Exercise 1 (Babai for CVP and BDD) Let $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a basis of $\mathcal{L}$.

1. Let $\mathbf{t} \in \mathbb{R}^n$ be a target satisfying $\mathrm{dist}(\mathcal{L}, \mathbf{t}) < 1/2 \min_{i \in [n]} \|\widetilde{\mathbf{b}}_i\|_2$. Show that Babai's algorithm applied to t finds the closest vector. (Hint: Recall that Babai's algorithm rounds to the "nearest plane". How far must the target be from the lattice if Babai rounds to the "wrong plane"?)

2. Now assume that $\mathbf{t}$ is arbitrary. Show that Babai algorithms applied to $\mathbf{B}$ and $\mathbf{t}$ outputs $\mathbf{y} \in \mathcal{L}$ satisfying
$$\|\mathbf{y} - \mathbf{t}\| \leq \max_{i \in [n]} \frac{\sqrt{\sum_{j=1}^{i} \|\widetilde{\mathbf{b}}_j\|^2}}{\|\widetilde{\mathbf{b}}_i\|} d(\mathcal{L}, \mathbf{t}) \ .$$
(Hint: Notice that distance to $\mathcal{L}$ only goes down at every iteration as long as Babai choose the "right plane". The moment Babai makes a mistake, combine the lower bound you get from this together with the worst-case distance Babai guarantees after that point.)

3. Conclude that if $\mathbf{B}$ is an LLL-reduced basis that Babai's nearest plane on $\mathbf{B}$ solves CVP up to a $2^{O(n)}$ approximation factor.

Exercise 2 (Diophantine Approximation) Let $\alpha \in \mathbb{Q}^n$ be a rational vector satisfying $\|\alpha\| \in [1/2, 1]$. For any $N \in \mathbb{N}$, show that one can use the LLL algorithm to compute $0 \leq k \leq N$ and $\mathbf{y} \in \mathbb{Z}^n$ satisfying $\|k\alpha - \mathbf{y}\| \leq 2^{O(n)}/N^{1/n}$ (note that this is only interesting for $N \geq 2^{n^2}$).
(Hint: Construct a lattice Λ in a one higher dimensional space such that a shortest vector in Λ satisfies the above criterion)

Exercise 3 (Worst-case LLL basis) Construct an LLL-reduced basis $\mathbf{B}$ such that $\|\mathbf{b}_1\| = \gamma_2^{n-1} \lambda_1(\mathcal{L}(\mathbf{B}))$.