Shor's Algorithm

N, g share a common factor

→

$g^{p} = m \cdot N + 1$

$g^{p} - 1 = m \cdot N$

$\underbrace{(g^{p/2} + 1)}_{a \cdot \text{factor}} \underbrace{(g^{p/2} - 1)}_{b \cdot \text{factor}} = m \cdot N$

not odd

$\underbrace{g \rightarrow \underbrace{g^{p/2} \pm 1}_{\text{not a multiple of } N}}_{37.5\% \text{ of the time}}$

→ the key behind why quantum computers are fast is quantum superposition which calculates a bunch of answers at a time but gives only a single output out of them randomly with different prob.

→ $g^{x} = m \cdot N + r \implies g^{x+p} = m_2 \cdot N + r$

→ <u>Shor's Algorithm to *factor N*</u> :-

1. For any guess at a number that shares factors with N, that guess to the power $p/2$

$\Rightarrow \quad g^{p/2} \pm 1$ is a better guess.

we can find $p \Rightarrow (g^{p} = m \cdot N + 1)$

① guess g

② $g \rightarrow \boxed{QC} \rightarrow p \quad (\because g^{p} = m \cdot N + 1)$

Quantum computation.

③ $g^{p/2} \pm 1$ is a better guess.

Qiskit:-

→ Fourier checking circuit.

let

$f = [1, -1, -1, -1]$

$g = [1, 1, -1, -1]$.

If ~~(f,g)~~ $P(f,g) > 0.05$ (g is correlated with f).

→ Shor's Algo with Qiskit:-

Part-1:- ~~Step~~ We can convert the factoring problem into a period finding problem using the modular exponential function.

Dividing the number by a guest number a and computing the remainder.

For good guesses of a, this f^n is periodic as we increase the power of a.

Part-2:- It finds the period of modular exponentiation f^n using Quantum Fourier Transform. It is responsible for quantum speed up of algo.

Part-3:- once we found period M.E.F. we can use this number to efficiently compute the factors of our original number using formula.

$P = a^{r/2} - 1$

$q = a^{r/2} + 1$

a = guess no.

r = period of M.E.F

x = # to factor.

FFT :- (Fast Fourier Transform).

$$y_k = \sum_{j=0}^{N-1} e^{\frac{2\pi i k j}{N}} x_j$$

QFT
↓
Quantum Fourier Transform

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$$

→ Phase estimation in shor's :-

First phase includes preparing a superposition with eigenvector $|u\rangle$ and then apply inverse Quantum Fourier Transform.

$$\frac{1}{2^{t/2}} \sum_{j=0}^{2^t-1} e^{2\pi i \phi j} |j\rangle|u\rangle \xrightarrow{QFT^{-1}} |\tilde{\phi}\rangle|u\rangle$$

① $|0\rangle|u\rangle$ — initial state

② → $\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|u\rangle$ — create superposition

③ → $\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle U^j|u\rangle$ — applying black box

$= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i j \phi_u} |j\rangle|u\rangle$ — result of black box

④ → $|\tilde{\phi}_u\rangle|u\rangle$ — applying inverse Fourier Transform.

⑤ → $\tilde{\phi}_u$ — measure first register.