Shor's Factoring Algorithm

School on Quantum Computing @Yagami

Day 2, Lesson 2

10:30-11:30, March 23, 2005

Eisuke Abe

Department of Applied Physics and Physico-Informatics,
and CREST-JST, Keio University

Outline

- Number theory for factoring
  - Greatest common deviser and Euclidian method
  - Chinese remainder theorem
  - Quadratic equation for factoring
  - Order of a modulo L
- Factoring algorithm
  - Reduction to order finding
  - Continued fractions algorithm
  - Modular exponentiation

The inventor

Peter Shor

© Aya Furuta

Number theory for factoring

Purpose

To reduce factoring to order finding

1. Greatest common divisor and Euclidian method
2. Chinese remainder theorem
3. Quadratic equation for factoring
4. Order of a modulo L

Greatest common divisor

Definition

The largest integer which is a divisor of two integers a and b is called “greatest common divisor of a and b”, and denoted as

$$\gcd(a, b)$$

If $\gcd(a, b)$ is equal to 1, it is said that “a and b are co-prime”

Example

$$\gcd(9,6) = 3 \qquad \gcd(5,3) = 1$$

Euclidian method

An efficient method for finding the gcd

Example

$$\gcd(494,\ 133) = 19$$

$$494 = 133 \times 3 + 95$$

$$133 = 95 \times 1 + 38$$

$$95 = 38 \times 2 + 19$$

$$38 = 19 \times 2$$

Filling the floor of a rectangular room with square tiles

Chinese remainder theorem

(Below n_1, n_2, s, t, L ... are all positive integers)

Let n_1 and n_2 be co-prime, *i.e.*,

$$\gcd(n_1, n_2) = 1$$

p and q are the remainders of n_1 and n_2, respectively, *i.e.*,

$$0 \le p \le n_1 - 1$$

$$0 \le q \le n_2 - 1$$

Then there *exists* a *unique* s $(1 \le s \le n_1 n_2)$ that satisfies

$$s \equiv p \pmod{n_1}$$

$$s \equiv q \pmod{n_2}$$

Chinese remainder theorem

Proof of uniqueness

Suppose there exists t $(1 \le t \le n_1 n_2, t < s)$ that satisfies

$$t \equiv p \pmod{n_1}$$

$$t \equiv q \pmod{n_2}$$

$\gcd(9,15) \ne 1$

$45 \equiv 0 \pmod{9}$

$45 \equiv 0 \pmod{15}$

$45 \not\equiv 0 \pmod{135}$

Then

$$\begin{array}{l} s - t \equiv 0 \pmod{n_1} \\ s - t \equiv 0 \pmod{n_2} \end{array} \Rightarrow s - t \equiv 0 \pmod{n_1 n_2}$$

$\gcd(n_1, n_2) = 1$

This means $s - t \ge n_1 n_2$, which contradicts the assumption $1 \le t < s \le n_1 n_2$

Chinese remainder theorem

Proof of existence

There are $n_1 n_2$ possible pairs of p and q, and that s $(1 \leq s \leq n_1 n_2)$ is unique

Thus there must exist s for any pair of p and q

(Q.E.D)

Example

$n_1 = 3, n_2 = 5$

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
p	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
q	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0

Quadratic equation for factoring

Consider the quadratic equation

$$x^2 \equiv 1 \pmod{L} \qquad \text{...(1)}$$

Here $L = n_1 n_2$ with $\gcd(n_1, n_2) = 1$

Then there exist *nontrivial solutions* such that

$$x \equiv \pm s \pmod{L}$$

Here s is in the range $1 < s < L - 1$, and the gcd of L and $s \pm 1$ gives a nontrivial factor of L

Trivial solutions

$$x = \pm 1 \pmod{L}$$

Thus $1, L-1, L$ are excluded as candidates for nontrivial solutions

Quadratic equation for factoring

Proof

Chinese remainder theorem assures there exists s $(1 < s < L - 1)$ that satisfies

$$s \equiv 1 \pmod{n_1}$$
$$s \equiv -1 \pmod{n_2}$$

$$s = 1 \Rightarrow \begin{cases} s \equiv 1 \pmod{n_1} \\ s \equiv 1 \pmod{n_2} \end{cases}$$
$$s = L - 1 \Rightarrow \begin{cases} s \equiv -1 \pmod{n_1} \\ s \equiv -1 \pmod{n_2} \end{cases}$$
$$s = L \Rightarrow \begin{cases} s \equiv 0 \pmod{n_1} \\ s \equiv 0 \pmod{n_2} \end{cases}$$

This is a nontrivial solution to Eq. (1), because

$$\begin{aligned} s^2 - 1 &\equiv 0 \pmod{n_1} \\ s^2 - 1 &\equiv 0 \pmod{n_2} \end{aligned} \quad \Rightarrow \quad s^2 - 1 \equiv 0 \pmod{L}$$

$$\gcd(n_1, n_2) = 1$$

Quadratic equation for factoring

Proof (cont'd)

Therefore,

$$(s+1)(s-1) \equiv 0 \pmod{L}$$

On the other hand,

$$0 < s-1 < s+1 < L \qquad 1 < s < L-1$$

Hence the gcd of L and $s \pm 1$ is a nontrivial factor of L, and much the same argument holds for

$$s \equiv -1 \pmod{n_1}$$

$$s \equiv 1 \pmod{n_2}$$

(Q.E.D)

Quadratic equation for factoring

Example

$n_1 = 3, n_2 = 5$

Trivial solutions

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
p	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
q	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0

Nontrivial solutions

$$\begin{cases} 4 \equiv 1 \pmod{3} \\ 4 \equiv -1 \pmod{5} \end{cases} \Rightarrow \begin{cases} \gcd(15,\ 3) = 3 \\ \gcd(15,\ 5) = 5 \end{cases}$$

$$\begin{cases} 11 \equiv -1 \pmod{3} \\ 11 \equiv 1 \pmod{5} \end{cases} \Rightarrow \begin{cases} \gcd(15,\ 10) = 5 \\ \gcd(15,\ 12) = 3 \end{cases}$$

Order of a modulo L

Definition

The least positive integer r that satisfies

$$a^r \equiv 1 \pmod{L}$$

a is in the range $0 \le a \le L-1$, and co-prime to L

Solving Eq. (1)

$$x^2 \equiv 1 \pmod{L}$$

Find r, and *if r is even*, set

$$s \equiv a^{r/2} \pmod{L}$$

If we are lucky, this is a nontrivial solution to Eq. (1), and we can factor L!

