2nd Bar-Ilan Winter School on Cryptography
Lattice-Based Cryptography and Applications: Day 1 Assignments

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 (finite) 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.

6. Show that for any lattice Λ that is contained in $\mathbb{Z}^n$, $\det(\Lambda) \cdot \mathbb{Z}^n \subseteq \Lambda$.

7. (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)

8 Prove that decision-LWE with multiple independent secrets is no easier than LWE with a single secret. More formally, show that distinguishing independent tuples

$$(\mathbf{a} \leftarrow \mathbb{Z}_q^n, b_1 = \langle \mathbf{a}, \mathbf{s}_1 \rangle + e_1, \ldots, b_w = \langle \mathbf{a}, \mathbf{s}_w \rangle + e_w)$$

from uniformly random, where $w = \text{poly}(n)$ is arbitrary, the secrets $\mathbf{s}_j$ are drawn independently from any (efficiently sampleable) distribution D, and the error terms e_i are drawn independently from any (efficiently sampleable) distribution χ, is no easier than distinguishing independent pairs $(\mathbf{a}, b = \langle \mathbf{a}, \mathbf{s} \rangle + e)$ from uniform, where $\mathbf{s}$ is drawn from D and the error terms e are drawn from χ.

9 (a) Prove that for sufficiently large m, the "inhomogeneous" SIS problem of finding a short solution to $\mathbf{A}\mathbf{x} = \mathbf{u}$, where both $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and $\mathbf{u} \in \mathbb{Z}_q^n$ are uniformly random, is no easier than solving the homogeneous SIS problem (of finding a short nonzero solution to $\mathbf{A}\mathbf{x} = \mathbf{0}$). *Hint*: consider the inhomogeneous problem with dimension $m' = m - 1$.

(b) Prove the above statement where the matrix $\mathbf{A}$ is exactly the same in both problems. *Hint*: use the fact that for $m \geq Cn \lg q$ where $C > 1$ is any fixed constant, the pair $(\mathbf{A}, \mathbf{A}\mathbf{x})$ is uniformly random when $\mathbf{x}$ is drawn uniformly from $\{0, 1\}^m$, and allow the homogeneous solution to be slightly longer than the inhomogeneous one.

10 Prove that if the columns of a parity-check matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ generate all of $\mathbb{Z}_q^n$, i.e., if $\mathbf{A} \cdot \mathbb{Z}^m = \mathbb{Z}_q^n$, then $\det(\Lambda^\perp(\mathbf{A})) = q^n$. More generally, prove that $\det(\Lambda^\perp(\mathbf{A})) = |G|$, where G is the subgroup of $\mathbb{Z}_q^n$ generated by the columns of $\mathbf{A}$. *Hint:* use the fact that for an m-dimensional integer lattice Λ, $\det(\Lambda) = |\mathbb{Z}^m / \Lambda|$, the number of distinct integer cosets of Λ.