1. The QFT and periodicity.

(a) Write down the circuit for the quantum Fourier transform $Q_4$ on 2 qubits. Multiply out the matrices corresponding to the circuit in the computational basis and check that the result is what you expect.

(b) Write the state $Q_4|3\rangle$ as a tensor product of two single-qubit states, each of the form $\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i z}|1\rangle)$ for some binary fraction $z$ (i.e. something of the form $(.x_{j-1} \ldots x_0)$). Expand out the resulting state and check that the answer is what you expect.

(c) Let $f: \mathbb{Z}_{16} \rightarrow \mathbb{Z}_4$ be the periodic function such that $f(0) = 2$, $f(1) = 1$, $f(2) = 3$, $f(3) = 0$, and $f(x) = f(x - 4)$ for all $x$ (so $f(4) = 2$, etc.).

   i. Work through all the steps of the periodicity determination algorithm, writing down the state at each stage, and assuming that the measurement outcome in step 3 is 1, and the measurement outcome in step 5 is 12. Does the algorithm succeed?

   ii. Now assume that the measurement outcome in step 5 is 8. Does the algorithm succeed?

2. Shor’s algorithm.

(a) Suppose we would like to factorise $N = 85$ and we choose $a = 3$, which is coprime to $N$. Follow steps 3-5 of the integer factorisation algorithm to factorise 85 using this value of $a$ (calculating the order of $a$ classically!). You might like to use a computer.

(b) Imagine we want to factorise $N = 21$ and we choose $a = 4$. Does the integer factorisation algorithm work or not?

3. Approximate implementation of the QFT (optional). This part proves a claim made at the end of Section 4 of the lecture notes. Define the distance $D(U, V)$ between unitary operators $U$ and $V$ as the maximum over all states $|\psi\rangle$ of $\|U|\psi\rangle - V|\psi\rangle\|$.

(a) Show that $D(\cdot, \cdot)$ is subadditive: $D(U_1 U_2, V_1 V_2) \leq D(U_1, V_1) + D(U_2, V_2)$. 

1
(b) Show that $D(R_d, I) = O(2^{-d})$ and argue that the same holds for controlled-$R_d$.

(c) Describe how to produce a quantum circuit for an operator $\tilde{Q}_{2^n}$ on $n$ qubits such that $\tilde{Q}_{2^n}$ uses $O(n \log n)$ gates and $D(\tilde{Q}_{2^n}, Q_{2^n}) = O(1/n)$. 