Exercise 1 (Fun with lattices - 20 pts)

1. Construct an explicit basis for the lattice \( \{ x \in \mathbb{Z}^n : x_1 + \sum_{i=2}^n a_i x_i \equiv 0 \text{ (mod } p) \} \), where \( a_i \in \mathbb{Z}/p\mathbb{Z}, \) \( p \) a prime.

2. For all large enough \( n \in \mathbb{Z} \), find an \( n \)-dimensional full-rank lattice \( \mathcal{L} \) in which vectors \( v_1, \ldots, v_n \) achieving the successive minima, i.e. \( \| v_i \| = \lambda_i(\mathcal{L}) \forall i \in [n] \), do not form a basis of \( \mathcal{L} \). (Hint: Cesium Chloride).

Exercise 2 (Lattice Point Counting - 40pts)

Let \( \mathcal{L} \subseteq \mathbb{R}^n \) be a full-rank lattice. For \( \epsilon \in (0,1) \), set \( r = \mu(\mathcal{L})/\epsilon \). The goal of this exercise is to prove the following:

\[
\frac{(1-\epsilon)^n \text{vol}(rB_2^n)}{\text{det}(\mathcal{L})} \leq |\mathcal{L} \cap rB_2^n| \leq \frac{(1+\epsilon)^n \text{vol}(rB_2^n)}{\text{det}(\mathcal{L})}.
\]

Let \( \mathcal{V} \) denote the Voronoi cell of \( \mathcal{L} \).

1. Show that \( \mathcal{L} \cap rB_2^n + \mathcal{V} \subseteq (1+\epsilon)rB_2^n \). Use this to deduce the upper bound.

2. Show that \( (1-\epsilon)rB_2^n \subseteq \mathcal{L} \cap rB_2^n + \mathcal{V} \). Use this to deduce the lower bound.

Exercise 3 (CVP using a dual HKZ basis - 40pts)

Let \( f(n) \) be the smallest number s.t. \( \mu(\Lambda)\lambda_1(\Lambda^*) \leq f(n) \) for any \( n \)-dimensional lattice \( \Lambda \). Recall that in class we proved that \( f(n) = O(n^{3/2}) \).

Let \( \mathcal{L} \subseteq \mathbb{R}^n \) be an \( n \)-dimensional lattice. Assume we are given a basis \( B = (b_1, \ldots, b_n) \) such that \( D = (b^*_n, \ldots, b^*_1) \) is a HKZ-reduced basis for \( \mathcal{L}^* \), where \( B^* = (b^*_1, \ldots, b^*_n) \) is the dual basis of \( B \). Recall that \( D \) is HKZ-reduced for \( \mathcal{L}^* \), if it is size-reduced and if \( \forall i \in [n], \|d_i\| = \lambda_1(\pi_{\text{span}(d_i, \ldots, d_{i+1})})(\mathcal{L}^*) \).

The goal of this exercise is to use \( B \) to give an enumeration based CVP algorithm for \( \mathcal{L} \).

1. Let \( t \in \mathbb{R}^n \) be a target. Fix \( c_{n-k+1}, \ldots, c_n \in \mathbb{Z} \) for \( 0 \leq k < n \). Pick

\[
y^k \in \text{argmin}\{\|y - t\| : y = Bz, z \in \mathbb{Z}^n, z_j = c_j \forall j \in \{n-k+1, \ldots, n\}\}.
\]

(note that \( y_0 \) is simply a closest vector in \( \mathcal{L} \) to \( t \).) Express \( y^k = Bz^k, z^k \in \mathbb{Z}^n \), and let

\[
p_{n-k} := \frac{\langle b_{n-k}, t - \sum_{i=n-k+1}^n c_i b_i \rangle}{\| b_{n-k} \|^2},
\]

Using the above notation, show that \( z^k_{n-k} \in [p_{n-k} - f(n-k), p_{n-k} + f(n-k)] \cap \mathbb{Z} \).

2. Use the previous part to give an enumeration based algorithm which uses \( B \) to find the closest lattice vector to \( t \) in \( 2^{O(n)} \prod_{i=1}^n f(i) \) time.