Prof. C. P. Schnorr Wintersemester 2008/09

Kryptographie

Blatt 12, 23.01.2008, Abgabe 30.01.2009

Seien $b_1, b_2 \in \mathbb{R}^m$ linear unabhängig und $\mathcal{L} = b_1\mathbb{Z} + b_2\mathbb{Z}$ das Gitter mit Basis b_1, b_2. Die Menge aller Basen von $\mathcal{L}$ ist $[b_1, b_2]\mathrm{GL}_2(\mathbb{Z})$.

Aufgabe 1 Zeige: Es gibt eine „reduzierte" Basis b_1, b_2 von $\mathcal{L}$, so dass

$$\|b_1\| = \lambda_1,\ |\langle b_1, b_2\rangle| \leq \tfrac{1}{2}\ \|b_1\|^2.$$

Aufgabe 2 Zeige: Für jede reduzierte Basis $b_1, b_2 \in \mathbb{R}^2$ von $\mathcal{L} \subset \mathbb{R}^2$ mit Grundmasche $= \{r_1b_1 + r_2b_2 \mid 0 \leq r_1, r_2 \leq 1\} \subset \mathbb{R}^2$ gilt

1. $\det \mathcal{L} \leq \lambda_1 \cdot \lambda_2$.

2. $\lambda_1^2 \leq \sqrt{\frac{4}{3}} \det \mathcal{L}$

Hinweis: $\det \mathcal{L} = |\det[b_1, b_2]| = \mathrm{vol}$ (Grundmasche).