Order of a modulo $L = 15$

Factoring 15

a	r	$a^{r/2} \pm 1$	gcd w/ 15	
2	4	3, 5	3, 5	$2^4 = 16 \equiv 1$
4	2	3, 5	3, 5	$4^2 = 16 \equiv 1$
7	4	48, 50	3, 5	$7^4 = (49)^2 \equiv 4^2 \equiv 1$
8	4	63, 65	3, 5	$8^4 \equiv (-7)^4 \equiv 1$
11	2	10, 15	5, 3	$11^2 \equiv (-4)^2 \equiv 1$
13	4	168, 170	3, 5	$13^4 \equiv (-2)^4 \equiv 1$

We already know “14” yields a trivial solution, so, may well set the range of a as $1 < a < 14$

Order of a modulo $L = 21$

Factoring 21

a	r	$a^{r/2} \pm 1$	gcd w/ 21	
2	6	7, 9	7, 3	
4	3			Odd r
5	6	124, 126	19, 21	Trivial solution
8	2	7, 9	7, 3	
10	6	999, 1001	3, 7	
11	6	1330, 1332	7, 3	
13	2	12, 14	3, 7	
16	3			Odd r
17	6	4912, 4914	19, 21	Trivial solution
19	6	6858, 6860	3, 7	

"ay modulo L" is a permutation

Define $\pi(y)$ as $ay \pmod{L}$

Example

$\gcd(L, a) = 1$

$L = 15, a = 7$

y	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\pi(y)$	0	7	14	6	13	5	12	4	11	3	10	2	9	1	8

$7 \times 0 \pmod{15} = 0$

$7 \times 1 \pmod{15} = 7$

$7 \times 2 \pmod{15} = 14$

$7 \times 3 \pmod{15} = 6$

$11 \times 0 \pmod{15} = 0$

$11 \times 1 \pmod{15} = 11$

$11 \times 2 \pmod{15} = 7$

$11 \times 3 \pmod{15} = 3$

$L = 15, a = 11$

y	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\pi(y)$	0	11	7	3	14	10	6	2	13	9	5	1	12	8	4

Reduction to order finding

Now we can identify "ay mod L" as "permutation"

$$\pi(y) \Leftrightarrow ay \pmod{L}$$

For instance,

$$\pi^3(y) \Leftrightarrow a(a(ay)) \pmod{L}$$
$$\Leftrightarrow a^3 y \pmod{L}$$

Thus "finding the order of a mod L" is equivalent to "finding the order of $\pi(1)$"

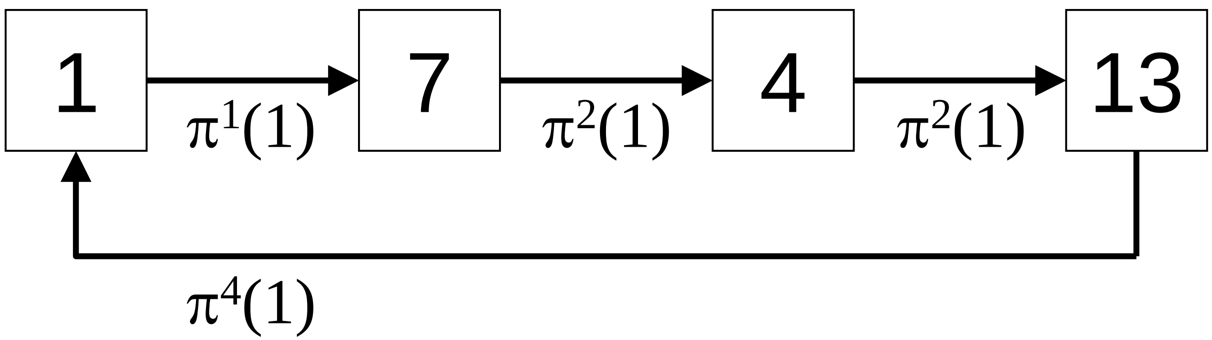
$$a^r \equiv 1 \pmod{L} \Leftrightarrow \pi^r(1) = 1$$

Order of a modulo L

Example

$L = 15,\ a = 7$

y	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\pi(y)$	0	7	14	6	13	5	12	4	11	3	10	2	9	1	8



$$7^{4/2} - 1 = 48 \quad \rightarrow \quad \gcd(15,\ 48) = 3$$

$$7^{4/2} + 1 = 50 \quad \rightarrow \quad \gcd(15,\ 50) = 5$$

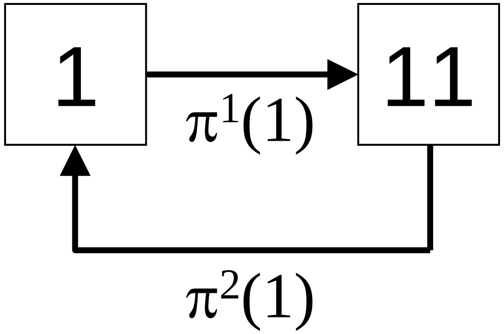
Succeed!

