1. **Dual Bounds on λ_1:** Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a k-dimensional lattice.

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

   (b) Let $\mathbf{b}_1, \dots, \mathbf{b}_k$ be a basis for $\mathcal{L}$, and let $\mathbf{b}_1^*, \dots, \mathbf{b}_k^* \in \mathcal{L}^*$ denote the associated dual basis (i.e. $\langle \mathbf{b}_i^*, \mathbf{b}_j \rangle = \delta_{ij}$ for $i, j \in [k]$). Define the sequence $\mathbf{b}_{1,r}^*, \dots, \mathbf{b}_{k,r}^*$ to be the sequence $\mathbf{b}_1^*, \dots, \mathbf{b}_k^*$ in reverse order. Let $\tilde{\mathbf{b}}_1, \dots, \tilde{\mathbf{b}}_k$ and $\tilde{\mathbf{b}}_{1,r}^*, \dots, \tilde{\mathbf{b}}_{k,r}^*$ 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 $\tilde{\mathbf{b}}_k / \|\tilde{\mathbf{b}}_k\|_2^2, \dots, \tilde{\mathbf{b}}_1 / \|\tilde{\mathbf{b}}_1\|_2^2$ and $\tilde{\mathbf{b}}_{1,r}^*, \dots, \tilde{\mathbf{b}}_{k,r}^*$ are equal.

   (c) Deduce that the above bound on $\lambda_1(\mathcal{L})$ 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 $\mathbf{v}_1, \dots, \mathbf{v}_k \in G$ be linearly independent vectors. Show that for any $\mathbf{x} \in \operatorname{span}(\mathbf{v}_1, \dots, \mathbf{v}_k)$, there exists $\mathbf{y} \in G \cap \operatorname{span}(\mathbf{v}_1, \dots, \mathbf{v}_k)$ such that $\|\mathbf{x} - \mathbf{y}\|_2 \leq \frac{1}{2} \sum_{i=1}^k \|\mathbf{v}_i\|_2$.

   (b) Let $W = \cap_{\varepsilon > 0} \operatorname{span}(G \cap \varepsilon B_2^n)$. Show that $G \cap W$ is dense in W, i.e. for all $\mathbf{x} \in W$ and $\varepsilon > 0$ there exists $\mathbf{y} \in G \cap W$ such that $\|\mathbf{x} - \mathbf{y}\|_2 \leq \varepsilon$.

   (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 $\mathbf{x} = (x_1, \dots, x_n)^t \in \mathbb{R}^n$ such that $x_1, \dots, x_n$ are linearly independent over the rationals, i.e.
   $$\sum_{i=1}^n \alpha_i x_i + \alpha_{n+1} = 0, \alpha_1, \dots, \alpha_{n+1} \in \mathbb{Q} \Leftrightarrow \alpha_1 = \dots = \alpha_{n+1} = 0.$$
   Prove that $G = \mathbb{Z}^n + \mathbb{Z}\mathbf{x}$ is dense in $\mathbb{R}^n$. Deduce that the set $\{(zx_1 \pmod 1), \dots, zx_n \pmod 1)) : z \in \mathbb{Z}\}$ is dense in $(0,1)^n$. (Hint: compute G^*)

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

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

   (b) Prove that the system
   $$A\mathbf{x} \equiv \begin{pmatrix} b_1 \pmod{c_1} \\ \vdots \\ b_n \pmod{c_n} \end{pmatrix}, \mathbf{x} \in \mathbb{Z}^m, \text{ has a solution,}$$
   if and only if there does not exist $\mathbf{y} \in \mathbb{R}^n$, $y_i \in \{0, \frac{1}{c_i}, \dots, \frac{c_i - 1}{c_i}\}$, $i \in [n]$, such that $\mathbf{y}^t A \in \mathbb{Z}^m$ and $\mathbf{y}^t \mathbf{b} \notin \mathbb{Z}$.

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 $\mathbf{y}_1, \ldots, \mathbf{y}_n \in \mathcal{L}(B)$ be linearly independent vectors. Let $M = B^{-1}(\mathbf{y}_1, \ldots, \mathbf{y}_n) \in \mathbb{Z}^{n \times n}$, and $U \in \mathbb{Z}^{n \times n}$ be the unimodular matrix such that $M^t U$ is in HNF. Letting $BU^{-t} = (\mathbf{b}'_1, \ldots, \mathbf{b}'_n)$, show that $\mathcal{L}(\mathbf{b}'_1, \ldots, \mathbf{b}'_i) = \mathcal{L} \cap \operatorname{span}(\mathbf{y}_1, \ldots, \mathbf{y}_i)$ for $i \in [n]$.

   (c) Take $A \in \mathbb{Z}^{n \times m}$, $\mathbf{b} \in \mathbb{Z}^n$. 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 $A\mathbf{x} = \mathbf{b}$, $\mathbf{x} \in \mathbb{Z}^m$, or returns a certificate that no such solution exists.