A random eigenvector

$$|\psi_j\rangle = \frac{|1\rangle + \omega_r^{-j}|a\rangle + \cdots + \omega_r^{-j(r-1)}|a^{r-1}\rangle}{\sqrt{r}}$$

$$M_a|\psi_j\rangle = \omega_r^j|\psi_1\rangle = e^{2\pi i \frac{j}{r}}|\psi_1\rangle$$

Suppose we're given $|\psi_j\rangle$ as a quantum state for a *random choice* of $j \in \{0, \ldots, r-1\}$. We can attempt to learn j/r as follows:

1. Perform phase estimation on the state $|\psi_j\rangle$ and a quantum circuit implementing M_a. The outcome is an approximation $y/2^m \approx j/r$.
2. Among the fractions u/v in lowest terms satisfying $u, v \in \{0, \ldots, N-1\}$ and $v \neq 0$, output the one closest to $y/2^m$. This can be done efficiently using the *continued fraction algorithm.*

How much precision do we need to correctly determine $u/v = j/r$?

$$\left|\frac{y}{2^m} - \frac{j}{r}\right| \leq \frac{1}{2N^2} \qquad \Rightarrow \qquad \frac{u}{v} = \frac{j}{r}$$

Choosing $m = 2\lg(N) + 1$ for phase estimation makes such an approximation likely.
We might get unlucky: j could have common factors with r.