

Title: PSI 17/18 - Quantum Information - Lecture 7

Date: Feb 28, 2018 11:30 AM

URL: <http://pirsa.org/18020050>

Abstract:

RSA (named for Rivest, Shamir, Adleman):

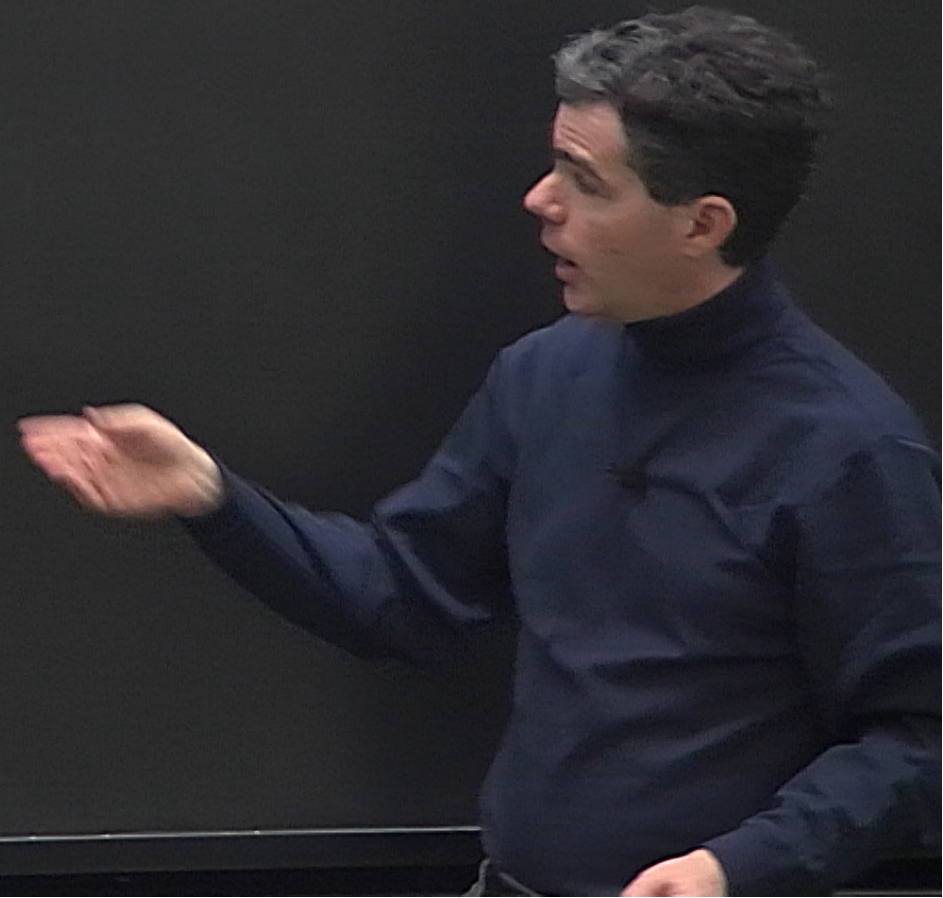
Key generation: Bob chooses 2 large primes p & q .

Let $N = pq$. Bob also chooses $e < N$, finds d s.t. $x^{ed} = x \pmod{N} \forall x$.

Private key: d

Public key: (N, e)

Encryption: Given message x ,
Ciphertext $y = x^e \bmod N$.



Encryption: Given message x ,

Ciphertext $y = x^e \bmod N$.

Decryption: Given y , decrypt to
 $x' = y^d \bmod N$.

Note: If y is a valid ciphertext
 $x' = (x^e)^d \bmod N \equiv x \pmod{N}$.

Thm. (Euler's thm): Let $\varphi(N)$ be Euler's totient function,

equal # of positive integers $< N$ & relatively prime to N .

In particular, $\varphi(pq) = (p-1)(q-1)$.

$$\forall x < N, \quad x^{\varphi(N)} = 1 \pmod{N}.$$

Thm. (Euler's thm): Let $\varphi(N)$ be Euler's totient function,

equal # of positive integers $< N$ & relatively prime to N .

In particular, $\varphi(pq) = (p-1)(q-1)$.

$$\forall x < N, \quad x^{\varphi(N)} = 1 \pmod{N}.$$

If $de = 1 \pmod{\varphi(N)}$, then $x^{de} = x^{e\varphi(N)+1}$

Thm. (Euler's thm): Let $\varphi(N)$ be Euler's totient function,

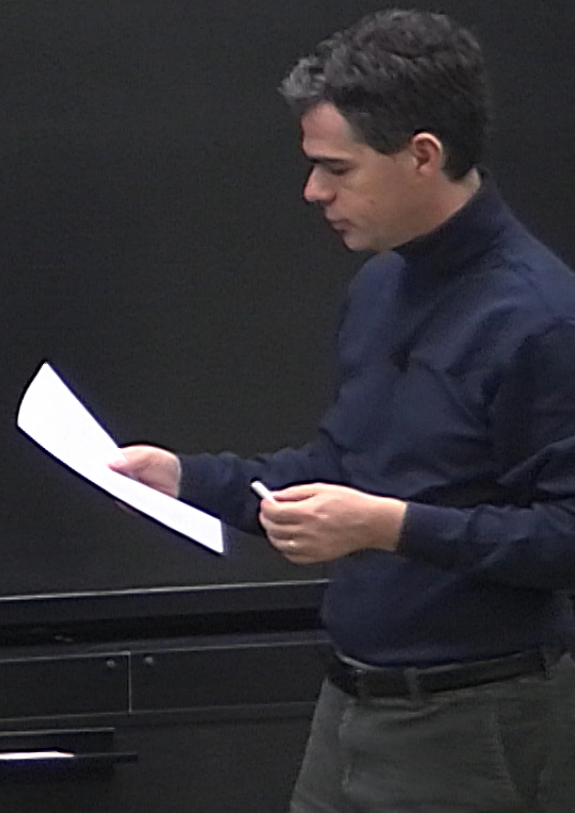
equal # of positive integers $< N$ & relatively prime to N .

