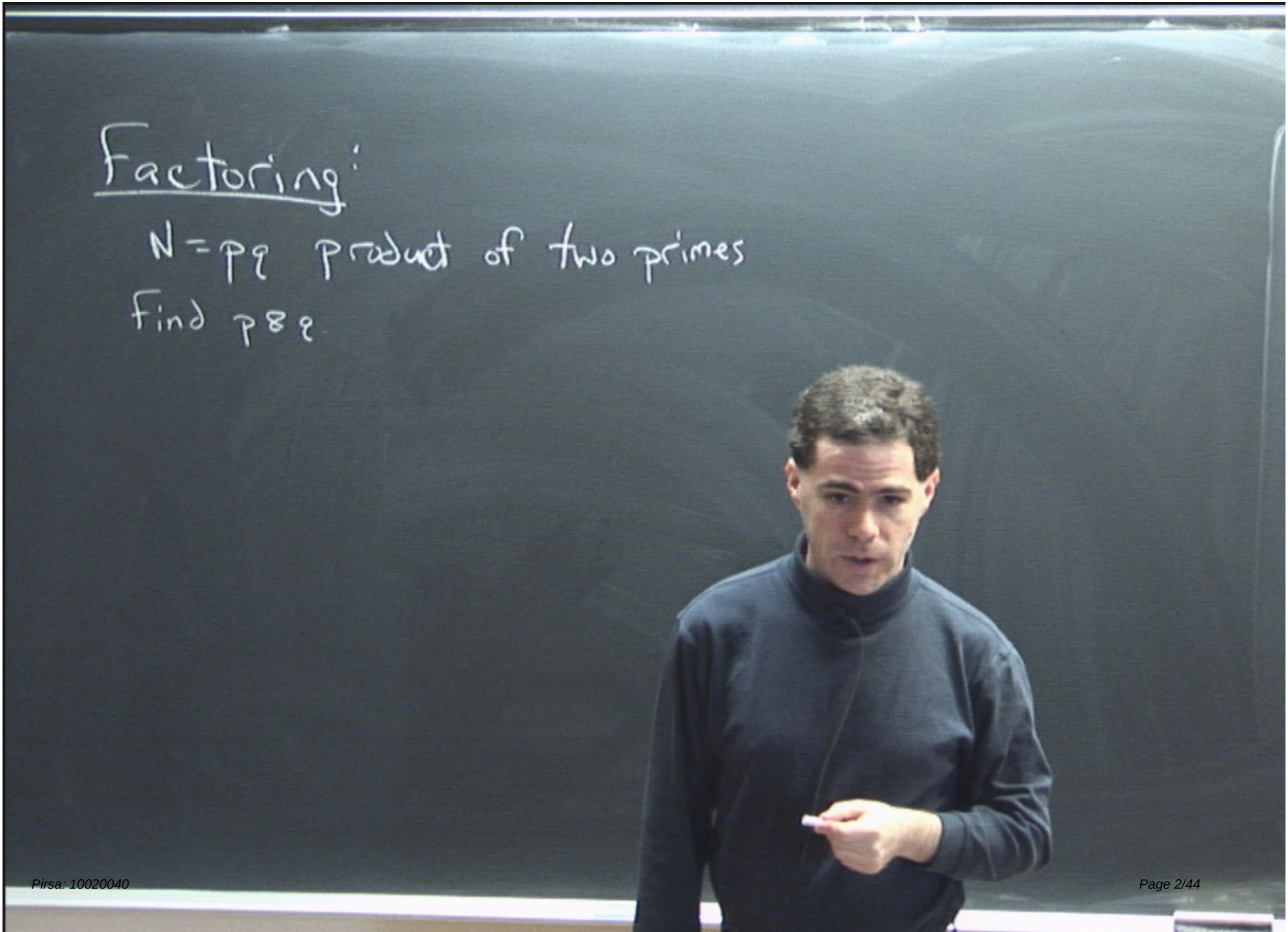
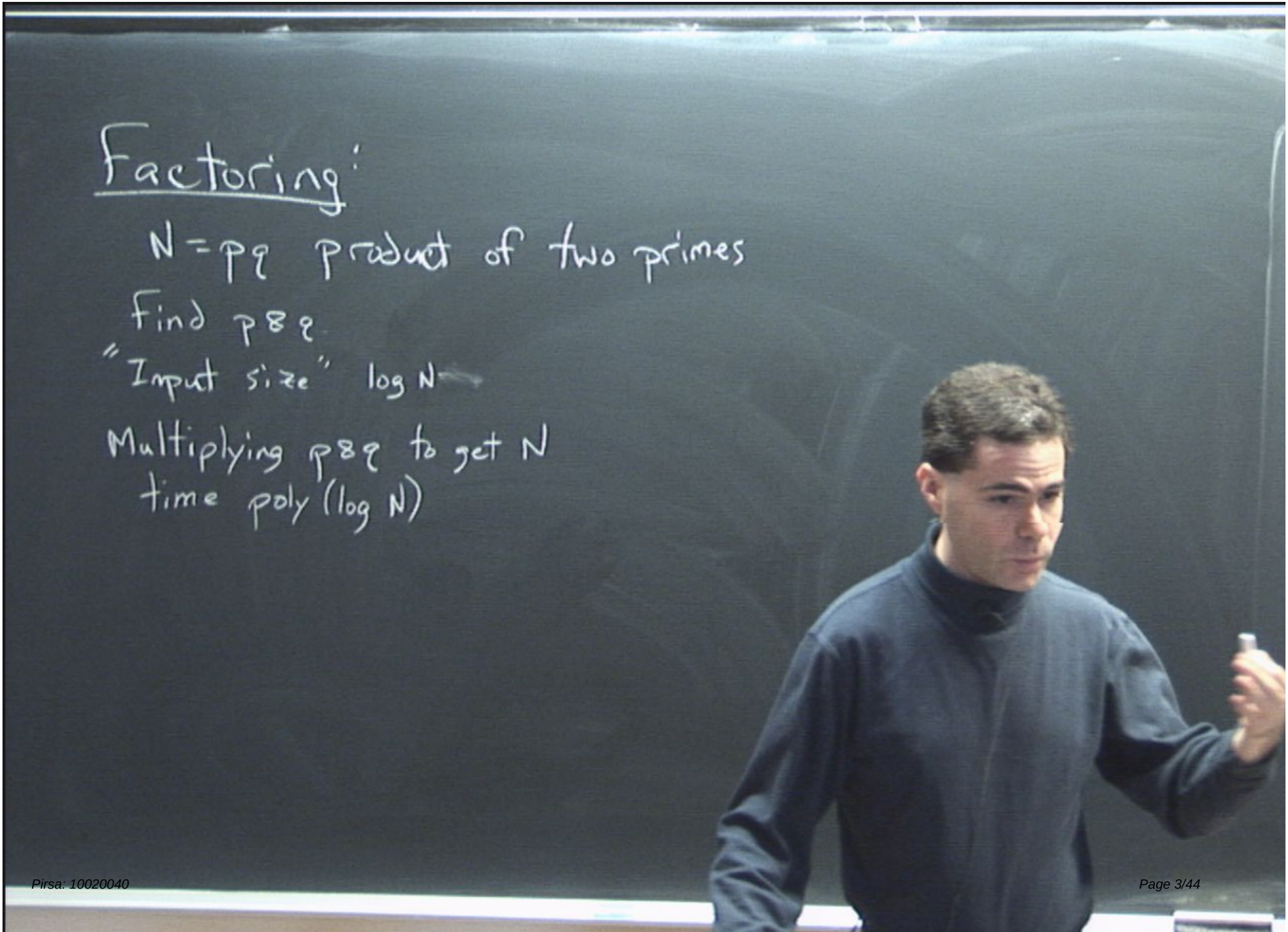
Title: Quantum Information - Review (PHYS 635) - Lecture 8