Order of a modulo L

Example

$L = 15,\ a = 11$

y	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\pi(y)$	0	11	7	3	14	10	6	2	13	9	5	1	12	8	4



$$11^{2/2} - 1 = 10 \quad \rightarrow \quad \gcd(15,\ 10) = 5$$

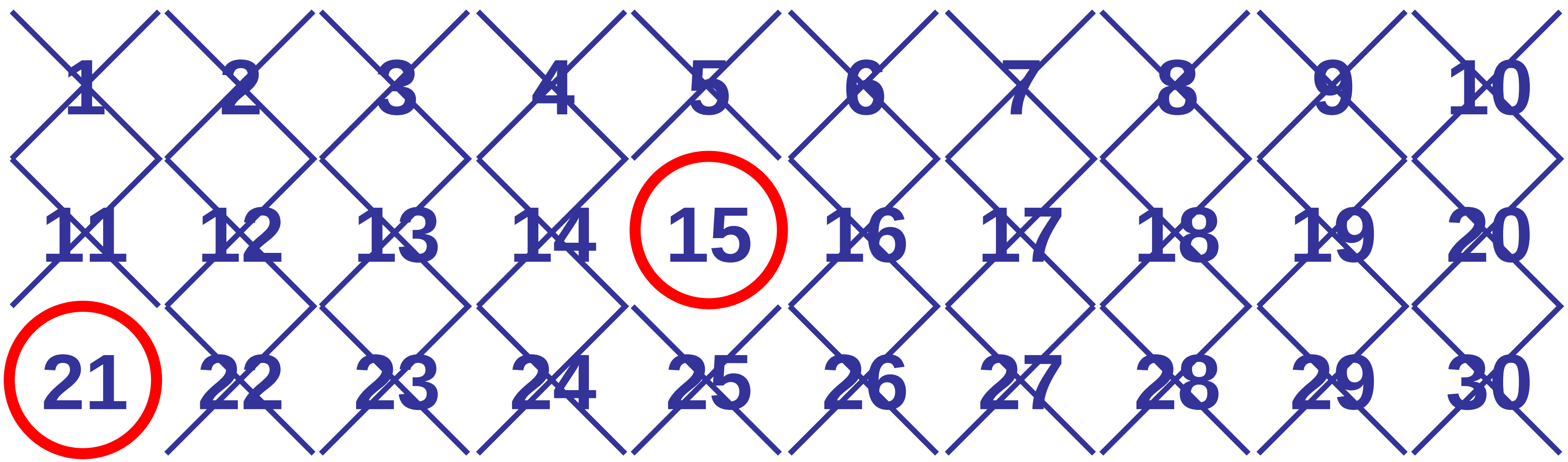
$$11^{2/2} + 1 = 12 \quad \rightarrow \quad \gcd(15,\ 12) = 3$$

Succeed!

Factoring algorithm

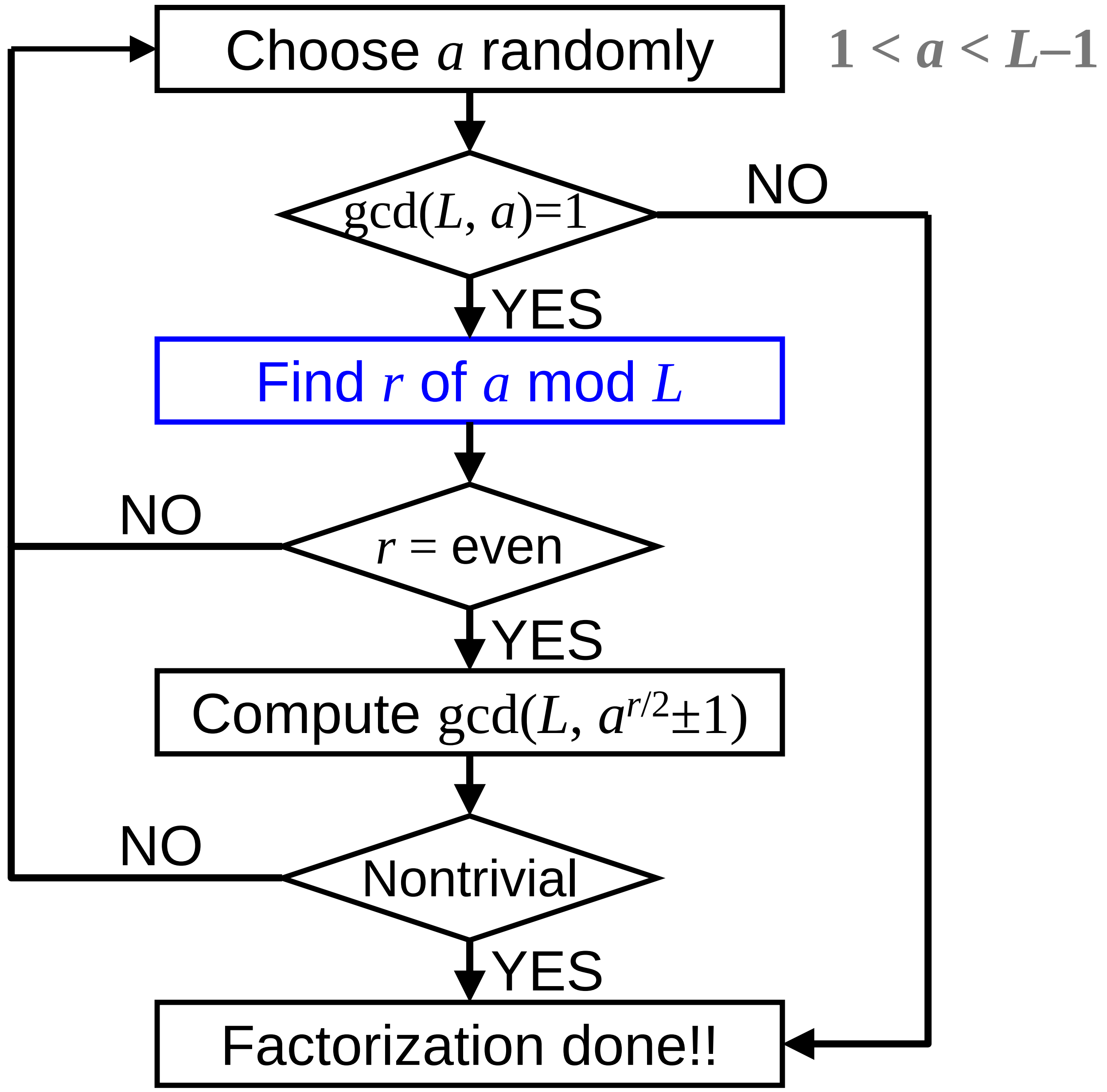
The algorithm ***fails*** when L is ...

