

Gitter und Kryptographie

Blatt 8, 07.12.2007, Abgabe 14.12.2007

Aufgabe 1. Beweise

$\prod_{i=1}^n \lambda_i(\mathcal{L}) \leq \gamma_n^{n/2} \det \mathcal{L}$ für Gitter \mathcal{L} der Dimension n .

Sei $\mathcal{L} = \mathcal{L}(B)$ und $R = \text{GNF}(B)$, arbeite mit $R = (r_{i,j})$.

Hinweis: Beweis von Satz 2.3.1, Skript.

Aufgabe 2. Sind die Gitter $\mathcal{L}(B)$ mit Gram-Matrizen

$$B^t B = \begin{pmatrix} 2 & 1 & & & \\ 1 & 2 & 1 & & \\ & 1 & 2 & 1 & \\ & & 1 & 2 & 1 \\ & & & 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 1 & 1 & \\ 1 & 2 & 1 & 1 & \\ 1 & 1 & 2 & 1 & \\ 1 & 1 & 1 & 2 & \\ & & & & \end{pmatrix}$$

kritisch? Berechne $R = \text{GNF}(B)$.

Aufgabe 3. Sei R_8 die GNF des Gitters Λ_8 und $\mathbf{y} = (0, 0, 0, 1, 0, 0, 0, 0)^t$.

Zeige: $\min\{\|\mathbf{y} - \mathbf{x}\|, \mathbf{x} \in \mathcal{L}(R_8)\} = 1$.

Hinweis: $(R_8|\mathbf{y})^t(R_8|\mathbf{y}) \in \frac{1}{2}\mathbb{Z}^{9 \times 9}$, $\|\mathbf{y}\| = 1$. Argumentiere wie in Lemma 2.2.3, Skript.

Aufgabe 4. Angenommen \mathbf{y} in Aufgabe 3 ist tiefes Loch von $\Lambda_8 = \mathcal{L}(R_8)$.

Konstruiere die GNF R_9 und die Gram-Matrix $R_9^t R_9$ des geschichteten Gitters Λ_9 , dabei habe $R_9^t R_9$ die Diagonale $(2, \dots, 2) \in \mathbb{Z}^9$.

Vegleiche mit den Angaben zu Λ_9 in Table 6.1, Conway, Sloane.