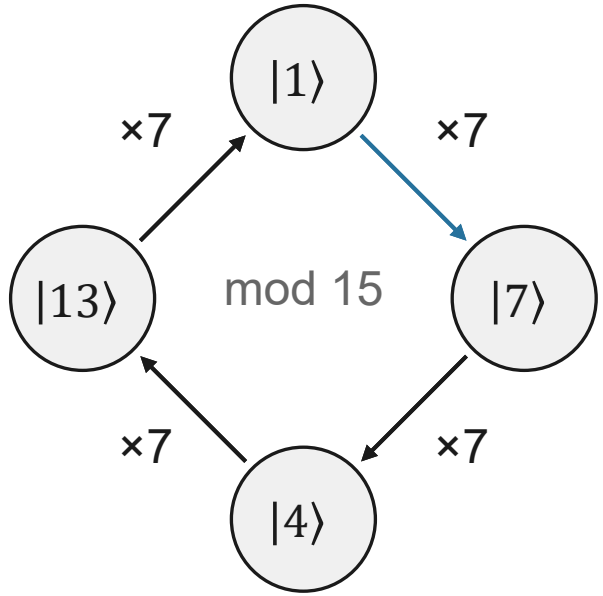
SAJID Lab
Smart & Advanced Junction of Intelligent Devices

EEE 6516 · QUANTUM COMPUTING

Order Finding and Shor's Algorithm

From phase estimation to the factors of N

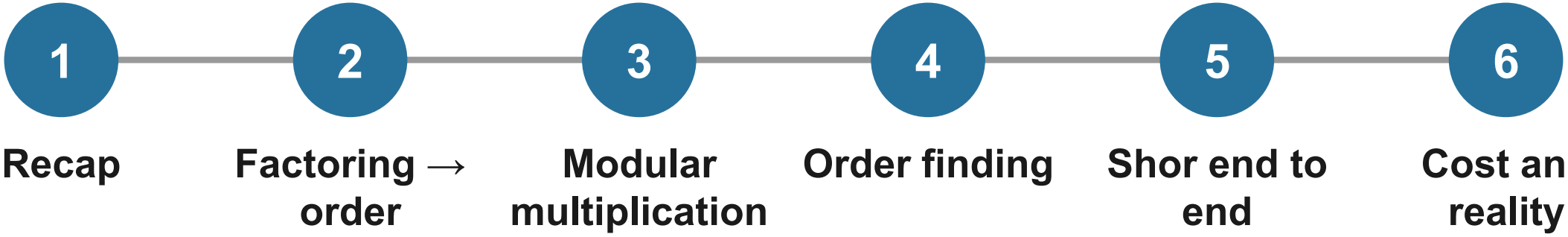


Chapter 6 · Lecture 14

Sajid Muhaimin Choudhury

Copyright © 2026 Sajid Muhaimin Choudhury. All rights reserved.

Today



By the end of this lecture you can

- carry out the reduction from factoring to order finding, with its conditions
- show that modular multiplication is unitary, find its eigenphases s/r, and explain why $|1\rangle$ suffices
- recover r from an outcome with continued fractions, and test it
- follow N = 15 end to end, and state honestly what factoring RSA-2048 would cost

YOUR TURN · RECALL

Recap: four eigenphases at once

Recall · 45 seconds

$U|u_s\rangle = e^{2\pi\, is/4}|u_s\rangle$ for s = 0, 1, 2, 3. Phase estimation with $t = 2$ runs on $\frac{1}{2}(|u_0\rangle + |u_1\rangle + |u_2\rangle + |u_3\rangle)$. The outcome is

A always 00, because the input is not an eigenvector

B 00, 01, 10 or 11, each with probability ¼

C always 01 or 10: the average phase 3/8, rounded

D uniformly random, and it carries no information

ANSWER

B: each two-bit string with probability ¼

$s/4 = 0.00, 0.01, 0.10, 0.11 \Rightarrow \text{outcomes } 00,01,10,11$

Each eigenvector alone is read exactly; the weights are |½|² = ¼ each.

C averages the phases: the mixture rule adds probabilities, never phases.

D: each outcome m tells us one s/4, a fraction with denominator 4.

An equal superposition of eigenstates returns s/r for a random s. The denominator is the prize.

