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 13

AUFGABE 1:
Faktorisieren Sie $n = 161$ mit Pollards $p-1$-Methode. Wählen Sie dafür als Schranke $C = 6$, sowie im ersten Schritt des Algorithmus $b = 6$ und im zweiten Schritt des Algorithmus $a = 2$.

AUFGABE 2:
Berechnen Sie die Wurzeln von 3 modulo 23 mit dem Algorithmus von Cipolla.

AUFGABE 3:
Faktorisieren Sie $n = 35$ mit Williams' $p+1$-Methode. Wählen Sie dafür als Schranke $C = 6$, sowie im ersten Schritt des Algorithmus $b = 6$ und im zweiten Schritt des Algorithmus $a = 2$.