1. **Dual Bounds on** $\lambda_1$: Let $L \subseteq \mathbb{R}^n$ be a $k$-dimensional lattice.

   (a) Let $v_1^*, \ldots, v_k^* \in L^*$ be linearly independent vectors. Show that
   \[
   \lambda_1(L) \geq \min_{1 \leq i \leq k} \frac{1}{\|v_i^*\|_2}
   \]
   where $\tilde{v}_1^*, \ldots, \tilde{v}_k^*$ are the Gram-Schmidt orthogonalization.

   (b) Let $b_1, \ldots, b_k$ be a basis for $L$, and let $b_1^*, \ldots, b_k^* \in L^*$ denote the associated dual basis (i.e. $\langle b_i^*, b_j \rangle = \delta_{ij}$ for $i, j \in [k]$). Define the sequence $b_1^{*,r}, \ldots, b_k^{*,r}$ to be the sequence $b_1^*, \ldots, b_k^*$ in reverse order. Let $\tilde{b}_1, \ldots, \tilde{b}_k$ and $\tilde{b}_1^{*,r}, \ldots, \tilde{b}_k^{*,r}$ denote the Gram Schmidt orthogonalizations of the associated sequences (note that the second gso is with respect to the dual basis in reverse order). Show the sequences $\tilde{b}_k / \|\tilde{b}_k\|_2, \ldots, \tilde{b}_1 / \|\tilde{b}_1\|_2$ and $\tilde{b}_1^{*,r}, \ldots, \tilde{b}_k^{*,r}$ are equal.

   (c) Deduce that the above bound on $\lambda_1(L)$ is equivalent to that of Lemma 4 of Lecture 1.

2. **Structure of Additive Subgroups**: Let $G \subseteq \mathbb{R}^n$ be an additive subgroup of dimension $n$.

   (a) Let $v_1, \ldots, v_k \in G$ be linearly independent vectors. Show that for any $x \in \text{span}(v_1, \ldots, v_k)$, there exists $y \in G \cap \text{span}(v_1, \ldots, v_k)$ such that $\|x - y\|_2 \leq \frac{1}{2} \sum_{i=1}^k \|v_i\|_2$.

   (b) Let $W = \cap_{\varepsilon > 0} \text{span}(G \cap \mathbb{Z}^n_\varepsilon)$. Show that $G \cap W$ is dense in $W$, i.e. for all $x \in W$ and $\varepsilon > 0$ there exists $y \in G \cap W$ such that $\|x - y\|_2 \leq \varepsilon$.

   (c) For $W$ as above, show that $\pi_{W^\perp}(G)$ is a lattice.

   (d) For $W$ as above, show that $G^* \subseteq W^\perp$. Deduce that $G^* = \pi_{W^\perp}(G)^*$ and that $\dim(G^*) = \dim(\pi_{W^\perp}(G))$.

   (e) **Kronecker’s Diophantine Approximation Theorem.** Take a vector $x = (x_1, \ldots, x_n)^t \in \mathbb{R}^n$ such that $x_1, \ldots, x_n$ are linearly independent over the rationals, i.e.
   \[
   \sum_{i=1}^n \alpha_i x_i = 0, \alpha_1, \ldots, \alpha_n \in \mathbb{Q} \iff \alpha_1 = \cdots = \alpha_n = 0.
   \]
   Prove that $G = \mathbb{Z}^n + \mathbb{Z}x$ is dense in $\mathbb{R}^n$. Deduce that the set\[
   \{(zx_1 \mod 1, \ldots, zx_n \mod 1) : z \in \mathbb{Z}\}
   \]
   is dense in $(0,1)^n$. (Hint: compute $G^*$)

3. **Duality for Integer Linear Systems**: Take $A \in \mathbb{Z}^{n \times m}$, $b \in \mathbb{Z}^n$, $c \in \mathbb{Z}^m_n$.

   (a) Prove that the system $Ax = b$, $x \in \mathbb{Z}^m$ has a solution if and only if there does not exist $y \in \mathbb{R}^n$ such that $y^t A \in \mathbb{Z}^m$ and $y^t b \notin \mathbb{Z}$. (Hint: split up the analysis based on whether $Ax = b$ has a real solution or not. If it has a real solution, examine the appropriate dual lattice.)

   (b) Prove that the system
   \[
   Ax = \begin{pmatrix}
   b_1 \pmod{c_1} \\
   \vdots \\
   b_n \pmod{c_n}
   \end{pmatrix}, x \in \mathbb{Z}^m,
   \]
   has a solution, if and only if there does not exist $y \in \mathbb{R}^n$, $y_i \in \{0, \frac{1}{c_i}, \ldots, \frac{c_i - 1}{c_i}\}$, $i \in [n]$, such that $y^t A \in \mathbb{Z}^m$ and $y^t b \notin \mathbb{Z}$.
4. Applications of Hermite Normal Form:

(a) Take \( U \in \mathbb{Z}^{n \times n} \) satisfying \( \det(U) = \pm 1 \). Show that the HNF of \( U \) is \( I_n \), the \( n \times n \) identity. Deduce that \( U \) is unimodular.

(b) Let \( \mathcal{L} = \mathcal{L}(B) \) for some basis \( B \in \mathbb{R}^{n \times n} \). Let \( y_1, \ldots, y_n \in \mathcal{L}(B) \) be linearly independent vectors. Let \( M = B^{-1}(y_1, \ldots, y_n) \in \mathbb{Z}^{n \times n} \), and \( U \in \mathbb{Z}^{n \times n} \) be the unimodular matrix such that \( M^tU \) is in HNF. Letting \( BU^{-1} = (b_1', \ldots, b_n') \), show that \( \mathcal{L}(b_1', \ldots, b_i') = \mathcal{L} \cap \text{span}(y_1, \ldots, y_i) \) for \( i \in [n] \).

(c) Take \( A \in \mathbb{Z}^{n \times m}, b \in \mathbb{Z}^n \). Let \( U \in \mathbb{Z}^{m \times m} \) be the unimodular matrix for which \( AU \) is in HNF. Describe an algorithm that given \( A, b \) and \( U \) either computes a solution to the system \( Ax = b \), \( x \in \mathbb{Z}^m \), or returns a certificate that no such solution exists.