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 black box 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 $\gcd(a^{r/2} - 1, n)$

1. 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 :)

(a) Apply Shor's algorithm with $a = 131\,928\,655$

(b) Apply Shor's algorithm with $a = 1\,618\,912$

(c) Apply Shor's algorithm with $a = 1\,061\,873\,236$

(d) What are the factors of n?

Shor's Algorithm to solve $\beta = \alpha^d \mod p$

- Assume $\operatorname{ord}(\alpha) = q$, a large prime
- Define $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{F}_p^*$ by $f(x, y) = \alpha^x \beta^y \mod p$
- There are two types of periods:
  - (i) $f(x + x_1, y + 0) = f(x, y)$
  - (ii) $f(x + x_1, y + y_1) = f(x, y), \; y_1 \neq 0$

  Note that $(q, 0)$ is a period of type (i), and
  $(d, -1)$ is a period of type (ii) so both types exist
- Use quantum black box to find $0 \leq x_1, y_1 < q$ s.t. $f(x + x_1, y + y_1) = f(x, y)$
  If period is of type (i), then look for another period
- Then $d \equiv -x_1 \, (y_1)^{-1} \mod q$ *Note this is* $(y_1)^{-1} \mod q$

2. Use today's Mathematica notebook and Shor's algorithm to solve these DLPs

(a) $5087^d \equiv 140 \mod 8039$

(b) $5087^d \equiv 4452 \mod 8039$

(c) $9^d \equiv 8371 \mod 22\,343$

(d) $9^d \equiv 3750 \mod 22\,343$

(e) $9^d \equiv 1\,185\,461 \mod 1\,300\,367$