1. **Properties of Voronoi Cell.** For a full-rank lattice $\mathcal{L} \subseteq \mathbb{R}^n$, let

$$\mathcal{V} = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\|_2 \leq \|\mathbf{x} - \mathbf{y}\|_2 \ \forall \mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}\}$$

denote its Voronoi cell. For $\mathbf{x} \in \mathbb{R}^n$, let $\mathrm{CVP}(\mathcal{L}, \mathbf{x})$ denote the *set* of closest lattice vectors to $\mathbf{x}$ under the Euclidean norm.

   (a) Show that $\mathbf{x} \in \mathcal{V} \Leftrightarrow \mathbf{0} \in \mathrm{CVP}(\mathcal{L}, \mathbf{x})$.

   (b) For $\mathbf{y} \in \mathbb{R}^n \setminus \{\mathbf{0}\}$, let $H_{\mathbf{y}}^{=(\leq,<)} = \{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{y} \rangle = (\leq, <)\ \frac{1}{2}\langle \mathbf{y}, \mathbf{y} \rangle\}$.
   Show that $\mathcal{V} = \bigcap_{\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}} H_{\mathbf{y}}^{\leq}$. Deduce that $\mathcal{V}$ is convex and symmetric.

   (c) Let $\lambda_1 = \lambda_1(\mathcal{L})$ and $\mu = \mu(B_2^n, \mathcal{L})$. Show that $\frac{1}{2}\lambda_1 B_2^n \subseteq \mathcal{V} \subseteq \mu B_2^n$. Deduce that

$$\mathcal{V} = \bigcap_{\substack{\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\} \\ \|\mathbf{y}\|_2 \leq 2\mu}} H_{\mathbf{y}}^{\leq} \quad (\mathcal{V} \text{ is defined by finitely many inequalites - i.e. a polytope}).$$

   (Hint: let r denote a ray through $\mathbf{0}$ and let $H_{\mathbf{y}}^{\leq}$ be the first halfspace that r crosses, how big can $\|\mathbf{y}\|_2$ be?)

   (d) Let $S = \mathcal{L} \cap 2\mu B_2^n \setminus \{\mathbf{0}\}$. For $\mathbf{v} \in S$, show that if $\mathcal{V} \neq \cap_{\mathbf{y} \in S \setminus \{\mathbf{v}\}} H_{\mathbf{y}}^{\leq}$ then $H_{\mathbf{v}}^{=} \cap \mathcal{V}$ is $n-1$ dimensional (known as a facet of $\mathcal{V}$). Deduce that

$$\mathcal{V} = \bigcap \{H_{\mathbf{y}}^{\leq} : \mathbf{y} \in S, H_{\mathbf{y}}^{=} \cap \mathcal{V} \text{ a facet of } \mathcal{V}\}.$$

   (Hint: Take a point $\mathbf{p} \in \cap_{\mathbf{y} \in S \setminus \{\mathbf{v}\}} H_{\mathbf{y}}^{\leq} \setminus \mathcal{V}$ and examine where the line from $\mathbf{0}$ to $\mathbf{p}$ intersects $H_{\mathbf{v}}^{=}$.)

   (e) We say that $\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}$ is *Voronoi relevant* if $H_{\mathbf{y}}^{=} \cap \mathcal{V}$ is a facet of $\mathcal{V}$. Let $\mathrm{VR}(\mathcal{L})$ denote the set of Voronoi relevant vectors. Show that $\mathbf{y} \in \mathrm{VR}(\mathcal{L})$ if and only if $\mathrm{CVP}(\mathcal{L}, \mathbf{y}/2) = \{\mathbf{0}, \mathbf{y}\}$.
   (Hint: Show that if there exists $\mathbf{z} \in \mathrm{CVP}(\mathcal{L}, \mathbf{y}/2) \setminus \{\mathbf{0}, \mathbf{y}\}$, then either $H_{\mathbf{y}}^{=} \cap \mathcal{V} = \emptyset$ or $H_{\mathbf{y}}^{=} \cap \mathcal{V} \subseteq H_{\mathbf{z}}^{=} \cap H_{\mathbf{y}-\mathbf{z}}^{=}$)

   (f) Show that for any $\mathbf{z} \in \mathcal{L}$ and target $\mathbf{x} \in \mathbb{R}^n$, either $\mathbf{z} \in \mathrm{CVP}(\mathcal{L}, \mathbf{x})$ or there exists $\mathbf{y} \in \mathrm{VR}(\mathcal{L})$ such that $\|(\mathbf{z} - \mathbf{y}) - \mathbf{x}\|_2 < \|\mathbf{z} - \mathbf{x}\|_2$.
   (Hint: Use part (a),(d) and (e).)

