Lattices and Homomorphic Encryption, Spring 2013	Instructors: Shai Halevi, Tal Malkin

Problem Set #1

January 22, 2013 — Due February 5, 2013

1. Consider the following 2×3 matrix,

$$A = \begin{pmatrix} 2 & 1 & 2 \\ 2 & 3 & 0 \end{pmatrix},$$

and the set $\mathcal{L}(A) = \{Ax : x \in \mathbb{Z}^3\} \subset \mathbb{R}^2$. Is $\mathcal{L}(A)$ a lattice? If so, find a basis for it, its determinant, its successive minima and vectors that relize them.

2. Prove or disprove: for every 2×3 matrix A, the set $\mathcal{L}(A) = \{Ax : x \in \mathbb{Z}^3\} \subset \mathbb{R}^2$ is a lattice.

3. Let $\mathcal{L} = \mathcal{L}(b_1, \ldots, b_n) \in \mathbb{R}^n$ be a full-rank lattice and let $\tilde{b}_1, \ldots, \tilde{b}_n$ be the Gram-Schmidt orthogonalization $b_1, \ldots, b_n$.

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

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

4. A subset of the Euclidean space $\mathcal{L} \subset \mathbb{R}^n$ is called *discrete* if there exists $\epsilon > 0$ such that the distance between any two points in $\mathcal{L}$ is at least ϵ. Prove that every discrete additive subset $\mathcal{L} \subset \mathbb{R}^n$ that spans the entire space $\mathbb{R}^n$ is a full-rank lattice with a basis.

Hint. Construct a basis $b_1, \ldots, b_n$ for $\mathcal{L}$ inductively such that the following property holds for each i: If F_i is the linear span of $b_1, \ldots, b_i$ then every point $u \in \mathcal{L} \cap F_i$ is an integer linear combination of $b_1, \ldots, b_i$.

5. Let $A \in \mathbb{Z}^{m \times n}$ be a (not necessarily square) integer matrix, and let $q \in \mathbb{Z}$ be an integer larger than one. Prove that the set $S = \{x \in \mathbb{Z}^n : Ax \equiv 0 \pmod{q}\}$ is a full-rank lattice.