1. Quantum Fourier Transform and Period Finding. For a standard basis state $|x\rangle \in \mathbb{C}^t$, $\text{QFT}_t |x\rangle = \frac{1}{\sqrt{t}} \sum_{y=0}^{t-1} e^{2\pi i xy/t} |y\rangle$, $\text{QFT}_t^{-1} |x\rangle = \frac{1}{\sqrt{t}} \sum_{y=0}^{t-1} e^{-2\pi i xy/t} |y\rangle$ \hspace{1cm} (1)

(a) [6 points] Show that $\text{QFT}_t |0\rangle = \frac{1}{\sqrt{t}} \sum_{y=0}^{t-1} |y\rangle$. 

(b) [6 points] Show that $\text{QFT}_t^{-1}$ really is the inverse of $\text{QFT}$. In other words, show: $\text{QFT}_t^{-1} \text{QFT}_t = I$. \hspace{1cm} (3)

(c) [3 points] Given a function $f$, let $P_k(f(x)) = f(x + k)$. What is a connection between $P_k$ and period finding? (There is nothing quantum in this problem.)

(d) [6 points] Let $P$ denote the unitary operation that adds 1 modulo $t$. In other words, for any $x \in \{0, 1, \ldots, t-1\}$, $P|x\rangle = |x + 1 \text{ mod } t\rangle$. Show that the states that result from applying $\text{QFT}_t$ to standard basis states are eigenvectors of $P$. That is, show $P \frac{1}{\sqrt{t}} \sum_{y=0}^{t-1} e^{2\pi i xy/t} |y\rangle = \lambda_y \frac{1}{\sqrt{t}} \sum_{y=0}^{t-1} e^{2\pi i xy/t} |y\rangle$ \hspace{1cm} (4)

where $\lambda_y$ is a complex number. What is $\lambda_y$? (This problem is meant to show you that there is some relationship between periodic functions and Fourier states.)

2. Let $p$ be a prime number. Suppose you are given a black-box function $f: \{0, 1, \ldots, p-1\} \times \{0, 1, \ldots, p-1\} \rightarrow \{0, 1, \ldots, p-1\}$ such that $f(x, y) = f(x', y')$ if and only if $y' - y = m(x' - x) \text{ mod } p$ for some unknown integer $m$. In other words $f(x, mx + b) = C_b$, where $C_b$ is a constant that depends on $b$. This means that for all points on the line $y = mx + b$, $f$ has the same value. However, for different values of $b$, the function takes different values. Your goal is to determine $m \text{ mod } p$ using as few queries as possible to $f$, which is given by a unitary operation $U_f$ satisfying $U_f |x\rangle_A |y\rangle_B |z\rangle_C = |x\rangle_A |y\rangle_B (z + f(x, y)) \text{ mod } p |z\rangle_C$ for all $x, y, z \in \{0, 1, \ldots, p-1\}$. (Note that each of the three registers is a $p$-dimensional state.)

See final page for hints.
Consider the case that $p = 3$. Here is a truth table for a function of the above form. What is $m$?

<table>
<thead>
<tr>
<th>$x$</th>
<th>$y$</th>
<th>$f(x, y)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

(b) [6 points] What is the classical query complexity of this problem?

(c) Consider the following circuit (which is very similar to the period finding circuit!!)

\[ \begin{array}{c}
|0\rangle_A \\
\hline
|0\rangle_B \\
|0\rangle_C \\
\end{array} \xrightarrow{QFT_p} \xrightarrow{U_f} \xrightarrow{QFT_p^{-1}} \xrightarrow{QFT_p^{-1}} \]

i. [3 points] What is the state of the system after the first time step (the two parallel QFTs)?

ii. [6 points] Show that the state after applying $U_f$ is

\[ \frac{1}{\sqrt{p}} \sum_{b=0}^{p-1} \left( \frac{1}{\sqrt{p}} \sum_{x=0}^{p-1} |x, mx + b\rangle_{AB} \right) |f(0, b)\rangle_C. \]  

iii. [3 points] Argue that when we measure register $C$, each outcome occurs with equal probability. If the outcome is $|f(0, b^*)\rangle$, what is the state of the system after measurement?

iv. [6 points] If the outcome on register $C$ is $|f(0, b^*)\rangle$, show that the final state after the last two inverse QFTs is

\[ \frac{1}{\sqrt{p}} \sum_{j,l=0}^{p-1} e^{-\frac{2\pi ilb^*}{p}} \left( \sum_{x=0}^{p-1} e^{-\frac{2\pi ix(j+lm)}{p}} \right) |l\rangle |j\rangle \]

v. [6 points] Explain why when you measure the remaining state in the standard basis, you will get an outcome $|l\rangle |j\rangle$ where $j \equiv -lm \mod p$.

vi. [6 points] It is a fact from number theory that every number except 0 has a multiplicative inverse $\mod p$. In other words, if $j \not\equiv 0 \mod p$, there exists $j^{-1}$ such that $jj^{-1} \equiv 1 \mod p$. Use this fact to explain how to learn $m$ from the outcome of the final measurement.
Hints!

• 1b: There are several ways to do this, but one way it to show that the operation takes every standard basis state to itself.

• 2bi : Since $y = mx + b$, we can replace the variable $y$ with the expression $mx + b$. Then $f(x, mx + b) = f(0, b)$ for all $x$ because of the promise.