Name: **Huan Q. Bui**
Course: **8.370 - QC**
Problem set: **#7**
Due: Wednesday, Nov 9, 2022
Collaborators/References:

1. Factoring 21. Suppose we use a unitary transformation which acts as

$$U\,|u \mod 21\rangle = |2y \mod 21\rangle$$

on binary representation of numbers between 0 and 20. For the factoring algorithm we start with the state $|1 \mod 21\rangle$ and use phase estimation on the unitary U. If we have an eigenvector with eigenvalue $e^{2\pi i a/b}$. we will assume that phase estimation combined with continued fraction returns a/b in reduced fraction form with probability 1.

(a) The state $|1 \mod 21\rangle$ can be represented as a superposition of the eigenvectors of U. To find what these are, we first have to find the smallest $r > 0$ for which $2^r \equiv 1 \mod 21$.

a^r	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8
$a^r \mod 21$	1	2	4	8	16	11	1	2	4

So $r = 6$. We conclude that there are $\boxed{6}$ eigenvectors of U. They are of the form

$$\begin{aligned}|\zeta_k\rangle = \frac{1}{\sqrt{6}}\Big(&\big|2^0 \mod 21\big\rangle + e^{2\pi i k/6}\big|2^1 \mod 21\big\rangle + e^{4\pi i k/6}\big|2^2 \mod 21\big\rangle \\ &+ e^{6\pi i/6}\big|2^3 \mod 21\big\rangle + e^{8\pi i k/6}\big|2^4 \mod 21\big\rangle + e^{10\pi i k/6}\big|2^5 \mod 21\big\rangle\Big), \quad k \in \{0, 1, \ldots, r-1\}\end{aligned}$$

The state $|1 \mod 21\rangle$ is then a superposition of these states $\{\zeta_k\}_{k=0}^{r-1}$:

$$|1 \mod 21\rangle = \frac{1}{\sqrt{6}}\sum_{k=0}^{r-1}|\zeta_k\rangle\,.$$

(b) Suppose the algorithm returns k'/r' (which is in reduced form) and if r' is even, we compute $2^{r'/2}$ and try to use it to factor. What is the probability that we get the right factors this way? To do this, we first list what we have donee right so far:

- $g = 2$ is relatively prime to 21, so it generates the cyclic group of order 21. The order of $g = 2$ is $r = 6$.
- $g = 2$ is also a good choice because $g^{r/2} - 1 = 2^{6/2} - 1 = 7 \neq 21$ and $g^{r/2} + 1 = 2^{6/2} + 1 = 9 \neq 21$.

This means that the algorithm fails when k'/r' (in reduced form) cannot be used to find r. The possible values that we can get are

$$\frac{k'}{r'} \in \left\{\frac{0}{6}, \frac{1}{6}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{5}{6}\right\}.$$

These values of k'/r' occur with equal probabilities. Of them, we find $r' = 3$ which is odd 1/3 of the time. When $r' = 2$ (which occurs 1/6 of the time), we also reject it. So, we get the right factors $\boxed{1/2}$ of the time this way.

2. Factoring algorithm failing. In the last problem, we saw that even if the phase estimation and continued fractions pieces of the algorithm work perfectly, and we choose a $g \in [1, N-1]$ that is relatively prime to N, use the unitary

$$U : |y \mod N\rangle \rightarrow |gy \mod N\rangle$$

and get the correct period r, the factoring algorithm still has some probability of failing.

(a) How bad is this problem for large N? To answer this question we first.

(b) Can you think of anything to do to make the factoring algorithm somewhat more efficient for large N? (Assume that quantum computation is expensive and classical computation is relatively cheap.)

3. For a prime p and two numbers a, b with $1 < a, b < p$, consider the quantum state

$$\frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} |j \mod p\rangle \, |(aj + b) \mod p\rangle$$

(a) Show that if you are given one copy of this quantum state, then with a quantum computer, you can find a with high probability (i.e., with probability going to 1 as p goes to ∞).

(b) Show that you can also find b with high probability (i.e., with probability going to 1 as p goes to ∞).

(c) Show that no quantum algorithm can identify a with probability 1.

Hint: there are two techniques that we've seen in class that you might use to attack parts (a) and (b). One is the quantum Fourier transform and the other is phase estimation. One of these techniques works substantially better than the other.