Aufgaben zu Kapitel 2 der Vorlesung „Randomisierte Algorithmen“

Aufgabe 2.1
Es sei $\mathbb{F}$ ein Körper und $P_1(x)$, $P_2(x)$ und $P_3(x)$ seien drei Polynome aus $\mathbb{F}[x]$ mit $\deg P_1 \leq n$, $\deg P_2 \leq n$ und $\deg P_3 \leq 2n$. Die Aufgabe besteht darin, herauszufinden, ob $P_1(x)P_2(x) = P_3(x)$ ist oder nicht. Betrachten Sie den folgenden

Algorithmus

$\langle$*Es sei* $S \subseteq \mathbb{F}$ *eine Teilmenge mindestens der Größe* $2n+1\rangle$
for $i \leftarrow 1$ **to** k **do**
  $r \leftarrow \langle$*zufällig gleichverteilt gewähltes Element aus* $S\rangle$
  if $P_1(r)P_2(r) \neq P_3(r)$ **then**
    return NO
  fi
od
return YES

- Beweisen Sie: Die Wahrscheinlichkeit, dass der Algorithmus fälschlicherweise YES ausgibt, ist kleiner gleich $(2n/\,|S|)^k$.
- Welche Zeit benötigt man mit dem naheliegenden deterministischen Algorithmus für die Lösung des Problems? Und welche Laufzeit hat man bei obigem randomisierten Algorithmus zu erwarten?

Lösung 2.1
$P_1P_2 - P_3$ ist ein Polynom mit höchstens $2n$ Nullstellen. Nur wenn das zufällige r eine solche Nullstelle ist, kann die falsche Antwort geliefert werden. Also passiert das in jedem Schleifendurchlauf höchstens mit Wahrscheinlichkeit $2n/|S|$.

Aufgabe 2.2
Gegeben sei ein deterministischer Algorithmus isPrime, der eine natürliche Zahl n als Eingabe, überprüft ob sie eine Primzahl ist oder nicht.

Finden Sie einen randomisierten Algorithmus, der zu einer natürlichen Zahl $m \geq 2$ als Eingabe als Ausgabe zufällig gleichverteilt jede Primzahl p mit $2 \leq p \leq m$ aus Ausgabe produziert.

Was können Sie über die Laufzeit Ihres Algorithmus sagen?

Lösung 2.2
Algorithmusidee:

```
randPrime(m)
repeat
        k ← randInteger(2 .. m)
    until (isPrime(k))
return k
```

Im Bereich $2\,..\,m$ gibt es näherungsweise $\pi(m) = m/\ln m$ viele Primzahlen. Also Erwartungswert für die Anzahl Aufrufe von randPrime:

$$\sum_{i=1}^{\infty} i \left(1 - \frac{1}{\ln m}\right)^{i-1} \frac{1}{\ln m} = \frac{1}{\ln m} \cdot \frac{1}{1/(\ln m)^2} = \ln m$$

Aufgabe 2.3
Beweisen Sie, dass für die n-te Harmonische Zahl gilt: $H_n = \sum_{i=1}^{n} \frac{1}{i} \in \Theta(\ln n)$.

Lösung 2.3
Einerseits

$$H_n \leq 1 + \int_{x=1}^{n} \frac{1}{x} dx = 1 + \ln n$$

Andererseits

$$H_n \geq \int_{x=1}^{n+1} \frac{1}{x} dx = \ln(n+1)$$