In particular, $\varphi(pq) = (p-1)(q-1)$.

$$\forall x < N, \quad x^{\varphi(N)} = 1 \pmod{N}.$$

If $de \equiv 1 \pmod{\varphi(N)}$, then $x^{de} = x^{e\varphi(N)+1} = x \pmod{N}$.

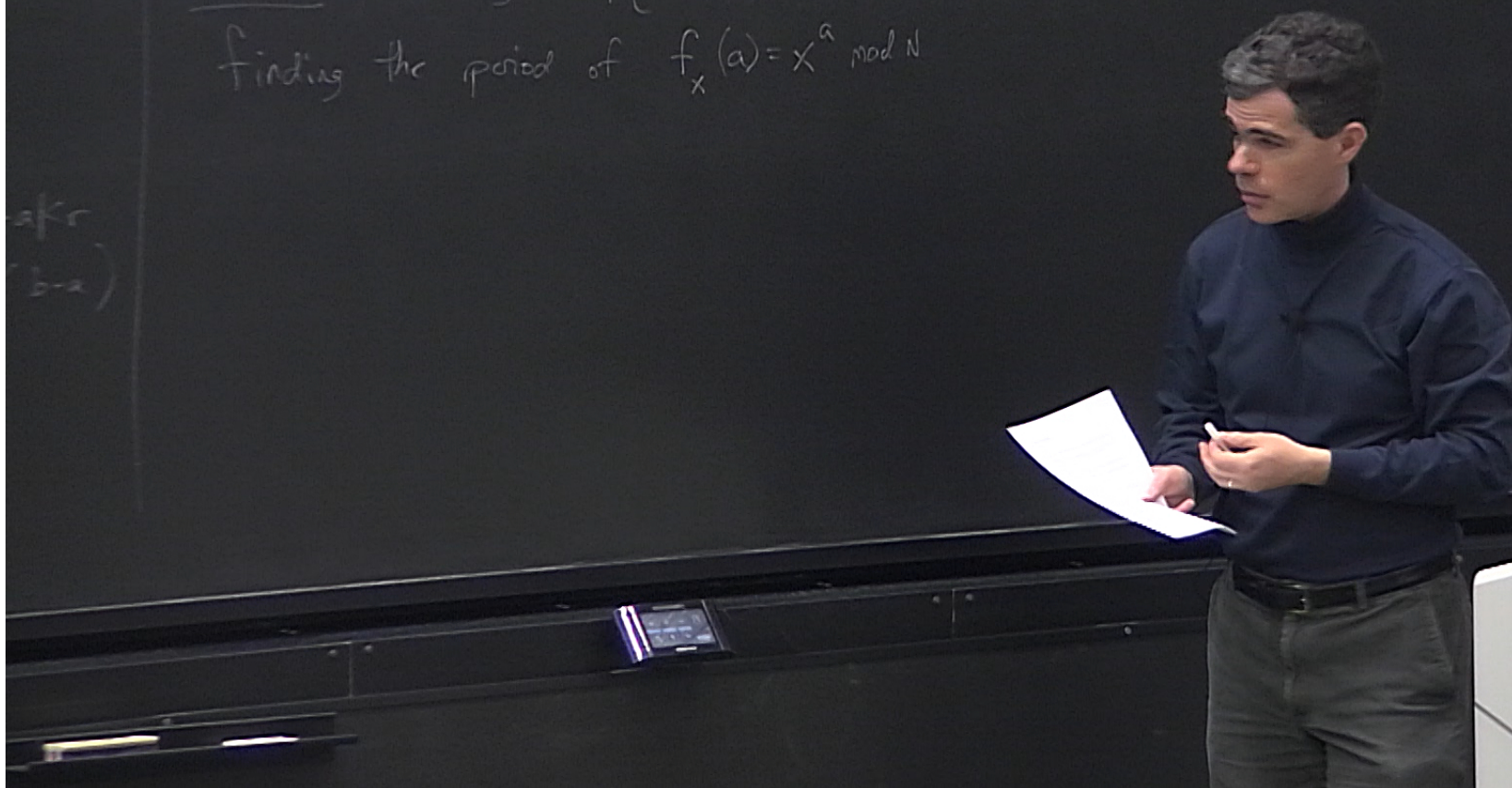
Period finding: Let $f: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$ be
a periodic function with period r that does
not otherwise repeat values. That is
 $f(a) = f(a+r)$, but $f(a) \neq f(b)$ if $|b-a| < r$



Period finding: Let $f: \mathbb{Z}_N \rightarrow \mathbb{Z}_N$ be
a periodic function with period r that does
not otherwise repeat values. That is
 $f(a) = f(a+r)$, but $f(a) \neq f(b)$ if $|b-a| < r$
(or $r \nmid b-a$)

Task: Find r .

