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 8

Abgabe bis 04. Juni 2012, 12 Uhr (vor der Vorlesung)

AUFGABE 1 F1 (6 Punkte)**:**
Zeigen Sie, dass das Legendre-Symbol $\left(\frac{a}{p}\right)$ für $p \in \mathbb{P}$, $a \in \mathbb{Z}$ mit $0 \leq a < p$ in Zeit $\mathcal{O}(\log^3(p))$ berechnet werden kann. Verwenden Sie dafür die Tatsache, dass für $p \in \mathbb{N}$ mit Bitlänge $n = \log(p)$ und $a, b \in \mathbb{Z}$ mit $0 \leq a, b < p$ in Zeit $\mathcal{O}(n^2)$ ein $c \in \mathbb{Z}$ mit $0 \leq c < p$ berechnet werden kann, sodass $a \cdot b \equiv c \mod p$.

AUFGABE 2 F2 (4 Punkte)**:**
Zeigen Sie für alle $p \in \mathbb{P} \backslash \{2\}$ folgende Identität:

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{falls } p \equiv \pm 1 \mod 8 \\ -1 & \text{falls } p \equiv \pm 3 \mod 8. \end{cases}$$

AUFGABE 3 F2 (6 Punkte)**:**
Beweisen oder widerlegen Sie mit den Rechenregeln des Legendre-Symbols, aber <u>ohne</u> Verwendung der Euler-Identität, dass

a) 333 quadratischer Rest modulo 547 ist,

b) 5289 quadratischer Rest modulo 3319 ist,

c) 2310 quadratischer Rest modulo 2543 ist.