1 From factoring to order finding

Why would knowing an order give us a factor?

Number theory in one slide

Powers of 7 modulo 15

$7^1 = 7$

$7^2 = 49 \equiv 4$

$7^3 \equiv 4 \cdot 7 = 28 \equiv 13$

$7^4 \equiv 13 \cdot 7 = 91 \equiv 1$

$\Rightarrow r = 4$

all congruences mod 15

a mod N: the remainder; $a \equiv b \pmod{N}$: N divides a − b.

Euclid: gcd(a, N) = gcd(N mod a, a), repeated; gcd(15, 48) = gcd(3, 15) = gcd(0, 3) = 3.

Coprime: gcd(a, N) = 1. Then the powers of a mod N return to 1.

Order r: the smallest r > 0 with $a^r \equiv 1 \pmod{N}$.

DERIVATION

From the order to a factor

N odd and composite, gcd(a, N) = 1, r the order of a; assume r even and $a^{r/2} \neq -1 \pmod{N}$.

$a^r \equiv 1 \Rightarrow N$ divides $a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1)$	r even: factor the difference
N does not divide $a^{r/2} - 1$	else $a^{r/2} \equiv 1$: the order would be ≤ r/2
N does not divide $a^{r/2} + 1$	the assumption $a^{r/2} \not\equiv -1$
$1 < \gcd(a^{r/2} \pm 1, N) < N$	N shares a factor with each bracket

Then $\gcd(a^{r/2} - 1, N)$ and $\gcd(a^{r/2} + 1, N)$ are non-trivial factors of N.

Worked example: factoring 15 by hand

a	1	2	4	7	8	11	13	14
r	1	4	2	4	4	2	4	2

1 Orders of every a coprime to 15: r = 1, 4, 2, 4, 4, 2, 4, 2.

Before the next slide

For a = 7: is r even, and is $7^2 \equiv -1$?

Worked example: factoring 15 by hand

a	1	2	4	**7**	8	11	13	14
r	1	4	2	**4**	4	2	4	2

1 Orders of every a coprime to 15: r = 1, 4, 2, 4, 4, 2, 4, 2.

2 a = 7: r = 4 is even, $7^2 = 49 \equiv 4 \not\equiv -1$. gcd(48, 15) = 3 and gcd(50, 15) = 5: 15 = 3 × 5.

$$7^{r/2} = 7^2 = 49 \equiv 4 \pmod{15}$$

$$\gcd(48,15) = 3, \qquad \gcd(50,15) = 5$$

Before the next slide

Which values of a would fail?

Worked example: factoring 15 by hand

a	1	2	4	**7**	8	11	13	14
r	1	4	2	**4**	4	2	4	2
	✗							✗

$$7^{r/2} = 7^2 = 49 \equiv 4 \pmod{15}$$

$$\gcd(48,15) = 3, \qquad \gcd(50,15) = 5$$

✗: r odd, or $a^{r/2} \equiv -1$: choose another a

1 Orders of every a coprime to 15: r = 1, 4, 2, 4, 4, 2, 4, 2.

2 a = 7: r = 4 is even, $7^2 = 49 \equiv 4 \not\equiv -1$. gcd(48, 15) = 3 and gcd(50, 15) = 5: 15 = 3 × 5.

3 a = 1 fails (r = 1 is odd); a = 14 fails (r = 2, but 14 ≡ −1). The other six succeed: 6 of 8.

2 Modular multiplication

Which unitary has the order of a in its eigenphases?

YOUR TURN · VOTE

Quick vote: why is modular multiplication unitary?