Date: Feb 03, 2010 09:00 AM

URL: http://pirsa.org/10020040

Abstract: Week 1: Basic topics (Qubits, quantum gates, quantum circuits, density matrices, quantum operations, entropy, entanglement) Week 2: Algorithms and complexity (Languages, complexity classes, oracles, RSA, Deutsch-Jozsa algorithm, Shor's algorithm, Grover's algorithm) Week 3: Information theory and implementations (Overview of implementations, quantum error correction, quantum cryptography, quantum information theory)


Factoring:
N = pq product of two primes
Find p & q


Factoring:
N = pq product of two primes
Find p & q
"Input size" log N
Multiplying p & q to get N
time poly (log N)

Factoring:

$N = pq$ product of two primes

Find p & q

"Input size" $\log N$

Multiplying p & q to get N

time poly $(\log N)$

Long multiplication $O((\log N)^2)$

Factoring:

$N = pq$ product of two primes

Find p & q

"Input size" $\log N$

Multiplying p & q to get N
time poly $(\log N)$

Long multiplication $O((\log N)^2)$

Decision problem version:
Given N & m, does N have
a non-trivial factor less then m?

Factoring:

$N = pq$ product of two primes

Find p & q

"Input size" $\log N$

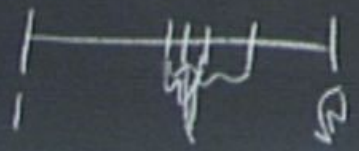
Multiplying p & q to get N

time poly $(\log N)$

Long multiplication $O((\log N)^2)$

Decision problem version:

Given N & m, does N have a non-trivial factor less then m?



Factoring:

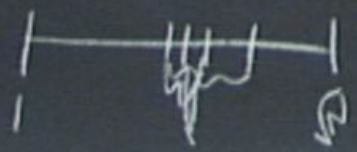
$N = pq$ product of two primes

Find p & q

"Input size" $\log N$

Multiplying p & q to get N
time poly $(\log N)$
Long multiplication $O((\log N)^2)$

Decision problem version:
Given N & m, does N have
a non-trivial factor less then m?



Factoring:

$N = pq$ Product of two primes

Find p & q

"Input size" $\log N$

Multiplying p & q to get N

time poly $(\log N)$

Long multiplication $O((\log N)^2)$

Decision problem version:

Given N & m, does N have a non-trivial factor less then m?

RSA ("Rivest-Shamir-Adleman")

Factoring:

$N = pq$ product of two primes

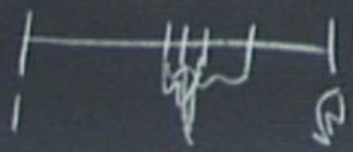
Find p & q

"Input size" $\log N$

Multiplying p & q to get N
time poly $(\log N)$

Long multiplication $O((\log N)^2)$

Decision problem version:
Given N & m, does N have
a non-trivial factor less then m?



RSA ("Rivest-Shamir-Adleman")

Public-key cryptosystem

A B

Factoring:

$N = pq$ product of two primes

Find p & q

"Input size" $\log N$

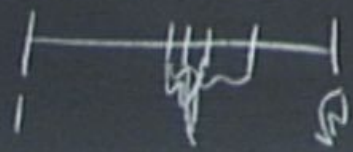
Multiplying p & q to get N

time poly $(\log N)$

Long multiplication $O((\log N)^2)$

Decision problem version:

Given N & m, does N have a non-trivial factor less than m?



RSA ("Rivest-Shamir-Adleman")

Public-key cryptosystem

A

Private key

B

Public key

Factoring:

$N = pq$ product of two primes

Find p & q

"Input size" $\log N$

Multiplying p & q to get N
time poly $(\log N)$
Long multiplication $O((\log N)^2)$

Decision problem version:
Given N & m, does N have a non-trivial factor less than m?

RSA ("Rivest-Shamir-Adleman")

Public-key cryptosystem

A ← decrypt — B

Private key

encrypt → Public key

Factoring:

$N = pq$ product of two primes

Find p & q

"Input size" $\log N$

Multiplying p & q to get N
time poly $(\log N)$
Long multiplication $O((\log N)^2)$

Decision problem version:
Given N & m, does N have a non-trivial factor less than m?

RSA ("Rivest-Shamir-Adleman")

Public-key cryptosystem

A ← decrypt — B

Private key

encrypt — Public key

(N, e)

Factoring:

$N = pq$ product of two primes

Find p & q

"Input size" $\log N$

Multiplying p & q to get N
time poly $(\log N)$
Long multiplication $O((\log N)^2)$

Decision problem version:
Given N & m, does N have a non-trivial factor less then m?

RSA ("Rivest-Shamir-Adleman")

Public-key cryptosystem

A ← decrypt — B

A: Private key (d)
q derived from p, q $(N = pq)$

B: encrypt Public key (N, e)

Factoring:

$N = pq$ product of two primes

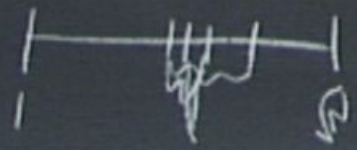
Find p & q

"Input size" $\log N$

Multiplying p & q to get N
time poly $(\log N)$

Long multiplication $O((\log N)^2)$

Decision problem version:
Given N & m, does N have a non-trivial factor less than m?



RSA ("Rivest-Shamir-Adleman")

Public-key cryptosystem

A ← decrypt — B

A: Private key (d); q derived from p, q $(N = pq)$

B: encrypt — Public key (N, e)

Encryption:

Factoring:

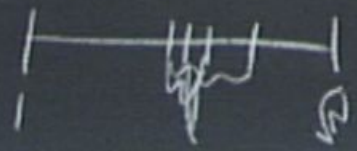
$N = pq$ product of two primes

Find p & q

"Input size" $\log N$

Multiplying p & q to get N
time poly $(\log N)$
Long multiplication $O((\log N)^2)$

Decision problem version:
Given N & m, does N have a non-trivial factor less than m?



