Wolfgang K. Seiler
Tel. 2515

B6, B4.08

11. Mai 2023

11. Übungsblatt Computeralgebra

Aufgabe 1:

a) Zeigen Sie, daß die Vektoren

$$b_1 = \begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \quad b_2 = \begin{pmatrix}1\\1\\-1\\-1\end{pmatrix}, \quad b_3 = \begin{pmatrix}1\\-1\\1\\-1\end{pmatrix} \quad \text{und} \quad b_4 = \begin{pmatrix}-1\\1\\1\\-1\end{pmatrix}$$

eine Orthogonalbasis des $\mathbb{R}^4$ bilden!

b) Wenden sie den LLL-Algorithmus an auf das Gitter $\Gamma = \mathbb{Z}\cdot 5b_1 \oplus \mathbb{Z}\cdot 3b_2 \oplus \mathbb{Z}\cdot 2b_3 \oplus \mathbb{Z}\cdot b_4$!

c) Wenden sie den LLL-Algorithmus an auf das Gitter $\Lambda = \mathbb{Z}\cdot 9b_1 \oplus \mathbb{Z}\cdot 8b_2 \oplus \mathbb{Z}\cdot 7b_3 \oplus \mathbb{Z}\cdot 6b_4$!

d) Allgemein sei Γ ein Gitter mit einer Basis $(b_1, \dots, b_n)$, die eine Orthogonalbasis von $\mathbb{R}^n$ ist. Was macht der LLL-Algorithmus mit einem solchen Gitter?

Aufgabe 2:

Das Untergitter Γ von $\mathbb{Z}^2$ wird aufgespannt von den Vektoren $\binom{28}{6}$ und $\binom{13}{3}$. Wenden Sie den LLL-Algorithmus darauf an!

Aufgabe 3:

x sei eine beliebige reelle Zahl und M eine große natürliche Zahl. Die Vektoren $b_i \in \mathbb{R}^{n+2}$ für $i = 1, \dots, n+1$ haben jeweils die i-te Komponente eins und die $(n+2)$-te Komponente Mx^{i-1}; alle anderen Komponenten sind Null. Der von diesen Vektoren aufgespannte Untervektorraum V wird mit $\mathbb{R}^{n+1}$ identifiziert, und wir betrachten darin das von $b_1, \dots, b_{n+1}$ erzeugte Gitter Γ. Welche Bedingung müssen $a_1, \dots, a_{n+1} \in \mathbb{Z}$ erfüllen, damit $a_1b_1 + \cdots + a_{n+1}b_{n+1}$ ein (bezüglich des Standardskalarprodukts von $\mathbb{R}^{n+2}$) „kurzer“ Vektor ist, und welche Rolle spielt hier die Zahl M ?

Abgabe bis zum Mittwoch, dem 17. Mai 2023, um 15.30 Uhr