Claim: Factoring $N=pq$ reduces to
finding the period of $f_x(a) = x^a \bmod N$



Claim: Factoring $N = pq$ reduces to
finding the period of $f_x(a) = x^a \bmod N$

We want to find x that has even order.

- Random x has even order w/ constant prob.

- Then compute $y = x^{t/2}$; then $y^2 = 1 \bmod N$.

$$y^2 - 1 = (y+1)(y-1) = kN \begin{matrix} \nearrow N/y+1 \\ \nearrow N/y-1 \\ \searrow p/y+1, q/y-1 \end{matrix}$$

Claim: Factoring $N = pq$ reduces to
finding the period of $f_x(a) = x^a \bmod N$

We want to find x that has even order.

- Random x has even order w/ constant prob.

- Then compute $y = x^{r/2}$, then $y^2 = 1 \bmod N$.

$$y^2 - 1 = (y+1)(y-1) = kN \begin{matrix} \nearrow N/y+1 \\ \searrow N/y-1 \end{matrix} \Rightarrow \begin{matrix} y \not\equiv 1 \pmod N \\ p|y+1, q|y-1 \end{matrix}$$

Claim: Factoring $N=pq$ reduces to
finding the period of $f_x(a) = x^a \bmod N$

We want to find x that has even order.

- Random x has even order w/ constant prob.

- Then compute $y = x^{r/2}$; then $y^2 = 1 \bmod N$.

$y^2 - 1 = (y+1)(y-1) = kN$ $\begin{cases} N \mid y+1 \Rightarrow y = -1 \bmod N \\ N \mid y-1 \Rightarrow y = 1 \bmod N \end{cases}$ sometimes happens,
but only constant prob.
 $\rightarrow p \mid y+1, q \mid y-1$

Claim: Factoring $N=pq$ reduces to

finding the period of $f_x(a) = x^a \bmod N$

We want to find x that has even order (i.e. period of f_x)

- Random x has even order w/ constant prob.

- Then compute $y = x^{r/2}$; then $y^2 = 1 \bmod N$.

$$y^2 - 1 = (y+1)(y-1) = kN$$

$$\begin{aligned} &\xrightarrow{N|y+1} y = -1 \bmod N \\ &\xrightarrow{N|y-1} y = 1 \bmod N \\ &\quad \rightarrow p|y+1, q|y-1 \end{aligned}$$

sometimes happens,
but only constant prob.

Claim: Factoring $N=pq$ reduces to

finding the period of $f_x(a) = x^a \bmod N$

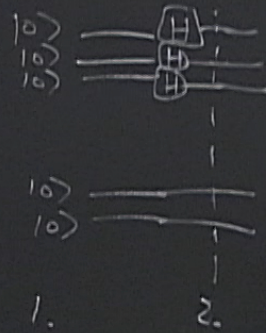
We want to find x that has even order (i.e. period of f_x)

- Random x has even order w/ constant prob.

- Then compute $y = x^{r/2}$; then $y^2 = 1 \bmod N$.

$y^2 - 1 = (y+1)(y-1) = kN$ $\rightarrow N | y+1 \Rightarrow y = -1 \bmod N$ sometimes happens, but only constant prob.
 $\rightarrow N | y-1 \Rightarrow y = 1 \bmod N$
 $\rightarrow p | y+1, q | y-1 \rightarrow p = \gcd(y+1, N)$
 $q = \gcd(y-1, N)$

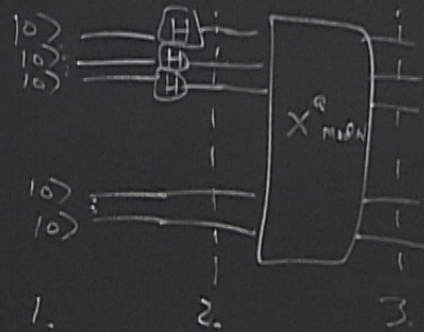
Shor's algorithm:



$$1. |0\rangle|0\rangle$$

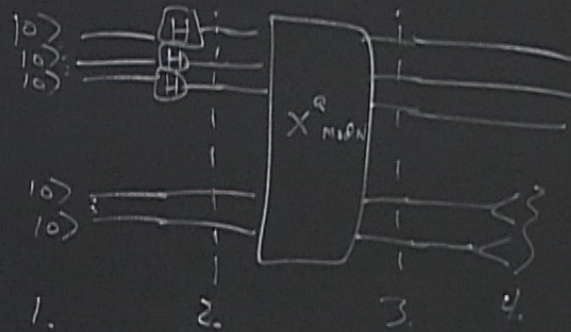
$$2. \sum_a |a\rangle|0\rangle$$

Shor's algorithm:



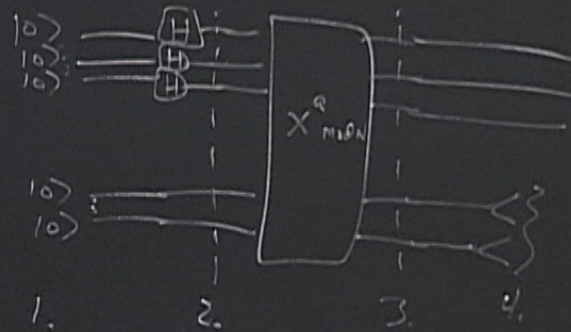
1. $|0\rangle|0\rangle$
2. $\sum_a |a\rangle|0\rangle$
3. $\sum_a |a\rangle|x^a \bmod N\rangle$

