1. Given an oracle that outputs the function: $f(x, y) = \sum_{ij} a_{ij} x_i y_j$, where x and y are n bit vectors, and A is an nxn boolean matrix. Show that there is a quantum algorithm that reconstructs A in $O(n)$ queries. Show that n queries are necessary.

   Now suppose the oracle outputs: $f(x) = \sum_{ij} a_{ij} x_i x_j$. Show that you can still reconstruct A using $O(n)$ queries.

2. Suppose there are K solutions in the table of N items. Analyze the running time of Grover's algorithm for picking a uniformly random solution among the K possibilities.

   Now give a $O(\sqrt{N})$ quantum algorithm for finding the minimum element in a list of N numbers.

3. Suppose you are given a 2^k-to-1 function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ such that there exist n-bit strings $a_1, \ldots, a_k$, such that for all $x \in \{0,1\}^n$ and for $1 \leq i \leq k$, $f(x + a_i) = f(x)$. What information about the a_i's can we hope to reconstruct from f? Cast this as an instance of the hidden subgroup problem. What is the underlying group G. What is the hidden subgroup H? Work out the details of the algorithm (including the classical reconstruction).

4. Suppose you wish to add 1 to your n qubit quantum register using as primitives a QFT and a controlled phase circuit that maps the state $|x\rangle$ to $\omega^x |x\rangle$. Show how to accomplish this task.

5. To solve the discrete log problem as a hidden subgroup problem, we assumed the ability to implement the QFT mod $p - 1$. Show how to carry out the algorithm given only the ability to implement QFT modulo powers of 2.

6. Suppose that $H \subseteq Z_2^n$. To solve the hidden subgroup problem, we creat the mixed state which is a uniform superposition over a random coset of H. Give an example of a subgroup H where each superposition in this mixture is highly entangled.

   Now show that this mixture is actually separable, i.e. it can be written as an equivalent mixture in which each pure state is completely unentangled (tensor product of qubit states).

   Hint: Fourier transform.