Goethe-Universität Frankfurt am Main
Institut für Informatik
Theorie komplexer Systeme
Prof. Dr. Nicole Schweikardt

Dienstag, 05.07.2011

Komplexitätstheorie

Sommersemester 2011

Übungsblatt 10

Zu bearbeiten bis Donnerstag, 14.07.2011

Aufgabe 1: **(25 Punkte)**

Entwerfen Sie einen Algorithmus, der bei Eingabe der Binärdarstellung einer beliebigen natürlichen Zahl $n > 2$ von einer Prozedur **rand** Gebrauch macht, die eine zufällig gleichverteilt aus $\{0, 1\}$ gewählte Zahl liefert, um die Binärdarstellung einer zufällig gleichverteilt aus $\{2, \ldots, n-1\}$ gewählten Zahl m zu erzeugen. Ihr Algorithmus darf dabei nur poly$(\log n)$ viele Schritte machen.

Aufgabe 2: **(25 Punkte)**

Geben Sie Algorithmen an, die bei Eingabe von $m, n \in \mathbb{N}$ in Zeit poly$(\log n + \log m)$ laufen und Folgendes berechnen:

(a) Das Jacobi–Symbol $(m|n)$.

(b) Den Wert $m^{\frac{n-1}{2}} \pmod n$.

Aufgabe 3: **(25 Punkte)**

Beweisen Sie Satz 7.15 aus der Vorlesung.

Aufgabe 4: **(25 Punkte)**

Zeigen Sie: BPL $\subseteq$ P.