TECHNISCHE UNIVERSITÄT BERLIN WS09/10
Fakultät II – Institut für Mathematik
Dozent: Tobias Finis
Assistent: Gerriet Möhlmann
www.math.tu-berlin.de/~kant/kryptows09

10. Übung Kryptographie

1. Aufgabe

Löst das folgenden DLP mit Pollig-Hellman:

$$5^x \equiv 54 \mod 73$$

Zeigt vorher ohne zu viel Aufwand, dass 5 ein Erzeuger der Einheitengruppe von $\mathbb{Z}/73\mathbb{Z}$ ist.

(5 Punkte)

2. Aufgabe

Zeigt, dass in der Notation der Vorlesung

$$\frac{Q(n)+1}{2} = E(\lambda)$$

gilt. Folgert daraus, dass

$$\frac{Q(n)-1}{2} = E(\mu)$$

gilt.

(5 Punkte)

3. Aufgabe

Sei $p \in \mathbb{N}$ und $f : \{0, \ldots, p-1\} \longrightarrow \{0, \ldots, p-1\}$ eine beliebige Funktion. Wir definieren eine Folge $x_0, x_1, \ldots$ wie folgt: Wähle $x_0 \in \{0, \ldots, p-1\}$ zufällig und $x_{i+1} = f(x_i)$ für $i \geq 0$.

(a) Begründet, warum es $l, t \in \mathbb{N}$ mit $l + t \leq p$ gibt, so dass $x_i = x_{i+l}$ für alle $i \geq t$ gilt.

(b) Gilt die Aussage auch für $l + t \leq p - 1$?

(c) Sei $(y_i)_{i \in \mathbb{N}}$ eine weitere Folge, für die gilt: $y_0 = x_0$ und $y_{i+1} = f(f(y_i))$ für $i \geq 0$. Zeigt, dass es $1 \leq i_0 \leq t + l$ gibt, so dass $x_{i_0} = y_{i_0}$ gilt.

(5 Punkte)

4. Aufgabe

Schreibt einen Pollard-ρ Algorithmus zum Lösen von DLPs in den multiplikativen Gruppen von Primkörpern.

(5 Punkte)