3.8 Shor's Algorithm

For this Problem Set instead of solving questions we are going to prove:

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |1\ mod(N)\rangle$$

In the lesson we defined the $|u_s\rangle$ state as:

$$|u_s\rangle = \frac{1}{\sqrt{r}}\Bigg(e^{-2\pi is(0)/r}|a^0\ mod(N)\rangle + e^{-2\pi is(1)/r}|a^1\ mod(N)\rangle + ...$$
$$+e^{-2\pi is(r-2)/r}|a^{r-2}\ mod(N)\rangle + e^{-2\pi is(r-1)/r}|a^{r-1}\ mod(N)\rangle\Bigg)$$

1. Represent $|u_s\rangle$ as a sum with sigma notation (Σ)

ANSWER:

$$|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}e^{-2\pi isk/r}|a^k\ mod(N)\rangle$$

So,

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}e^{-2\pi isk/r}|a^k\ mod(N)\rangle$$
$$= \frac{1}{r}\sum_{k=0}^{r-1}\left(\sum_{s=0}^{r-1}e^{-2\pi isk/r}\right)|a^k\ mod(N)\rangle$$

Now let's consider this part of the equation:

$$\sum_{s=0}^{r-1}e^{-2\pi isk/r}$$

2. What does it equal when $k = 0$?

ANSWER:

$$\sum_{s=0}^{r-1} e^{-2\pi is(0)/r} = \sum_{s=0}^{r-1} e^0$$
$$= \sum_{s=0}^{r-1} 1$$
$$= r$$

Now let's consider when $k \neq 0$. lets define $\omega = e^{-2\pi isk/r}$

$$\sum_{s=0}^{r-1} e^{-2\pi isk/r} = \sum_{s=0}^{r-1} \omega^s$$
$$= 1 + \omega + \omega^2 + ... + \omega^{r-1}$$

From our geometric series formula we find that:

$$\sum_{s=0}^{r-1} \omega^s = \frac{1-\omega^r}{1-\omega}$$
$$= \frac{1-e^{-2\pi isk}}{1-e^{-2\pi isk/r}}$$
$$= \frac{1-1}{1-e^{-2\pi isk/r}}, \text{ since } e^{2\pi mi} = 1, \text{ for all integers } m$$
$$= 0$$

From this we can see that when $k = 0$ the part of the equation we are considering is equal to r. And when $k \neq 0$ it is 0. This means that our state will only contain the part when $k = 0$, making our equation this:

$$\frac{1}{r}\sum_{k=0}^{r-1}\left(\sum_{s=0}^{r-1} e^{-2\pi isk/r}\right)|a^k \; mod(N)\rangle = \frac{1}{r} r |a^0 \; mod(N)\rangle = |1 \; mod(N)\rangle$$

Therefore,

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1} |u_s\rangle = |1 \; mod(N)\rangle$$

For formal proof of the reduction of factoring to period-finding see the Appendix of Quantum Computation and Quantum Information (section A4.3)