Shor's Factorization Algorithm.

Integer factorization is the core idea of RSA.

$N = u \times v$.

We discuss

1. Background
2. Basic idea
3. Shor's algorithm
4. Shor's Example

Modulus Arithmatic: $20 \equiv 2 \pmod 3$ $\Rightarrow$ 20 is congruent to 2 mod 3

Also write it as : $2 \equiv 20 \pmod 3$

$20 \bmod 3 = 2$.

$a \equiv 0 \bmod N$ then N devides a.

order: Given N, x then order is the smallest positive number 'r' such that $x^r \equiv 1 \bmod N$ then find r

Ex: $N = 17$, ~~x=2~~ $x = 2$

$2^r \equiv 1 \bmod 17$

Enumerate $r = 1$ to n, to get r value, $\underline{r = 8}$

Key idea of Shor's algorithm:-

Input N

Goal: find u, v s.t $N = u \times v$.

$x^r \equiv 1 \bmod N$ // r is even.

$(x^{\frac{r}{2}})^2 - 1 \equiv 0 \bmod N$

$(x^{\frac{r}{2}} + 1)(x^{\frac{r}{2}} - 1) \equiv 0 \bmod N$.

Trivial case:

$a^{\frac{r}{2}} = \pm 1$

Non-trivial

$a^{\frac{r}{2}} \neq \pm 1$

$\gcd(x^{\frac{r}{2}} - 1, N) = u$ & $v = \frac{N}{u}$

Shor's algorithm

while (true) {

1. choose $x \in \{2, N-1\}$
2. if ($d = gcd(x, N) \geq 2$)

   return $u = d$, $v = \frac{N}{u}$

3. find r such that $x^r \equiv 1 \bmod N$
4. If (r is even, && $d = gcd(x^{\frac{r}{2}} - 1, N) \geq 2$)

   return $u = d$, $v = \frac{N}{u}$

Example: $N = 221$

1: $x = 5$

2: $gcd(5, 221) = 1$

3: $5^r \bmod 221 = 1 \Rightarrow r = 16$ // brute force method

4. $d = gcd(5^8 - 1, 221)$

$d = u = 13 \Rightarrow v = \frac{221}{13} = 17$

return 13, 17

Next we will see order finding algorithm which is quantum part of Shor's algorithm.

First register with 2 qubits, second register with n qubit