RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

Präsenzübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 7 / 27.–29. Mai 2013

AUFGABE 1:
Sei $n > 0$ beliebig und $k \in \mathbb{Z}$ mit $\text{ggT}(k, \phi(n)) = 1$. Zeigen Sie:

(a) $f_k : U_n \to U_n, x \mapsto x^k$ ist ein Gruppenisomorphismus.

(b) Geben Sie einen Algorithmus an, der $f_k^{-1}(y)$ in Zeit $\mathcal{O}(\log(n)^3)$ berechnet (bei Eingabe $n, 0 < k < n, 0 < y < n$ und $\phi(n)$).

AUFGABE 2:
Geben Sie jeweils alle $n \in \mathbb{N}$ an (sofern existent) mit

(a) $U_n \cong \mathbb{Z}/14\mathbb{Z}$

(b) $U_n \cong \mathbb{Z}/8\mathbb{Z}$

(c) $U_n \cong \mathbb{Z}/42\mathbb{Z}$

AUFGABE 3:

(a) Bestimmen Sie die Ordnung von 3 in $\mathbb{F}_{11}^*$

(b) Bestimmen Sie die Lösungsmenge der Gleichung $3^x \equiv 4 \mod 11$

(c) Bestimmen Sie die Lösungsmenge der Gleichung $3^x \equiv 2 \mod 11$

AUFGABE 4:

(a) Zeigen Sie, dass 2 eine Primitivwurzel in $\mathbb{F}_{37}^*$ ist.

(b) Berechnen Sie $\log_2(3)$ in $\mathbb{F}_{37}^*$

AUFGABE 5:
Sei $p > 2$ prim und sei g ein Erzeuger von U_p. Beweisen oder widerlegen Sie:
Für alle r, p ist genau eines g oder $g + p$ ein Erzeuger von U_{p^r}.