Prof. C. P. Schnorr Sommersemester 2009

Gitter und Kryptographie

Blatt 6, 27.05.2009, Abgabe Mittwoch, 03.06.2009

Aufgabe 1. Zeige:
Die LLL-Reduktion, Alg. 3, transformiert linear abhängige Eingabevektoren $\mathbf{b}_1, ..., \mathbf{b}_n \in \mathbb{Z}^m$ in $[\mathbf{b}_1, ..., \mathbf{b}_n]T = [\mathbf{0}^i, \mathbf{b}'_{i+1}, ..., \mathbf{b}'_n]$ so dass $\mathbf{b}'_{i+1}, ..., \mathbf{b}'_n \in \mathbb{Z}^m$ linear unabhängig sind.

Aufgabe 2. Zeige:
Jedes Gitter $\mathcal{L} \subset \mathbb{Z}^n$ hat eine Basis $B = [b_{i,j}]$ in oberer Dreiecksform,
d.h. $b_{i,j} = 0$ für $i < j$.

Aufgabe 3. Zeige, dass die Gitter

$$A_n = \{\mathbf{x} \in \mathbb{Z}^{n+1} \mid \langle \mathbf{x}, \mathbf{1} \rangle = 0\}$$
$$D_n = \{\mathbf{x} \in \mathbb{Z}^n \mid \langle \mathbf{x}, \mathbf{1} \rangle = 0 \bmod 2\}$$

für $n = 3$ isometrisch sind. Transformiere die gegebenen Basen im Skript, Seite 7, in isometrische Basen.