Exercise 1 (Fun with lattices - 20 pts)

1. Construct an explicit basis for the lattice $\{\mathbf{x} \in \mathbb{Z}^n : x_1 + \sum_{i=2}^n a_i x_i \equiv 0 \pmod{p}\}$, 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 $\mathbf{v}_1, \dots, \mathbf{v}_n$ achieving the successive minimina, i.e. $\|\mathbf{v}_i\| = \lambda_i(\mathcal{L})\ \forall i \in [n]$, 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 $\varepsilon \in (0,1)$, set $r = \mu(\mathcal{L})/\varepsilon$. The goal of this exercise is to prove the following:

$$\frac{(1-\varepsilon)^n \mathrm{vol}(r\mathcal{B}_2^n)}{\det(\mathcal{L})} \leq |\mathcal{L} \cap r\mathcal{B}_2^n| \leq \frac{(1+\varepsilon)^n \mathrm{vol}(r\mathcal{B}_2^n)}{\det(\mathcal{L})} .$$

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

1. Show that $\mathcal{L} \cap r\mathcal{B}_2^n + \mathcal{V} \subseteq (1+\varepsilon)r\mathcal{B}_2^n$. Use this to deduce the upper bound.

2. Show that $(1-\varepsilon)r\mathcal{B}_2^n \subseteq \mathcal{L} \cap r\mathcal{B}_2^n + \mathcal{V}$. 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 Λ. 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 $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ such that $\mathbf{D} = (\mathbf{b}_n^*, \dots, \mathbf{b}_1^*)$ is an HKZ-reduced basis for $\mathcal{L}^*$, where $\mathbf{B}^* = (\mathbf{b}_1^*, \dots, \mathbf{b}_n^*)$ is the dual basis of $\mathbf{B}$. Recall that $\mathbf{D}$ is HKZ-reduced for $\mathcal{L}^*$, if it is size-reduced and if $\forall i \in [n]$, $\|\widetilde{\mathbf{d}}_i\| = \lambda_1(\pi_{\mathrm{span}(\mathbf{d}_1,\dots,\mathbf{d}_{i-1})^\perp}(\mathcal{L}^*))$.

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

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

$$\mathbf{y}^k \in \mathrm{argmin}\{\|\mathbf{y} - \mathbf{t}\| : \mathbf{y} = \mathbf{B}\mathbf{z}, \mathbf{z} \in \mathbb{Z}^n, z_j = c_j\ \forall j \in \{n-k+1, \dots, n\}\} .$$

   (note that $\mathbf{y}_0$ is simply a closest vector in $\mathcal{L}$ to $\mathbf{t}$.) Express $\mathbf{y}^k = \mathbf{B}\mathbf{z}^k$, $\mathbf{z}^k \in \mathbb{Z}^n$, and let

$$p_{n-k} := \frac{\langle \widetilde{\mathbf{b}}_{n-k}, \mathbf{t} - \sum_{i=n-k+1}^n c_i \mathbf{b}_i \rangle}{\|\widetilde{\mathbf{b}}_{n-k}\|^2} ,$$

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

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