RUHR UNIVERSITÄT BOCHUM

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

Hausübungen zur Vorlesung

Zahlentheorie

Sommersemester 2012

Blatt 9

Abgabe bis 11. Juni 2012, 12 Uhr (vor der Vorlesung)

AUFGABE 1 F2 (6 Punkte)**:**
Sei p eine Primzahl der Form $p = 4q + 1$ mit einer anderen Primzahl q. Beweisen Sie, dass dann 2 eine Primitivwurzel modulo p ist.

AUFGABE 2 F1 (4 Punkte)**:**
Sei $p > 3$ prim. Bestimmen Sie alle p für die $\left(\frac{3}{p}\right) = 1$ gilt. Für welche dieser Primzahlen gibt es keine Darstellung der Form $p = x^2 - 3y^2$ mit $x, y \in \mathbb{Z}$?

AUFGABE 3 F1 (4 Punkte)**:**
Überprüfen Sie, ob die Gleichungen $x^2 \equiv 3934 \mod 5863$ und $x^2 \equiv 50001 \mod 57691$ eine Lösung besitzen.