Question 1

Recall the Gram-Schmidt orthogonalization algorithm:

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j<i} \mu_{i,j} \mathbf{b}_j^*$$

where $\mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle}$. Re-arranging the procedure gives us a decomposition of the original base vector by the orthogonalized vector:

$$\mathbf{b}_i = \mathbf{b}_i^* + \sum_{j<i} \mu_{i,j} \mathbf{b}_j^*$$

Because $\mathbf{b}_i \perp \mathbf{b}_j$ when $i \neq j$, it is easy to see that for any $j > i$, $\mathbf{b}_j^* \perp \mathbf{b}_i$. This is true because $\mathbf{b}_i$ is a linear combination of orthogonalized base vector with index less than or equal to i, all such base vectors are orthogonal to $\mathbf{b}_j^*$ as is its linear combination.

Let $B = [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n]$ be the basis of the lattice $\mathcal{L}$ and $B^* = [\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_n^*]$ be its orthogonalization. For each $\mathbf{v} \in \mathcal{L}$ lattice point, there exists a unique $\mathbf{x} \in \mathbb{Z}^n$ such that $\mathbf{v} = B\mathbf{x}$.

Because $\mathbf{x}$ has finite number of entries, there exists a maximal index $k \in \{1, 2, \ldots, n\}$ such that x_k is non-zero (in other words, $x_l = 0$ for all $l > k$). Observe the inner product between $\mathbf{v}$ and $\mathbf{b}_k^*$:

$$\begin{aligned}
\langle \mathbf{v}, \mathbf{b}_k^* \rangle &= \langle B\mathbf{x}, \mathbf{b}_k^* \rangle \\
&= \langle x_k \mathbf{b}_k, \mathbf{b}_k^* \rangle \\
&= x_k \|\mathbf{b}_k^*\|^2
\end{aligned}$$

By Cauchy-Schwarz inequality we know that:

$$\|\mathbf{v}\|^2 \cdot \|\mathbf{b}_k^*\|^2 \geq \langle \mathbf{v}, \mathbf{b}_k^* \rangle^2 = x_k^2 \|\mathbf{b}_k^*\|^4$$

Because x_k is non-zero and an integer, $x_k^2 \geq 1$. Re-arranging the inequality gives us:

$$\|\mathbf{v}\| \geq \|\mathbf{b}_k^*\|$$

In other words, for each lattice point $\mathbf{v} \in \mathcal{L}$, there exists some orthogonalized base vector $\mathbf{b}_k^*$ that is at most as long as $\mathbf{v}$. Therefore, the shortest lattice point is at least as long as the shortest orthogonalized base vector. ■