RUHR UNIVERSITÄT BOCHUM

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

Präsenzübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 8 / 3.–5. Juni 2013

AUFGABE 1:
Sei $p > 3$ Primzahl. Zeigen Sie, dass 3 ein Quadratischer Rest modulo p ist gdw. $p \equiv \pm 1 \mod 12$ gilt.

AUFGABE 2:

(a) Zeigen Sie, dass 2 ein Erzeuger von U_{11003} ist, ohne Potenzen zu berechnen.

(b) Zeigen Sie, dass 3 ein Erzeuger von U_{65537} ist, ohne Potenzen zu berechnen.

Hinweis: 11003 und 5501 und $65537 = 2^{16} + 1$ sind allesamt Primzahlen.

AUFGABE 3:
Sei p Primzahl. $\zeta = \zeta_p = e^{\frac{2\pi i}{p}} \in \mathbb{C}$ sei primitive p-te Einheitswurzel. Für $a \in \mathbb{Z}$ sei

$$g_a = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \zeta^{aj}$$

die Gaußsumme. (Beachte, dass wir $a \equiv 0 \mod p$ erlauben)
Zeigen Sie:

(a) $g_a = \left(\frac{a}{p}\right) g_1$ gilt auch für $a \equiv 0 \mod p$

(b) $(g_a)^2 = p$ für $a \not\equiv 0 \mod p$ und $p \equiv 1 \mod 4$

(c) $g_a = \sum_{j=1}^{p-1} \left(\frac{aj}{p}\right) \zeta^j$

AUFGABE 4:
Sei $p = 7$ und $\zeta = \zeta_7$ und g_a wie oben (bzw. in der Vorlesung). Zeigen Sie, dass $g_1 = +i\sqrt{7}$ ist.

AUFGABE 5:
Berechnen Sie die Jacobi-Symbole $\left(\frac{62}{119}\right), \left(\frac{51}{119}\right), \left(\frac{3}{119}\right)$. Geben Sie alle Quadratwurzeln von $62, 51$ bzw. 3 in $\mathbb{Z}/(119)$ an, sofern existent.