Prof. C. P. Schnorr Wintersemester 2017/18

Gitteralgorithmen zur Faktorisierung ganzer Zahlen

Blatt 1, 23.10.2017, Abgabe 30.10.2017

Entnehme die Hermite-Konstante γ_n der Tabelle 2.2.2 auf Seite 21 des Skripts zu Gitter und Kryptographie und ebenso die Matrix $\mathbf{R}_8$ auf Seite 21.

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 $n = 4, 5, 6, 7, 8$: $\lambda_1^2 = 2 = \gamma_n(\det \mathbf{R}_n)^{2/n}$.
Damit sind die Gitter $\mathcal{L}(\mathbf{R}_n)$ kritisch. Benutze dass $\lambda_1(\mathcal{L}(\mathbf{R}_8))^2 = 2$.
(Dies folgt mit Lemma 2.2.3 des Skripts. 2 Zusatzpunkte für den Beweis)

Ein Gitter $\mathcal{L}$ der Dim n hat die Hermite-Invariante $\gamma(\mathcal{L}) = \lambda_1^2/(\det(\mathcal{L})^{2/n} = rd(\mathcal{L})^2\gamma_n$. $\mathcal{L}$ ist kritisch gdw $\gamma(\mathcal{L}) = \gamma_n$, also wenn $rd(\mathcal{L}) = 1$.

Aufgabe 2. Sei $\mathbf{R}_n$ die Untermatrix der ersten n Zeilen und Spalten der Basis $\mathbf{R}_{24}$ des Leech-Gitters (Skript S.22). Berechne die Hermite-Invarianten $\gamma(\mathcal{L}(\mathbf{R}_n))$ für $n = 8, 9, 10, 11, 12, 16, 20, 23, 24$. Für welche n wird der Maximalwert $\gamma(\mathcal{L}(\mathbf{R}_n))$ der Tabelle 2.2.3 (Skript Seite 24) erreicht ?

Aufgabe 3. Sei $\mathbf{R}'_n$ (bzw. $\mathbf{R}_n$) die Matrix der ersten n Zeilen, Spalten der Basis $\mathbf{R}_{24}$ des Leech-Gitters (bzw. der Matrix $\mathbf{R}_{10}$, Skript Seite 23).
Vergleiche die Werte $\gamma(\mathbf{R}_n), \gamma(\mathbf{R}'_n)$ für $n = 9, 10$ mit den Maximalwerten der Tabelle 2.2.3 (Skript Seite 24).

5 Punkte pro Aufgabe