Problem Set 3
CSE 599S - Lattices
Winter 2023

Exercise 1.5 (10pts)
Let $\Lambda \subseteq \mathbb{R}^n$ be a full rank lattice. Show that $\lambda_1(\Lambda) \cdot \lambda_n(\Lambda^*) \geq 1$, where $\Lambda^*$ is the dual lattice.

Exercise 1.6 (10pts)
Prove that for any lattice $\Lambda \subseteq \mathbb{R}^n$, one has $\lambda_1(\Lambda) \cdot \lambda_1(\Lambda^*) \leq n$.

Remark 1: You will need a fact that we will see in the Monday, Jan 23 lecture.

Remark 2: A stronger theorem of Banaszczyk that we will see in Chapter 4 shows that even $\lambda_1(\Lambda) \cdot \lambda_n(\Lambda^*) \leq n$. This has an important consequence. Consider the following computational problem: Given a lattice $\Lambda$ and a parameter $K$, distinguish the cases $\lambda_1(\Lambda) \leq L$ and $\lambda_1(\Lambda) > n \cdot L$. The consequence of this exercise is that this problem is in $\text{NP} \cap \text{coNP}$ in the sense that one can give an efficiently checkable proof for $\lambda_1(\Lambda) \leq L$ (simply give me a short vector) and one can also certify is $\lambda_1(\Lambda) > n \cdot L$ (give me the short dual basis). The remarkable fact is that this gap problem is not known to be in $\text{P}$.

Exercise 1.12 (10pts)
Let $\Lambda \subseteq \mathbb{R}^n$ be a full rank lattice and let $B \in \mathbb{R}^{n \times n}$ be an LLL-reduced basis for $\Lambda$. Prove that for all $i \in \{1, \ldots, n\}$ one has $\|b_i\|_2 \leq 2^{(n+1)/2} \lambda_i(\Lambda)$.

Hint. You may use following observation: Consider an LLL-reduced $B = (b_1, \ldots, b_n)$ and for some index $i \in \{1, \ldots, n\}$, define the subspace $U := \text{span}\{b_1, \ldots, b_{i-1}\}$ and let $\tilde{b}_j := \Pi_{U^\perp}(b_j)$ where $\Pi_{U^\perp}$ denotes the projection into the subspace $U^\perp$. Then $\tilde{b}_i, \ldots, \tilde{b}_n$ is an LLL-reduced basis for the lattice $\tilde{\Lambda} := \{\sum_{j=i}^n y_j \tilde{b}_j : y_j \in \mathbb{Z}\}$. 