Kryptographie *WS 2015/16*
Barbara Baumeister
Tutoren: Apolonia Gottwald, Soeren Senkovic

2. Übungsblatt

Abgabe: Donnerstag, 5.11.2015

Aufgabe 1 (a) Lösen Sie $122x \equiv 1 \bmod 343$.

(b) Sei p eine Primzahl und $p \equiv 3 \bmod 4$. Sei a eine ganze Zahl, die ein Quadrat mod p ist. Zeigen Sie, dass $a^{(p+1)/4}$ eine Quadratwurzel von a mod p ist.

Aufgabe 2 Seien $n, m \in \mathbb{N}$ zwei teilerfremde Zahlen grösser als 1. Zeigen Sie, dass $\mathbb{Z}^*_{n \cdot m}$ und $\mathbb{Z}^*_n \times \mathbb{Z}^*_m$ isomorphe Gruppen sind.

Seien $a, b \in \mathbb{N}$ mit $a > b$. Ziel der nächsten zwei Aufgaben ist es, die Anzahl n der Iterationen im euklidischen Algorithmus zur Berechnung von $\mathrm{ggT}(a, b)$ nach oben abzuschätzen. Wir benutzen die in der Vorlesung eingeführte Notation.

Aufgabe 3 (a) Zeigen Sie: Es gilt $q_k \geq 1$ für $1 \leq k \leq n$ und $q_{n+1} \geq 2$.

(b) Sei $\mathrm{ggt}(a, b) = 1$. Setzen Sie $r_0 = b$.
Zeigen Sie, dass $r_k \geq \Theta^{n-k}$ gilt für $0 \leq k \leq n$, wobei Θ der goldene Schnitt ist.

Aufgabe 4 (a) Zeigen Sie, dass n nur von a/b abhängt.

(b) Zeigen Sie $n \leq \log_2(b)/\log_2(\Theta)$.
Hinweis: Zeigen Sie zuerst, dass $\mathrm{ggT}(a, b) = 1$ angenommen werden kann.