RSA ("Rivest-Shamir-Adleman")

Public-key cryptosystem

A ← decrypt ← B

A: Private key (d) — d derived from p, q $(N = pq)$

B: encrypt — Public key (N, e)

Encryption: $x \longmapsto x^e \bmod N = y$

Factoring:

$N = pq$ product of two primes

Find p & q

"Input size" $\log N$

Multiplying p & q to get N

time poly $(\log N)$

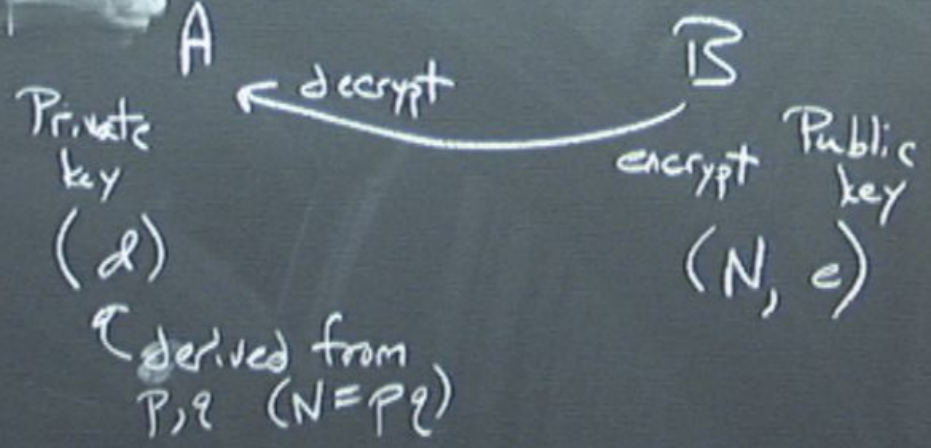
Long multiplication $O((\log N)^2)$

Decision problem version:

Given N & m, does N have a non-trivial factor less than m?

RSA ("Rivest-Shamir-Adleman")

Public-key cryptosystem



Encryption: $x \longmapsto x^e \bmod N = y$

Decryption: $y \longmapsto y^d \bmod N$

Factoring:

$N = pq$ product of two primes

Find p & q

"Input size" $\log N$

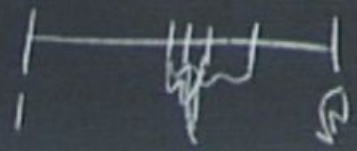
Multiplying p & q to get N

time poly $(\log N)$

Long multiplication $O((\log N)^2)$

Decision problem version:

Given N & m, does N have a non-trivial factor less than m?



RSA ("Rivest-Shamir-Adleman")

Public-key cryptosystem

A ← decrypt — B

A: Private key (d)

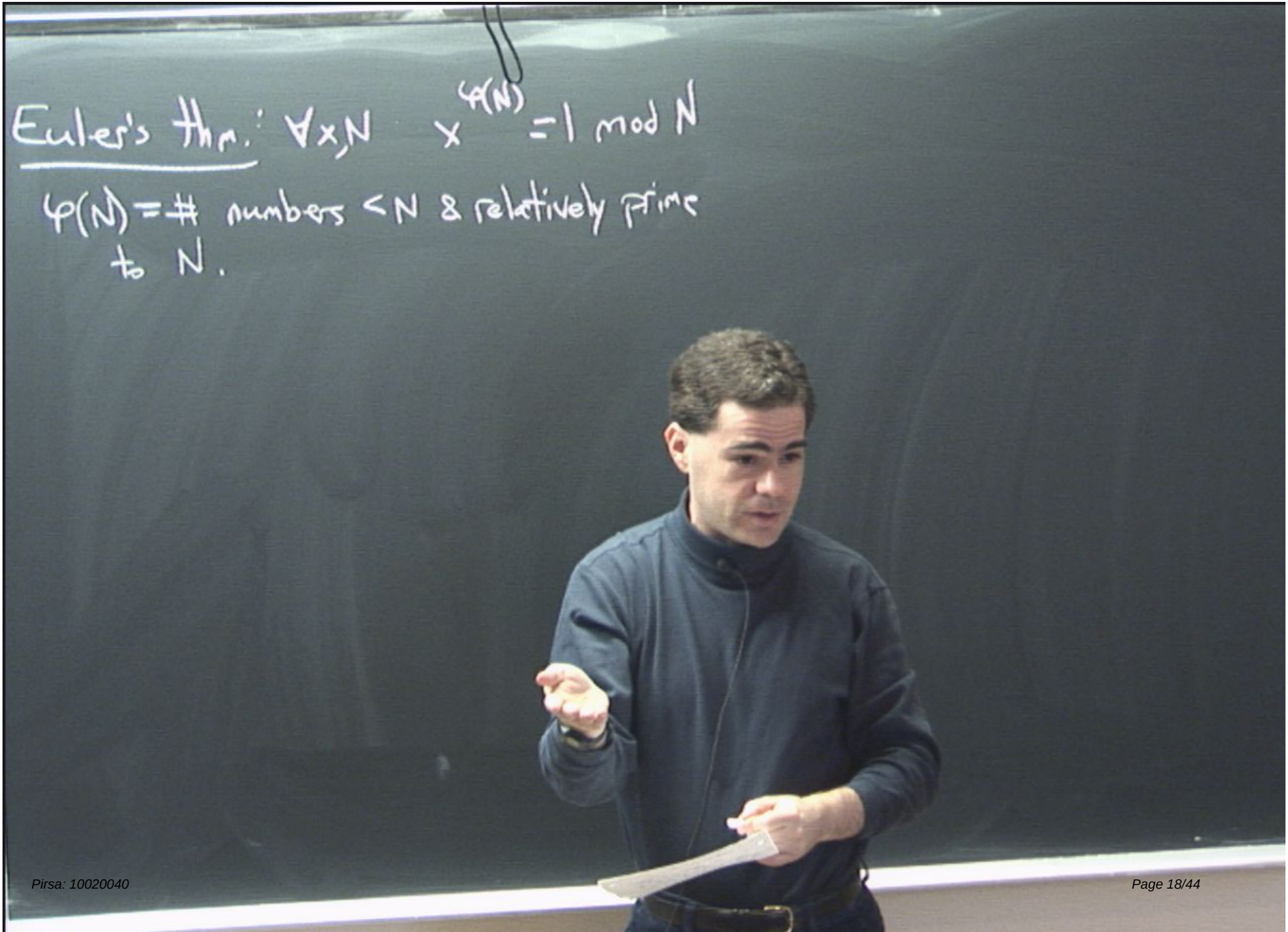
B: encrypt — Public key (N, e)

