The Shor Algorithm

1 The Motivation:

1) Generate very large primes P and Q.
2) Create $M = PQ$.
3) Now randomly generate k, such that $(k, \phi(M)) = 1$.
4) Find k^{-1} such that $kk^{-1} = j\phi(M) + 1$.

To turn a message T, where $T < M$, into cyphertext C:
$C = T^k \, Mod \, M$
To decrypt:
$C^{k^{-1}} = T^{kk^{-1}} = T^{j\phi(M)+1} = T^{j\phi(M)}T = T$

2 The Function:

$$f(x) = a^x \, Mod \, M \tag{1}$$

Define r as a number such that $a^r \, Mod \, M = 1$. Then if r is even,
$a^r \, Mod \, M = 1$
$a^r - 1 \, Mod \, M = 0$
$(a^{\frac{r}{2}})^2 - 1 \, Mod \, M = 0$
$(a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1) \, Mod \, M = 0$
So $(a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1)$ is equal to some multiple of M, but neither factor alone will be a multiple of M. Therefore the gcd of either factor with M will yield one of M's two prime factors. If r is not even, then pick a new a and repeat.

3 Machine states:

$$[\text{Input state}] \rightarrow |\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|0\rangle \tag{2}$$

$$[\text{Apply } U_f\text{, where } U_f(|x\rangle|0\rangle) = |x\rangle|f(x)\rangle] \rightarrow \quad |\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle \tag{3}$$

$$[\text{Measure } f(x)\text{, with result } f(x_0)] \rightarrow \quad |\Psi\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle \tag{4}$$

$$[\text{Apply QFT}] \rightarrow \quad |\Psi\rangle = \frac{1}{\sqrt{NA}} \sum_{k=0}^{N-1} \left[\sum_{j=0}^{A-1} e^{-\frac{2\pi ik}{N}(x_0+jr)} \right] |k\rangle \tag{5}$$

$$= \frac{1}{\sqrt{NA}} \sum_{k=0}^{N-1} e^{-\frac{2\pi ik}{N}x_0} \left[\sum_{j=0}^{A-1} e^{-2\pi ij\frac{kr}{N}} \right] |k\rangle \tag{6}$$

$$\tag{7}$$

The probability distribution on k will tend to spike strongly where $\frac{kr}{N} \approx \mathbb{Z}$.

4 It works:

Some notes and notation:

- *i)* A is the number of times that $f(x) = f(x_0)$, so $\lfloor \frac{N}{r} \rfloor \leq A \leq \lfloor \frac{N}{r} \rfloor + 1 \leq \frac{N}{r} + 1$
- *ii)* $\theta_k = \frac{2\pi kr}{N}$
- *iii)* There are r values of k such that $-\frac{r}{2} \leq kr\, Mod\, N \leq \frac{r}{2}$ or $-\frac{\pi r}{N} \leq \theta_k \leq \frac{\pi r}{N}$
- *iv)* $|e^{i\alpha} - 1| \leq |\alpha|$
- *v)* $\frac{2|\alpha|}{\pi} \leq |e^{i\alpha} - 1|$ (When $|\alpha| \leq \pi$)
- *vi)* $r \leq \frac{1}{2}\phi(M) < M \leq \sqrt{N}$

Now, for some k such that $-\frac{r}{2} \leq kr\, Mod\, N \leq \frac{r}{2}$, we have $-\frac{\pi r}{N} \leq \theta_k \leq \frac{\pi r}{N}$ and:

$$
\begin{aligned}
&\sqrt{P(k)} = |\langle k|\Psi\rangle| \\
&= \tfrac{1}{\sqrt{NA}} \left| \sum_{s=0}^{N-1} e^{-\frac{2\pi i s}{N}x_0} \left[\sum_{j=0}^{A-1} e^{-2\pi i j \frac{sr}{N}} \right] \langle k|s\rangle \right| \\
&= \tfrac{1}{\sqrt{NA}} \left| e^{-\frac{2\pi i k}{N}x_0} \sum_{j=0}^{A-1} e^{2\pi i j \frac{kr}{N}} \right| \\
&= \tfrac{1}{\sqrt{NA}} \left| \sum_{j=0}^{A-1} e^{2\pi i j \frac{kr}{N}} \right| && \left(\left| e^{-\frac{2\pi i s}{N}x_0} \right| = 1 \right) \\
&= \tfrac{1}{\sqrt{NA}} \left| \sum_{j=0}^{A-1} e^{i j \theta_k} \right| && \left(\theta_k = 2\pi \tfrac{kr}{N} \right) \\
&= \tfrac{1}{\sqrt{NA}} \left| \tfrac{e^{iA\theta_k}-1}{e^{i\theta_k}-1} \right| \\
&= \tfrac{1}{\sqrt{NA}} \left| \tfrac{e^{iA\theta_k}-e^{i(A-1)\theta_k}+e^{i(A-1)\theta_k}-1}{e^{i\theta_k}-1} \right| \\
&= \tfrac{1}{\sqrt{NA}} \left| \tfrac{e^{i(A-1)\theta_k}-1}{e^{i\theta_k}-1} + e^{i(A-1)\theta_k} \right| \\
&= \tfrac{1}{\sqrt{NA}} \left(\left| \tfrac{e^{i(A-1)\theta_k}-1}{e^{i\theta_k}-1} \right| - 1 \right) \\
&\geq \tfrac{1}{\sqrt{NA}} \left(\frac{\left| e^{i(A-1)\theta_k}-1 \right|}{|\theta_k|} - 1 \right) && \left(|e^{i\theta_k}-1| \leq |\theta_k| \right) \\
&\geq \tfrac{1}{\sqrt{NA}} \left(\tfrac{2(A-1)|\theta_k|}{\pi|\theta_k|} - 1 \right) && \left(\begin{array}{l} (A-1)|\theta_k| \leq \frac{N}{r}\frac{r\pi}{N} = \pi \\ \Rightarrow \frac{2}{\pi}|(A-1)\theta_k| \leq |e^{i(A-1)\theta_k}-1| \end{array} \right) \\
&= \tfrac{1}{\sqrt{NA}} \left(\tfrac{2}{\pi}A - (1+\tfrac{2}{\pi}) \right)
\end{aligned}
$$

