Prof. C. P. Schnorr Sommersemester 2009

Gitter und Kryptographie

Blatt 11, 01.07.2009, Abgabe Mittwoch, 08.07.2009

Aufgabe 1. 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: $[R_8, \mathbf{y}]^t[R_8, \mathbf{y}] \in \frac{1}{2}\mathbf{Z}^{9\times 9}$, $\|\mathbf{y}\| = 1$. Argumentiere wie in Lemma 2.2.3 des Skripts.

Aufgabe 2. Nehme an, dass $\mathbf{y}$ tiefes Loch von $\Lambda_8 = \mathcal{L}(R_8)$ ist und konstruiere die GNF R_9 und die Gram-Matrix $R_9^t R_9$ des geschichteten Gitters Λ_9 so dass $\lambda_1^2 = 2$. Zeige, dass $\lambda_1^2 = 2$. Welche untere Schranke von γ_9^9 liefert $\lambda_1^2 \le \gamma_9(\det R_9)^{2/9}$?

Aufgabe 3. Sei $R_8 \in \mathbb{R}^{8\times 8}$ die R–Matrix des Gitters maximaler Dichte mit Dimension 8 und $\lambda_1 = \sqrt{2}$ (Skript, Seite 21).
Zeige für $\Lambda_8 := \mathcal{L}(\frac{1}{2}R_8)$, dass $\Lambda_8 = \Lambda_8^*$.

Bem.: Die Selbstdualität von Λ_8 erklärt, dass es keine Gram–Matrix $R_g^t R_g$ gibt mit derselben Form wie $R_i^t R_i$ für $i = 1, \ldots, 8$.