Integer Points in Polyhedra

Spring 2009

Assignment Sheet 3

Exercise 1 (Well-ordered basis)
Let $b_1, b_2 \in \mathbb{Z}^2$ be a basis of two-dimensional lattice. Show that we can transform this basis, in constant time, into a well-ordered basis, i.e., basis b_1', b_2' satisfying

$$\|b_1'\| \leq \|b_2' - b_1'\| \leq \|b_2'\| \leq \|b_2' + b_1'\|.$$

Exercise 2 (Running time of the generalized Gauss algorithm)
Prove that the generalized Gauss reduction algorithm in $\mathbb{R}^2$ runs in polynomial time.

Exercise 3 (Closest vector in $\mathbb{R}^2$)
Describe an efficient algorithm that, provided a lattice $\Lambda \subseteq \mathbb{R}^2$ and a vector $v \in \mathbb{R}^2$, finds a lattice vector $z \in \Lambda$ with $\|z - v\|$ as small as possible.

Exercise 4 (Integral points in fundamental parallelepiped)
Let $b_1, b_2, \ldots, b_n$ be linearly independent integral vectors in $\mathbb{R}^n$. Show that the fundamental parallelepiped

$$P(b_1, b_2, \ldots, b_n) = \left\{ \sum_{i=1}^{n} \lambda_i b_i : 0 \leq \lambda_i < 1,\ i = 1, 2, \ldots, n \right\}$$

contains exactly $\det(b_1, b_2, \ldots, b_n)$ integral vectors.

Exercise 5 (Integral points in ellipsoids)
Given an algorithm computing the shortest lattice vector wrt $\|\cdot\|_2$, describe an algorithm to find an integral point in a given ellipsoid $\|Ax\|_2 \leq b$.