Shor's algorithm:



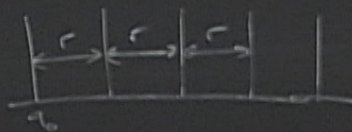
1. $|0\rangle|0\rangle$
2. $\sum_a |a\rangle|0\rangle$
3. $\sum_a |a\rangle|x^a \bmod N\rangle$
4. Result $z = X^a = x^{a+jr}$

Shor's algorithm:

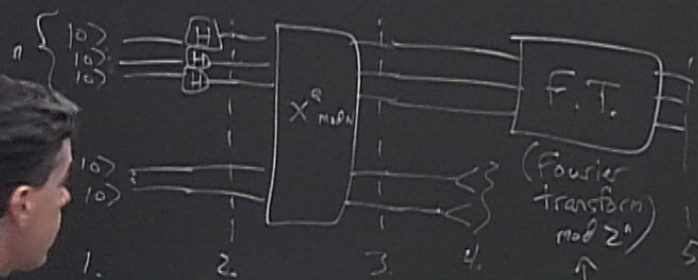


1. $|0\rangle|0\rangle$
2. $\sum_a |a\rangle|0\rangle$
3. $\sum_a |a\rangle|x^a \bmod N\rangle$
4. Result $z = x^s = x^{qr+jr}$
 $\sum_j |q+jr\rangle$

1. $|0\rangle|0\rangle$
2. $\sum_a |a\rangle|0\rangle$
3. $\sum_a |a\rangle|x^a \bmod N\rangle$
4. Result $z = x^{a_0} = x^{a_0 + jr}$
 $\sum_j |a_0 + jr\rangle$



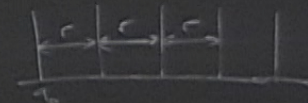
Shor's algorithm:



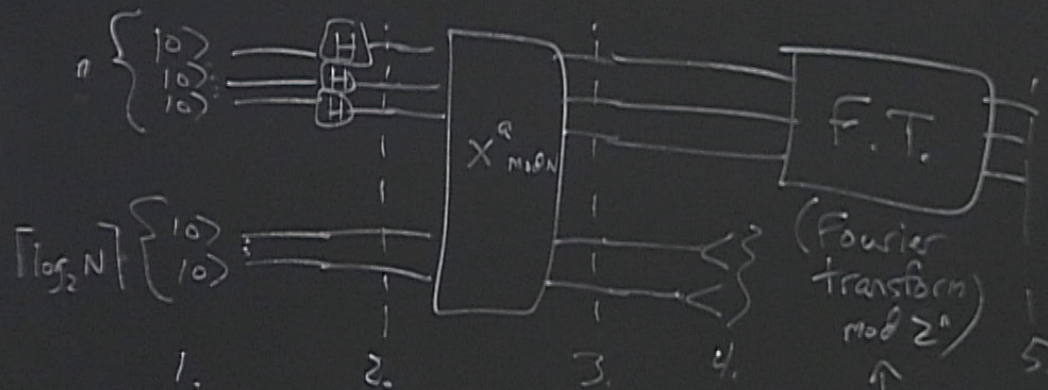
$$\mathcal{F}|a\rangle = \sum_b \omega^{ab} |b\rangle$$

$$\omega = e^{2\pi i / 2^n}$$

1. $|0\rangle|0\rangle$
2. $\sum_a |a\rangle|0\rangle$
3. $\sum_a |a\rangle|x^a \bmod N\rangle$
4. Result $z = X^a = x^{a+jr}$
 $\sum_j |a_0 + jr\rangle$



Shor's algorithm:



$$\mathcal{F}|a\rangle = \sum_b \omega^{ab} |b\rangle$$

$$\omega = e^{2\pi i / 2^n}$$

1. $|0\rangle|0\rangle$
2. $\sum_a |a\rangle|0\rangle$
3. $\sum_a |a\rangle|x^a$
4. Result $z = \sum_j |a_0 + jr\rangle$
- 5.

$$\sqrt{\omega} |a\rangle = \sum_b \omega^{ab} |b\rangle$$

$$\omega = e^{2\pi i / 2}$$

2. $\sum_a |a\rangle \langle 0|$

$$3. \sum_a |a\rangle |x^a \bmod N\rangle$$

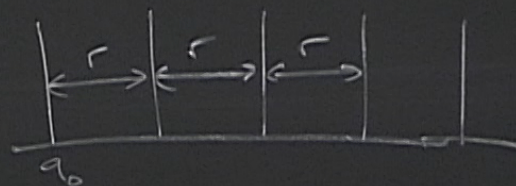
4. Result $z = x^q = x^{q+jr}$
 $\sum |a_0 + jr\rangle$

