RUHR UNIVERSITÄT BOCHUM

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

Präsenzübungen zur Vorlesung

Zahlentheorie

SS 2013

Blatt 9 / 10.–12. Juni 2013

AUFGABE 1:
Sei $p > 2$ prim, $p-1 = r \cdot 2^s$, r ungerade (nicht notwendig prim) und $z \in U_p$ mit $(\frac{z}{p}) = -1$. Was ist die Ordnung von z^r in U_p?

AUFGABE 2:
Sei $p > 2$ prim. Zeigen Sie, dass die kleinste positive Zahl z mit $(\frac{z}{p}) = -1$ stets eine Primzahl ist.

AUFGABE 3:

(a) Berechnen Sie, sofern existent, jeweils die Quadratwurzeln von 2 und von 3 in $\mathbb{Z}/(17)$ mit Hilfe des Tonelli-Shanks-Algorithmus.

(b) Berechnen Sie, sofern existent, die Quadratwurzeln von $\overline{7}$ in U_{53}

AUFGABE 4:
Bestimmen Sie die ersten 5 Zahlen a_0, a_1, a_2, a_3, a_4 der Kettenbruchentwicklung $[a_0, a_1, \ldots]$ von $-\sqrt{3}$ mit $a_i \in \mathbb{Z}, a_i > 0$ für $i > 0$.

AUFGABE 5:
Beweisen oder widerlegen Sie: Für beliebige $n \in \mathbb{N}$, $a_0, a_1, \ldots, a_n \in \mathbb{R}$ gilt:

(a) $[a_0, a_1, \ldots, a_n] = [[a_0, \ldots, a_k], a_{k+1}, \ldots, a_n]$

(b) $[a_0, a_1, \ldots, a_n] = [a_0, \ldots, a_k, [a_{k+1}, \ldots, a_n]]$

(c) $[a_0, a_1, \ldots, a_n] = [a_0, \ldots, a_k, [a_{k+1}, \ldots, a_n]^{-1}$

AUFGABE 6:
Bestimmen die die Kettenbruchentwicklung von $\frac{-13}{21}$ sowie die Konvergenten (d.h. die Näherungsbrüche $\frac{p_i}{q_i}$ in der Notation der Vorlesung).

AUFGABE 7:
Sei x der (bis auf den Startwert) peroidische Kettenbruch $x = [1, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, \ldots]$. Geben Sie eine quadaratische Gleichung an, deren Lösung x ist.