Shor's Algorithm

1. Pick x at random s.t. $1 < x < N$
2. If $GCD(x, N) = d \neq 1$ then d is a factor of N, so we recurse on N/d. Else x and N are coprime, so we try to find the multiplicative order of x modulo N.

   The quantum computer is initialized to $|\psi_0\rangle = |0\rangle\,|0\rangle$. Register one has t qubits ($N^2 \leq 2^t < 2N^2$), and register two has $n = \lceil \log_2 N \rceil$ qubits.
3. Apply the Hadamard operator t times to the first register, yielding
$$|\psi_1\rangle = H^{\otimes t}\,|\psi_0\rangle = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle\,|0\rangle \ . \tag{1}$$
4. Apply the linear operator $V_x(|j\rangle\,|k\rangle) = |j\rangle\,|k + x^j\rangle$ to obtain
$$\begin{aligned}
|\psi_2\rangle &= V_x\,|\psi_1\rangle \\
&= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle\,|x^j\rangle \\
&= \frac{1}{\sqrt{2^t}} \sum_{b=0}^{r-1} \sum_{a=0}^{\frac{2^t}{r}-1} |ar + b\rangle\,|x^b\rangle \ .
\end{aligned} \tag{2}$$
5. Measure the second register, fixing $b = b_0$, where b_0 is a random number between 0 and $r-1$, obtaining
$$|\psi_3\rangle = \sqrt{\frac{r}{2^t}} \sum_{a=0}^{\frac{2^t}{r}-1} |ar + b_0\rangle\,|x^{b_0}\rangle \ . \tag{3}$$
6. Apply the inverse Fourier transform, $DFT^\dagger(|k\rangle) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-2\pi i jk/N}\,|j\rangle$, yielding
$$|\psi_4\rangle = \frac{1}{\sqrt{r}} \left(\sum_{j=0}^{2^t-1} \left[\frac{1}{2^t/r} \sum_{a=0}^{\frac{2^t}{r}-1} e^{\frac{-2\pi i j a}{2^t/r}} \right] e^{-2\pi i j b_0/2^t}\,|j\rangle \right) |x^{b_0}\rangle \ . \tag{4}$$
7. Measuring the first register, we get the value $k_0 2^t/r$, for some $k_0 \in \{0, 1, ..., r-1\}$. If we obtain $k_0 = 0$ we run the algorithm again. Else we divide $k_0 2^t/r$ by 2^t, obtaining k_0/r.
8. To extract r, we represent k_0/r by a finite continued fraction, and then ... ???