## Shor's Algorithm to factor $n=p q$

1. Pick a random value $a<n$
2. Compute $\operatorname{gcd}(a, n)$

- If $\operatorname{gcd}(a, n) \neq 1$, then we have a factor of $n$ and we're done
- If $\operatorname{gcd}(a, n)=1$ then continue

3. Use the quantum algorithm to find $r=\operatorname{ord}(a)$ in $\mathbb{Z}_{n}^{*}$
4. If $r$ is odd, then go to step 1 and pick another $a$
5. If $a^{r / 2}+1 \equiv 0 \bmod n$, then go to step 1 and pick another $a$
6. The factors of $n$ are $\operatorname{gcd}\left(a^{r / 2}+1, n\right)$ and $\operatorname{gcd}\left(a^{r / 2}-1, n\right)$

## Let $n=1199885077$

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 $a=131928655$
2. Apply Shor's algorithm with $a=1618912$
3. Apply Shor's algorithm with $a=1061873236$
4. What are the factors of $n$ ?
