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 10

AUFGABE 1:
Berechnen Sie mit dem Algorithmus von Tonelli und Shanks die Lösungen von $x^2 \equiv 10 \mod 13$ und $x^2 \equiv 6 \mod 43$.

AUFGABE 2:
Entwickeln Sie $\frac{48}{11}$, $\frac{225}{136}$ und $\frac{225}{43}$ in Kettenbrüche. Verwenden Sie dafür den Kettenbruchalgorithmus aus der Vorlesung. Welche rationale Zahl hat die Kettenbruchentwicklung $[2, 1, 2, 2]$?

AUFGABE 3:
Sei $(N, e) = (7387, 4811)$ ein öffentlicher RSA Schlüssel. Dann existiert ein $d \in \mathcal{U}_{\varphi(n)}$ mit $e \cdot d \equiv 1 \mod \varphi(n)$, welches der geheime RSA Schlüssel ist. Versuchen Sie den geheimen Schlüssel d mit Hilfe des Wiener Angriffs zu bestimmen. Bestimmen Sie dafür die Kettenbruchentwicklung von $\frac{e}{N}$ und testen Sie, ob einer der Nenner q_i der Konvergenten $\frac{p_i}{q_i}$ des Kettenbruchs das gesuchte d ist. Warum kann man hier das geheime d bestimmen?