Vote · 30 seconds

The map $U_a|y\rangle = |ay \bmod N\rangle$ (for y < N) is unitary because

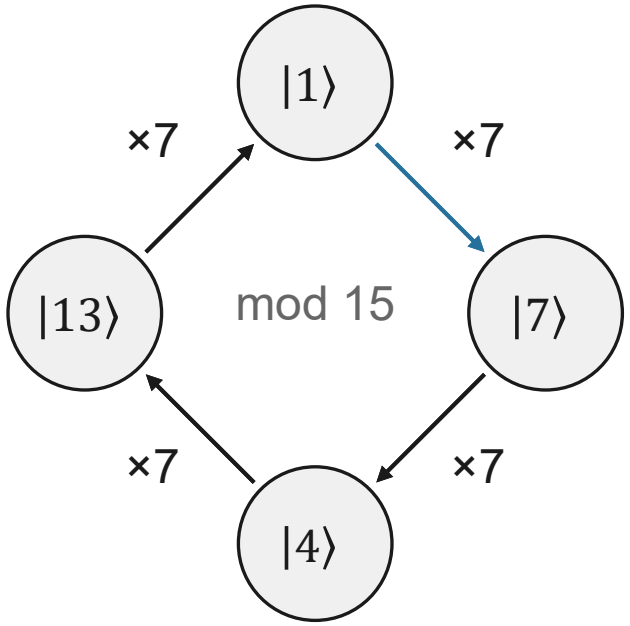
A a is prime, so multiplication by a can be reversed

B N is odd, so every residue has an inverse modulo N

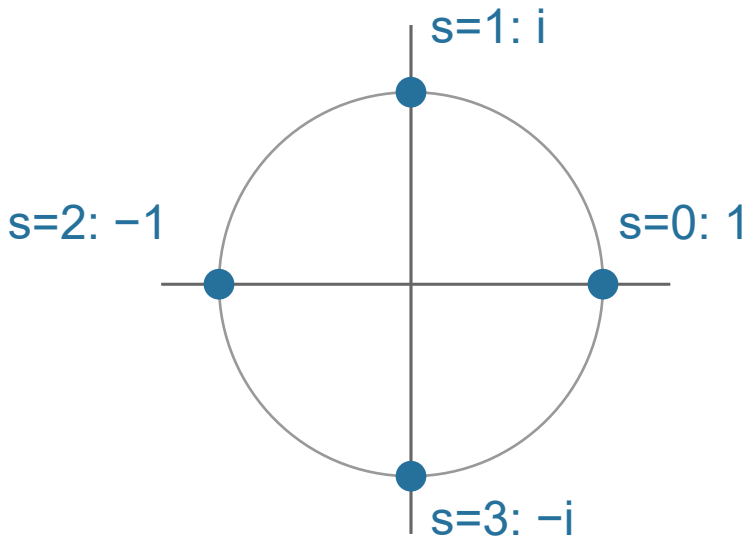
C $\gcd(a, N) = 1$, so y ↦ ay mod N permutes the basis states

D it is not unitary; it is implemented with a measurement

Multiplication by a is a permutation



(a) U_7 on the orbit of $|1\rangle$



(b) eigenvalues $e^{2\pi\, is/4}$

$U_a|y\rangle = |ay \bmod N\rangle$ for y < N.

gcd(a, N) = 1: y ↦ ay mod N is one to one, a permutation, so U_a is unitary.

From $|1\rangle$ the powers of a cycle with length r.

On the cycle: eigenvalues $e^{2\pi\, is/r}$, the r-th roots of unity.

DERIVATION

The eigenstates of the cycle

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k/r} \left| a^k \bmod N \right\rangle$$

Fourier modes of the cycle

$$U_a |u_s\rangle = (1/\sqrt{r}) \sum_k e^{-2\pi i s k/r} \left| a^{k+1} \right\rangle$$

each state moves one step on the cycle

$$= e^{2\pi i s/r} (1/\sqrt{r}) \sum_k e^{-2\pi i s(k+1)/r} \left| a^{k+1} \right\rangle$$

take out the factor $e^{2\pi i s/r}$

$$= e^{2\pi i s/r} |u_s\rangle$$

relabel k + 1 → k; $a^r \equiv 1$ closes the cycle

The eigenphases of U_a are s/r, s = 0, 1, …, r − 1: phase estimation would reveal the order.

DERIVATION

Check on N = 15: the eigenstate u_1

$$|u_1\rangle = \tfrac{1}{2}\left(|1\rangle + e^{-i\pi/2}|7\rangle + e^{-i\pi}|4\rangle + e^{-3i\pi/2}|13\rangle\right)$$ — s = 1, r = 4, a = 7

$$= \tfrac{1}{2}(|1\rangle - i|7\rangle - |4\rangle + i|13\rangle)$$ — evaluate the phases

$$U_7|u_1\rangle = \tfrac{1}{2}(|7\rangle - i|4\rangle - |13\rangle + i|1\rangle)$$ — move each state: 1 → 7 → 4 → 13 → 1

$$= i \cdot \tfrac{1}{2}(|1\rangle - i|7\rangle - |4\rangle + i|13\rangle) = i|u_1\rangle$$ — factor out i

Eigenvalue $i = e^{2\pi\, i/4}$: eigenphase ¼ = s/r, as the formula says.

