zahl $n = 7729$ mit dem Quadratischen Sieb.