Homework 1
Due 2009/11/12

Oded Regev
School of Computer Science
Tel Aviv University

1. Consider the lattice $\mathcal{L}(b_1, b_2, b_3)$ where $b_1 = (2,0,0)^T$, $b_2 = (0,2,0)^T$, and $b_3 = (1,1,1)^T$. Find the successive minima in the l_1 norm and in the l_∞ norm. What are the vectors that achieve these minima?

2. Let $\Lambda = \mathcal{L}(b_1, \ldots, b_n)$ be some rank n lattice and let $\tilde{b}_1, \ldots, \tilde{b}_n$ be the Gram-Schmidt orthogonalization of $b_1, \ldots, b_n$.

   (a) Show that it is *not* true in general that $\lambda_n(\Lambda) \geq \max_i \|\tilde{b}_i\|$.

   (b) Show that for any $j = 1, \ldots, n$, $\lambda_j(\Lambda) \geq \min_{i=j,\ldots,n} \|\tilde{b}_i\|$.

3. (a) Show that any unimodular matrix $U \in \mathbb{Z}^{n \times n}$ can be transformed to the identity matrix by the following three basic column operations: $a_i \leftrightarrow a_j$, $a_i \leftarrow -a_i$, and $a_i \leftarrow a_i + k a_j$ for some integer k. Hint: Euclid's algorithm

   (b) Show that for any unimodular matrix $U \in \mathbb{Z}^{n \times n}$, U^{-1} is also a unimodular matrix in $\mathbb{Z}^{n \times n}$.

   (c) Show that two lattice bases $B_1, B_2 \in \mathbb{R}^{m \times n}$ are equivalent (i.e., $\mathcal{L}(B_1) = \mathcal{L}(B_2)$) if and only if one can be obtained from the other by a sequence of three basic column operations: $b_i \leftrightarrow b_j$, $b_i \leftarrow -b_i$, and $b_i \leftarrow b_i + k b_j$ for some integer k.

   (d) Describe a procedure that given any set of vectors $b_1, \ldots, b_n \in \mathbb{Z}^m$, finds a basis for the lattice $\mathcal{L}(b_1, \ldots, b_n)$ (notice that these vectors are not necessarily linearly independent and that in particular, n might be greater than m). There is no need to analyze the running time. Deduce that any set of vectors in $\mathbb{Z}^m$ spans a lattice.

   (e) Show that any finite set of vectors in $\mathbb{Q}^m$ spans a lattice. Show that this is not necessarily true for vectors in $\mathbb{R}^m$.

4. Find an analogue of Minkowski's First Theorem for the l_1 and l_∞ norms.

5. Give an efficient algorithm for each of the following tasks.

   (a) Given two bases $B_1, B_2 \in \mathbb{Z}^{m \times n}$, check if $\mathcal{L}(B_1) \subseteq \mathcal{L}(B_2)$, i.e., $\mathcal{L}(B_1)$ is a sublattice of $\mathcal{L}(B_2)$.

   (b) Given a basis B, check if $\mathcal{L}(B)$ is a *cyclic* lattice, where a lattice Λ is called cyclic if for every lattice vector $x \in \Lambda$, any cyclic rotation of the coordinates of x is also in Λ. For example, the lattice $\mathcal{L}(b_1, b_2, b_3)$ where $b_1 = (2,0,0)^T$, $b_2 = (0,2,0)^T$, and $b_3 = (1,1,1)^T$ is cyclic.