Prof. C. P. Schnorr Sommersemester 2009

Gitter und Kryptographie

Blatt 4, 13.05.2009, Abgabe Mittwoch, 20.05.2009

Aufgabe 1. Zeige: Für jede LLL–Basis $b_1, \ldots, b_n$ von $\mathcal{L}$ gilt:

1. $\|b_1\|^2 \leq \alpha^{n-1}(\det \mathcal{L})^{\frac{2}{n}}$.

2. $\prod_{i=1}^{n} \|b_i\|^2 \leq \alpha^{\binom{n}{2}}(\det \mathcal{L})^2$.

Aufgabe 2. (Worst Case Gitterbasis zur Gauss-Reduktion $\| \ \| = \| \ \|_2$)

Sei $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{R}^n$ 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. $\lceil \frac{\langle \mathbf{b}_{k+1}, \mathbf{b}_k \rangle}{\langle \mathbf{b}_k, \mathbf{b}_k \rangle} \rfloor = 2, \ \|\mathbf{b}_k\| \leq \|\mathbf{b}_{k+1}\|$.
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 3.2.1 im Skript beweist, dass $[\mathbf{b}_k, \mathbf{b}_{k+1}]$, *minimale* k-te Vorängerbasis zu $\mathbf{b}_1, \mathbf{b}_2$ ist.

Aufgabe 3. Sei p Primzahl mit $p = 1 \bmod 4$, $i^2 = -1 \mod p$ und $\mathcal{L}_p = \{(a, b)^t \in \mathbb{Z}^2 : \ a - ib = 0 \mod p\}$. Zeige:

1. $\det \mathcal{L}_p = p$,
2. Für den kürzesten Vektor $(a_0, b_0)^t \in \mathcal{L}_p \backslash \{\mathbf{0}\}$ gilt: $p = a_0^2 + b_0^2$,
3. Löse $269 = a_0^2 + a_1^2$ mit $a_0, a_1 \in \mathbb{N}$ mittels Gauss-Redukton.

Hinweis: Für $(a, b)^t \in \mathcal{L}_p$ gilt $a^2 + b^2 = 0 \mod p$. $\lambda_1^2 \leq \sqrt{\frac{4}{3}} \det \mathcal{L}_p$.

Aufgabe 4. Zeige $\gamma_4 \geq \sqrt{2}, \ \gamma_8 \geq 2$.

Benutze R_8 von S. 21 Skript und Lemma 2.2.3, sowie $\lambda_1^2 \leq \gamma_n (\det \mathcal{L})^{2/n}$.