$$1. |0\rangle|0\rangle$$

$$2. \sum_a |a\rangle|0\rangle$$

$$3. \sum_a |a\rangle|x^a \bmod N\rangle$$

$$4. \text{Result } z = x^{a_0} = x^{a_0 + jr} \\ \sum |a_0 + jr\rangle$$



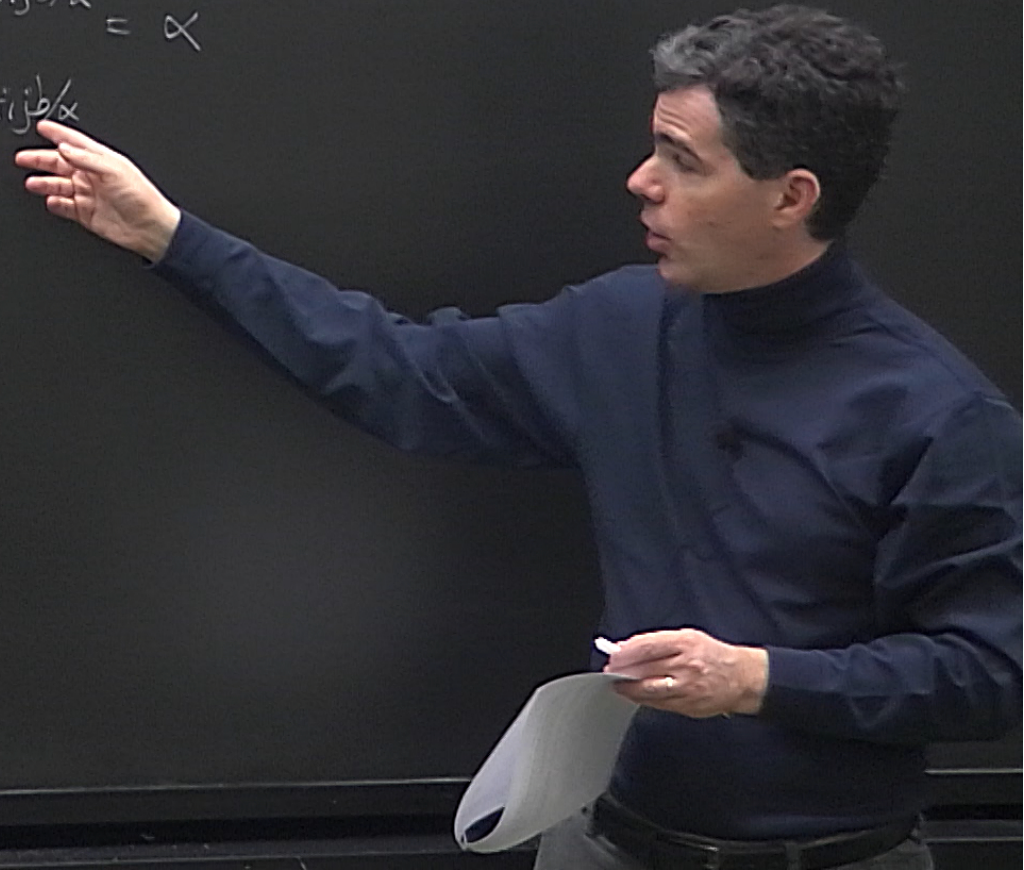
$$5. \sum_j \sum_b \omega^{(a_0 + jr)b} |b\rangle = \sum_b \omega^{a_0 b} \left(\sum_j e^{2\pi i j b / (2^k/r)} \right) |b\rangle$$

$$= \sum_b \omega^{a_0 b} |b\rangle$$

$$\omega = e^{2\pi i / 2^k}$$

Assume $r \mid z^n$. Let $\alpha = \frac{z^n}{r}$

Then if $b = c\alpha$, $\sum_j e^{2\pi i j b/\alpha} = \alpha$
 $b \neq c\alpha$, $\sum_j e^{2\pi i j b/\alpha} = 0$



Assume $r \mid z^n$. Let $\alpha = \frac{z^n}{r}$

$$\begin{aligned} \text{Then if } b = c\alpha, \quad \sum_j e^{2\pi i j b/\alpha} &= \alpha \\ b \neq c\alpha, \quad \sum_j e^{2\pi i j b/\alpha} &= 0 \end{aligned}$$

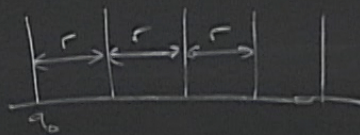
$$1. |0\rangle|0\rangle$$

$$2. \sum_a |a\rangle|0\rangle$$

$$3. \sum_a |a\rangle |x^a \bmod N\rangle$$

$$4. \text{Result } z = x^{a_0} = x^{a_0 + jr}$$

$$\sum |a_0 + jr\rangle$$



$$5. \sum_j \sum_b \omega^{(a_0 + jr)b} |b\rangle = \sum_b \omega^{a_0 b} \left(\sum_j e^{2\pi i j b / (N/r)} \right) |b\rangle$$

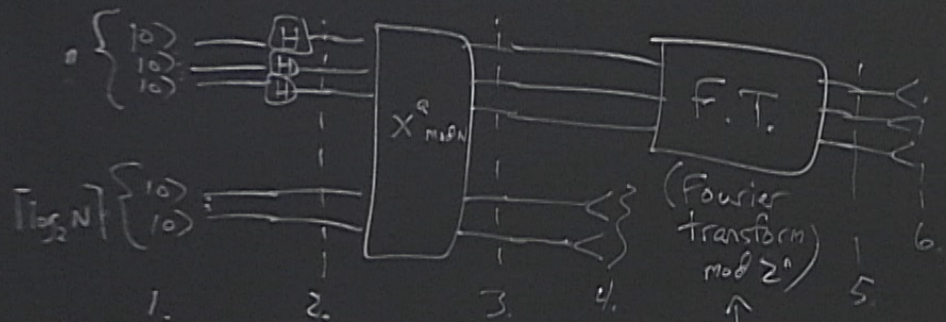
$$= \sum_c \omega^{a_0 c x} |cx\rangle$$