d derived from p, q $(N = pq)$

Encryption: $x \longmapsto x^e \bmod N = y$

Decryption: $y \longmapsto y^d \bmod N = x$

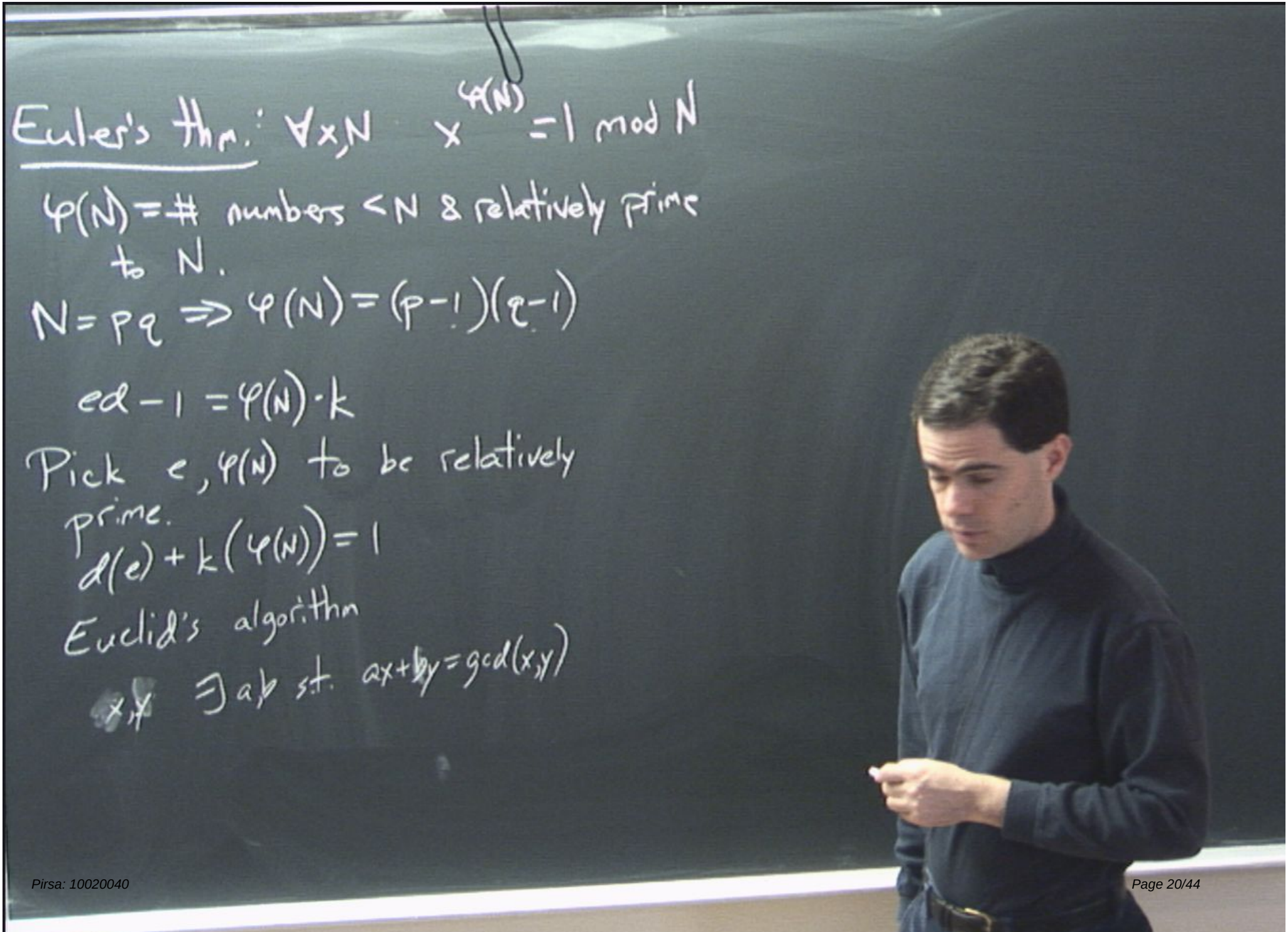
$x^{ed} = x \bmod N$

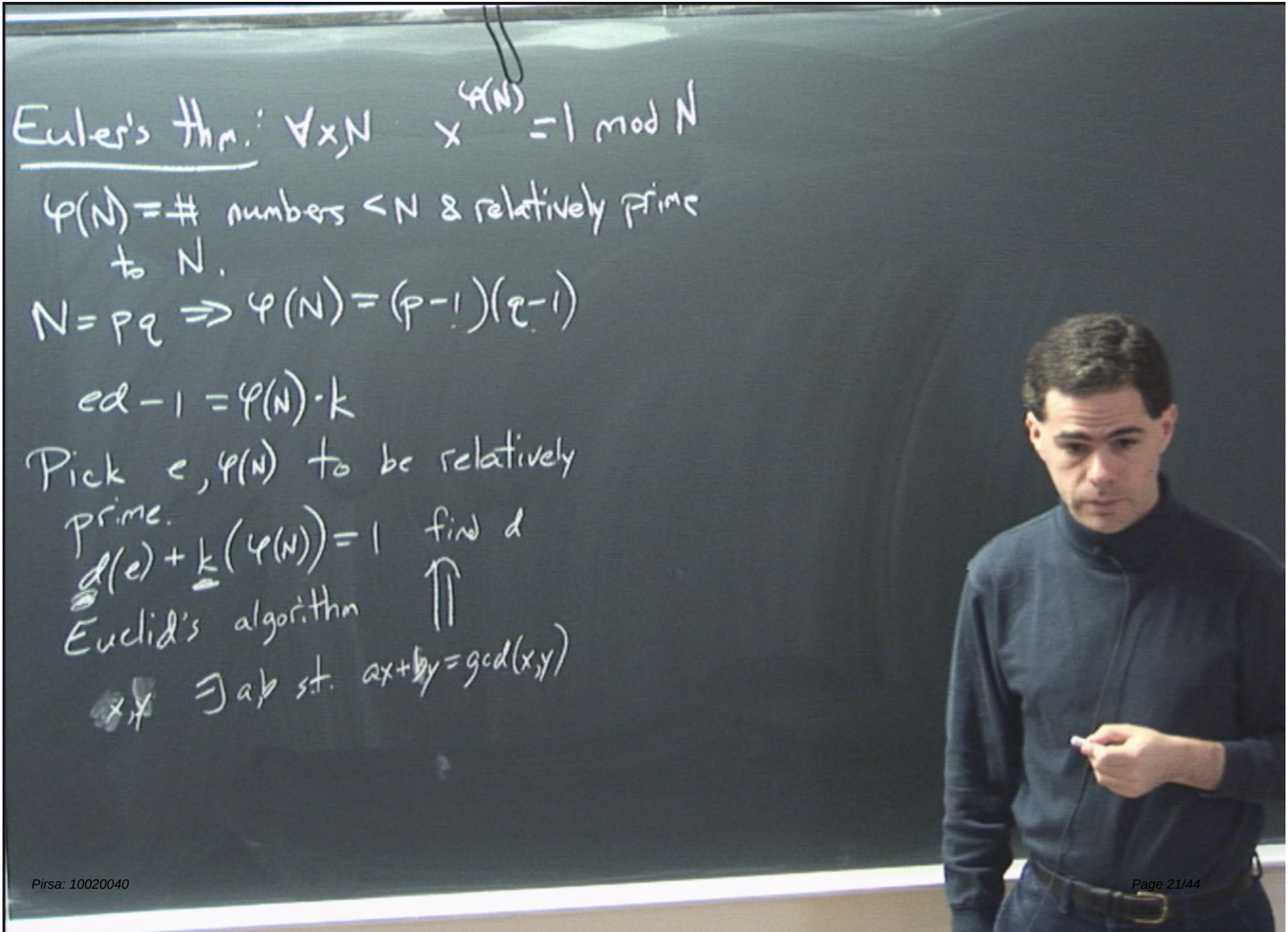

Euler's thm.: $\forall x, N \quad x^{\varphi(N)} = 1 \bmod N$
$\varphi(N)$ = # numbers $< N$ & relatively prime to N.

