Technische Universität München
Institut für Informatik
Lehrstuhl für Effiziente Algorithmen
Prof. Dr. Angelika Steger

SS 1998
Übungsblatt 11
17. Juli 1998

Diskrete Strukturen II

Aufgabe 1

Geben Sie ein effizientes Verfahren an, mit dem man eine Zahl $\geq 2^{800}$ bestimmen kann, die (mit sehr hoher Wahrscheinlichkeit) eine Primzahl ist.

TIP: Verwenden Sie dabei den *Primzahlsatz*, der folgendes besagt:
Mit $\pi(x) := |\{p \mid p \text{ ist Primzahl mit } p \leq x\}|$ gilt

$$\lim_{x\to\infty}\left(\frac{\pi(x)}{x/\ln x}\right) = 1,$$

d.h. für großes x gibt es in $\{1, \ldots, x\}$ etwa $\frac{x}{\ln x}$ Primzahlen.

Aufgabe 2

Geben Sie einen Algorithmus an, der als Eingabe eine Primzahl n erhält und in Zeit polynomiell in $\log(n)$ ein Element $x \in Z_n^*$ bestimmt, das mit Wahrscheinlichkeit mindestens $1/2$ ein erzeugendes Element von Z_n^* ist.

TIP: Zeigen Sie, daß die Anzahl der erzeugenden Elemente in Z_n^* von der Ordnung $\Omega\left(\frac{n}{\log(n)}\right)$ ist.