1. even
2. a prime number
3. a prime power



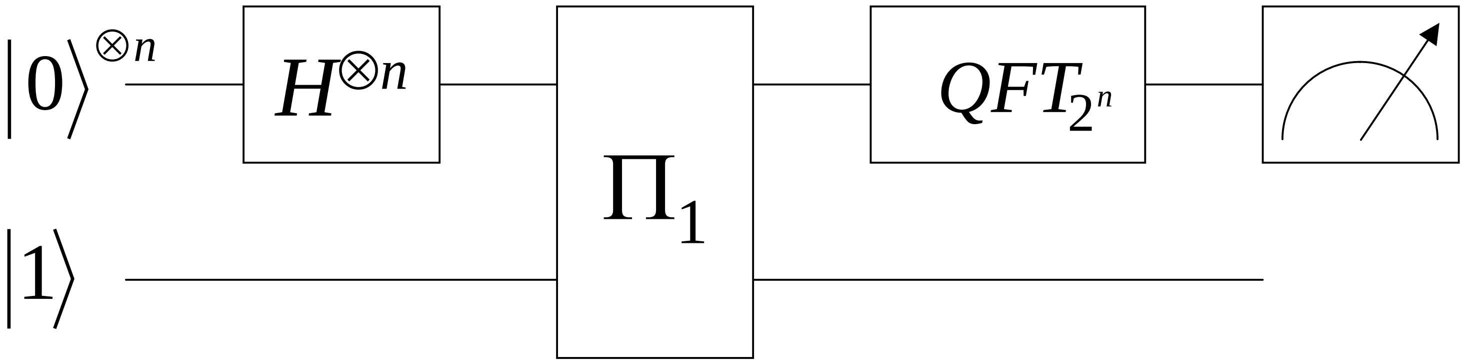
Those can be checked efficiently by classical methods before we run the algorithm

Flowchart



Choose a randomly
$1 < a < L-1$
$\gcd(L, a)=1$
NO
YES
Find r of a mod L
NO
r = even
YES
Compute $\gcd(L, a^{r/2}\pm 1)$
NO
Nontrivial
YES
Factorization done!!

Order finding for factoring



$$\Pi_1 |x\rangle|1\rangle = |x\rangle|\pi^x(1)\rangle$$
$$= |x\rangle|a^x (\mathrm{mod}\, L)\rangle$$

Nothing changes...
We have only to replace $\pi(y)$
by $ay\ (\mathrm{mod}\ L)$ with $y = 1$

Remaining issues

Now is the time to answer those questions!

- The measurement does not give us r itself, then how to obtain r out of the measurement result?
- What if r does not divide N?
- How to construct the Π_1 gate?
- If it remains a black box, how can the algorithm be useful?

Remaining issues

Now is the time to answer those questions!

- The measurement does not give us r itself, then how to obtain r out of the measurement result?
- What if r does not divide N?
- How to construct the Π_1 gate?
- If it remains a black box, how can the algorithm be useful?

Continued fractions algorithm

Split | **Invert**

$$\alpha = \frac{31}{13} = 2 + \frac{5}{13} = 2 + \frac{1}{\frac{13}{5}}$$

$$= 2 + \cfrac{1}{2 + \cfrac{3}{5}} = 2 + \cfrac{1}{2 + \cfrac{1}{\frac{5}{3}}}$$

$$= 2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{2}{3}}} = 2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{\frac{3}{2}}}}$$

$$= 2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}} = [2,2,1,1,2]$$

Continued fractions algorithm

$$\frac{p_0}{q_0} = [2] = \frac{2}{1} = 2$$

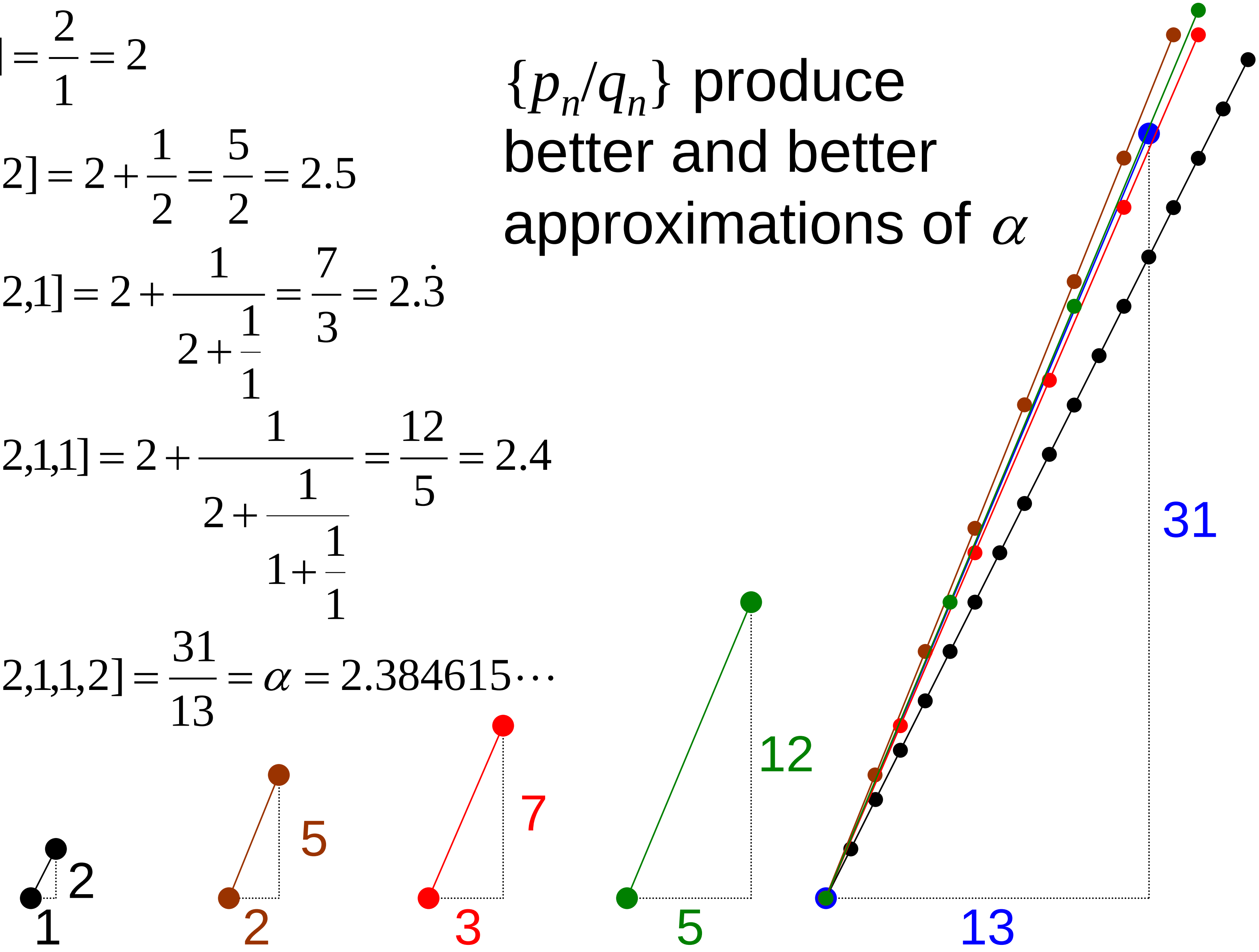
$$\frac{p_1}{q_1} = [2,2] = 2 + \frac{1}{2} = \frac{5}{2} = 2.5$$