$$
\begin{aligned}
&\Rightarrow P(k) = \tfrac{1}{NA}\left(\tfrac{2}{\pi}A - (1+\tfrac{2}{\pi})\right)^2 \\
&= \tfrac{1}{NA}\left(\tfrac{4}{\pi^2}A^2 - \tfrac{4}{\pi}(1+\tfrac{2}{\pi})A + (1+\tfrac{2}{\pi})^2\right) \\
&= \tfrac{4}{\pi^2}\tfrac{A}{N} - \tfrac{4}{\pi}(1+\tfrac{2}{\pi})\tfrac{1}{N} + (1+\tfrac{2}{\pi})^2\tfrac{1}{NA} \\
&\approx \tfrac{4}{\pi^2}\tfrac{1}{r}
\end{aligned}
$$

In general, there are a different solutions for b in the equation: $-\frac{a}{2} \leq ab \, Mod \, M \leq \frac{a}{2}$ for any M. Therefore, for $\ell \in \{0, \ldots, r-1\}$:

$$
P\left(\ell\frac{N}{r} - \frac{1}{2} \leq k \leq \ell\frac{N}{r} + \frac{1}{2}\right) = P\left(-\frac{r}{2} \leq kr \, Mod \, N \leq \frac{r}{2}\right) \geq \frac{4}{\pi^2} \approx 40.5\% \tag{8}
$$

5 Here's what you do with the results:

Looking at these values in the form:

$\frac{\ell}{r} - \frac{1}{2N} \leq \frac{k}{N} \leq \frac{\ell}{r} + \frac{1}{2N}$

$\Rightarrow \left|\frac{k}{N} - \frac{\ell}{r}\right| \leq \frac{1}{2N}$

This value of $\frac{\ell}{r}$ is unique. For two distinct rational numbers $\frac{a}{b}$ and $\frac{c}{d}$, with $c, d < M$, we have $\left|\frac{a}{b} - \frac{c}{d}\right| = \left|\frac{ad-bc}{bd}\right| \geq \frac{1}{M^2}$. So, assuming there are two solutions, $\frac{\ell'}{r'}, \frac{\ell}{r}$ we have:

$$
\left|\frac{\ell'}{r'} - \frac{\ell}{r}\right| \leq \left|\frac{k}{N} - \frac{\ell}{r}\right| + \left|\frac{k}{N} - \frac{\ell'}{r'}\right| \leq \frac{1}{2N} + \frac{1}{2N} \leq \frac{1}{M^2} \tag{9}
$$

Which is impossible for $\frac{\ell'}{r'}, \frac{\ell}{r}$ distinct and $r, r' < M$.

Now, find the continued fraction expansion of $\frac{k}{N}$, and take successfully longer and longer approximations until $\frac{\ell}{r}$ is found.

If $(\ell, r) = 1$, then r is found. Otherwise, some fraction of r is found. However, $P((\ell, r) = 1) = \frac{6}{\pi^2} \approx 61\%$, which is pretty good. Also, most of the remaining 39% take the form of ℓ and r sharing 2, 3, or 5.

6 QFT in detail:

$\omega = e^{\frac{2\pi i}{N}}$

$$U_{QFT}|k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega^{jk} |j\rangle \tag{10}$$

$$U_{QFT} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{(N-1)} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{(N-1)} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{pmatrix} \tag{11}$$

$$|x_1, x_2, \ldots, x_n\rangle \mapsto \frac{1}{\sqrt{N}} \left(|0\rangle + e^{2\pi i \left[\frac{x_n}{2}\right]}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i \left[\frac{x_{n-1}}{2} + \frac{x_n}{4}\right]}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{2\pi i \left[\frac{x_1}{2} + \frac{x_2}{4} + \cdots + \frac{x_n}{2^n}\right]}|1\rangle\right) \tag{12}$$