   (g) Let $<_{\mathrm{lex}}$ denote the standard lexicographic ordering in $\mathbb{R}^n$ (i.e., $(x_1, \ldots, x_n) <_{\mathrm{lex}} (y_1, \ldots, y_n)$ iff $x_1 < y_1$ or $x_1 = y_1$ and $(x_2, \ldots, x_n) <_{\mathrm{lex}} (y_2, \ldots, y_n)$). Let

$$\mathcal{V}_{tile} = \mathcal{V} \ \cap \bigcap_{\substack{\mathbf{y} \in \mathcal{L} \\ \mathbf{0} <_{\mathrm{lex}} \mathbf{y}}} H_{\mathbf{y}}^{<}.$$

   Show that for any $\mathbf{x} \in \mathbb{R}^n$, $(\mathcal{L} + \mathbf{x}) \cap \mathcal{V}_{tile}$ is a set containing just one element which is the lexicographically minimal shortest vector in $\mathcal{L} + \mathbf{x}$. Deduce that $\mathcal{V}_{tile}$ is a fundamental domain and that $\mathrm{vol}_n(\mathcal{V}) = \det(\mathcal{L})$.

2. **Lattice Point Bounds.**

   (a) Show that for any $C \geq 1$, one can construct a lattice $\mathcal{L} \subseteq \mathbb{R}^2$, $\det(\mathcal{L}) = 1$, such that $|\mathcal{L} \cap B_2^2| \geq C$.

   (b) Let $A \subseteq \mathbb{R}^n$ be any measurable set and let $\mathcal{L} \subseteq \mathbb{R}^n$ be an n-dimensional lattice. Show that

   $$\mathop{\mathrm{E}}_{X}[|A \cap (\mathcal{L} + X)|] = \frac{\mathrm{vol}_n(A)}{\det(\mathcal{L})}$$

   where X is chosen uniformly from $\mathbb{R}^n/\mathcal{L}$ (equivalently, uniformly from any fundamental domain). Deduce that

   $$\max_{\mathbf{x} \in \mathbb{R}^n} |(A + \mathbf{x}) \cap \mathcal{L}| \geq \frac{\mathrm{vol}_n(A)}{\det(\mathcal{L})}.$$

   (c) Let $K \subseteq \mathbb{R}^n$ be a centrally symmetric convex body. Show that $|K \cap \mathcal{L}| \geq 2^{-n} \frac{\mathrm{vol}_n(K)}{\det(\mathcal{L})}$ (Hint: extend proof of Minkowski's First Theorem)

   (d) Let $\mathcal{V} = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\|_2 \leq \|\mathbf{x} - \mathbf{y}\|_2 \ \forall \mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}\}$ denote the Voronoi cell of $\mathcal{L}$. Show that $rB_2^n + \mathcal{L} = (rB_2^n \cap \mathcal{V}) + \mathcal{L}$. Show that for any $r > 0$,

   $$\frac{\mathrm{vol}_n(rB_2^n)}{\mathrm{vol}_n(rB_2^n \cap \mathcal{V})} \leq \max_{\mathbf{x} \in \mathbb{R}^n} |(rB_2^n + \mathbf{x}) \cap \mathcal{L}| \leq 2^n \frac{\mathrm{vol}_n(rB_2^n)}{\mathrm{vol}_n(rB_2^n \cap \mathcal{V})}.$$

   (Hint: extend proof of the Gaussian Heuristic from last lecture).

3. **Minkowski SVP.**

   (a) As a warmup, recall that there are n-dimensional lattices $\mathcal{L}$ in which $\lambda_1(\mathcal{L})$ is arbitrarily smaller than $\det(\mathcal{L})^{1/n}$ (already for $n = 2$).

   (b) Assume we are given an oracle MinkowskiSVP that on a k-dimensional lattice $\mathcal{L}$ outputs a vector $\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}$, such that $\|\mathbf{y}\|_2 \leq \gamma \det(\mathcal{L})^{1/k}$, for some $\gamma \geq 1$.
   Examine the following algorithm:

   Require: n-dimensional lattice $\mathcal{L} \subseteq \mathbb{R}^n$.
   $\mathcal{L}_1 \leftarrow \mathcal{L}$
   for $i = 1$ **to** n **do**
   $\mathbf{x}_i \leftarrow \text{MinkowskiSVP}(\mathcal{L}_i)$
   $\mathbf{y}_i \leftarrow \text{MinkowskiSVP}(\mathcal{L}_i^*)$
   $\mathcal{L}_{i+1} \leftarrow \mathcal{L}_i \cap \mathbf{y}_i^{\perp}$
   return shortest vector among $\mathbf{x}_1, \ldots, \mathbf{x}_n$.

   Show that the algorithm returns a non-zero vector of length at most $\gamma^2 \lambda_1(\mathcal{L})$.
   (Hint: take a shortest non-zero vector $\mathbf{v}$ of $\mathcal{L}$ and examine the first time $\mathbf{v} \notin \mathcal{L}_i$)