$$\frac{p_2}{q_2} = [2,2,1] = 2 + \cfrac{1}{2 + \cfrac{1}{1}} = \frac{7}{3} = 2.\dot{3}$$

$$\frac{p_3}{q_3} = [2,2,1,1] = 2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1}}} = \frac{12}{5} = 2.4$$

$$\frac{p_4}{q_4} = [2,2,1,1,2] = \frac{31}{13} = \alpha = 2.384615\cdots$$

$\{p_n/q_n\}$ produce better and better approximations of α



Continued fractions algorithm

Given the continued fraction expansion

$$\alpha = [a_0, a_1, \cdots, a_m]$$

Then the nth convergent of α is given by

$$p_n = a_n p_{n-1} + p_{n-2}$$
$$q_n = a_n q_{n-1} + q_{n-2}$$

with

$$(p_{-2}, q_{-2}) = (0,1)$$
$$(p_{-1}, q_{-1}) = (1,0)$$

n	–2	–1	0	1	2	3	4
a_n	–	–	2	2	1	1	2
p_n	0	1	**2**	**5**	**7**	**12**	**31**
q_n	1	0	**1**	**2**	**3**	**5**	**13**

It can be shown that p_n and q_n are co-prime

Continued fractions algorithm

Suppose k/r is a rational number such that

$$\left|\frac{k}{r} - \varphi\right| \le \frac{1}{2r^2}$$

Then k/r is a convergent of the continued fraction for φ

The inequality holds if φ is an approximation of k/r accurate to $2l + 1$ bits

$$\left|\frac{k}{r} - \varphi\right| \le \frac{1}{2^{2l+1}} \le \frac{1}{2r^2}$$

$$l \equiv \lceil \log_2 L \rceil \quad (2^{l-1} < L \le 2^l)$$

$$2^{2l+1} = 2(2^l)^2 \ge 2L^2 \ge 2r^2$$

Case study: Factoring 39

Step 1: Choose random a coprime to L

$$a = 7$$

Step 2: Find r

$$r = 12$$

Continued fractions algorithm after measurement

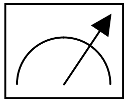
Step 3: Compute $\gcd(L,\ a^{r/2} \pm 1)$

$$7^{12/2} - 1 \equiv 24 \pmod{39} \quad \rightarrow \quad \gcd(39,\ 24) = 3$$

$$7^{12/2} + 1 \equiv 26 \pmod{39} \quad \rightarrow \quad \gcd(39,\ 26) = 13$$

Determining r after measurement

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



$$\longrightarrow \quad |\lambda\rangle \approx \left| \frac{N}{r} k \right\rangle$$

<u>Example</u>

$$L = 39$$

$$a = 7$$

$$r = 12$$

$$l = \lceil \log_2 L \rceil = 6$$

$$N = 2^{2l+1} = 8192$$

$$k = 5$$

$$\lambda = 3413$$

$$\frac{Nk}{r} = \frac{8192 \cdot 5}{12} = 3413.\dot{3}$$

$$\frac{\lambda}{N} \approx \frac{k}{r}$$

$$\frac{3413}{8192} = 0 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{170 + \cfrac{1}{4}}}}}$$

$$= [0,2,2,2,170,4]$$

Determining r after measurement

n	–2	–1	0	1	2	3	4	5
a_n	–	–	0	2	2	2	170	4
p_n	0	1	**0**	**1**	**2**	**5**	**852**	**3413**
q_n	1	0	**1**	**2**	**5**	**12**	**2045**	**8192**

$$\underbrace{\frac{p_1}{q_1}=\frac{1}{2} \quad \frac{p_2}{q_2}=\frac{2}{5} \quad \frac{p_3}{q_3}=\frac{5}{12}} \quad \underbrace{\frac{p_4}{q_4}=\frac{852}{2045} \quad \frac{p_5}{q_5}=\frac{3413}{8192}}$$

Candidates for k/r

$r \le L = 39$

Compute $a^{q_n} \pmod{L}$

Know that $q_3 = 12$ is the order

Remaining issues

Now is the time to answer those questions!

- The measurement does not give us r itself, then how to obtain r out of the measurement result?
- What if r does not divide N?
- How to construct the Π_1 gate?
- If it remains a black box, how can the algorithm be useful?