YOUR TURN · VOTE

Quick vote: which state goes in?

Vote · 30 seconds

Order finding prepares the work register in $|1\rangle$ rather than in an eigenstate of U_a because

A $|1\rangle$ is itself an eigenstate of U_a, with eigenvalue 1

B $|1\rangle$ is an equal superposition of all the eigenstates $|u_s\rangle$

C any initial state gives the same outcome distribution

D the Hadamard gates turn $|1\rangle$ into an eigenstate of U_a

DERIVATION

The state |1⟩ is enough

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = \frac{1}{r}\sum_{k=0}^{r-1}\left(\sum_{s=0}^{r-1}e^{-2\pi\, isk/r}\right)\left|a^k\right\rangle$$

insert the definition; swap the sums

$$\sum_{s=0}^{r-1}e^{-2\pi\, isk/r} = r \text{ for } k = 0, \qquad 0 \text{ otherwise}$$

a full set of roots of unity

$$\frac{1}{\sqrt{r}}\sum_{s}|u_s\rangle = \frac{1}{r}\cdot\ r|a^0\rangle = |1\rangle$$

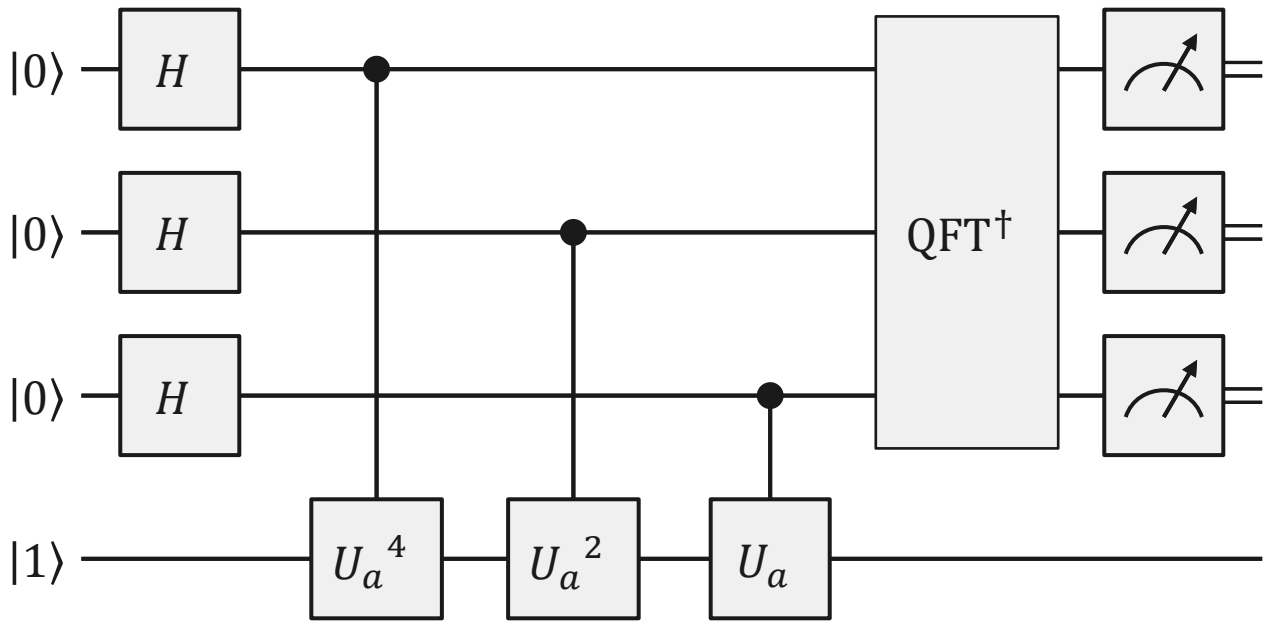
only k = 0 survives

|1⟩ is an equal superposition of all r eigenstates: no eigenstate has to be prepared.