Euler's thm.: $\forall x, N \quad x^{\varphi(N)} = 1 \bmod N$

$\varphi(N) = \#$ numbers $< N$ & relatively prime to N.

$N = pq \Rightarrow \varphi(N) = (p-1)(q-1)$


Euler's thm.: $\forall x,N \quad x^{\varphi(N)} = 1 \bmod N$
$\varphi(N)$ = # numbers < N & relatively prime to N.
$N = pq \Rightarrow \varphi(N) = (p-1)(q-1)$
$ed - 1 = \varphi(N) \cdot k$
Pick e, $\varphi(N)$ to be relatively prime.
$d(e) + k(\varphi(N)) = 1$
Euclid's algorithm
$x,y \ \exists a,b$ s.t. $ax + by = gcd(x,y)$


Euler's thm.: $\forall x,N \quad x^{\varphi(N)} = 1 \bmod N$
$\varphi(N)$ = # numbers < N & relatively prime to N.
$N = pq \Rightarrow \varphi(N) = (p-1)(q-1)$
$ed - 1 = \varphi(N) \cdot k$
Pick e, $\varphi(N)$ to be relatively prime.
$d(e) + k(\varphi(N)) = 1$ find d
Euclid's algorithm
$x,y \ \exists a,b$ s.t. $ax + by = gcd(x,y)$

Euler's thm.: $\forall x, N \quad x^{\varphi(N)} = 1 \bmod N$

$\varphi(N)$ = # numbers $< N$ & relatively prime to N.

$N = pq \Rightarrow \varphi(N) = (p-1)(q-1)$

$ed - 1 = \varphi(N) \cdot k$

Pick $e, \varphi(N)$ to be relatively prime.

$d(e) + k(\varphi(N)) = 1$ find d

Euclid's algorithm ⇑

$x, y \ \exists a, b$ s.t. $ax + by = \gcd(x, y)$

Euler's thm.: $\forall x, N \quad x^{\varphi(N)} \equiv 1 \bmod N$

$\varphi(N)$ = # numbers $< N$ & relatively prime to N.

$N = pq \Rightarrow \varphi(N) = (p-1)(q-1)$

$ed - 1 = \varphi(N) \cdot k$

Pick $e, \varphi(N)$ to be relatively prime.

$d(e) + k(\varphi(N)) = 1$ find d

Euclid's algorithm ⇑

$x, y \ \exists a, b$ s.t. $ax + by = gcd(x, y)$

Euler's thm.: $\forall x, N \quad x^{\varphi(N)} \equiv 1 \bmod N$

$\varphi(N) = \#$ numbers $< N$ & relatively prime to N.

$N = pq \Rightarrow \varphi(N) = (p-1)(q-1)$

$ed - 1 = \varphi(N) \cdot k$

Pick $e, \varphi(N)$ to be relatively prime.

$d(e) + k(\varphi(N)) = 1$ find d

Euclid's algorithm

$x, y \ \exists a, b$ s.t. $ax + by = \gcd(x, y)$

Order-finding:

$x < N$, Find minimal r s.t. $x^r = 1 \bmod N$

Euler's thm.: $\forall x, N \quad x^{\varphi(N)} \equiv 1 \bmod N$

$\varphi(N)$ = # numbers $< N$ & relatively prime to N.

$N = pq \Rightarrow \varphi(N) = (p-1)(q-1)$

$ed - 1 = \varphi(N) \cdot k$

Pick e, $\varphi(N)$ to be relatively prime.

$d(e) + k(\varphi(N)) = 1$ find d

Euclid's algorithm ⇑

$x, y \Rightarrow \exists a, b$ s.t. $ax + by = \gcd(x, y)$

Order-finding:

$x < N$, Find minimal $r > 0$ s.t. $x^r = 1 \bmod N$

Finding r in general ⇒ Factoring N

$=$

- Find y with $y^2 = 1 \bmod N$

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

Euler's thm.: $\forall x, N \quad x^{\varphi(N)} \equiv 1 \bmod N$

$\varphi(N)$ = # numbers $< N$ & relatively prime to N.

$N = pq \Rightarrow \varphi(N) = (p-1)(q-1)$

$ed - 1 = \varphi(N) \cdot k$

Pick $e, \varphi(N)$ to be relatively prime.

$d(e) + k(\varphi(N)) = 1$ find d

Euclid's algorithm ⇑⇑

$x, y \ \exists a, b$ s.t. $ax + by = \gcd(x, y)$

Order-finding:

$x < N$, Find minimal $r > 0$ s.t. $x^r = 1 \bmod N$

Finding r in general ⇒ Factoring N

- Find y with $y^2 = 1 \bmod N$

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

If $y \neq \pm 1 \bmod N$, then $p \mid y+1$, $q \mid y-1$

Euler's thm.: $\forall x, N \quad x^{\varphi(N)} \equiv 1 \bmod N$

$\varphi(N)$ = # numbers $< N$ & relatively prime to N.

$N = pq \Rightarrow \varphi(N) = (p-1)(q-1)$

$ed - 1 = \varphi(N) \cdot k$

Pick $e, \varphi(N)$ to be relatively prime.

$d(e) + k(\varphi(N)) = 1$ find d

Euclid's algorithm

$x, y \ \exists a, b$ s.t. $ax + by = \gcd(x, y)$

Order-finding:

$x < N$, Find minimal $r > 0$ s.t. $x^r = 1 \bmod N$

Finding r in general $\Rightarrow$ Factoring N

- Find y with $y^2 = 1 \bmod N$

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

If $y \neq \pm 1 \bmod N$, then $p \mid y+1$, $q \mid y-1$

Find $\gcd(N, y+1)$, $\gcd(N, y-1)$

Euler's thm.: $\forall x,N \quad x^{\varphi(N)} \equiv 1 \bmod N$

$\varphi(N)$ = # numbers $< N$ & relatively prime to N.

$N = pq \Rightarrow \varphi(N) = (p-1)(q-1)$

$ed - 1 = \varphi(N) \cdot k$

Pick $e, \varphi(N)$ to be relatively prime.

