COL866: Quantum Computation and Information
Homework: 3 (*This is for practice. You need not submit.*)

1. Exercises from the book: 5.1 to 5.25.

2. Which gate would you apply to compute the Fourier Transform in a single qubit system where $N = 2$? Recall that the Fourier transform is defined as:
$$|k\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_j e^{(2\pi i)\frac{kj}{N}} |j\rangle$$

3. Let us consider the following variation of the Fourier transform in an $n > 1$ qubit system. We will consider the computational basis states of the system as n-bit strings (rather than integers in the set $\{0, 1, ..., 2^n - 1\}$).
$$|s\rangle \rightarrow \frac{1}{2^{n/2}} \sum_{t \in \{0,1\}^n} e^{(2\pi i)\frac{\langle s,t\rangle}{2}} |t\rangle$$
where $\langle s, t\rangle$ denotes the bit-wise dot product of strings s and t modulo 2.

   How would you apply the above variation of the Fourier transform in an n-qubit system? *Do you see the connection between the quantum order finding algorithm and the algorithm for Simon's problem using the above formulation?*

4. Write the pseudocode for computing $x^z \ (mod\ N)$ given x, z, N as input. You may assume that x, z, and N can be expressed using n bits. Do a running time analysis in terms of n.

5. Let $N \geq 2$ be an arbitrary positive integer and let $a \in \mathbb{Z}_N^*$ such that order of a modulo N divides N. Suppose you are given the following n-qubit quantum gates, where $2 \leq N \leq 2^n - 1$.

   (a) U_N: This gate returns a uniform superposition of states $|0\rangle, |1\rangle, ..., |N-1\rangle$ when given input $|0\rangle$.
   (b) QFT_N: This performs the Quantum Fourier transform on orthonormal basis $|0\rangle, ..., |N-1\rangle$.
   (c) $\mathsf{ME}_{a,N}$: This performs the operation $|z\rangle |y\rangle \rightarrow |z\rangle |a^z y \ (mod\ N)\rangle$.

   Construct a quantum circuit that finds the order of a modulo N using just the above gates. You may also use controlled operations. Discuss correctness and running time of your algorithm.