Exercise 1 (Mordell's Inequality)
The goal of this exercise is to prove Mordell's inequality: $\gamma_n \leq \gamma_{n-1}^{\frac{n-1}{n-2}}$, for $n \geq 2$.

Let $\mathcal{L} \subset \mathbb{R}^n$ be a full rank lattice.

1. For any $\mathbf{y} \in \mathcal{L}^* \setminus \{\mathbf{0}\}$, who show that $\det(\mathcal{L} \cap \mathbf{y}^\perp) = \det(\mathcal{L})\|\mathbf{y}\|$.
2. Show that $\min\{\det(M) : M \subseteq \mathcal{L} \text{ rank } n-1 \text{ sublattice } \} \leq \gamma_n^{1/2}\det(\mathcal{L})^{\frac{n-1}{n}}$.
   (Hint: Apply the n-dimensional Hermite bound on $\mathcal{L}^*$ and use the first part.)
3. Apply the $n-1$-dimensional Hermite bound to the minimizer M_{opt} above to deduce Mordell's inequality.

Exercise 2 (Exact Enumeration in a Ball)
Show how to modify the $\text{Enum}(\mathbf{B}, \mathbf{t}, r)$ algorithm so that it exactly returns the points in $\mathcal{L}(\mathbf{B}) \cap (\mathbf{t} + r\mathcal{B}_2^n)$. As done in class, the algorithm returns a strict superset of these points.

Exercise 3 (CVP via LLL)
Given an LLL-reduced basis $\mathbf{B} \in \mathbb{R}^{n \times n}$ for $\mathcal{L}$, given an enumeration based algorithm to solve CVP in $2^{O(n^2)}$ time.
(Hint: Once you've fixed the coefficients for $\mathbf{b}_{n-k+1}, \ldots, \mathbf{b}_n$, show that the effective enumeration radius can be reduced to $\frac{1}{2}\sqrt{\sum_{i=1}^{n-k}\|\widetilde{\mathbf{b}}_i\|^2}$.)