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 10

Abgabe bis 18. Juni 2012, 12 Uhr (vor der Vorlesung)

AUFGABE 1 F2 (4 Punkte)**:**
Berechnen Sie mit dem Algorithmus von Tonelli und Shanks die Lösungen von $x^2 \equiv 5 \mod 41$ und $x^2 \equiv 5 \mod 89$.

AUFGABE 2 F2 (6 Punkte)**:**
Endliche Kettenbrüche lassen sich nicht eindeutig darstellen, denn für $a_n > 1$ gilt

$$[a_0, ..., a_{n-1}, a_n] = [a_0, ..., a_{n-1}, a_n - 1 + \frac{1}{1}] = [a_0, ..., a_{n-1}, a_n - 1, 1].$$

Angenommen das letzte Element ist größer als 1. Zeigen Sie, dass die Darstellung endlicher Kettenbrüche dann eindeutig ist.
Hinweis: Zeigen Sie zunächst, dass falls $[a_0, ..., a_n, \xi] = [b_0, ..., b_n, \zeta]$ mit $a_0, b_0 \in \mathbb{Z}$, $a_1, ..., a_n, b_1, ..., b_n \in \mathbb{N}$ mit reellen Zahlen $\xi, \zeta > 1$, dann gilt $a_i = b_i \; \forall i \in \{0, ..., n\}$ und $\xi = \zeta$.

AUFGABE 3 F1 (6 Punkte)**:**
Zeigen Sie, dass die Näherungsbrüche $\frac{p_n}{q_n}$ für $n > 1$ eine *Bestapproximation* für irrationale Zahlen $x \in \mathbb{R} \setminus \mathbb{Q}$ liefern, das heißt, dass

$$|x - \frac{p_n}{q_n}| \leq |x - \frac{p}{q}|$$

für alle Brüche $\frac{p}{q} \in \mathbb{Q}$ mit $\mathrm{ggT}(p, q) = 1$ und $1 \leq q \leq q_n$ gilt.
Hinweis: Zeigen Sie zunächst mit gleichen Voraussetzungen die stärkere Aussage

$$|q_n \cdot x - p_n| \leq |q \cdot x - p|.$$

AUFGABE 4 F1 (4 Punkte)**:**
Sei $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $\mathrm{ggT}(a, n) = 1$. Konstruieren Sie mit Hilfe von Kettenbrüchen ein Inverses x von a in $\mathcal{U}_n$, das heißt ein x mit $ax \equiv 1 \mod n$. Schauen Sie sich dazu den Beweis vom Satz von Wiener an. Es werden genau zwei Kettenbruchentwicklungen benötigt, um in allen Fällen das Inverse x erzeugen zu können.