When preparing your written solutions, please show all steps involved in obtaining your answer. This will make it easier to assign partial credit (for partially correct answers) and will also help me (or the grader) in helping you to see where (if anywhere) you made a mistake.

1. (Exercise 5.10 in NC) Show that the order of $x = 5$ modulo $N = 21$ is 6.

2. (Exercise 5.11 in NC) Show that the order of $x$ satisfies $r \leq N$.

3. Having shown that factoring a number $B$ classically efficiently (though probabilistically) reduces to “order-finding” in $\mathbb{Z}_B$, show the opposite reduction, thereby showing that factoring and order-finding are of “equivalent” complexity. More precisely, suppose you had a subroutine that could factor any number $B = P \cdot Q$ (for simplicity, just consider the product of two primes). Using it, give an efficient (deterministic) algorithm for finding the order of $A \in \mathbb{Z}_B^*$, given $A$ and $B$.

4. (Problem 5.6 in NC) (Addition by Fourier transforms) Consider the task of constructing a quantum circuit to compute $|x\rangle \rightarrow |x + y \mod 2^n\rangle$, where $y$ is a fixed constant and $0 \leq x < 2^n$. Show that one way to do this, for values of $y$ such as 1, is to first perform a Fourier transform, then to apply single qubit phase shifts, then an inverse Fourier transform. What values of $y$ can be easily added this way, and how many operations are required?

5. (Exercise 6.2 in NC) Show that the operation $(2 \langle \psi | |\psi\rangle - I)$ applied to a general state $\sum_k \alpha_k |k\rangle$ produces

$$\sum_k (-\alpha_k + 2\langle \alpha \rangle) |k\rangle,$$

where $\langle \alpha \rangle \equiv \sum_k \alpha_k / N$ is the mean value of $\alpha_k$. For this reason $(2 \langle \psi | |\psi\rangle - I)$ is sometimes referred to as the inversion about mean operation.