Homework 2
Due 2004/11/29

Oded Regev
Department of Computer Science
Tel Aviv University

1. Show that for any full-rank integer lattice Λ, $\det(\Lambda) \cdot \mathbb{Z}^n \subseteq \Lambda$.

2. (a) Describe a simple algorithm that given a basis $b_1, \ldots, b_n \in \mathbb{Q}^n$ of a full-rank lattice and a point $t \in \mathbb{Q}^n$, finds a point $x \in \mathcal{L}(b_1, \ldots, b_n)$ such that $\|x - t\| \leq \frac{1}{2}(\|b_1\| + \ldots + \|b_n\|)$.

   (b) Describe an improved algorithm that finds x such that $\|x-t\|^2 \leq \frac{1}{4}(\|b_1\|^2 + \ldots + \|b_n\|^2)$. Hint: try to show this first without the $\frac{1}{4}$ factor

3. (a) For all large enough $n \in \mathbb{Z}$, find an n-dimensional full-rank lattice in which the successive minima $v_1, \ldots, v_n$ (in the l_2 norm) do not form a basis of the lattice. Hint: Cesium Chloride

   (b) Show that for any 2-dimensional full-rank lattice Λ, the successive minima v_1, v_2 *do* form a basis of Λ. Hint: consider the lattice obtained by projecting Λ on the one-dimensional subspace $\{v_1\}^\perp$ and show that the projection of v_2 must be a basis of this lattice

   (c) Among all 2-dimensional full-rank lattices with $\lambda_1(\Lambda) = 1$, which one has the smallest $\det \Lambda$? (this lattice is unique up to rotation). Can you guess which 3-dimensional lattice with $\lambda_1(\Lambda) = 1$ has the smallest $\det \Lambda$? (no proof necessary for this)

4. Show that a δ-LLL reduced basis $b_1, \ldots, b_n$ of a lattice Λ with $\delta = \frac{3}{4}$ satisfies the following properties.

   (a) $\|b_1\| \leq 2^{(n-1)/4}(\det \Lambda)^{1/n}$

   (b) For any $1 \leq i \leq n$, $\|b_i\| \leq 2^{(i-1)/2}\|\tilde{b_i}\|$

   (c) $\Pi\|b_i\| \leq 2^{n(n-1)/4} \det \Lambda$
   Remark: the quantity $\Pi\|b_i\|/\det \Lambda$ is known as the *orthogonality defect* of the basis; to see why, notice that it is 1 iff the basis is orthogonal; it can never be less than one by Hadamard's inequality.

   (d) For any $1 \leq i \leq j \leq n$, $\|b_i\| \leq 2^{(j-1)/2}\|\tilde{b_j}\|$

   (e) For any $1 \leq i \leq n$, $\lambda_i(\Lambda) \leq 2^{(i-1)/2}\|\tilde{b}_i\|$

   (f) For any $1 \leq i \leq n$, $\lambda_i(\Lambda) \geq 2^{-(n-1)/2}\|b_i\|$

   (g) Let i be such that $\|b_i\|$ is maximal. Let H be $\mathrm{span}\{\mathrm{b_1}, \ldots, \mathrm{b_{i-1}}, \mathrm{b_{i+1}}, \ldots, \mathrm{b_n}\}$. Show that $2^{-n(n-1)/4}\|b_i\| \leq \mathrm{dist}(H, b_i) \leq \|b_i\|$. Hint: use (c)