A. Let $m = 1022117$. Assume that m is a product of two distinct primes. Suppose that, using Shor's algorithm, you compute the following periods in $(\mathbb{Z}/m\mathbb{Z})^*$:

1. The period of $k = 966244$ is $p = 7084$.
2. The period of $k = 713912$ is $p = 7728$.
3. The period of $k = 788451$ is $p = 255024$.

Is this enough information to factor m? Execute the factoring algorithm.

B. Suppose that a and b are distinct large primes and $m = ab$. Given m, you wish to discover a and b. Rephrase this integer factoring problem as an example of Grover's problem (with $\sum_\alpha f(\alpha) = 1$), carefully specifying n and f. What is the running time of this Grover-based factoring algorithm, as a function of the number of bits needed to represent m?

C. For any unit $|\rho\rangle \in \mathbb{C}^{2^n}$, let $R = 2\,|\rho\rangle\,\langle\rho| - I$. Verify that R acts on $\mathbb{C}^{2^n}$ as reflection across $|\rho\rangle$, by completing the following subproblems.

1. Prove that $R\,|\rho\rangle = |\rho\rangle$.
2. Prove that if $|\psi\rangle$ is perpendicular to $|\rho\rangle$, then $R\,|\psi\rangle = -\,|\psi\rangle$.
3. Prove that $R^2 = I$.
4. Also prove that R is unitary.