3 Order finding

How do we turn an outcome m into the order r?

Order finding is phase estimation of U_a



drawn with t = 3; in practice t ≈ 2n, and the work register has n qubits

Work register in |1⟩: each run gives m/M ≈ s/r, with s uniform in {0, …, r − 1}.

Controlled $U_a^{2^j}$ is multiplication by $a^{2^j} \bmod N$, precomputed by repeated squaring.

Building these as reversible arithmetic is the expensive part of the algorithm.

Choose M ≥ N², about t = 2n counting qubits (N = 15: t = 8, M = 256).

Continued fractions recover s/r

Continued fraction

$$\frac{m}{M} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}} = [a_0; a_1, a_2, \ldots]$$

Theorem (N&C Thm 5.1)

$$\left|\frac{s}{r} - \frac{m}{M}\right| \leq \frac{1}{2r^2} \Rightarrow \frac{s}{r} \text{ is a convergent}$$

Expand m/M like Euclid: integer part, invert the remainder, repeat.

Convergents (truncations) are the best approximations with small denominators.

M ≥ N²: the nearest outcome is within 1/(2M) ≤ 1/(2r²) of s/r.

Take the last convergent with denominator < N; test $a^r \equiv 1 \pmod{N}$.

s/r comes out in lowest terms: if gcd(s, r) > 1 the test fails. Rerun; lcm.

WORKED EXAMPLE · STEP 1 OF 3

Worked example: continued fractions for N = 21

$N = 21, a = 2, t = 9\ (M = 512)$

$512 = 2 \cdot 171 + 170$

$171 = 1 \cdot 170 + 1$

$170 = 170 \cdot 1$

$\Rightarrow\ [0; 2,1,170]\colon\ 0, \frac{1}{2}, \frac{1}{3}, \frac{171}{512}$

1 Outcome m = 171: $171/512 = [0; 2,1,170]$; convergents 0, ½, ⅓, …
Candidate r = 3: $2^3 = 8 \not\equiv 1$. Rejected.

Before the next slide

Now expand 85/512. What candidate do you get?

Worked example: continued fractions for N = 21

$N = 21, a = 2, t = 9\ (M = 512)$

$512 = 6 \cdot 85 + 2$

$85 = 42 \cdot 2 + 1$

$2 = 2 \cdot 1$

$\Rightarrow\ [0; 6,42,2]:\ 0, \frac{1}{6}, \frac{42}{253}, \frac{85}{512}$

1 Outcome m = 171: $171/512 = [0; 2,1,170]$; convergents 0, ½, ⅓, … Candidate r = 3: $2^3 = 8 \not\equiv 1$. Rejected.

2 Outcome m = 85: $85/512 = [0; 6,42,2]$; convergents 0, ⅙, 42/253, … Candidate r = 6: $2^6 = 64 \equiv 1$. Accepted.

Before the next slide

Why did the first run give 3?

Worked example: continued fractions for N = 21

$N = 21, a = 2, t = 9\ (M = 512)$

$$\left|\frac{171}{512} - \frac{1}{3}\right| \approx 0.00065, \qquad \left|\frac{85}{512} - \frac{1}{6}\right| \approx 0.00065$$

$$\frac{1}{2 \cdot 6^2} \approx 0.014$$

$$\mathrm{lcm}(3,6) = 6 = r$$

1 Outcome m = 171: $171/512 = [0; 2,1,170]$; convergents 0, ½, ⅓, … Candidate r = 3: $2^3 = 8 \not\equiv 1$. Rejected.

2 Outcome m = 85: $85/512 = [0; 6,42,2]$; convergents 0, ⅙, 42/253, … Candidate r = 6: $2^6 = 64 \equiv 1$. Accepted.

3 First run: s/r = 2/6 reduced to ⅓ (gcd(2, 6) = 2). lcm(3, 6) = 6 = r. Both outcomes are within 0.00065 of s/r, far inside $1/(2 \cdot 6^2) \approx 0.014$.

YOUR TURN · CALCULATE

Your turn: an outcome for N = 15

Think · 45 seconds

Order finding for $N = 15$, $a = 7$, $t = 8$ (M = 256) returns $m = 128$. Which statement is right?