Π_1 gate

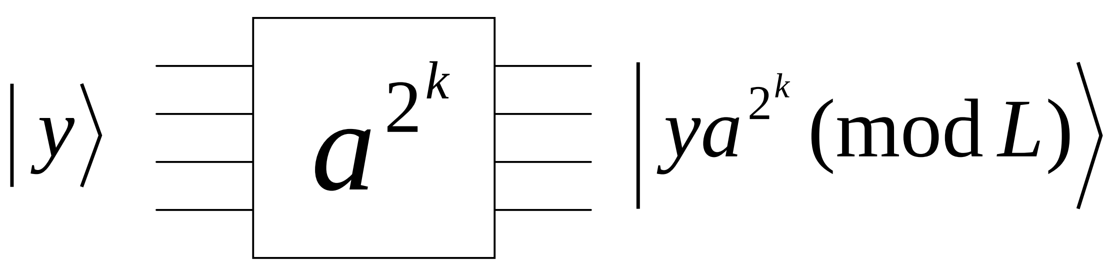
$$\Pi_1 |x\rangle|1\rangle = |x\rangle\left|a^x (\mathrm{mod}\, L)\right\rangle$$

$$x = 2^{n-1}x_n + 2^{n-2}x_{n-1} + \cdots + 2x_1 + x_0$$

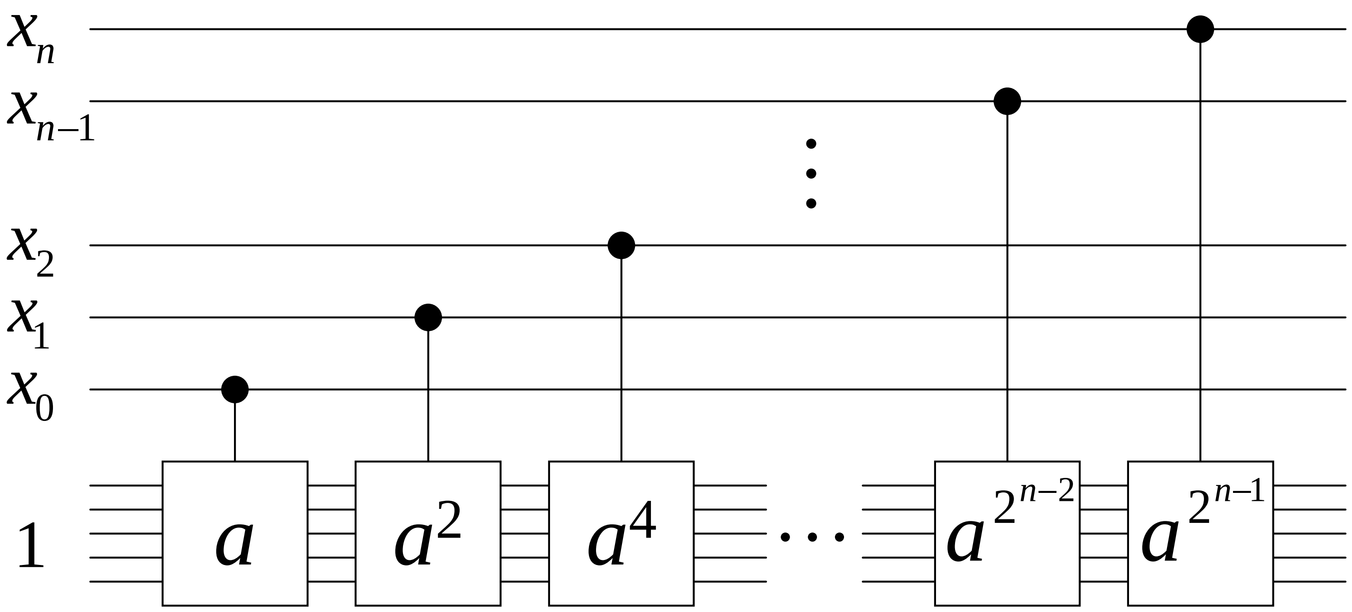
$$a^x (\mathrm{mod}\, L) = a^{2^{n-1}x_n + 2^{n-2}x_{n-1} + \cdots 2x_1 + x_0} (\mathrm{mod}\, L)$$

$$= \underbrace{[a^{2^{n-1}} (\mathrm{mod}\, L)]^{x_n} [a^{2^{n-2}} (\mathrm{mod}\, L)]^{x_{n-1}} \cdots [a \ (\mathrm{mod}\, L)]^{x_0}}_{\text{Controlled-}U\text{ gates}}$$

Controlled-U gates



Modular exponentiation



We must at least calculate $a^{2^k} \pmod{L}$ classically by repeated squaring

$$(a^{2^{k-1}})^2 = a^{2^k}$$

The circuit is constructed without knowing the order itself

Case study: Factoring 15

<u>Step 1: Choose random a coprime to L</u>

$$a = 7$$

<u>Step 2: Find r</u>

$$r = 4$$

Concrete construction of Π gate due to Vandersypen *et al*. will be given in the following slides

<u>Step 3: Compute $\gcd(L, a^{r/2} \pm 1)$</u>

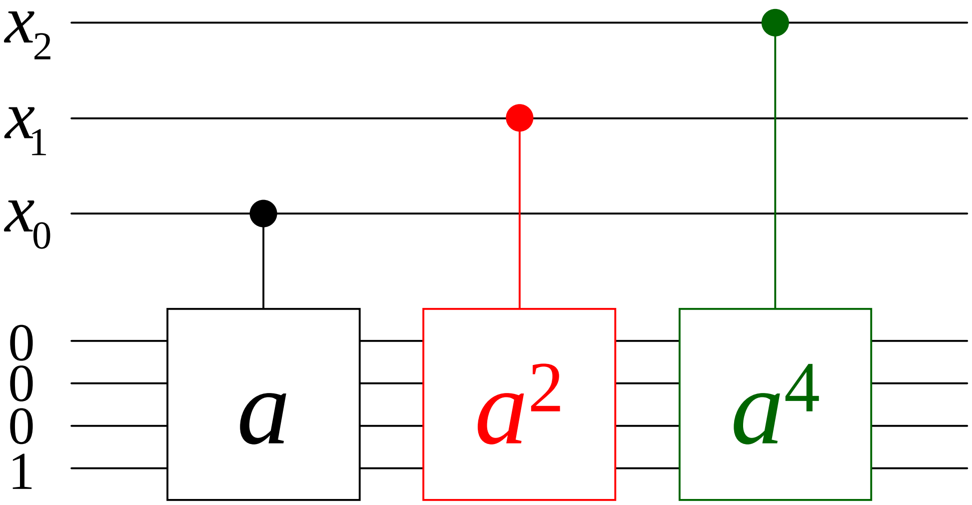
$$7^{4/2} - 1 = 48 \quad \rightarrow \quad \gcd(15,\ 48) = 3$$

$$7^{4/2} + 1 = 50 \quad \rightarrow \quad \gcd(15,\ 50) = 5$$

Finding r of a modulo 15

$$a^{2^k}\left|y\right\rangle = \left|ya^{2^k}\,(\mathrm{mod}\,L)\right\rangle$$

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



Only needed when $a = 2, 7, 8, 13$

Trivial

In reality, if $r = 2^k$, a quantum computer is not necessary (Know r during repeated squaring)

