Prof. C. P. Schnorr Sommersemester 2009

Gitter und Kryptographie

Blatt 3, 06.05.2009, Abgabe Mittwoch, 13.05.2009

Aufgabe 1. Sei $\mathcal{L} \subset \mathbb{R}^m$ Gitter der Dim. n und $\mathcal{B}_n(\mathbf{0}, r) \subset \text{span}(\mathcal{L})$ die n-dim. Kugel mit Mittelpunkt $\mathbf{0}$ und Radius r. Zeige

$$\lim_{r\to\infty} |\mathcal{L} \cap \mathcal{B}_n(\mathbf{0}, r)|/\text{vol}(\mathcal{B}_n(\mathbf{0}, r)) = \tfrac{1}{\det \mathcal{L}(B)}$$

d.h. $\det \mathcal{L}(B)$ ist der Kehrwert der Dichte der Gitterpunkte.

Hinweis: Satz 1.1.2 , Skript.

Aufgabe 2. Zeige, dass die Basis $B = \begin{bmatrix} 0 & 1/2 \\ 1 & \sqrt{3/4} \end{bmatrix}$ global extrem (kritisch) ist.

Aufgabe 3. Gib ein Verfahren an, das $A = A^t \in \mathbb{Z}^{3\times 3}$ derart in $A' = T^t A T$, $T \in \text{GL}_3(\mathbb{Z})$, reduziert, dass

1. $a'_{1,3} = 0$

2. $|a'_{1,2}| \le |a'_{1,1}|/2$, $|a'_{2,3}| \le |a'_{3,3}|/2$,, sofern $a'_{1,1}, a'_{3,3} \neq 0$.

Aufgabe 4. Seien $\mathcal{L}' \subset \mathcal{L}$ Gitter. Zeige die Äquivalenz folgender Aussagen:

1. $\text{span}(\mathcal{L}') \cap \mathcal{L} = \mathcal{L}'$.
2. Jede Basis von $\mathcal{L}'$ ist zu einer Basis von $\mathcal{L}$ erweiterbar.

Hinweis : Kap. 1.3 Skript.