

Gitter und Kryptographie

Blatt 2, 25.10.2007, Abgabe 02.11.2007

Aufgabe 1. Beweise Theorem 1 von [Hartung, Schnorr] für $t = 1$. Skizziere einen Algorithmus, der ein $\bar{S} \in \mathcal{O}(f_1)S$ berechnet, indem er $(\tilde{P}, \mathcal{V})_1$ im Mittel $(\varepsilon - 1/2)^{-1}$ mal ausführt. Gegeben sei \tilde{P} als resettable black box.

Zusatz: Wie geht der Beweis für $t = 2$?

Aufgabe 2. Gib ein Verfahren an, welches eine gegebene, reguläre ternäre Form f_A zu $f_{A'} = f_{AT}$ derart reduziert, dass

1. $a'_{1,3} = 0$,
2. $|a'_{1,2}| \leq |a'_{1,1}|/2$, $|a'_{2,3}| \leq |a'_{3,3}|/2$, sofern $a'_{1,1}, a'_{3,3} \neq 0$.

Aufgabe 3. Zeige, dass das Verfahren zu Aufgabe 2 pol. Zeit ist und entwickle eine Laufzeitschranke mit Analyse.

Aufgabe 4. Sei $B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ aN & bN \end{pmatrix}$ Basismatrix mit $a, b, N \in \mathbb{Z}$. Zeige:

1. $\det \mathcal{L} = (1 + N^2(a^2 + b^2))^{1/2}$,
2. Für $N > \left(\sqrt{\frac{4}{3}}(a^2 + b^2)\right)^{1/2}$ gilt für jede *reduzierte* Basis $\mathbf{b}_1, \mathbf{b}_2$:

$$\mathbf{b}_1 = \begin{pmatrix} * \\ * \\ 0 \end{pmatrix}, \quad \mathbf{b}_2 = \begin{pmatrix} * \\ * \\ N \cdot \text{ggT}(a, b) \end{pmatrix}.$$

Hinweis. Benutzen Sie dass :

$$\|\mathbf{b}_1\|^2 \leq \sqrt{\frac{4}{3}} \det \mathcal{L} = \sqrt{\frac{4}{3}} (\det B^t B)^{1/2} \text{ für jede reduzierte Basis } B = [\mathbf{b}_1, \mathbf{b}_2],$$

$$\text{ggT}(a, b) = \min\{|t_1 a + t_2 b| \mid (t_1, t_2) \in \mathbb{Z}^2 \setminus \mathbf{0}\} \text{ für } a, b \in \mathbb{Z}.$$