Prof. C. P. Schnorr Sommersemester 2009

# Gitter und Kryptographie

Blatt 2, 24.04.2009, Abgabe Mittwoch, 06.05.2009

**Aufgabe 1.** Sei $B \in \mathbb{R}^{m\times n}$ Basismatrix, Rang $B = n$. Zeige $B$ ist eindeutig zerlegbar als $B = QR$ mit $Q \in \mathbb{R}^{m\times n}$ isometrisch und $R = [r_{i,j}] \in \mathbb{R}^{n\times n}$ obere Dreiecksmatrix mit $r_{i,i} > 0$ für $i = 1, \ldots, n$.

**Aufgabe 2.** Sei $A = A^t = [a_{i,j}] \in \mathbb{R}^{n\times n}$ regulär. Zeige, dass es eine eindeutige Zerlegung $A = R^t D R$ gibt, derart, dass $R = [r_{i,j}] \in \mathbb{R}^{n\times n}$ eine obere Dreiecksmatrix ist (also $r_{i,j} = 0$ für $i > j$ und $r_{i,i} > 0$) und $D$ Diagonalmatrix mit Diagonale $(\sigma_1, \ldots, \sigma_n) \in \{\pm 1\}^n$.

**Aufgabe 3.** Zeige: Für jede Basis $\mathbf{b}_1, ..., \mathbf{b}_n \in \mathbb{Z}^m$ gilt für $D_i := (\det \mathcal{L}(\mathbf{b}_1, ..., \mathbf{b}_i))^2$ gilt: 1. $D_{i-1}\mathbf{b}_i^* \in \mathbb{Z}^m$, 2. $D_j\, \mu_{i,j} \in \mathbb{Z}$ für $j < i$.

*Hinweis*: Lemma 4.2.3, Skript.

**Aufgabe 4.** Sei $B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ aN & bN \end{bmatrix}$ Basismatrix mit $a, b, N \in \mathbb{Z}$. Zeige:

1. $\det \mathcal{L} = (1 + N^2(a^2 + b^2))^{1/2}$,
2. Für $N > \left(\sqrt{\frac{4}{3}}(a^2 + b^2)\right)^{1/2}$ gilt für jede *reduzierte* Basis $\mathbf{b}_1, \mathbf{b}_2$ :

$$\mathbf{b}_1 = \begin{bmatrix} * \\ * \\ 0 \end{bmatrix},\ \mathbf{b}_2 = \begin{bmatrix} * \\ * \\ N \cdot \mathrm{ggT}(a, b) \end{bmatrix}.$$

*Hinweis.* Benutzen Sie dass :
$\|\mathbf{b}_1\|^2 \le \sqrt{\frac{4}{3}} \det \mathcal{L} = \sqrt{\frac{4}{3}} (\det B^t B)^{1/2}$ für jede *reduzierte* Basis $B = [\mathbf{b}_1, \mathbf{b}_2]$.