$d(e) + k(\varphi(N)) = 1$ find d

Euclid's algorithm ⇑

$x, y \ \exists a, b$ s.t. $ax + by = \gcd(x,y)$

Order-finding:

$x < N$, Find minimal $r > 0$ s.t. $x^r = 1 \bmod N$

Finding r in general ⇒ Factoring N

- Find y with $y^2 = 1 \bmod N$

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

  If $y \neq \pm 1 \bmod N$, then $p \mid y+1$, $q \mid y-1$

  Find $\gcd(N, y+1)$, $\gcd(N, y-1)$

- Find x with even order $r/2$ integer $y = x^{r/2}$ then $y^2 = 1 \bmod N$, $y \neq$

Euler's thm.: $\forall x, N \quad x^{\varphi(N)} = 1 \bmod N$

$\varphi(N)$ = # numbers $< N$ & relatively prime to N.

$N = pq \Rightarrow \varphi(N) = (p-1)(q-1)$

$ed - 1 = \varphi(N) \cdot k$

Pick e, $\varphi(N)$ to be relatively prime.

$d(e) + k(\varphi(N)) = 1$ find d

Euclid's algorithm ⇑

$x, y \ \exists a, b$ s.t. $ax + by = \gcd(x, y)$

Order-finding:

$x < N$, Find minimal $r > 0$ s.t. $x^r = 1 \bmod N$

Finding r in general ⇒ Factoring N

- Find y with $y^2 = 1 \bmod N$

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

  If $y \neq \pm 1 \bmod N$, then $p \mid y+1$, $q \mid y-1$

  Find $\gcd(N, y+1)$, $\gcd(N, y-1)$

- Find x with even order $r/2$ integer $y = x^{r/2}$ then $y^2 = 1 \bmod N$, $y \neq 1 \bmod N$

Euler's thm.: $\forall x, N \quad x^{\varphi(N)} \equiv 1 \bmod N$

$\varphi(N)$ = # numbers $< N$ & relatively prime to N.

$N = pq \Rightarrow \varphi(N) = (p-1)(q-1)$

$ed - 1 = \varphi(N) \cdot k$

Pick e, $\varphi(N)$ to be relatively prime.

$d(e) + k(\varphi(N)) = 1$ find d

Euclid's algorithm ⇑

$x, y \ \exists a, b$ s.t. $ax + by = \gcd(x, y)$

Order-finding:

$x < N$, Find minimal $r > 0$ s.t. $x^r \equiv 1 \bmod N$

Finding r in general ⇒ Factoring N

- Find y with $y^2 \equiv 1 \bmod N$

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

  If $y \not\equiv \pm 1 \bmod N$, then $p \mid y+1$, $q \mid y-1$

  Find $\gcd(N, y+1)$, $\gcd(N, y-1)$

- Find x with even order $r/2$ integer $y = x^{r/2}$ then $y^2 \equiv 1 \bmod N$, $y \not\equiv 1 \bmod N$

- Choose random x, with constant prob. x has even order r & $x^{r/2} \not\equiv -1 \bmod N$.

Euler's thm.: $\forall x, N \quad x^{\varphi(N)} \equiv 1 \bmod N$

$\varphi(N) = \#$ numbers $< N$ & relatively prime to N.

$N = pq \Rightarrow \varphi(N) = (p-1)(q-1)$

$ed - 1 = \varphi(N) \cdot k$

Pick $e, \varphi(N)$ to be relatively prime.

$d(e) + k(\varphi(N)) = 1$ find d

Euclid's algorithm ⇑

$x, y \ \exists a, b$ s.t. $ax + by = \gcd(x, y)$

Order-finding:

$x < N$, Find minimal $r > 0$ s.t. $x^r = 1 \bmod N$

Finding r in general ⇒ Factoring N

- Find y with $y^2 = 1 \bmod N$

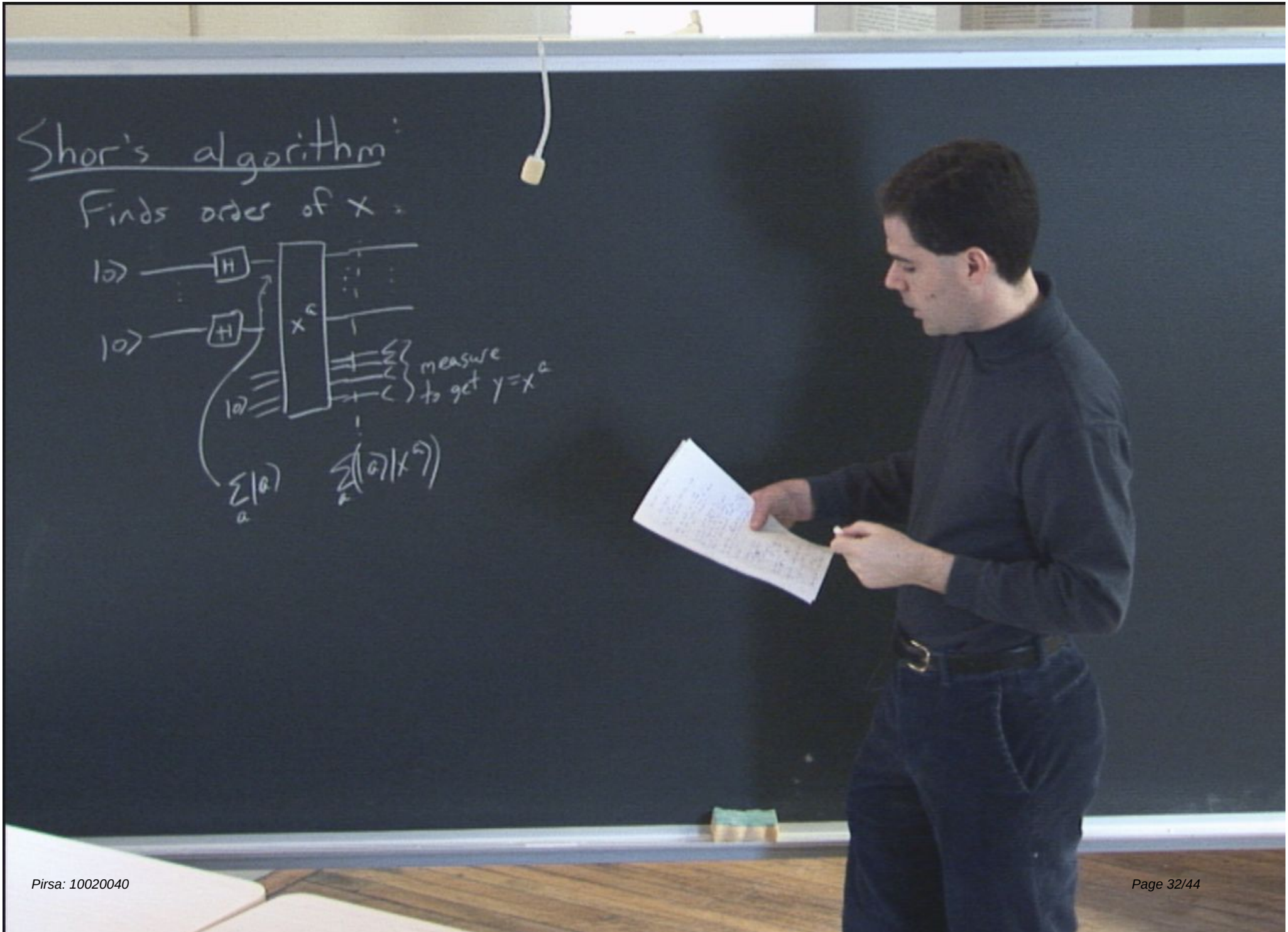
  $y^2 - 1 = (y+1)(y-1) = kN = kpq$

  If $y \neq \pm 1 \bmod N$, then $p \mid y+1$, $q \mid y-1$

  Find $\gcd(N, y+1)$, $\gcd(N, y-1)$

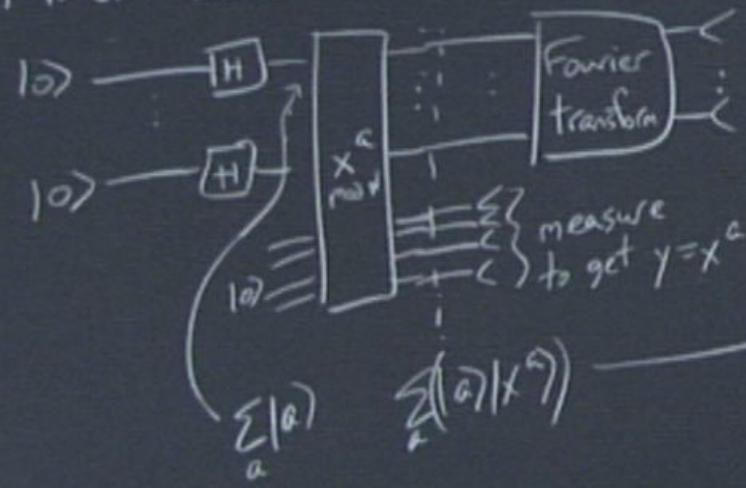
- Find x with even order $r/2$ integer $y = x^{r/2}$ then $y^2 = 1 \bmod N$, $y \neq 1 \bmod N$

- Choose random x, with constant prob (relative to $\log N$) x has even order r & $x^{r/2} \neq -1 \bmod N$.


Shor's algorithm:
Finds order of x:
|0⟩
|0⟩
H
H
x^a
measure to get $y = x^a$
|0⟩
$\sum_a |a\rangle$
$\sum_a |a\rangle|x^a\rangle$

Shor's algorithm:

Finds order of x.



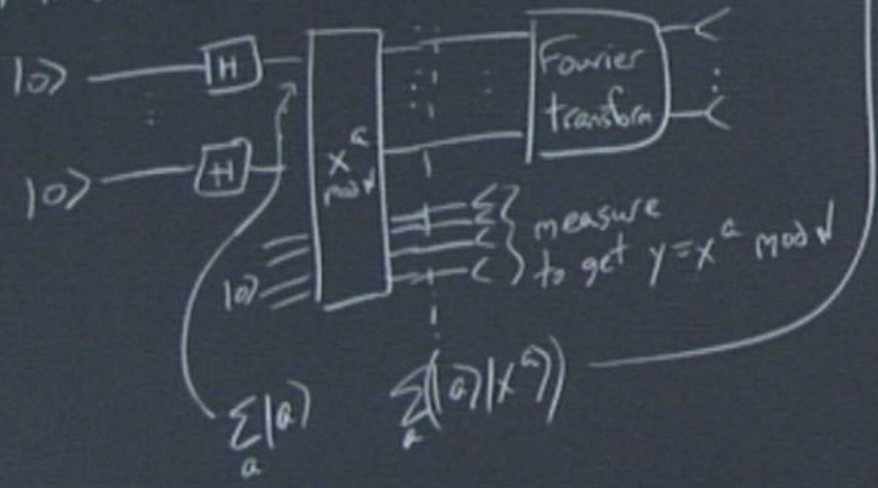
Measurement

Different x's with $x^a = y \bmod N$ are related by multiples of r

$x^{a_0} = y \bmod N$, $x^{a_0+r} = y \bmod N$, x^{a_0+}

Shor's algorithm:

Finds order of x:



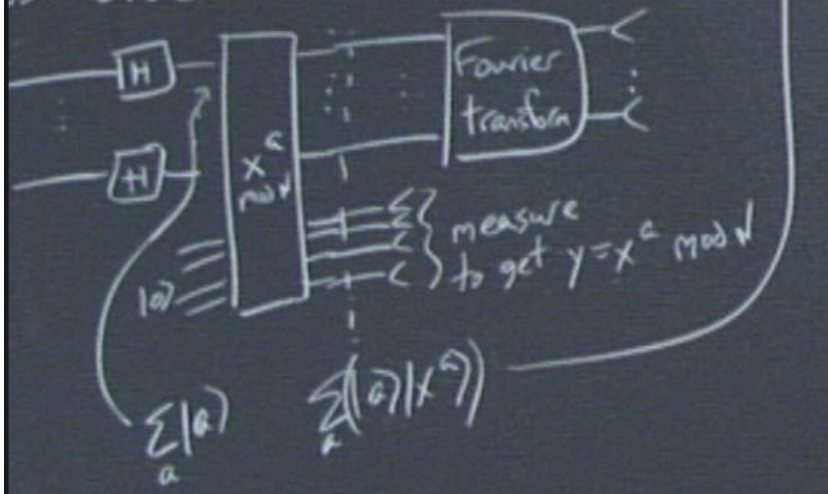
Measurement

Different x's with $x^a = y \bmod N$ are related by multiples of r

$x^{a_0} = y \bmod N$, $x^{a_0+r} = y \bmod N$, $x^{a_0+jr} = y$

algorithm:

...s order of x.



Measurement

Different x's with $x^a = y \bmod N$ are related by multiples of r

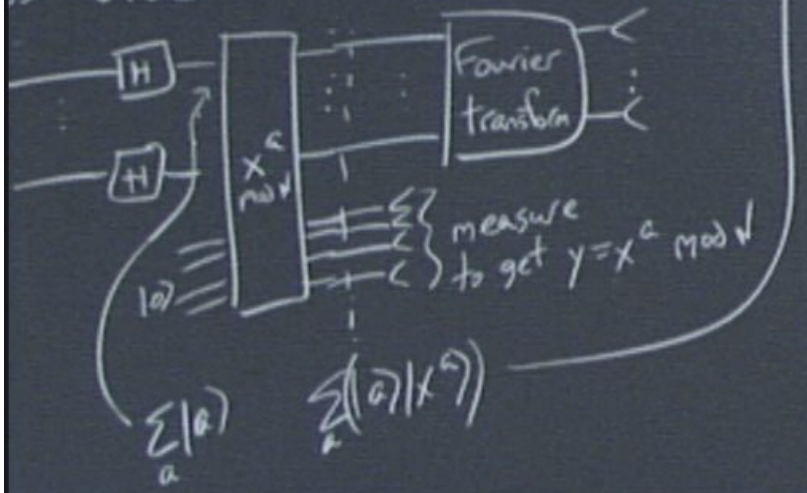
$x^{a_0} = y \bmod N$, $x^{a_0+r} = y \bmod N$, $x^{a_0+jr} = y \bmod N$