Assume $r \mid N$. Let $\alpha = \frac{N}{r}$

Then if $b = cx$, $\sum_j e^{2\pi i j b / \alpha} = \alpha$
 $b \neq cx$, $\sum_j e^{2\pi i j b / \alpha} = 0$



Shor's algorithm:



$$f(a) = \sum_b \omega^{ab} |b\rangle$$

$$\omega = e^{2\pi i / N}$$

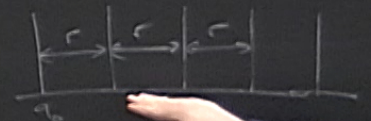
$$1. |0\rangle |0\rangle$$

$$2. \sum_a |a\rangle |0\rangle$$

$$3. \sum_a |a\rangle |x^a \bmod N\rangle$$

$$4. \text{Result } z = x^s = x^{a+jr}$$

$$\sum_j |a_0 + jr\rangle$$



$$5. \sum_j \sum_b \omega^{(a_0+jr)b} |b\rangle = \sum_b \omega^{a_0 b} \left(\sum_j e^{2\pi i j r b / N} \right) |b\rangle$$

$$= \sum_c \omega^{a_0 c} |c\rangle$$

$$6. c \text{ for random } c.$$

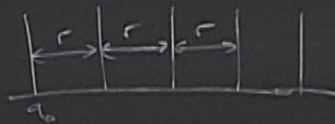
$$1. |0\rangle|0\rangle$$

$$2. \sum_a |a\rangle|0\rangle$$

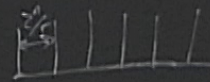
$$3. \sum_a |a\rangle |x^a \bmod N\rangle$$

$$4. \text{Result } z = x^{a_0} = x^{a_0 + jr}$$

$$\sum_j |a_0 + jr\rangle$$



$$5. \sum_j \sum_b \omega^{(a_0 + jr)b} |b\rangle = \sum_b \omega^{a_0 b} \left(\sum_j e^{2\pi i j b / (N/r)} \right) |b\rangle$$



$$= \sum_c \omega^{a_0 c} |c\rangle$$

6. $c\alpha$ for random c .

Assume $r \mid N$. Let $\alpha = \frac{N}{r}$

Then if $b = c\alpha$, $\sum_j e^{2\pi i j b / \alpha} = \alpha$
 if $b \neq c\alpha$, $\sum_j e^{2\pi i j b / \alpha} = 0$

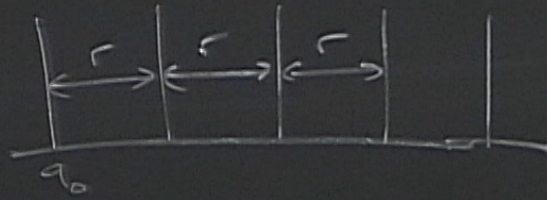
Assume $r \mid z^n$. Let

Then if $b = c\alpha$,

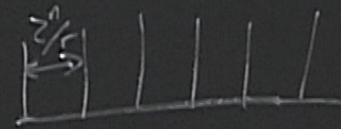
$b \neq c\alpha$,

mod N)

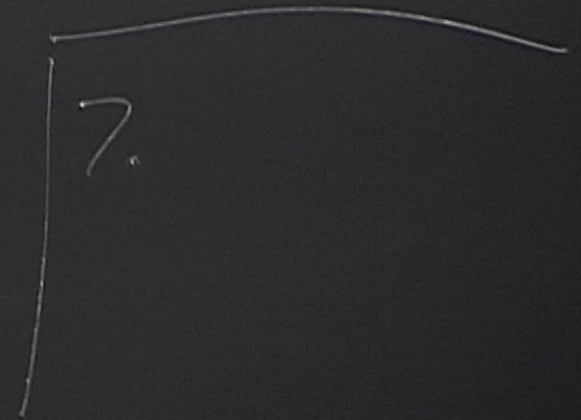
$$X^3 = X^{a+jr}$$



$$|b\rangle = \sum_b \omega^{a_0 b} \left(\sum_j e^{2\pi i j b / (z^n/r)} \right) |b\rangle$$



$$= \sum_c \omega^{a_0 c \alpha} |c\alpha\rangle$$



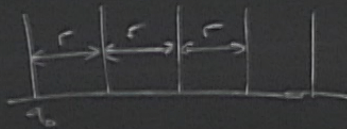
$$1. |0\rangle|0\rangle$$

$$2. \sum_a |a\rangle|0\rangle$$

$$3. \sum_a |a\rangle |x^a \bmod N\rangle$$

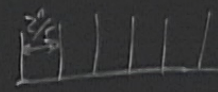
$$4. \text{Result } z = x^b = x^{a+jr}$$

$$\sum |a+jr\rangle$$



$$5. \sum_j \sum_b \omega^{(a_0+jr)b} |b\rangle = \sum_b \omega^{a_0 b} \left(\sum_j e^{2\pi i j b / (2^a/r)} \right) |b\rangle$$

$$= \sum_c \omega^{a_0 c} |c\rangle$$



7. Do this a few times.
 $c_1 \alpha, c_2 \alpha, c_3 \alpha, \dots$

Assume $r \mid 2^n$. Let $\alpha = \frac{2^n}{r}$

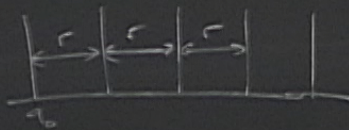
Then if $b = c\alpha$, $\sum_j e^{2\pi i j b / \alpha} = \alpha$
 $b \neq c\alpha$, $\sum_j e^{2\pi i j b / \alpha} = 0$

