Shor's Algorithm

1) **Problem**: Shor's algorithm is used to solve the following problem:

Factorize $N = pq$, where 'p' and 'q' are prime and very large numbers.

The problem is solvable on a classical computer in $O(\exp(c \cdot n^{1/3} \cdot (\log n)^{2/3}))$ i.e. exponential time complexity, where $\log_2 N = n$.

2) **Prerequisite (Modular Arithmetic)**:

$7 \div 3 = 2$ quotient

1 remainder ($7 \bmod 3$)

$7 \equiv 1 \pmod 3$.

$x =$	1	2	3	4	5	6	7	8	9	10	
$x \equiv$	1	2	0	1	2	0	1	2	0	1	$\pmod 3$

generally, $x \equiv y \pmod N \rightarrow x = Nk + y$, for some $k \in \mathbb{Z}$.

$x \equiv y \pmod{N}$ means $y = \{0, 1, 2, 3, \ldots, N-1\}$.

3) Shor's Algorithm :

Steps:

a) If N is even return the factor 2.

b) Determine if $N = A^b$ for integers $A \geq 1$ and $b \geq 2$, and if so return the factor 'A'.

c) Randomly choose 'a' in the range 1 to $N-1$.
If $\gcd(a, N) > 1$ then return the factor $\gcd(a, N)$.

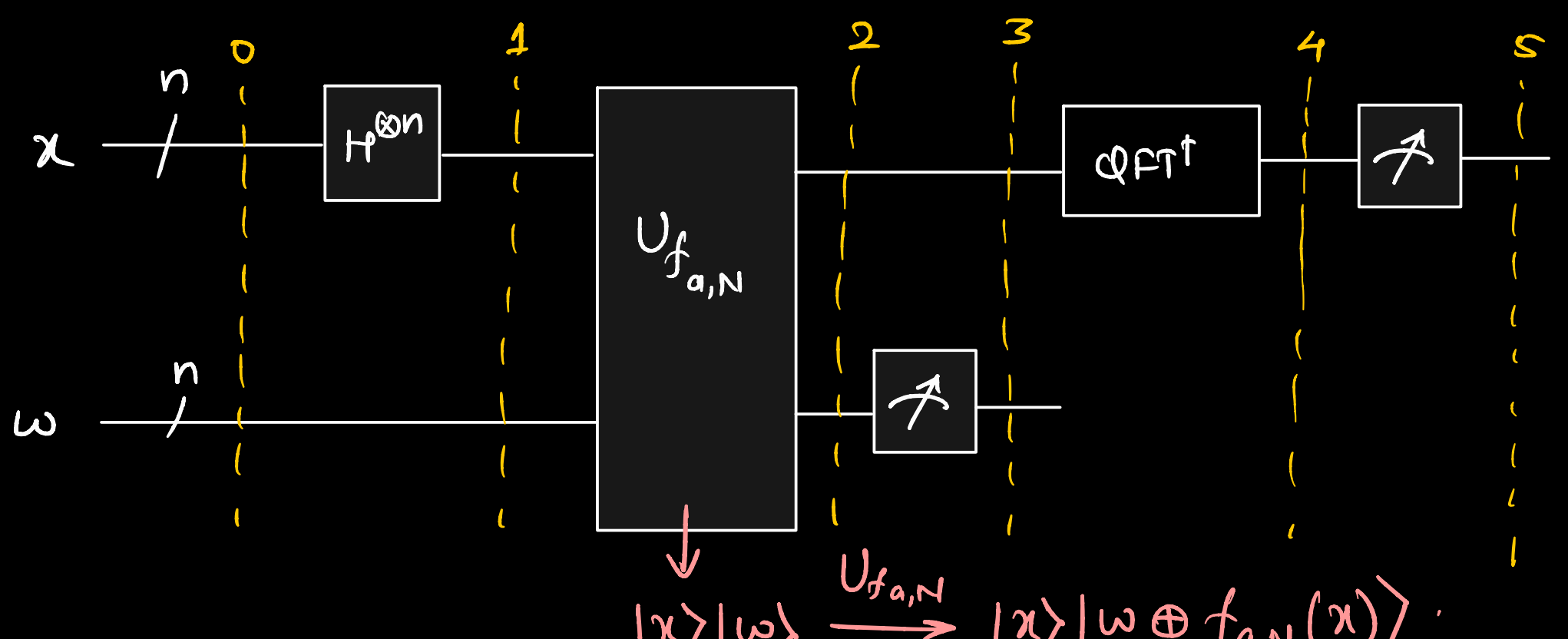
d) Use the quantum order finding subroutine to find the order 'r' of 'a' modulo 'N' i.e