A candidate r = 2, and it passes the test, so r = 2

B candidate r = 2; $7^2 \equiv 4 \not\equiv 1$, so it is rejected and we run again

C the order is 128

D r = 4 directly, because 128/256 = 2/4

ANSWER

B: candidate 2 fails the test; run again

$128/256 = 1/2 \Rightarrow r = 2?\quad 7^2 = 49 \equiv 4 \neq 1 \pmod{15}$

It was s/r = 2/4: s and r share the factor 2, so the fraction reduced to ½.

A skips the test; C confuses m with r; D uses knowledge of r that we do not have.

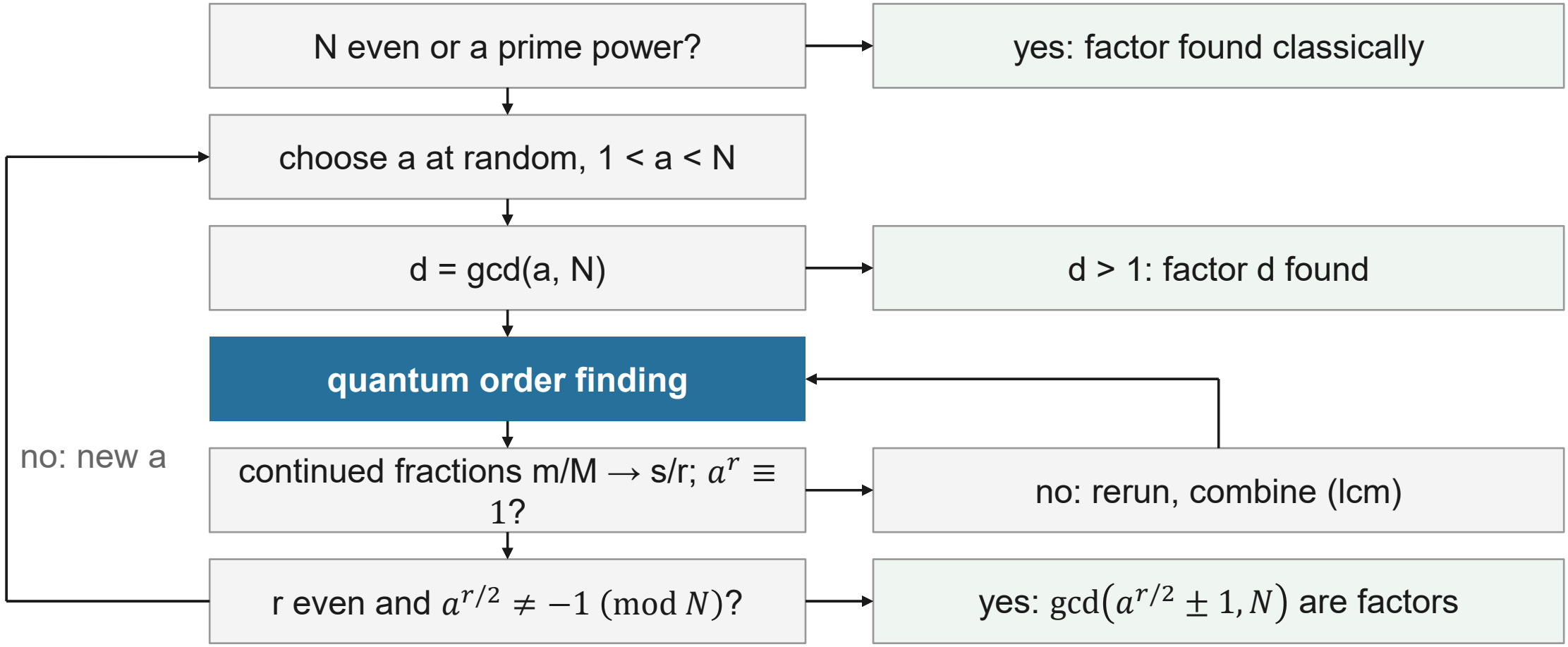
Outcomes 64 and 192 give ¼ and ¾: candidate 4, which passes.

Every candidate is tested with $a^r \equiv 1$; a failed test costs one more run.

4 Shor's algorithm, end to end

What does the whole algorithm look like, and how can it fail?

