Einführung in das symbolische Rechnen
Ferienblatt

1. Sei $L \subset \mathbb{R}^n$ ein Gitter von Rang n und $(v_1, ..., v_n)$ eine $\delta - LLL$-reduzierte Basis von L. Seien weiter $y_1, ..., y_l$ linear unabhängige Vektoren in L. Zeigen Sie, dass mit
$$\tau = \frac{4}{4\delta - 1}$$
gilt
$$\|v_j\| \leq \tau^{\frac{n-1}{2}} \cdot \max\{\|y_1\|, ..., \|y_l\|\}$$
für alle $j = 1, ..., l$.

2. Sei $\mathbb{F}_q$ ein endlicher Körper mit q Elementen.
   (a) Zeigen Sie, dass es unendlich viele irreduzible Polynome in $\mathbb{F}_q[x]$ gibt, indem Sie Euklids Beweis für $\mathbb{Z}$ auf den Polynomring $\mathbb{F}_q[x]$ übertragen. Lässt sich auch Eulers Beweis übertragen?
   (b) Bestimmen Sie alle normierten irreduziblen Polynome vom Grad ≤ 4 in $\mathbb{F}_2[x]$.
   (c) Schreiben Sie eine Funktion, die alle normierten, irreduziblen Polynome vom Grad $\leq d$ in $\mathbb{F}_p[x]$ aufzählt.
   (d) Implementieren Sie die Faktorisierung von Polynomen $f \in \mathbb{F}_p[x]$ mittels Probedivision.

3. (a) Implementieren Sie den LLL-Algorithmus für Gitter $L \subset \mathbb{Z}^n$.
   (b) Berechnen Sie mit Ihrer Implementierung eine LLL-reduzierte Basis des Gitters L erzeugt von den Vektoren
$$\begin{pmatrix} 4 \\ 4 \\ 6 \end{pmatrix}, \begin{pmatrix} 5 \\ 8 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 6 \end{pmatrix} \in \mathbb{Z}^3$$

4. (a) Schreiben Sie eine Funktion, die für Polynome f in $\mathbb{Q}[x]$ oder in $\mathbb{F}_p[x]$ die quadratfreie Faktorisierung bestimmt.
   (b) Erproben Sie Ihre Funktion an Beispielen.

5. (a) Implementieren Sie den Algorithmus von Berlekamp zur Faktorisierung eines quadratfreien Polynoms $f \in \mathbb{F}_p[x]$.
   (b) Vergleichen Sie die Laufzeit des Berlekamp-Algorithmus anhand von Beispielen mit der Probedivision.