PROF. C. P. SCHNORR Wintersemester 2005/06

Gitter und Kryptographie

Blatt 9, 06.01.2006, Abgabe 13.01.2006

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: $[R_8, \mathbf{y}]^t[R_8, \mathbf{y}] \in \frac{1}{2}\mathbf{Z}$, $\|\mathbf{y}\| = 1$. Argumentiere wie in Lemma 2.2.3, Skript vom 04.01.06.

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. Vergleiche $\det R_9$ mit der Angabe $\lambda_9 = 512$ in Table 6.1 CONWAY, SLOANE.

Aufgabe 3. 1. Erläutere die Beziehung zwischen $\det R_n$ und λ_n in Tafel 6.1 CONWAY, SLOANE. Zeige für $n = 1, ..., 8$ dass $\det R_n$ dem Wert λ_n entspricht, $(\lambda_1, \ldots, \lambda_8) = (4, 12, 32, 64, 128, 192, 256, 256)$.

2. Erläutere die Grössen π_n, h_n in Tafel 6.1 von Conway, Sloane. Welchen Grössen der Matrix R_n entsprechen π_n, h_n ?

Aufgabe 4. Zeige mit der Gauss'schen Volumen-Heuristik:

$$|\gamma_n - \tfrac{n}{2e\pi}| = O(\ln n).$$

Hinweis: Skript, Seite 20 vom 04.01.06