Prof. C. P. Schnorr Sommersemester 2016

Gitter und Kryptographie

Blatt 3, 29.04.2016, Abgabe Freitag 06.05.2016

Aufgabe 1. Sei $\mathbf{R}_i$ die Untermatrix der ersten i Zeilen und Spalten von $\mathbf{R}_8$ (Skript Seite 21). Zeige mittels Lemma 2.2.3 dass $\lambda_1^2(\mathcal{L}(\mathbf{R}_i)) = 2$ für $i = 1, ..., 8$. Zeige die Übereinstimmung von $\lambda_1^2/\det(\mathbf{R}_i)^{2/i}$ mit den Werten γ_i der Tabelle 2.2.2.

Aufgabe 2. Sei $\mathbf{B}_i$ die Untermatrix der ersten i Zeilen und Spalten der Basis $\mathbf{B}_{24}$ des Leech-Gitters Zeige mitteLl Lemma 2.2.3 dass $\lambda_1^2(\mathcal{L}(\mathbf{B}_i)) \in 2\mathbb{N}$ für $i = 2, ..., 23$. Wie kommt man zu $\lambda_1^2(\mathcal{L}(\mathbf{B}_i)) \in 4\mathbb{N}$?

Aufgabe 3. Sei $\mathbf{B} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ aN & bN \end{bmatrix}$ Basismatrix mit $a, b, N \in \mathbb{Z}$. Zeige:

1. $\det \mathcal{L}(\mathbf{B}) = (1 + N^2(a^2 + b^2))^{1/2}$,
2. $\lambda_1(\mathcal{L}(\mathbf{B}))^2 \leq a^2 + b^2$
3. Für $N^2 > a^2 + b^2$ gilt für jede *Gauss-reduzierte* Basis $\mathbf{b}_1, \mathbf{b}_2$:

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

Hinweis zu 2. Es gilt $\pm(b, -a, \mathbf{0})^t \in \mathcal{L}(\mathbf{B})$. Benutze zu 3.: Der Eukl. Alg. löst $[a, b] \begin{bmatrix} c & d \\ e & f \end{bmatrix} = [0, \mathrm{ggT}(a, b)]$ so dass $c^2 + e^2, d^2 + f^2 \leq a^2 + b^2$.

Punktezahl $5, 5, 8$ **für Aufgabe** $1, 2, 3$