Shor's algorithm: one quantum step in a classical loop



SIMULATION · LIVE

Simulation 6.5 (live): factoring 15

```
N, a, t, w = 15, 7, 8, 4
U[y * pow(a, k, N) % N if y < N else y, y] = 1
qc.x(work[0])
qc.h(range(t))
for j in range(t):
    qc.append(power(2 ** (t - 1 - j)), [j] + work)
c = {k[::-1]: v for k, v in c.items()}
    f = estimate(int(k, 2), 2 ** t, N)
h = pow(a, r // 2, N)
```

Each power of U is built from its multiplication table: NOT a scalable circuit.

Inverse QFT: QFTGate on the reversed counting qubits; comments omitted.

m	counts	m/256	r
0	242	0	1 ✗
64	**260**	**1/4**	**4 ✓**
128	240	1/2	2 ✗
192	**258**	**3/4**	**4 ✓**

r = 4: 7^2 mod 15 = 4
factors 3 and 5
1000 shots; ✓ = passes $a^r \equiv 1$

YOUR TURN · VOTE

Quick vote: when does the reduction fail?

Vote · 30 seconds

For odd composite N and $\gcd(a, N) = 1$, the classical reduction fails when

A a is not prime

B r > N/2

C r is odd, or $a^{r/2} \equiv -1 \pmod{N}$

D r is even

DERIVATION

Worked example: a failing choice, N = 21 and a = 5

$5^k \bmod 21\colon\ 5, 4, 20, 16, 17, 1 \ \Rightarrow\ r = 6$	order finding works: r is even
$5^3 = 125 = 5 \cdot 21 + 20 \equiv 20 \equiv -1 \pmod{21}$	the second condition fails
$\gcd(126,21) = 21, \qquad \gcd(124,21) = 1$	both factors trivial
$a = 2\colon\ r = 6, 2^3 = 8 \neq -1\colon\ \gcd(7,21) = 7, \gcd(9,21) = 3$	a new a succeeds

Order finding worked; the classical reduction did not. A new a fixes it: 21 = 3 × 7.

5 Cost and reality

What would factoring a real RSA key take?

Gate counts: polynomial against sub-exponential

Shor's algorithm

$$O(n^3) \text{ gates}$$

modular multiplications dominate

Number field sieve (classical)

$$\exp\left(\Theta\left(n^{1/3}\log^{2/3} n\right)\right)$$

grows faster than any polynomial

n = number of bits of N (RSA-2048: n = 2048).

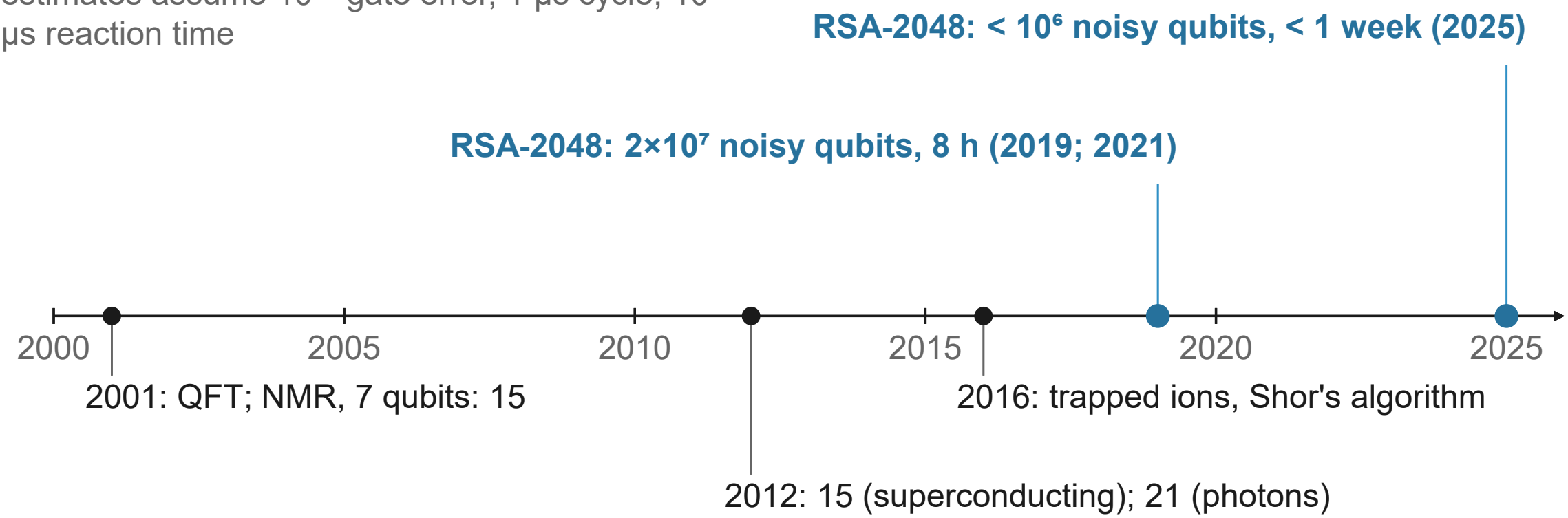
Modular multiplications with schoolbook arithmetic: O(n³); the QFT adds only O(n²).

