Einführung in das symbolische Rechnen
Praktikumsblatt 1

Abgabetermin Montag, den 30.04.2018 per Email an `yweber@rhrk.uni-kl.de`.

1. Implementieren Sie

   (a) das Sieb des Eratosthenes und

   (b) die Faktorisierung von ganzen Zahlen mittels Probedivision.

   Faktorisieren Sie mit Ihrer Implementierung in $\mathbb{Z}$ die Zahl

   $$183720878269532761066013208021559169596728115426694118764 03.$$

2. Implementieren Sie das Faktorisierungsverfahren von Pollard.

   Testen Sie Ihre Implementierung an Beispielen, und vergleichen Sie die Performance mit der Funktion `factor` von JULIA/NEMO.

3. Auf dem Ring der Gaußschen Zahlen

   $$R = \mathbb{Z}[i] = \{a_1 + i \cdot a_2 \mid a_1, a_2 \in \mathbb{Z}\} \subset \mathbb{C}$$

   mit $i^2 = -1$ ist durch

   $$\begin{array}{rccc} d: & R \backslash \{0\} & \to & \mathbb{N}_0 \\ & a + b \cdot i & \mapsto & a^2 + b^2 \end{array}$$

   eine Euklidische Norm gegeben.

   (a) Implementieren Sie einen Algorithmus zur Durchführung der Division mit Rest in (R, d).

   (b) Verwenden Sie Ihren Divisionsalgorithmus, um den Eukldischen Algorithmus in R zu implementieren.

   (c) Berechnen Sie damit

   $$\mathrm{ggT}(3 + 4i, \quad -1 + 12i) \in R.$$

4. Schreiben Sie eine Funktion, die die Lösungsmenge der simultanen Kongruenzen

   $$\begin{gathered} x \equiv a_1 \bmod n_1 \\ \vdots \\ x \equiv a_r \bmod n_r \end{gathered}$$

   für $a_1, \ldots, a_r \in \mathbb{Z}$ und paarweise teilerfremde Moduli $n_1, \ldots, n_r \in \mathbb{Z}_{>0}$ bestimmt. Vergleichen Sie mit der JULIA/NEMO-Funktion `crt`.