You have 60 minutes. No notes, books, computers, phones, etc. are allowed, except that you are allowed one two-sided "crib sheet" of notes as described in recent e-mail.

You may cite any definitions and theorems discussed in class, homework, or project work. You do not have to re-derive that material unless you are explicitly asked to. You should not use material, that we haven't studied, without developing it first.

If a problem is ambiguous, then ask for clarification. If it remains unclear, then explain your interpretation in your answer. Never interpret a problem in a manner that renders the problem trivial.

Show all of your work, in as organized a manner as possible. Incorrect answers with solid work often earn partial credit. Correct answers without explanatory work rarely earn full credit.

Good luck. :)

A. Here are some periods in $(\mathbb{Z}/m\mathbb{Z})^*$ for $m = 65$: The period of 17 is 12, the period of 16 is 3, and the period of 12 is 4. Execute the factoring-from-period-finding algorithm on one or more of these periods, to find a non-trivial factor of m. Or, if the algorithm fails, then explain why.

B. This problem concerns Grover's algorithm. It is worth about as many points as other problems, but it is split over two pages, in case any student wants to use a lot of space.

B.A. We've studied three versions of Grover's problem: known $k = 1$, known $k \geq 1$, and unknown $k \geq 1$. How do the circuit diagrams *differ* in these three versions?

B.B. In the unknown $k \geq 1$ version, how do we choose ℓ (the number of repetitions of $(R \otimes I) \cdot F$)?

B.C. Explain how to handle the unknown $k \geq 0$ case, using invocations of the algorithm for unknown $k \geq 1$. (This was a homework problem. You are being asked to solve it again.)

C. What is the complexity of the n-qbit quantum Fourier transform gate, in terms of primitive one- and two-qbit gates? Answer in $\mathcal{O}$ notation. Include the swaps, using only as many swaps as is necessary. (This was a homework problem. You are being asked to solve it again.)

D. An adiabatic quantum computation is governed by its Hamiltonian (meaning either $\tilde{Q}(\tilde{t})$ for $\tilde{t} \in [0,1]$ or $Q(t) = \tilde{Q}(t/u)$ for $t \in [0,u]$). The Hamiltonian is a time-dependent $2^n \times 2^n$ matrix. What requirements should it satisfy?