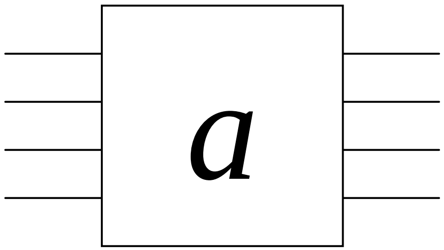
Modular exponentiation

Example: $a = 7$

$$
\begin{aligned}
& a \pmod{15} \\
= \quad & (a-1)+1 \pmod{15} \\
= \quad & (4\cdot 1 + 2\cdot 1)+1 \pmod{15}
\end{aligned}
$$

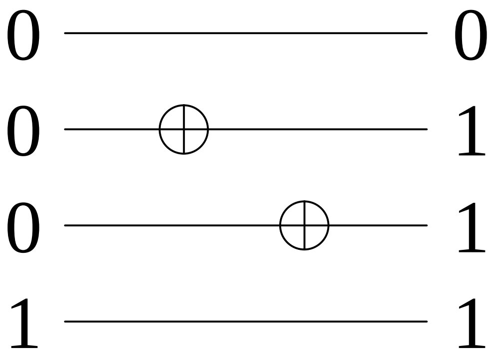
$$y = 8y_3 + 4y_2 + 2y_1 + y_0$$

$|y_3 y_2 y_1 y_0\rangle$
$= |0001\rangle$



$|0111\rangle$

$=$



For other a, the gate is constructed in a similar fashion

Modular exponentiation

Example: $a = 7$ (and 2, 8, 13)

$$a^2 y \pmod{15}$$

$$= 4 \times (8y_3 + 4y_2 + 2y_1 + y_0) \pmod{15}$$

$$= 32y_3 + 16y_2 + 8y_1 + 4y_0 \pmod{15}$$

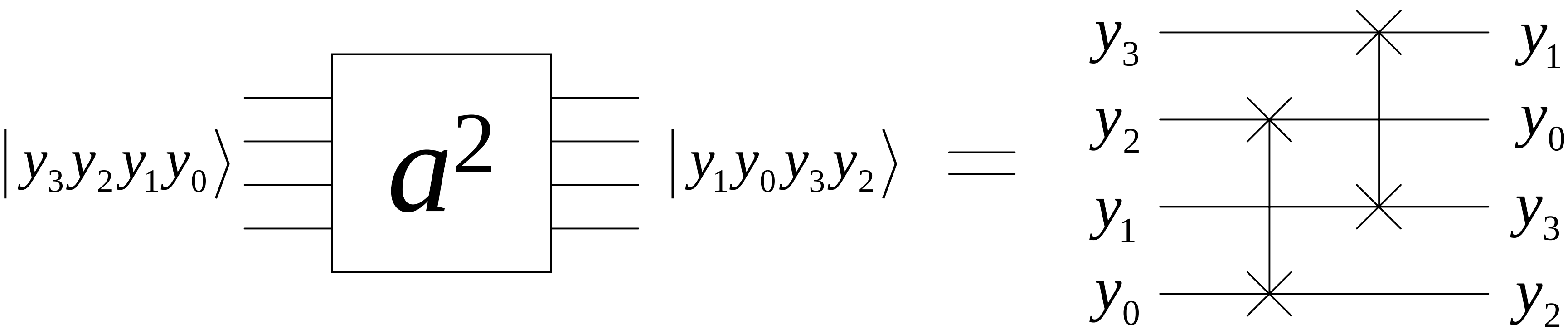
$$= 2y_3 + y_2 + 8y_1 + 4y_0 \pmod{15}$$

