Problem 1. (***Solving order-finding with QPE [N&C Section 5.3.1]***).
Let $N = 2^n$ and $0 < x \leq N$ be an integer with no common factors (i.e., $\gcd(x, N) = 1$). The *order* of x modulo N is the least positive integer r, such that $x^r = 1 \mod N$. In this problem you will show how to efficiently compute the order of x modulo N using QPE.

1. Show that the order of $x = 5$ modulo $N = 21$ is 6.

2. Argue that the following linear operator U_x is *unitary*,
$$U_x |k\rangle = |k \cdot x \mod N\rangle, \; 1 \leq k \leq N.$$

3. Show that for $0 \leq s \leq r - 1$ the following states $|u_s\rangle$ are eigenstates of U_x,
$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k/r} |x^k \mod N\rangle.$$

4. What are the eigenvalues of $|u_s\rangle$, for $0 \leq s \leq r - 1$?

By the previous question, using the quantum phase estimation procedure allows us to obtain, with high accuracy, the eigenphases s/r from which a procedure called "Continued Fraction" allows us to obtain r. The problem that remains is how to prepare a state $|u_s\rangle$ with nonzero eigenphase to apply the quantum phase estimation procedure to.

Turns out that preparing $|u_s\rangle$ requires knowing r, so this is out of the question. Fortunately, there is a clever observation which allows us to circumvent this problem.

5. (*) Show that the following equality holds
$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle. \tag{1}$$
Hint: $\sum_{s=0}^{r-1} e^{2\pi i s k/r} = \begin{cases} r \text{ if } k = 0, \\ 0 \text{ otherwise.} \end{cases}$.

6. Show what happens when you apply the quantum phase estimation procedure with unitary U_x to the state $|1\rangle$. What are the possible outcomes when you measure the eigenvalue register?
Hint: use Equation 1.

Problem 2. (***Finding the minimum in a database [N&C Section 6.7]***).
Let $N = 2^n$ and suppose $x_1, ..., x_N$ is a database of positive integers. Suppose you have access to this database by being able to query oracles O_y, for $y \geq 0$, that map
$$|i\rangle \mapsto (-1)^{\delta(x_i, y)} |i\rangle, \; 1 \leq i \leq N,$$
where $\delta(a, b) = 1$ if $a = b$, and 0 otherwise. Show that only $O(\log(N)\sqrt{N})$ queries to the oracle are required on a quantum computer in order to find the smallest element on the list

Remark. *Again you may reason on a high-level, no need to draw quantum circuits.*