1. Describe an algorithm that given a basis \( b_1, \ldots, b_n \in \mathbb{Q}^n \) of a lattice and a point \( t \in \mathbb{Q}^n \), finds a point \( x \in L(b_1, \ldots, b_n) \) such that \( \| x - t \|^2 \leq \frac{1}{2}(\| \tilde{b}_1 \|^2 + \cdots + \| \tilde{b}_n \|^2) \).

2. Show that an LLL reduced basis \( b_1, \ldots, b_n \) of a lattice \( \Lambda \) satisfies the following properties.
   
   (a) \( \| b_1 \| \leq 2^{(n-1)/4(\det \Lambda)^{1/n}} \)
   
   (b) For any \( 1 \leq i \leq n \), \( \| b_i \| \leq 2^{(i-1)/2} \| \tilde{b}_i \| \)
   
   (c) \( \Pi \| b_i \| \leq 2^{n(n-1)/4} \det \Lambda \)
   
   Remark: the quantity \( \Pi \| b_i \| / \det \Lambda \) is known as the orthogonality defect of the basis; to see why, notice that it is 1 iff the basis is orthogonal; it can never be less than one by Hadamard’s inequality.
   
   (d) For any \( 1 \leq i \leq j \leq n \), \( \| b_i \| \leq 2^{(j-1)/2} \| \tilde{b}_j \| \)
   
   (e) For any \( 1 \leq i \leq n \), \( \lambda_i(\Lambda) \leq 2^{(i-1)/2} \| \tilde{b}_i \| \)
   
   (f) For any \( 1 \leq i \leq n \), \( \lambda_i(\Lambda) \geq 2^{-(n-1)/2} \| b_i \| \)
   
   (g) For \( 1 \leq i \leq n \) consider \( H = \text{span}\{b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n\} \). Show that \( 2^{-n(n-1)/4} \| b_i \| \leq \text{dist}(H, b_i) \leq \| b_i \| \). Hint: use (c)

3. Show an algorithm that solves SVP exactly in time \( 2^{O(n^2)} \cdot \text{poly}(D) \) where \( n \) is the rank of the lattice and \( D \) is the input size. Hint: show that if we represent the shortest vector in an LLL-reduced basis, none of the coefficients can be larger than \( 2^c n \) for some \( c \).

4. (a) Let \( S \in \mathbb{Z}^{m \times m} \) be a basis for \( \Lambda^⊥(A) \) (i.e., \( AS = 0 \) and \( S \) is nonsingular over the integers), and suppose that the columns of \( A \) generate all of \( \mathbb{Z}_q^m \) (i.e., \( A \cdot \mathbb{Z}^m = \mathbb{Z}_q^m \)). Let \( A' = [A|A_1] \) be an arbitrary extension of \( A \). Show how, given \( S \) and \( A' \), to efficiently compute a basis \( T \) of \( \Lambda^⊥(A') \) so that \( \max \| \tilde{t}_i \| = \max \| \tilde{s}_i \| \) (where \( s_i, t_j \) are the \( i \)th columns of \( S, T \) respectively, and the tilde notation \( \tilde{\cdot} \) denotes the Gram-Schmidt orthogonalization).

   (b) In the second trapdoors talk we defined \( R \) to be a (strong) trapdoor for \( \Lambda^⊥(A) \) if
      \[
      A \begin{bmatrix} R \ 1 \end{bmatrix} = G,
      \]
   
      the special gadget matrix. Prove that the order of the rows in \( \begin{bmatrix} R \ 1 \end{bmatrix} \) is immaterial, i.e., that we can still efficiently invert LWE and sample Gaussian-distributed SIS preimages for \( A \) even if the rows of \( \begin{bmatrix} R \ 1 \end{bmatrix} \) are arbitrarily permuted. \( \text{Hint} \): show that \( \begin{bmatrix} R \ 1 \end{bmatrix} \) is a trapdoor (in the above sense) for some matrix \( A' \) whose columns are a permutation of the columns of \( A \). Then show why inverting LWE and sampling SIS preimages are equivalent for \( A \) and \( A' \).

   (c) Using the previous part, give a very simple and efficient algorithm for extending a trapdoor \( R \) for \( A \) into a trapdoor \( R' \) for any extended matrix \( A' = [A|A_1] \), so that \( s_1(R') = s_1(R) \). (Recall that \( s_1(R) = \max_{u \neq 0} \| Ru \| / \| u \| \) is the spectral norm of \( R \).)