Best classical method known: the number field sieve, super-polynomial.

The advantage is real but asymptotic: constants, error correction and engineering decide.

Resource estimates and demonstrations, dated

estimates assume 10^{-3} gate error, 1 μs cycle, 10 μs reaction time



Demonstrations factor 15 or 21. Estimates for RSA-2048 assume error-corrected machines.

DERIVATION

Worked example: logical and physical qubits

$$\text{logical qubits} = 3n + 0.002\, n\log_2 n$$

2019/2021 construction (Gidney–Ekerå)

$$n = 2048\text{: } \log_2 n = 11$$

$$3 \cdot 2048 + 0.002 \cdot 2048 \cdot 11 = 6144 + 45 \approx 6.2 \times 10^3$$

logical qubits

$$\frac{2 \times 10^7}{6.2 \times 10^3} \approx 3 \times 10^3$$

physical per logical

Each logical qubit is an error-corrected block of many noisy qubits: Chapter 8 explains the 10^3.

YOUR TURN · VOTE

Quick vote: what do the estimates say?

Vote · 30 seconds

Under their stated hardware assumptions, which statement about factoring a 2048-bit RSA modulus is supported by the surface-code estimates?

A It was achieved on a superconducting processor in 2019

B About 4096 physical qubits would suffice for the task

C It is impossible with fewer than 10^9 physical qubits

D It needs fewer than 10^6 noisy qubits and under a week

COMMON MISTAKE

“RSA is broken; a simulation of 15 proves it”

✗ Broken, and proven by simulation

“RSA is already broken.”

“The simulation factored 15,

so Shor works.”

Confuses estimates, demonstrations and simulations.

✓ Dated, with assumptions

Demonstrations: 15 and 21.

2025 estimate: ~10^6 noisy qubits, days.

Simulation: 2^{12} amplitudes and a table.

A simulation tests logic, not scaling.

Tie every statement about RSA-2048 to a date and its assumptions; N = 15 on a simulator shows the logic only.

Recap

1

Reduction

r even, $a^{r/2} \neq -1$: $\gcd\left(a^{r/2} \pm 1, N\right)$ are factors

2

Modular multiplication

U_a permutes; eigenphases s/r; $|1\rangle = \sum_s |u_s\rangle / \sqrt{r}$

3

Order finding

phase estimation on |1⟩; continued fractions; test $a^r \equiv 1$

4

Cost and reality

O(n³) gates; estimates $2\times10^7 \rightarrow < 10^6$ noisy qubits; demos 15, 21

Next week: Lecture 15 (Chapter 7)

Noise: density matrices, partial trace and the Bloch ball

Read: handout 6.5–6.7; 6.8 is self-study.

Exit ticket

For $N = 15$ and $a = 2$ the order is $r = 4$. Carry out the reduction: which factors do you get?

Copyright © 2026 Sajid Muhaimin Choudhury. All rights reserved.

Rights and attributions

Copyright (c) 2026 Sajid Muhaimin Choudhury. All rights reserved.

Public edition of Lecture 14: Order Finding and Shor's Algorithm. Release qc-2026-10-15, prepared 2026-10-15 from source revision 3df9449aa6.

This edition omits speaker notes, instructor-only material and every figure whose publication rights are not cleared for public distribution.