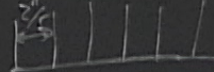
$$1. |0\rangle|0\rangle$$

$$2. \sum_a |a\rangle|0\rangle$$

$$3. \sum_a |a\rangle |x^a \bmod N\rangle$$

$$4. \text{Result } z = x^b = x^{a+jr} \\ \sum |a+jr\rangle$$



$$5. \sum_j \sum_b \omega^{(a+jr)b} |b\rangle = \sum_b \omega^{ab} \left(\sum_j e^{2\pi i j b / (2^k/r)} \right) |b\rangle$$


$$= \sum_c \omega^{ac} |c\rangle$$

6. c for random c .

Assume $r \mid 2^n$. Let $\alpha = \frac{2^n}{r}$

Then if $b = c\alpha$, $\sum_j e^{2\pi i j b / \alpha} = \alpha$
 $b \neq c\alpha$, $\sum_j e^{2\pi i j b / \alpha} = 0$

7. Do this a few times.
 $c_1\alpha, c_2\alpha, c_3\alpha, \dots$
 Find $\gcd(c_1\alpha, c_2\alpha, c_3\alpha, \dots)$

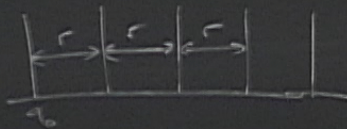
$$1. |0\rangle|0\rangle$$

$$2. \sum_a |a\rangle|0\rangle$$

$$3. \sum_a |a\rangle|x^a \bmod N\rangle$$

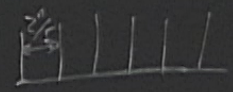
$$4. \text{Result } z = x^b = x^{a+jr}$$

$$\sum |a+jr\rangle$$



$$5. \sum_j \sum_b \omega^{(a+jr)b} |b\rangle = \sum_b \omega^{ab} \left(\sum_j e^{2\pi i j b / (N/r)} \right) |b\rangle$$

$$= \sum_c \omega^{ac} |c\rangle$$



6. $c\alpha$ for random c .

Assume $r | N$. Let $\alpha = \frac{N}{r}$

Then if $b = c\alpha$, $\sum_j e^{2\pi i j b / \alpha} = \alpha$
 $b \neq c\alpha$, $\sum_j e^{2\pi i j b / \alpha} = 0$

7. Do this a few times.
 $c_1\alpha, c_2\alpha, c_3\alpha, \dots$
 Find $\gcd(c_1\alpha, c_2\alpha, c_3\alpha, \dots)$
 Probably α .

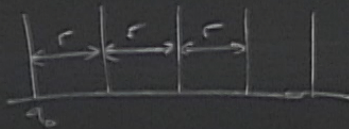
$$1. |0\rangle|0\rangle$$

$$2. \sum_a |a\rangle|0\rangle$$

$$3. \sum_a |a\rangle |x^a \bmod N\rangle$$

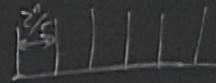
$$4. \text{Result } z = x^b = x^{a+jr}$$

$$\sum |a+jr\rangle$$



$$5. \sum_j \sum_b \omega^{(a+jr)b} |b\rangle = \sum_b \omega^{ab} \left(\sum_j e^{2\pi i j b / (N/r)} \right) |b\rangle$$

$$= \sum_c \omega^{ac} |c\rangle$$



6. Col for random c.

Assume $r \mid N$. Let $\alpha = N/r$

Then if $b = c\alpha$, $\sum_j e^{2\pi i j b / \alpha} = \alpha$
 $b \neq c\alpha$, $\sum_j e^{2\pi i j b / \alpha} = 0$

7. Do this a few times.

$c_1\alpha, c_2\alpha, c_3\alpha, \dots$

Find $\gcd(c_1\alpha, c_2\alpha, c_3\alpha, \dots)$

Probably $\alpha = N/r \Rightarrow r = N/\alpha$

Modular exponentiation:

x is fixed.

- Pre-calculate $x^2, x^4, \dots, x^{2^{n-1}} \bmod N$

$n-1$ multiplications of $\log N$ bit numbers.

$$- a = \sum_i a_i 2^{n-1-i}$$

Modular exponentiation:

x is fixed.

— Pre-calculate $x^2, x^4, \dots, x^{2^{n-1}} \bmod N$
 $n-1$ multiplications of $\log N$ bit numbers.

