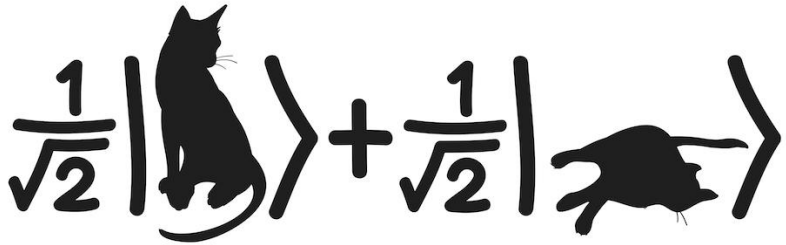
# Quantum Mechanics & Quantum Computation

**Umesh V. Vazirani**
University of California, Berkeley

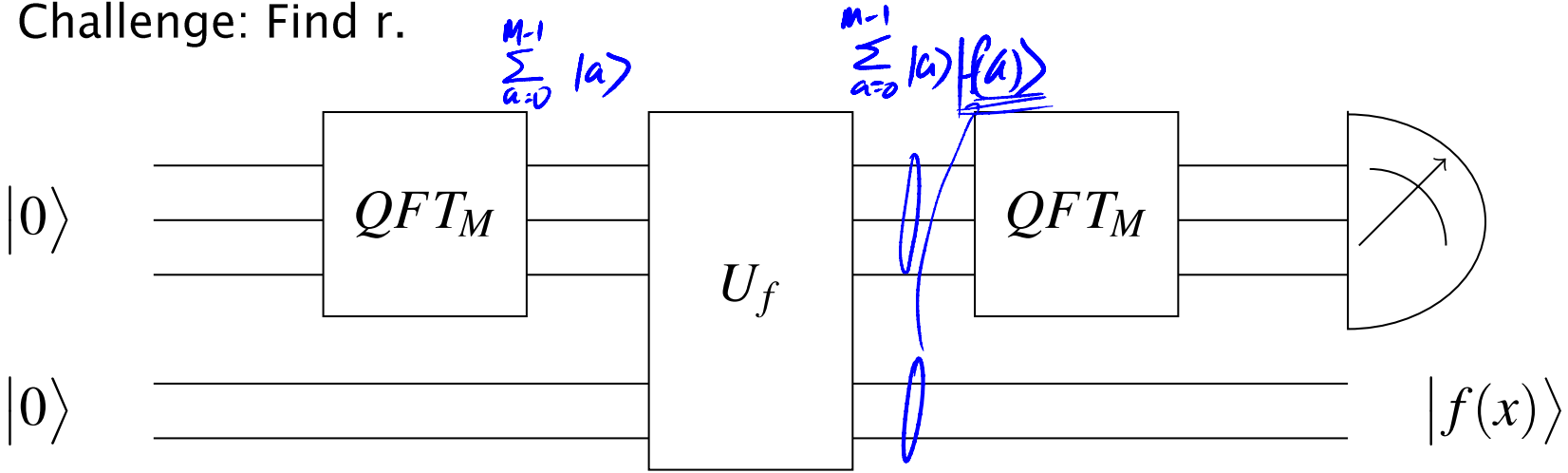



## Lecture 14: Quantum Factoring

Shor's Algorithm

# Period finding

f: {0, 1, …, M−1} → S, such that for all x, f(x) = f(x+r).
Challenge: Find r.



$N = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$

$N = P \cdot Q$

$N \approx 2^n$

1000 digit

500 digit $10^{500}$

$n$ bits $\exp(O(\sqrt{n}))$

↑ Classical

quantum – $O(n^3)$

modular arithmetic

- Modular arithmetic.
- a = b (mod N). e.g. 3 = 15 (mod 12)
- “Algorithms” by Dasgupta, Papadimitriou, Vazirani

  www.cs.berkeley.edu/~vazirani/algorithms.html

  Chapter 1: Modular Arithmetic
  Chapter 2 (2nd half): Fast fourier transform
  Chapter 10: Quantum factoring.

