Problem set 7: Shor's factoring algorithm
Due 9 November 2007

1) Factor the number 15 classically, using the following procedure:

- Randomly pick a number $a < 15$, with no factors in common with 15.
  NOTE: let us agree to all randomly pick $a = 13\ldots$
- Compute $13^0 \mathrm{mod} 15, 13^1 \mathrm{mod} 15, 13^2 \mathrm{mod} 15\ \ldots$ until you discover the period r of $f(x) = 13^x \mathrm{mod} 15$.
- Find the greatest common denominator of $13^{r/2} \pm 1$ and 15. Check whether the result is a prime factor of 15.

If you think the answer came out right by chance, try another value of a, e.g. 11 or 7.

2) Now go through the steps of Shor's algorithm in order to find the period r of $13^x \mathrm{mod} 15$, by writing down the state after each step. Use only three qubits for the first registor, in order to keep things simple. The second register must have four qubits. *I recommend that you use decimal instead of binary notation for the states of each register, so for instance write* $|011\rangle$ *simply as* $|3\rangle$.

- Initialize each register to $|0\rangle$.
- Apply the Hadamard gate to each qubit in the first register.
- Add $13^x \mathrm{mod} 15$ to the second register, where x is the state of the first register.
- Rewrite this state so you group all terms with identical $f(x)$ — observe the periodicity in the amplitudes which emerges, and observe also that you cannot efficiently reveal the period by any measurement.
- Apply the Quantum Fourier Transform to the first register.
- Measure the final state of the first register. What are the possible measurement outcomes, and how to they relate to r?

What would the possible measurement outcomes be if you had taken 8 qubits for the first register and how would you extract r?