Shor's Algorithm to factor $n = pq$

1. Pick a random value $a < n$

2. Compute $\gcd(a, n)$
   - If $\gcd(a, n) \neq 1$, then we have a factor of n and we're done
   - If $\gcd(a, n) = 1$ then continue

3. Use the quantum algorithm to find $r = \text{ord}(a)$ in $\mathbb{Z}_n^*$

4. If r is odd, then go to step 1 and pick another a

5. If $a^{r/2} + 1 \equiv 0 \mod n$, then go to step 1 and pick another a

6. The factors of n are $\gcd(a^{r/2} + 1, n)$ and $\gcd(a^{r/2} - 1, n)$

Let $n = 1\,199\,885\,077$

The goal is to factor n using Shor's algorithm

Since n is small enough, Mathematica's MultiplicativeOrder[ ] command can be used rather than a quantum computer :)

1. Apply Shor's algorithm with $a = 131\,928\,655$
2. Apply Shor's algorithm with $a = 1\,618\,912$
3. Apply Shor's algorithm with $a = 1\,061\,873\,236$
4. What are the factors of n?