1. Let $f : \{0,1\}^n \to \{0,1\}^n$ be a bijection on the n-bit strings. We showed in class that if there is an efficient classical circuit (say of size m) for computing $f(x)$ on input x, then there is an efficient reversible circuit (of size $O(m+n)$) that outputs $x \cdot f(x) \cdot 0^k$ on input $x \cdot 0^{n+k}$.

   Now suppose that you are also given an efficient circuit for computing f^{-1} (of size m'). Show that there is an efficient reversible circuit that outputs $f(x) \cdot 0^l$ on input $x \cdot 0^l$. What is the size of your circuit as a function of n, m, m'?

   One application of this result is the following: Let $N = pq$ where p and q are primes. The Chinese remainder theorem says that there is a bijection between the numbers $x \bmod N$ and ordered pairs $(x \bmod p, x \bmod q)$. Moreover, given N, p, q, there is an efficient circuit that on input $x \bmod N$ outputs $(x \bmod p, x \bmod q)$, and an efficient circuit that on input $(x \bmod p, x \bmod q)$ outputs $x \bmod N$. By the above result, it follows that there is an efficient reversible circuit (and therefore an efficient quantum circuit) to convert $x \bmod N$ into $(x \bmod p, x \bmod q)$ and vice-versa.

2. Consider a quantum bit in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. What unitary transformation U would you perform to this qubit to change its state to $|0\rangle$? What is the result of now measuring this qubit in the standard basis?

   Now consider a second qubit whose state is $|0\rangle$. Suppose you perform a CNOT from the first qubit in state $|\psi\rangle$ into this second qubit. What is state of the two qubits? Now apply U to the first qubit. What is the resulting state? What is the result of measuring the first qubit in the standard basis?

   Can you relate the outcome to the principle of safe storage (principle of deferred measurements).

3. Consider the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$. What is the state that results from applying the 2-qubit Hadamard transform to $|\psi\rangle$?

   Now regard ψ as a superposition over numbers modulo 4 (i.e. it is a superposition of 0 and 2 written in binary notation). What is the state that results from applying the Fourier transform modulo 4 to ψ?

4. Consider a superposition on n bit strings $|\psi\rangle = \frac{1}{\sqrt{M}} \sum_{x: u \cdot x = 0} |x\rangle$ where u is a fixed non-zero n bit string and $u \cdot x = u_1 x_1 + u_2 x_2 \ldots u_n x_n (mod\ 2)$. What is M?

   Apply the n-bit Hadamard transform to $|\psi\rangle$ and let the result be $|\phi\rangle = \sum_x \alpha_x |x\rangle$. What is $\alpha_{00\ldots0}$?

   What is $|\phi\rangle$?

5. (Extra Credit:) Suppose you are given quantum circuits to compute the Fourier transform modulo p and modulo q for primes p and q. Give an efficient quantum circuit to compute the Fourier transform modulo $N = pq$. What is the size of your quantum circuit?