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

3. Übung Kryptographie

1. Aufgabe

Gebt eine Turingmaschine an, die die Binärdarstellung von n in die von $n+1$ überführt. Wieviele Schritte werden im worst-case benötigt.

(6 Punkte)

2. Aufgabe

Findet raus was die Turingmaschine $M = (Q, \Sigma, \Gamma, \delta, q_0, F)$ mit $\Sigma = \Gamma = \{1\}$, $Q = \{0, \ldots, 6\}$, $q_0 = 0$, $F = \{6\}$ macht. Dabei ist δ durch

p	a	p'	a'	d
0	1	1	*	+1
0	*	6	*	+1
1	1	1	1	+1
1	*	2	*	+1
2	1	2	1	+1
2	*	3	1	+1
3	*	4	1	-1
4	1	4	1	-1
4	*	5	*	-1
5	1	5	1	-1
5	*	0	*	+1

gegeben.

(6 Punkte)

3. Aufgabe

Gebt Beispiele oder begündet, dass solche ein Algorithmus nicht existiert.

(a) Die Laufzeit ist durch ein Polynom in der Inputlänge beschränkt aber es wird exponentiell viel Speicherplatz benötigt.

(b) Der benötigte Speicher ist durch ein Polynom in der Inputlänge beschränkt aber die Laufzeit ist exponentiell.

(4 Punkte)

4. Aufgabe

Implementiert zwei Algorithmen, die als Input zwei ganze Zahlen a und b bekommen und als Output den größten gemeinsamen Teiler der beiden liefern. Der eine Algorithmus soll der Euklidische Algorithmus sein, der andere irgendwie mit Probedivision arbeiten. Wie verhalten sich die Laufzeiten bei wachsender Inputlänge.

(4 Punkte)