$$a^r \equiv 1 \pmod{N}.$$

e) If 'r' is even and $a^{r/2} \neq -1 \pmod{N}$ then compute $\gcd(a^{r/2} - 1, N)$ and $\gcd(a^{r/2} + 1, N)$, and test to see if one of these is a non-trivial factor, returning that factor if so. Otherwise, the algorithm fails (or restart the algorithm from step c).

The algorithm requires $\approx O(n^3)$.

4) Quantum circuit (simplified):



$$f_{a,N}(x) \equiv a^x \pmod N.$$

Solving for example $N = 15$, $n = 4$, let $a = 13$.

Step 0: $\underbrace{|0\rangle^{\otimes 4}}_{x} \quad \underbrace{|0\rangle^{\otimes 4}}_{w}$

Step 1: $\left(H^{\otimes 4}|0\rangle^{\otimes 4}\right)|0\rangle^{\otimes 4}$

$$= \frac{1}{4}\left[|0\rangle + |1\rangle + |2\rangle + \cdots + |15\rangle\right]|0\rangle$$

Step 2: $\frac{1}{4}\left[|0\rangle|0 \oplus 13^0 \pmod{15}\rangle + |1\rangle|0 \oplus 13^1 \pmod{15}\rangle + \cdots\right]$

$$= \frac{1}{4}\left[|0\rangle|1\rangle + |1\rangle|13\rangle + |2\rangle|4\rangle + |3\rangle|7\rangle\right.$$

$$+|4\rangle|1\rangle + |5\rangle|13\rangle + |6\rangle|4\rangle + |7\rangle|7\rangle$$

$$+|8\rangle|1\rangle + |9\rangle|13\rangle + |10\rangle|4\rangle + |11\rangle|7\rangle$$

$$+|12\rangle|1\rangle + |13\rangle|13\rangle + |14\rangle|4\rangle + |15\rangle|7\rangle\Big]$$

Step 3: assume that '7' is measured in 'w' register:

$$\frac{1}{2}\Big[|3\rangle + |7\rangle + |11\rangle + |15\rangle\Big]|7\rangle$$

Step 4: apply $QFT^\dagger$ on the 'x' register:

$$QFT^\dagger|x\rangle = \frac{1}{8}\sum_{y=0}^{15}\Big[\exp(-i\tfrac{3\pi}{8}y) + \exp(-i\tfrac{7\pi}{8}y) + \exp(-i\tfrac{11\pi}{8}y) + \exp(-i\tfrac{15\pi}{8}y)\Big]|y\rangle$$

$$= \frac{1}{8}\Big[4|0\rangle + 4i|4\rangle - 4|8\rangle - 4i|12\rangle\Big]$$

Step 5: Measure the $|x\rangle$ register:

get $|0\rangle$ or $|4\rangle$ or $|8\rangle$ or $|12\rangle$ with equal probability of 1/4.

measured result is $j\frac{2^n}{8}$ for some $j \in \mathbb{Z}$.

($\frac{2^n}{8}$ ← integer)

Case $|0\rangle$: is trivial. Rerun algorithm.

Case $|4\rangle$: $j\frac{16}{r} = 4 \rightarrow r = 4$ if $j = 1$.

Since r is even:

$$\left.\begin{aligned} \gcd(a^{r/2}+1, N) &= \gcd(13^{4/2}+1, 15) = 5. \\ \gcd(a^{r/2}-1, N) &= \gcd(13^{4/2}-1, 15) = 3. \end{aligned}\right\} \text{complete result.}$$

Case $|8\rangle$: $j\cdot\frac{16}{r} = 8 \rightarrow$ $r = 2$ when $j = 1$

or $r = 4$ when $j = 2$

works as previous.

$$\left.\begin{aligned} \gcd(a^{r/2}+1, N) &= 3 \\ \gcd(a^{r/2}-1, N) &= 1 \end{aligned}\right\} \text{partial result}$$

Case $|12\rangle$: $j\cdot\frac{16}{r} = 12 \rightarrow r = 4$ if $j = 3$, same as the case $|4\rangle$.

