Exercise 1 In Lecture 4 we showed that the number of iterations in the Lagrange Reduction algorithm (Algorithm 1) is polynomial in the size of the input (if we assume the input is rational), while in Lecture 5 Section 2.2 we claim that the entire algorithm is polynomial time.

Assume $\mathbf{B} \in \mathbb{Q}^{2\times 2}$. Show that in every loop, the integer k and the vector $\mathbf{b}_2 - k\mathbf{b}_1$ have heights that are polynomially bounded in the size of the input (the heights of the original values for $\mathbf{b}_1, \mathbf{b}_2$). This proves that Lagrange reduction is a polynomial time algorithm.

Exercise 2 Complete the proof of Theorem 12 from Lecture 5 by proving part 5.

Exercise 3 We consider a basis with orthogonal columns $\mathbf{B} = \mathbf{B}^\star$ as input to the LLL algorithm and set $\varepsilon = 0$.

i) Show that at any point of the algorithm, the columns of $\mathbf{B}$ are given by a permutation of the columns of the input basis.

ii) Characterize the output basis in simple terms.

iii) Based on an argument using a *potential* (but a different one!), prove that this algorithm terminates after $O(n^2)$ steps.
(Hint: What quantity decreases by 1 at each step?)

Exercise 4 From Lecture 5, prove the following, using the discussion in Lecture 5, Section 2.4 for guidance.

i) Lemma 13: If $\mathbf{B}$ is an ε-LLL reduced basis of L then $\|\mathbf{b}_i^\star\| \geq \alpha^{-i} \cdot \lambda_1(L)$, where $\alpha = \gamma_2 + \varepsilon$.

ii) Theorem 14: For any $\alpha > \gamma_2$, there exists a polynomial time algorithm solving $(\alpha^{-n}/2)$-BDD in lattices of dimension n.

iii) Theorem 15: There exists an algorithm solving exact SVP in time $2^{O(n^2)}$ for lattices of dimension n.

Theorem 15 requires re-using bounds from Exercise 2 of Sheet 3. **The old version of sheet 3 had mistakes. Be sure to use the up-to-date version**.