$N = 21$

$\sqrt{1} = \pm 1.$

$1^2 \equiv 1 \pmod{21}$

$-1^2 = 20^2 \equiv 1 \pmod{21}$

$400 \equiv 1 \pmod{21}$

$8^2 = 64 \equiv 1 \pmod{21}$

$-8^2 = 13^2 \equiv 1 \pmod{21}$

$\gcd(\overbrace{8+1}^{9}, 21) = 3$

$\gcd(\overbrace{13+1}^{14}, 21) = 7$

$\gcd(\underbrace{8-1}_{7}, 21) = 7$

$\gcd(\underbrace{13-1}_{12}, 21) = 3$

**Lemma:** If x is a nontrivial square root of 1 (mod N), then gcd(x+1, N) (and gcd(x−1,N)) is a nontrivial factor of N.

$x \not\equiv \pm 1 \pmod N \iff N \nmid (x \pm 1)$

$x^2 \equiv 1 \pmod N \iff x^2 - 1 \equiv 0 \pmod N$

$\iff N \mid (x^2 - 1)$

$\iff N \mid (x+1)(x-1)$

$\gcd(x+1, N)$ $\qquad$ $\gcd(x-1, N)$

P $\qquad$ Q

$2^0 = 1 \pmod{21}$

$2^1 = 2 \pmod{21}$

$2^2 = 4 \pmod{21}$

$2^3 = 8 \pmod{21}$

$2^4 = 16 \pmod{21}$

$2^5 = 11 \pmod{21}$

$2^6 = 1 \pmod{21}$

$$2^6 \equiv 1 \pmod{21}$$

$$(2^3)^2 \equiv 2^6 \equiv 1 \pmod{21}$$

$$8^2 \equiv 1 \pmod{21}$$

**Lemma:** Let N be an odd composite, with at least two distinct prime factors, and let x be uniformly random between 0 and N−1. If gcd(x, N) = 1, then with probability at least ½, the order r of x (mod N) is even, and $x^{r/2}$ is a nontrivial square root of 1 (mod N)

order of x

$1 \equiv x^r \pmod N$

r even & $y = x^{r/2} \not\equiv \pm 1 \bmod N$

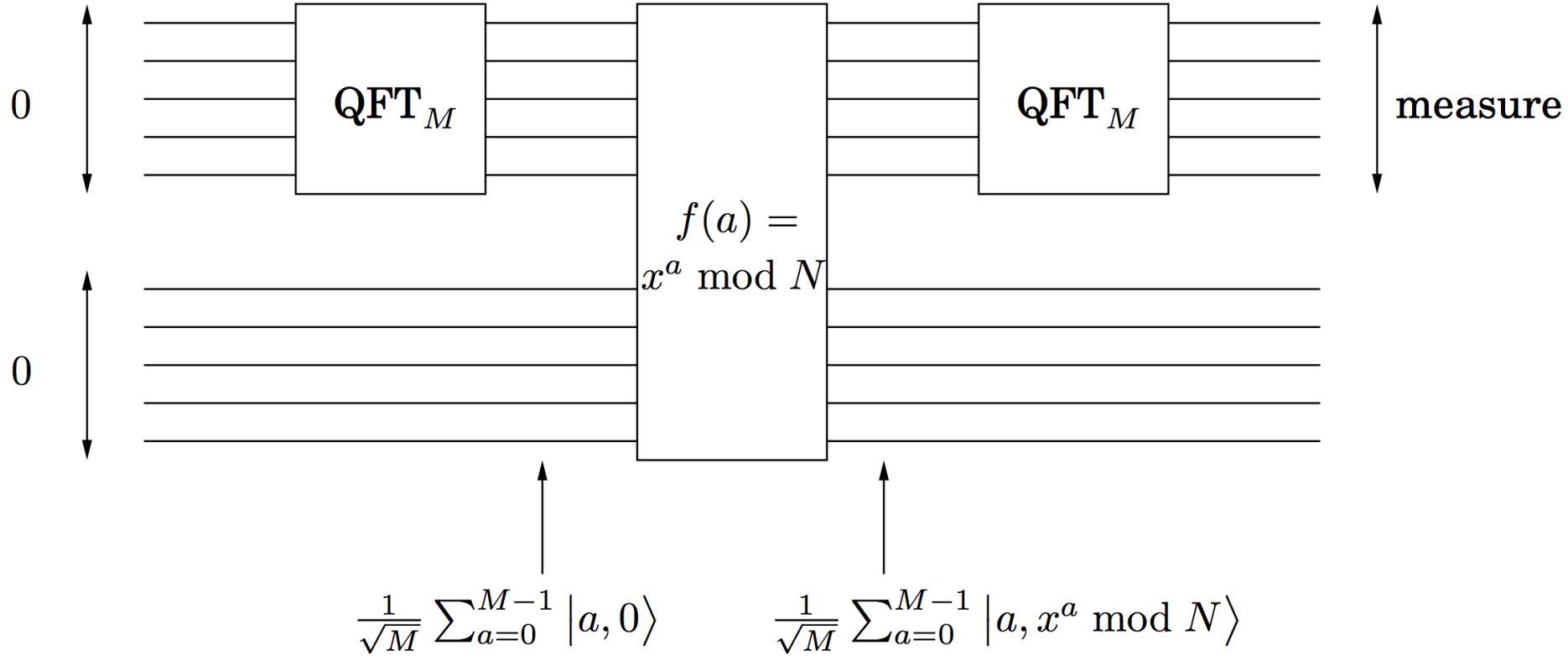
$y \not\equiv \pm 1 \bmod N$ $\qquad$ $y^2 = x^r \equiv 1 \pmod N$

$X = 2$

$N = 21$

$$\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1}$$

| $a$ | $f(a) = X^a \pmod N$ |
|---|---|
| 0 | 1 |
| 1 | 2 |
| 2 | 4 |
| 3 | 8 |
| 4 | 16 |
| 5 | 11 |
| 6 | 1 |
| 7 | 2 |
| 8 | 4 |
| 9 | 8 |
| 10 | 16 |
| 11 | 11 |
| 12 | 1 |
| 13 | 2 |
| 14 | 4 |
| ⋮ | |


0
0
$\mathbf{QFT}_M$
$f(a) = x^a \bmod N$
$\mathbf{QFT}_M$
measure
$\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$
$\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, x^a \bmod N\rangle$