Prof. C. P. Schnorr Wintersemester 2005/06

# Gitter und Kryptographie

Blatt 8, 16.12.2005, Abgabe 06.01.2006

**Aufgabe 1.** Sei $B = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix} \in \mathbf{R}^{(n+1)\times n}$.

Zeige: $\det(B^t B) = 1 + \sum_{i=1}^n a_i^2$.

**Aufgabe 2.** Zeige für $n \geq n_0$: $\gamma_n \geq \frac{1}{\pi}\,\Gamma\,(1+\frac{n}{2})^{\frac{2}{n}} \geq \frac{n-\ln n}{2e\pi}$.

*Hinweis*: Benutze $\triangle_n \geq 2^{-n+1}$ für $n \geq n_0$ und die Stirling Approximation.

**Aufgabe 3.** Zeige:

1. Folgende Basis ist LLL-reduziert für $\delta = 1$ und $\alpha = \frac{4}{3}$ mit $\rho := 1/\sqrt{\alpha} = \sqrt{3/4}$:

$$[\mathbf{b}, \ldots, \mathbf{b}_n] = \begin{bmatrix} 1 & 1/2 & 0 & \cdots & \cdots & 0 \\ 0 & \rho & \rho/2 & \cdots & \cdots & \vdots \\ \vdots & \ddots & \rho^2 & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 \\ \vdots & & & \ddots & \rho^{n-2} & \rho^{n-2}/2 \\ 0 & \cdots & \cdots & \cdots & 0 & \rho^{n-1} \end{bmatrix} \in \mathbf{R}^{n\times n}.$$

2. $\|\mathbf{b}_1\|^2 = \alpha^{\frac{n-1}{2}} \det(\mathcal{L})^{2/n}$ und vergleiche mit Korollar 5.1.5.

**Aufgabe 4.** Sei $R_2 = \sqrt{2}\begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \sqrt{3/4} \end{bmatrix}$. Zeige:

$\Lambda_2 = \mathcal{L}(R_2)$ ist global extrem / kritisch,

d.h. $\max\{\|\mathbf{b}_1\|^2 / \det \mathcal{L}(\mathbf{b}_1, \mathbf{b}_2) \mid \mathbf{b}_1, \mathbf{b}_2 \text{ Gauss-reduziert}\} = \gamma_2^2 = \frac{4}{3}$.

*Hinweis:* O.B.d.A.: $[\mathbf{b}_1, \mathbf{b}_2] = \sqrt{2}\begin{bmatrix} 1 & r_{1,2} \\ 0 & r_{2,2} \end{bmatrix}$.