Prof. C. P. Schnorr Wintersemester 2015/16

Gitteralgorithmen zur Faktorisierung ganzer Zahlen

Blatt 1, 28.10.2015, Abgabe 11.11.2015

Entnehme γ_n der Tabelle 2.2.2, Seite 21 des Skripts zur Vorlesung Gitter und Kryptographie. Entnehme $\mathbf{R}_8$, $\mathbf{B}_{24}$ den Seiten 21, 22 des Skripts.

Aufgabe 1. Sei $\mathbf{R}_n \in \mathbb{R}^{n\times n}$ die Untermatrix der ersten n Zeilen und Spalten von $\mathbf{R}_8$. Zeige für $n = 4, 5, 6, 7, 8$: $\|\mathbf{b}_1\|^2 = 2 = \gamma_n(\det \mathbf{R}_n)^{\frac{2}{n}}$.
Zeige $\lambda_1(\mathcal{L}(\mathbf{R}_n))^2 = 2$ für $n = 1, \ldots, 8$ mittels Lemma 2.2.3 des Skripts.

Aufgabe 2. Sei $\mathbf{B}_8$ die Matrix der ersten 8 Zeilen und Spalten der Basis $\mathbf{B}_{24}$ zum Leech Gitter. Gebe 240 Vektoren $\mathbf{b}$ in $\mathcal{L}(\mathbf{B}_8)$ an mit $||\mathbf{b}|| = 2 = \lambda_1$. Begründe dass die Aufzählung vollständig ist.

Aufgabe 3. Beweise Kor. 4.1.5 des Skripts aus Satz 4.1.4, Lemma 4.1.2.
Zeige, dass für jede LLL–Basis gilt $\|\mathbf{b}_1\|/\lambda_1 \le \alpha^{\frac{n-1}{4}}/(\mathrm{rd}(\mathcal{L})\sqrt{\gamma_n})$.
Dabei sei $\mathrm{rd}(\mathcal{L}) = \lambda_1/(\sqrt{\gamma_n}(\det \mathcal{L})^{1/n})$ die relative Dichte des Gitters $\mathcal{L}$.

Aufgabe 4. Sei $\mathbb{A}_n = \mathcal{L}(\mathbf{B}_n) = \{(x_0, x_1, \cdots, x_n) \in \mathbb{Z}^{n+1} \mid \sum_{i=0}^{n} x_i = 0\}$

für $\mathbf{B}_n := \begin{bmatrix} -1 & 0 & 0 & \cdots & 0 \\ 1 & -1 & 0 & \cdots & 0 \\ 0 & 1 & -1 & \cdots & 0 \\ & & \cdots & \cdots & \\ 0 & 0 & \cdots & 1 & -1 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \in \mathbb{Z}^{(n+1)\times n}$.

Zeige durch Induktion über n dass $\det(\mathrm{GNF}(\mathbf{B}_n)) = \sqrt{n+1}$.

5 Punkte pro Aufgabe