5) Quantum circuit for $U_{f_{a,N}}$:

$$f_{a,N}(x) \equiv a^x \pmod N$$

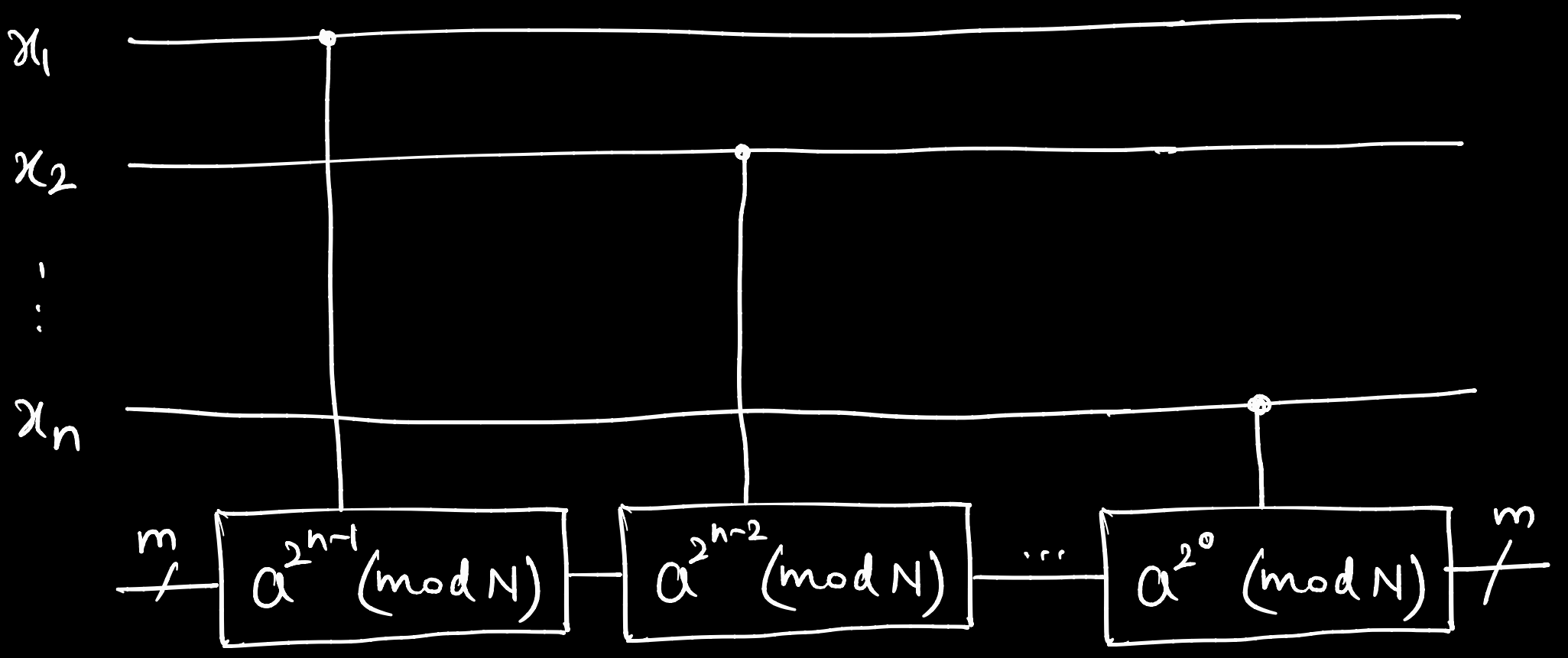
$$x = [x_1\ x_2 \cdots x_n] = 2^{n-1}x_1 + 2^{n-2}x_2 + \cdots + 2^0 x_n$$

↑ binary form

$$f_{a,N}(x) = a^x \pmod N$$

$$= a^{2^{n-1}x_1 + \cdots + 2^0 x_n} \pmod N$$

$$= a^{2^{n-1}x_1} a^{2^{n-2}x_2} \cdots a^{2^0 x_n} \pmod N$$



↳ depth is polynomial in 'n'.

Similar design as quantum phase estimation.