Prof. C. P. Schnorr Wintersemester 2005/06

Gitter und Kryptographie

Blatt 3, 11.11.2005, Abgabe 18.11.2005

Aufgabe 1. Ändere die Micciancio-Vadhan Identifikation so ab, dass $\mathcal{V}$ ein zufälliges $q \in_R \{0, 1, \ldots, p-1\}$ wählt und in Schritt 4 prüft dass $\sum_{i=1}^{k} c_i = q \bmod p$. Wie verändern sich die Lemmata 1–3 von Blatt 1 so, dass ihr Sinn erhalten bleibt?

Aufgabe 2. Sei $\mathcal{L} \subset \mathbf{R}^m$ Gitter und $B(\mathbf{0}, r) \subset \mathrm{span}(\mathcal{L})$ die Kugel mit Mittelpunkt $\mathbf{0}$ und Radius r. Zeige

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

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

Aufgabe 3. Zwei Basen $\mathbf{b}_1, \mathbf{b}_2$ und $\mathbf{b}'_1, \mathbf{b}'_2$ heißen *äquivalent*, wenn entweder $\mathbf{b}_1 = \pm\mathbf{b}'_1, \mathbf{b}_2 = \pm\mathbf{b}'_2$ oder $\mathbf{b}_1 = \pm\mathbf{b}'_2, \mathbf{b}_2 = \pm\mathbf{b}'_1$.
Zeige: Bei der allgemeinen Gauss-Reduktion bleibt die Äquivalenz erhalten.

Aufgabe 4. (Worst Case Gitterbasis zur Gauss-Reduktion $\| \ \| = \| \ \|_2$)
Sei $\mathbf{b}_1, \mathbf{b}_2 \in \mathbf{R}^n$ eine reduzierte Basis und $[\mathbf{b}_k, \mathbf{b}_{k+1}] := [\mathbf{b}_1, \mathbf{b}_2] \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}^{k-1}$.
Zeige für $k = 2, 3, \ldots$:

1. $\lceil \frac{\langle \mathbf{b}_{k+1}, \mathbf{b}_k \rangle}{\langle \mathbf{b}_k, \mathbf{b}_k \rangle} \rfloor = 2, \ \|\mathbf{b}_k\| \le \|\mathbf{b}_{k+1}\|$.
2. Die Basis $\mathbf{b}_k, \mathbf{b}_{k+1}$ ist wohlgeordnet, und wird in einer Runde der Gauss-Reduktion in $\mathbf{b}_{k-1}, \mathbf{b}_k$ transformiert.

Hinweis : Satz 4.2.1 im Skript S.31 beweist, dass $[\mathbf{b}_k, \mathbf{b}_{k+1}]$ *minimale* k-te Vorängerbasis zu $\mathbf{b}_1, \mathbf{b}_2$ ist.