Einführung in das symbolische Rechnen
Praktikumsblatt 2

Abgabe bis Montag, den 14.05.2018 per Email an `yweber@rhrk.uni-kl.de`.

1. Sei $M = \{0, \ldots, 2^{64} - 1\}$.

   (a) Schreiben Sie eine Funktion `add64`, die für $a, b \in M$ Zahlen $c \in M$ und $d \in \{0, 1\}$ bestimmt mit
   $$a + b = c + d \cdot 2^{64}.$$

   (b) Schreiben Sie eine Funktion `mult64`, die für $a, b \in M$ Zahlen $c, d \in M$ bestimmt mit
   $$a \cdot b = c + d \cdot 2^{64}.$$

   (c) Erproben Sie Ihre Funktionen an Beispielen.

2. Sei $B = 2^{64}$ und
   $$\begin{array}{cccc} \phi_{B,r}: & \{0, \ldots, B-1\}^r & \longrightarrow & \{0, \ldots, B^r - 1\} \\ & (a_{r-1}, \ldots, a_0) & \longmapsto & \sum_{i=0}^{r-1} a_i B^i \end{array}$$
   die B-adische Entwicklung zur Basis B mit r Stellen.

   (a) Schreiben Sie eine Funktion, die aus zwei Zahlen in B-adischer Darstellung $a, b \in \{0, \ldots, B-1\}^r$ mittels Schulbuchmultiplikation das Produkt bestimmt, d.h. für minimal mögliches $s \in \mathbb{N}_0$ ein $c \in \{0, \ldots, B-1\}^s$ mit
   $$\phi_{B,s}(c) = \phi_{B,r}(a) \cdot \phi_{B,r}(b).$$

   (b) Implementieren Sie für $r = 2^k$ eine Zweierpotenz die rekursive Anwendung der Karatsuba-Multiplikation zur Berechnung des Produkts von a und b.

   (c) Erproben Sie Ihre Funktionen an Beispielen und vergleichen Sie die Performance.

   Hinweis: Verwenden Sie Ihre Funktionen `add64` und `mult64`.

3. Implementieren Sie den Miller-Rabin Primzahltest. Erproben Sie Ihr Programm an Beispielen.

4. (a) Implementieren Sie die Faktorisierung mit dem quadratischen Sieb.

   (b) Vergleichen Sie anhand von Beispielen die Laufzeit mit der Probedivision und dem Pollard-Verfahren. Können Sie jeweils ein Beispiel produzieren, bei dem das quadratische Sieb schneller ist als das Pollard-Verfahren und umgekehrt?