— $a = \sum_i a_i 2^{n-1-i}$ (binary)

$$|a\rangle|0\rangle \mapsto |a\rangle|x^{a_{n-1}}\rangle|(x^2)^{a_{n-2}}\rangle|(x^4)^{a_{n-3}}\rangle \dots |(x^{2^{n-1}})^{a_0}\rangle$$

Modular exponentiation:

x is fixed.

— Pre-calculate $x^2, x^4, \dots, x^{2^{n-1}} \bmod N$

$n-1$ multiplications of $\log N$ bit numbers.

— $a = \sum_i a_i 2^{n-1-i}$ (binary)

$$|a\rangle|0\rangle \mapsto |a\rangle|x^{2^{n-1}}\rangle|(x^2)^{2^{n-2}}\rangle|(x^4)^{2^{n-3}}\rangle \dots |(x^{2^{n-1}})^{a_0}\rangle$$

n additions

Modular exponentiation:

x is fixed.

- Pre-calculate $x^2, x^4, \dots, x^{2^{n-1}}$ mod N

$n-1$ multiplications of $\log N$ bit numbers.

- $a = \sum_i a_i 2^{n-1-i}$ (binary)

$$|a\rangle|0\rangle \mapsto |a\rangle \underbrace{|x^{2^{n-1}}\rangle |x^{2^{n-2}}\rangle |x^4\rangle \dots |x^{2^{n-1}}\rangle}_{\text{ancillas}}$$

n additions

→ multiply together and

→ multiply together ancillas (mod N)

$$|a\rangle |x^{a_{n-1} + 2a_{n-2} + 4a_{n-3} + \dots + 2^{n-1}a_0}\rangle |x^2\rangle \dots |x^{2^{n-1}}\rangle$$

$n-1$ multiplications

→ uncompute ancillas
 n additions

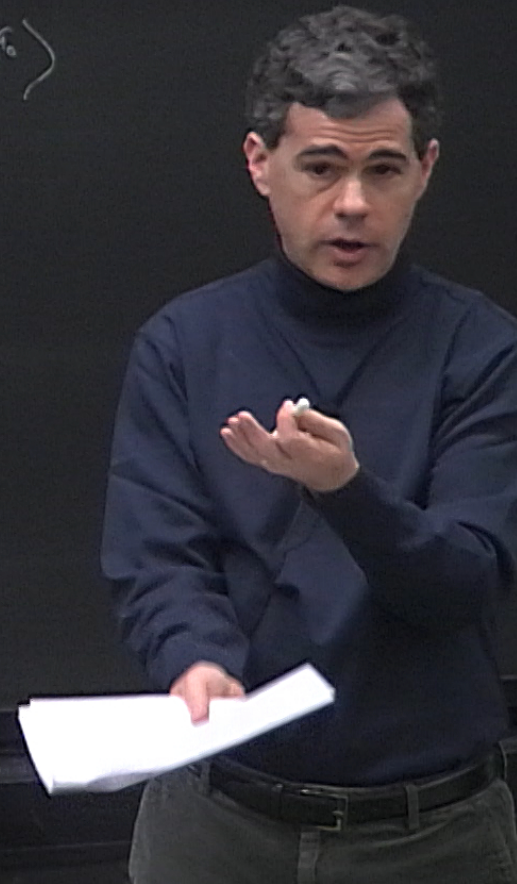
→ multiply together ancillas (mod N)

$$|a\rangle |x^{q_{n-1} + 2q_{n-2} + 4q_{n-3} + \dots + 2^{n-1}q_0}\rangle |x^{q_{n-2}}\rangle \dots |x^{q_0}\rangle$$

$n-1$ multiplications

→ uncompute ancillas
 n additions

$2n$ additions of $\log N$ bit #s
 $2(n-1)$ multiplications of $\log N$ bit #s



→ multiply together ancillas (mod N)

$$|a\rangle |x^{q_{n-1} + 2q_{n-2} + 4q_{n-3} + \dots + 2^{n-1}q_0}\rangle |x^{2^0}q_0\rangle \dots |x^{2^{n-1}}q_0\rangle$$

$n-1$ multiplications

→ uncompute ancillas
 n additions

$2n$ additions of $\log N$ bit #s
 $2(n-1)$ multiplications of $\log N$ bit #s
multiplication takes $(\log N)^2$

→ multiply together ancillas (mod N)

$$|a\rangle |x^{q_{n-1} + 2q_{n-2} + 4q_{n-3} + \dots + 2^{n-1}q_0}\rangle |x^{q_{n-2}}\rangle \dots |x^{q_0}\rangle$$

$n-1$ multiplications

→ uncompute ancillas
 n additions

$2n$ additions of $\log N$ bit #s

$2(n-1)$ multiplications of $\log N$ bit #s

multiplication takes $(\log N)^2 \Rightarrow O(n(\log N)^2)$

multiply together ancillas (mod N)

$$|a\rangle |x^{a_{n-1} + 2a_{n-2} + 4a_{n-3} + \dots + 2^{n-1}a_0}\rangle |x^{a_{n-2}}\rangle \dots |x^{2^{n-1}a_0}\rangle$$

$n-1$ multiplications

recompute ancillas
 n additions

Fast multiplication:

$$O(n^2 \log n \log \log n)$$

$2n$ additions of $\log N$ bit #s

$2(n-1)$ multiplications of $\log N$ bit #s

multiplication takes $(\log N)^2 \Rightarrow O(n(\log N)^2) = O(n^3)$
 $n = O(\log N)$