$$= 8y_1 + 4y_0 + 2y_3 + y_2 \pmod{15}$$

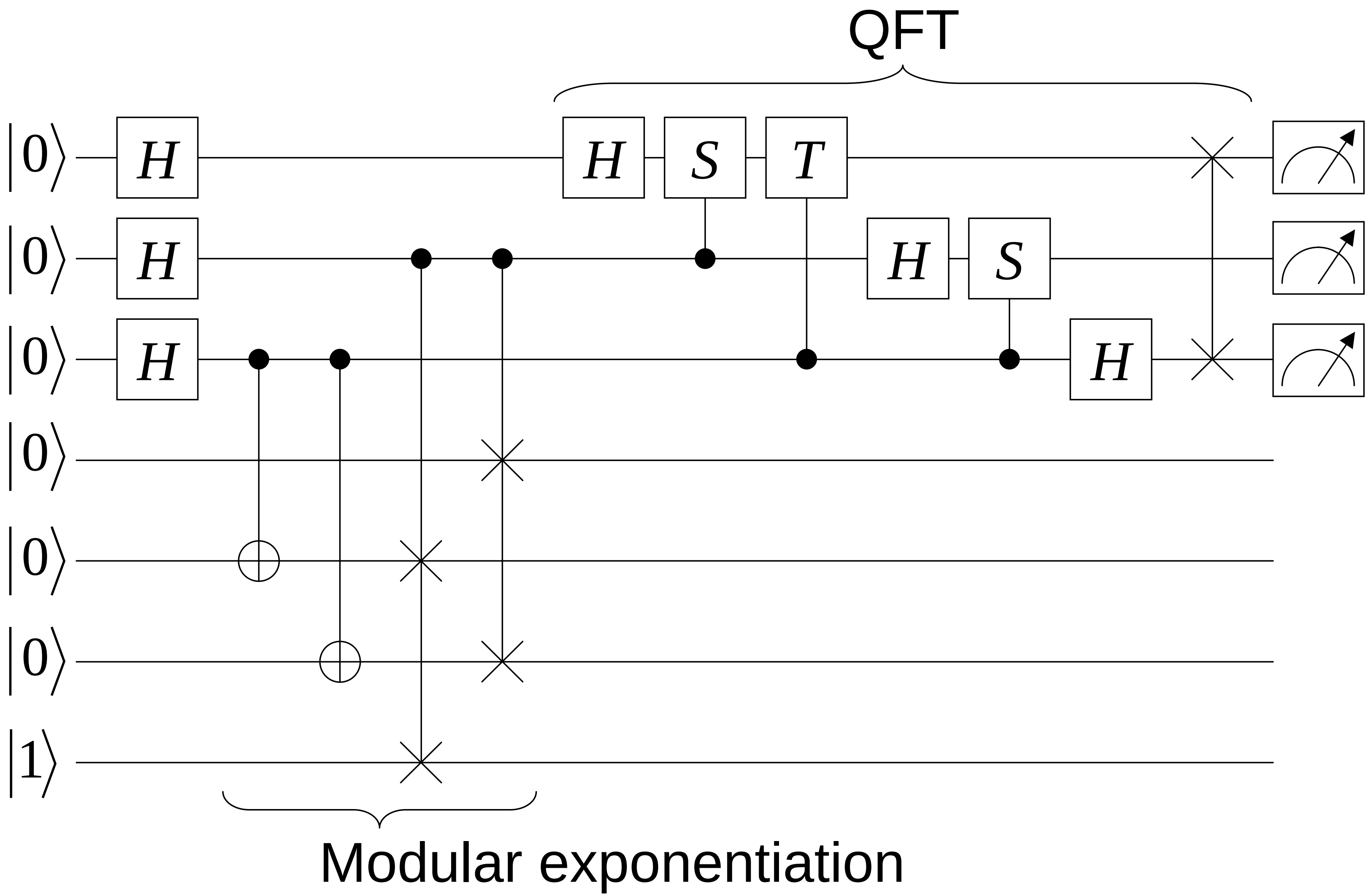
$$a^2 = 4 \pmod{15}$$

$$32 = 2 \pmod{15}$$

$$16 = 1 \pmod{15}$$

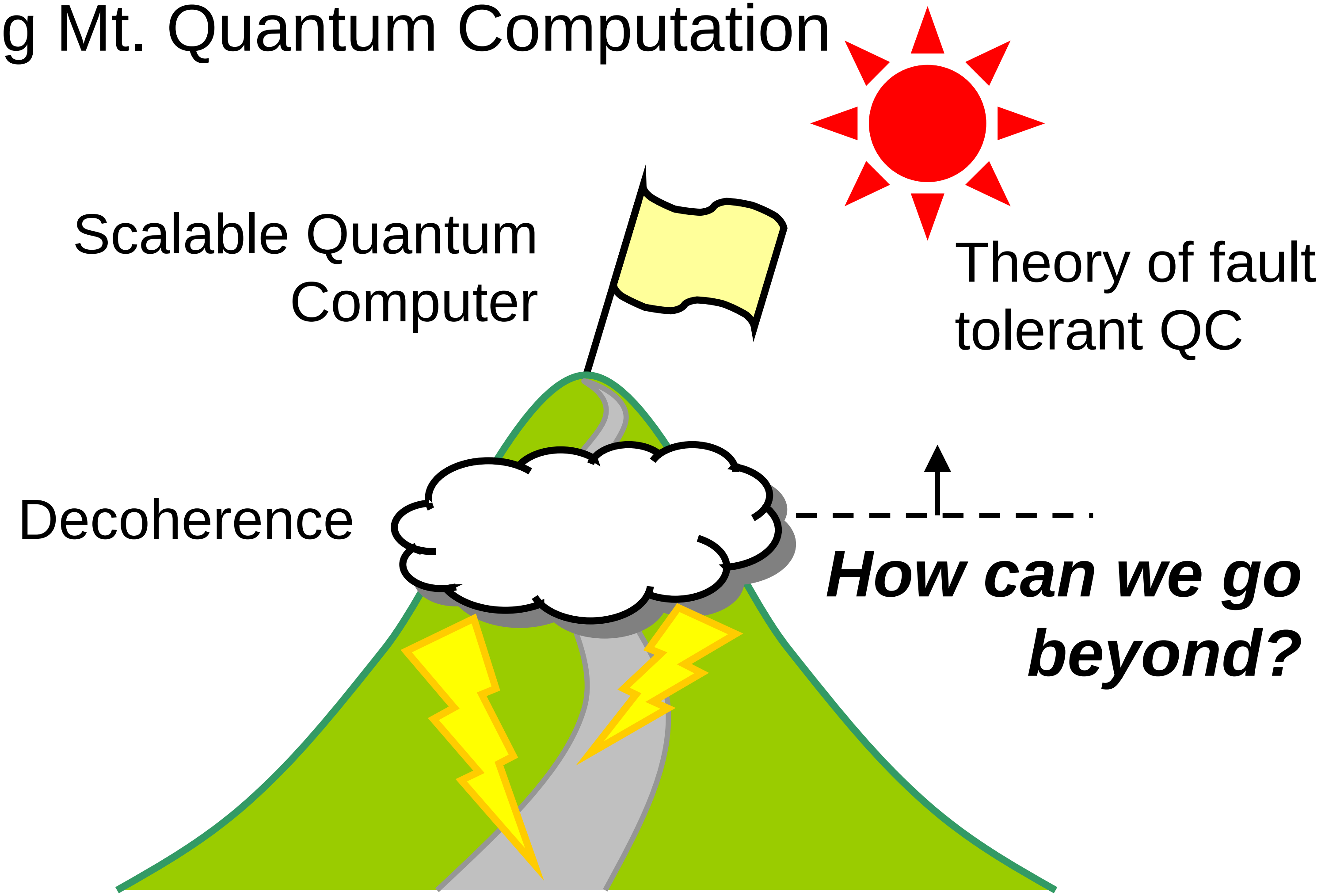


Quantum circuit for factoring 15



Where are we now?

Climbing Mt. Quantum Computation



We are still at the foot of the mountain…

Thank you for your attention!!