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 7

Abgabe bis 21. Mai 2012, 12 Uhr (vor der Vorlesung)

AUFGABE 1 F2 (3 Punkte)**:**
Beweisen Sie: Es gibt entweder gar keine oder genau $\varphi(\varphi(n))$ Primitivwurzeln modulo n.

AUFGABE 2 F1 (6 Punkte)**:**
Wir haben in der Vorlesung bewiesen, dass für $p \in \mathbb{P}\backslash\{2\}, r \geq 2$ und $x \in \mathbb{Z}$ gilt:

$$x^p \equiv 1 \bmod p^r \Leftrightarrow x \equiv 1 \bmod p^{r-1}.$$

Zeigen Sie, dass dieses Lemma für $p = 2, r = 3$ nicht gilt. An welcher Stelle des Beweises benötigt man $p \neq 2$? Modifizieren Sie den Beweis, um zu zeigen: Sei $x \in \mathbb{Z}$ mit $x \equiv 1 \bmod 4$ und $r > 2$, dann gilt

$$x \equiv 1 \bmod 2^{r-1} \Leftrightarrow x^2 \equiv 1 \bmod 2^r.$$

AUFGABE 3 F2 (3 Punkte)**:**
Zeigen Sie, dass $f_k : U_n \to U_n, \overline{x} \mapsto \overline{x}^k$ für $\mathrm{ggT}(k, \varphi(n)) = 1$ ein Isomorphismus ist. Geben Sie einen Algorithmus zum Berechnen von f_k^{-1} in Zeit $\mathcal{O}(\log^3 n)$ an.

AUFGABE 4 F1 (3 Punkte)**:**
Berechnen Sie $\log_2 \overline{9}$ in U_{59} mit Hilfe des Baby-Step Giant Step Algorithmus. Geben Sie alle Zwischenwerte an.