

Gitter und Kryptographie

Blatt 4, 09.11.2007, Abgabe 16.11.2007

Aufgabe 1. 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: Die allgemeine Gauss-Reduktion erhält die Äquivalenz.

Hinweis: Behandle erst $\|\cdot\|_2$, dann beliebige $\|\cdot\|$. Betrachte den Fall dass der Reduktionskoeffizient μ nicht eindeutig ist.

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

Sei $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{R}^n$ eine reduzierte Basis und $(\mathbf{b}_k, \mathbf{b}_{k+1}) := (\mathbf{b}_1, \mathbf{b}_2) \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^{k-1}$.

Zeige für $k = 2, 3, \dots$:

1. $\lceil \frac{\langle \mathbf{b}_{k+1}, \mathbf{b}_k \rangle}{\langle \mathbf{b}_k, \mathbf{b}_k \rangle} \rceil = 2, \|\mathbf{b}_k\| \leq \|\mathbf{b}_{k+1}\|$.
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 Vorrängerbasis zu $\mathbf{b}_1, \mathbf{b}_2$ ist.

Aufgabe 3. Sei p Primzahl mit $p \equiv 1 \pmod{4}$, $i^2 \equiv -1 \pmod{p}$ und

$\mathcal{L}_p = \{(a, b)^t \in \mathbb{Z}^2 : a - ib = 0 \pmod{p}\}$. Zeige:

1. $\det \mathcal{L}_p = p$,
2. Für den kürzesten Vektor $(a_0, b_0)^t \in \mathcal{L}_p \setminus \{\mathbf{0}\}$ 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-Reduktion.

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

Aufgabe 4. Seien $\mathcal{L}' \subset \mathcal{L}$ Gitter. Zeige die Äquivalenz folgender Aussagen:

1. $\text{span}(\mathcal{L}') \cap \mathcal{L} = \mathcal{L}'$.
2. Jede Basis von \mathcal{L}' ist zu einer Basis von \mathcal{L} erweiterbar.

Hinweis: Kap. 1.3 Skript.