Math 410 Quantum Computing **Homework 7**

Exercises in textbook. 8.1 - 8.4. (12 points each)

- **EXERCISE 8.1** Let $N = 35$. Repeat the above steps to find the factors of N. (There are M whose orders are less than 10. If your m does not give $P < 10$, try another m. Good luck!) *Answer:* Given $N = 35$, we want to find the factors of N using the steps outlined in the example.

  1. Select an m such that $\gcd(N, m) = 1$. Let us choose $m = 3$.
  2. Now, we find the period P, where $m^P \equiv 1 \mod N$. Let $P = 12$.
  3. This period is even, so we may proceed to the next step.
  4. Now, we compute $\gcd(m^{P/2} - 1, N) = 7$ and $\gcd(m^{P/2} + 1, N) = 5$. These are both nontrivial factors of $N = 35$.
  5. Given one factor, we may divide $N = 35$ by it to obtain the other.

- **EXERCISE 8.2** Let $N = 21$ and $m = 11$. Find n which satisfies $N^2 \leq 2^n < 2N^2$. Find the order P. Repeat the above steps to find the wave function $|\psi_3\rangle$ and $\text{Prob}(y)$, $y \in S_n$.

  Answer: $n = 9$ satisfies the condition. The order $P = 6$ works, $11^6 \equiv 1 \mod 21$.

  1. We first set the registers to the initial state:

  $$|\psi_0\rangle = |REG1\rangle|REG2\rangle = |0\rangle|0\rangle.$$

  2. We first apply the Walsh-Hadamard transform on the first register. Like the QFT, it also produces a uniform superposition of the first register. This yields the following updated $|\psi_0\rangle$:

  $$|\psi_1\rangle = (W_n \otimes I)|\psi_0\rangle = \frac{1}{\sqrt{2^9}} \sum_{x \in \{0,1\}^9} |x\rangle|0\rangle.$$

  3. Now, we apply a unitary gate U_f that realizes the action of $f(x) = m^x \mod N$, for $x \in S_n$, in such a way that $U_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$.

  $$|\psi_2\rangle = (U_f \otimes I)|\psi_1\rangle = \frac{1}{\sqrt{2^9}} \sum_{x \in 0,1^9} |x\rangle|f(x)\rangle.$$

  4. Finally, we may again apply the Walsh-Hadamard transform to yield $|\psi_3\rangle$.

  $$|\psi_3\rangle = (W_n \otimes I)|\psi_2\rangle = \frac{1}{2^9} \sum_{x \in \{0,1\}^9} \sum_{y \in \{0,1\}^9} (-1)^{xy}|y\rangle|f(x)\rangle$$

  To find $\text{Prob}(y)$, we calculate:

  $$\text{Prob}(y) = \left\| \frac{1}{2^9} \sum_{x \in 0,1^n} (-1)^{xy}|f(x)\rangle \right\|^2$$

- **EXERCISE 8.3** Find the continued fraction expansion of $x = 61/45$ and $x = 121/13$.

  Answer:

  1. To find the continued fraction expansion of $x = \frac{61}{45}$, we perform a modified Euclidean algorithm:

     $$\frac{61}{45} = 1 + \frac{16}{45} = 1 + \frac{1}{2 + \frac{13}{16}} = 1 + \frac{1}{2 + \frac{1}{1+\frac{3}{13}}} = 1 + \frac{1}{2 + \frac{1}{1+\frac{3}{13}}} = 1 + \frac{1}{2 + \frac{1}{1+\frac{1}{4+\frac{1}{3}}}}.$$

     Therefore the continued fraction expansion of $x = \frac{61}{45}$ is $\boxed{[1, 2, 1, 4, 3]}$.

  2. We apply the same idea for $x = \frac{121}{13}$.

     $$\frac{121}{13} = 9 + \frac{4}{13} = 9 + \frac{1}{3 + \frac{1}{4}}.$$

     Therefore the continued fraction expansion of $x = \frac{121}{13}$ is $\boxed{[9, 3, 4]}$.

- **EXERCISE 8.4** Suppose $y = 37042$ is the measurement outcome in the above example. Find the order P by repeating the above algorithm. Suppose $y = 65536$ has been obtained in the next measurement. Apply the above algorithm. What is the “order” you find?

  Answer: To reiterate, $N = 799$, $Q = 1048576$, $m = 7$. The continued fraction expansion of $37042/1048576$ is $[0, 28, 3, 4, 88, 1, 4, 3]$. We find the order $\boxed{368}$.

  The continued fraction expansion of $65536/1048576$ is $[0, 16]$. Let $p_0 = 0, q_0 = 1$. This choice of y does not yield a valid order.