Prof. C. P. Schnorr Wintersemester 2005/06

Gitter und Kryptographie

Blatt 12, 27.01.2006, Abgabe 03.02.2006

Sei $\tilde{\mathbf{s}}' := (\sqrt[p]{\ln a_1}/2, \ldots, \sqrt[p]{\ln a_k}/2, \alpha \ln b)^t \in \mathbf{R}^{k+1}$. Ferner sei $\tilde{\mathbf{L}}$ nach (5.1) [GM02] und $g := \prod_{i=1}^{k} a_i^{|z_i|}$ mit $z_i \in \mathbf{Z}$ wie im Beweis von Le 5.3, 5.4 [GM02].

Aufgabe 1. Zeige, dass für $\mathbf{z} \in \mathbf{Z}^k$ mit $b \le g \le b + b/\alpha$ gilt:

$$\|\tilde{\mathbf{L}}\mathbf{z} - \tilde{\mathbf{s}}'\|_p^p \le 2^{-p} \ln b + 2.$$

Hinweis: Beweis von Lemma 5.4 [GM02].

Konklusion. Für $\alpha = b^{(1-\varepsilon)}$ gilt einerseits

$$\lambda_1(\mathcal{L}(\tilde{\mathbf{L}})) > \lambda := \sqrt[p]{2(1-\varepsilon)\ln b}.$$

Andererseits gibt es viele Gitterpunkte mit Distanz

$$\le \tfrac{1}{2}\sqrt[p]{\ln b + 2 \cdot 2^p} \approx \lambda/(2\sqrt[p]{2}) \quad \text{zu} \quad \tilde{\mathbf{s}}',$$

sofern das Intervall $[b, b + b^{\varepsilon}]$ viele Produkte $\Pi_{i \in S} a_i$ mit $S \subset \{1, \ldots, k\}$ enthält, siehe [MG02], Seite 100, Mitte.

Aufgabe 2. Verifiziere, dass Lemma 4.3 (und somit Theorem 4.4) für alle $\gamma < 2\sqrt[p]{2}$ und nicht nur für $\gamma < \sqrt[p]{2}$ gilt.

Hinweis. Ersetze in [MG02] nur $\tilde{\mathbf{s}}$ in (5.4) durch $\tilde{\mathbf{s}}'$. Verifiziere dass die Beweise von Le 5.5, Cor 5.6, Thm 5.7, Le 5.11, Le 5.12, Thm 4.5 für $\gamma < 2\sqrt[p]{2}$ gültig bleiben.

Aufgabe 3. Sei $B \in \mathbf{R}^{k \times m}, \alpha \ne 0$. Zeige

$$\det(\alpha I_k + \tfrac{1}{\alpha} B B^t)\, \alpha^n = \det(\alpha I_n + \tfrac{1}{\alpha} B^t B)\, \alpha^k.$$

Hinweis.

$$\begin{bmatrix} \alpha I_k + \frac{1}{\alpha} B B^t & , & B \\ O & , & \alpha I_n \end{bmatrix} = \begin{bmatrix} \alpha I_k & , & B \\ -B^t & , & \alpha I_n \end{bmatrix} \begin{bmatrix} I_k & , & O \\ \frac{1}{\alpha} B^t & , & I_n \end{bmatrix}$$

$$\cong \begin{bmatrix} \alpha I_k & , & B \\ -B^t & , & \alpha I_n \end{bmatrix} \begin{bmatrix} I_k & , & -\frac{1}{\alpha} B \\ O & , & I_n \end{bmatrix} = \begin{bmatrix} \alpha I_k & , & O \\ -B^t & , & \alpha I_n + \frac{1}{\alpha} B^t B \end{bmatrix}.$$