

Gitter und Kryptographie

Blatt 7, 30.11.2007, Abgabe 07.12.2007

Aufgabe 1. Löse $|\pi - \frac{p_1}{q}| \leq \frac{0.1}{q}$, $|e - \frac{p_2}{q}| \leq \frac{0.1}{q}$, $0 \leq q \leq 100$ durch Konstruktion eines kürzesten Gittervektors in $\mathcal{L}(B)$ zur ℓ_∞ -Norm,

$$B = \begin{bmatrix} 1 & e \\ & 1 & \pi \\ & & 0.001 \end{bmatrix}.$$

Def.: Die Vektoren $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathcal{L}$ heißen *paarweise reduziert*, wenn

1. $|\langle \mathbf{b}_i, \mathbf{b}_j \rangle| \|\mathbf{b}_j\|^{-2} \leq \frac{1}{2}$ für $1 \leq j < i \leq n$
2. $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \dots \leq \|\mathbf{b}_n\|$.

Aufgabe 2. Erweitere Alg. 1.4.2 (Skript) zur paarweise Reduktion von Basen $\mathbf{b}_1, \dots, \mathbf{b}_n$ auf beliebige (möglicherweise linear abhängige) $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathcal{L}$.

Zeige: Jedes Gitter \mathcal{L} hat eine paarweise reduzierte Basis.

Aufgabe 3. Zeige: der erweiterte Alg. 1.4.2. führt höchstens $\sum_{i=1}^n \|\mathbf{b}_i\|^2 / \varepsilon$ Reduktionsschritte $\mathbf{b}_i := \mathbf{b}_i - [r] \mathbf{b}_j$ mit $|r| \geq \frac{1}{2} + \varepsilon$ aus.

Ist kein solcher Reduktionsschritt ausführbar, dann gilt

$$|\langle \mathbf{b}_i, \mathbf{b}_j \rangle| \|\mathbf{b}_j\|^{-2} \leq \frac{1}{2} + \varepsilon \text{ für } 1 \leq j < i \leq n.$$

Aufgabe 4. Zeige: Es gibt paarweise reduzierte Basen $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3 \in \mathbb{R}^3$, so dass $\|\mathbf{b}_1\| / \|\mathbf{b}_1 - \mathbf{b}_2 + \mathbf{b}_3\|$ beliebig groß ist.

HINWEIS: Wähle $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$ so dass $\|\mathbf{b}_1\| = \|\mathbf{b}_2\| = \|\mathbf{b}_3\|$

$$\langle \mathbf{b}_1, \mathbf{b}_2 \rangle = \frac{1}{2} \approx \langle \mathbf{b}_2, \mathbf{b}_3 \rangle, \langle \mathbf{b}_1, \mathbf{b}_3 \rangle \approx -\frac{1}{2}.$$