(Suppose $x^{a_0+s} = y \bmod N$

$\Rightarrow x^{-a_0}\left(x^{a_0+s}\right) = x^s = x^{-a_0} y \bmod N = 1 \bmod N$

algorithm:

...s order of x:



Measurement

Different x's with $x^a = y \bmod N$ are related by multiples of r

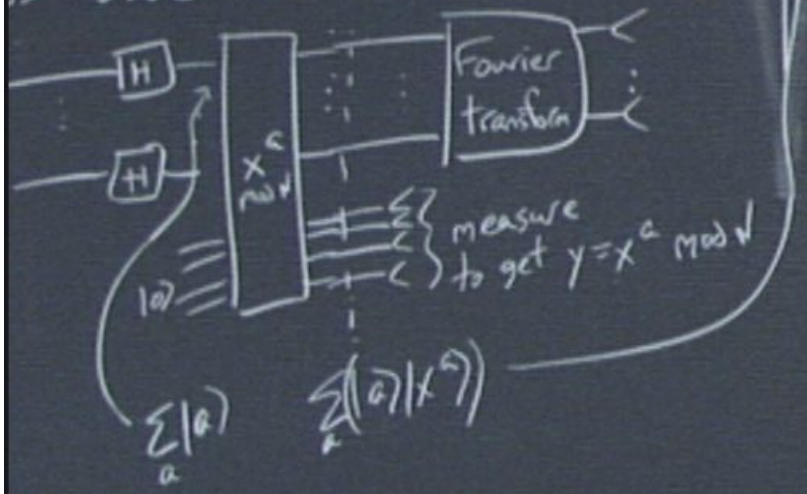
$x^{a_0} = y \bmod N$, $x^{a_0+r} = y \bmod N$, $x^{a_0+jr} = y \bmod N$

(Suppose $x^{a_0+s} = y \bmod N$

$\Rightarrow x^{-a_0}\left(x^{a_0+s}\right) = x^s = \underbrace{x^{-a_0} y}_{1} \bmod N = 1 \bmod N$)

algorithm:

...s order of x:



Measurement

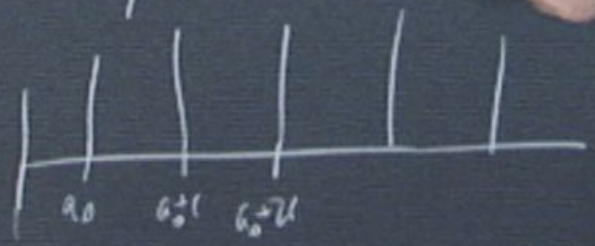
Different x's with $x^a = y \bmod N$ are related by multiples of r

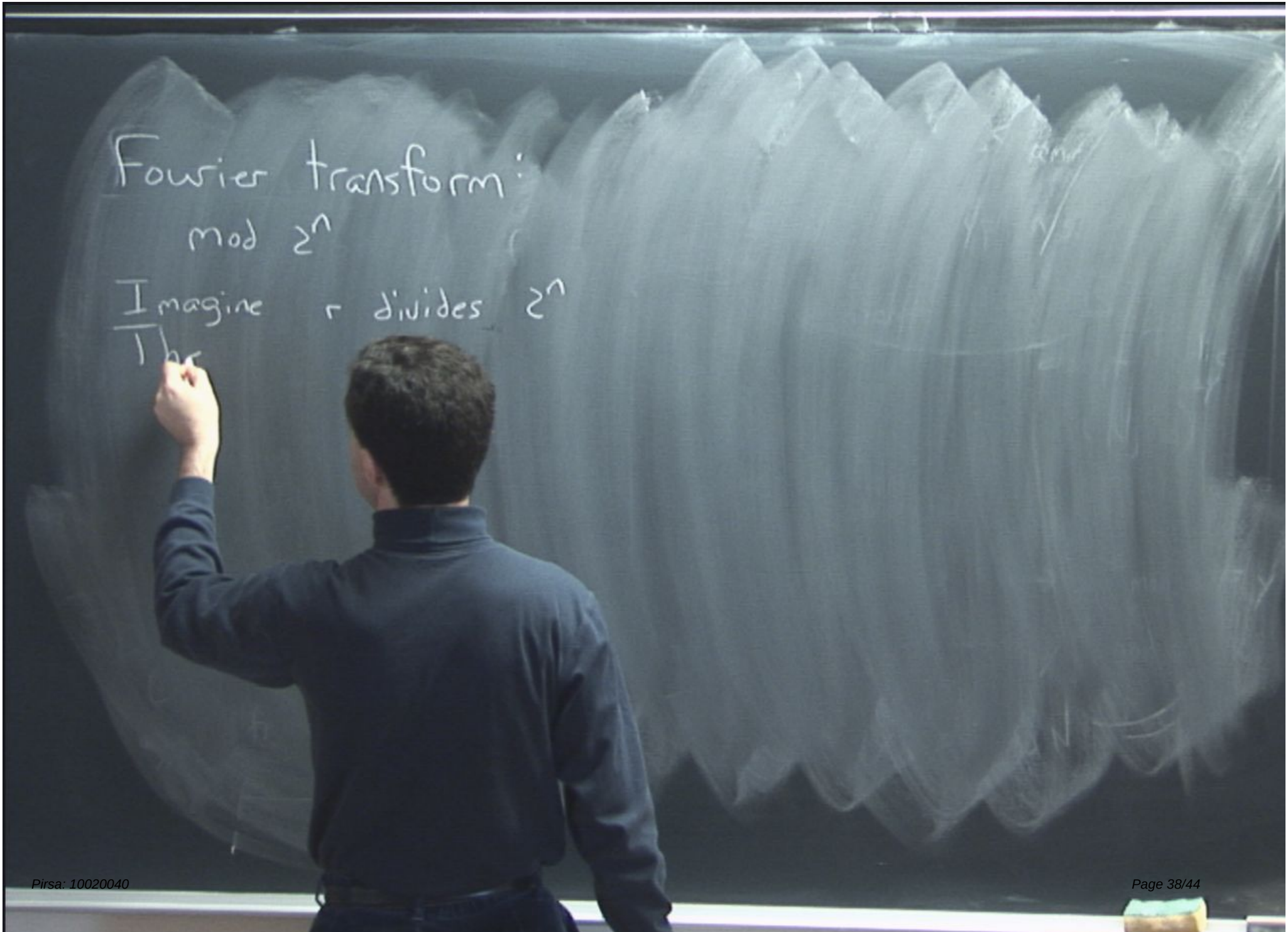
$x^{a_0} = y \bmod N$, $x^{a_0+r} = y \bmod N$, $x^{a_0+jr} = y \bmod N$

(Suppose $x^{a_0+s} = y \bmod N$

$\Rightarrow x^{-a_0}(x^{a_0+s}) = x^s = x^{-a_0} y \bmod N = 1 \bmod N$)

$\left(\sum_j |a_0 + jr\rangle\right)|y\rangle$




Fourier transform:
mod 2^
Imagine r divides 2^

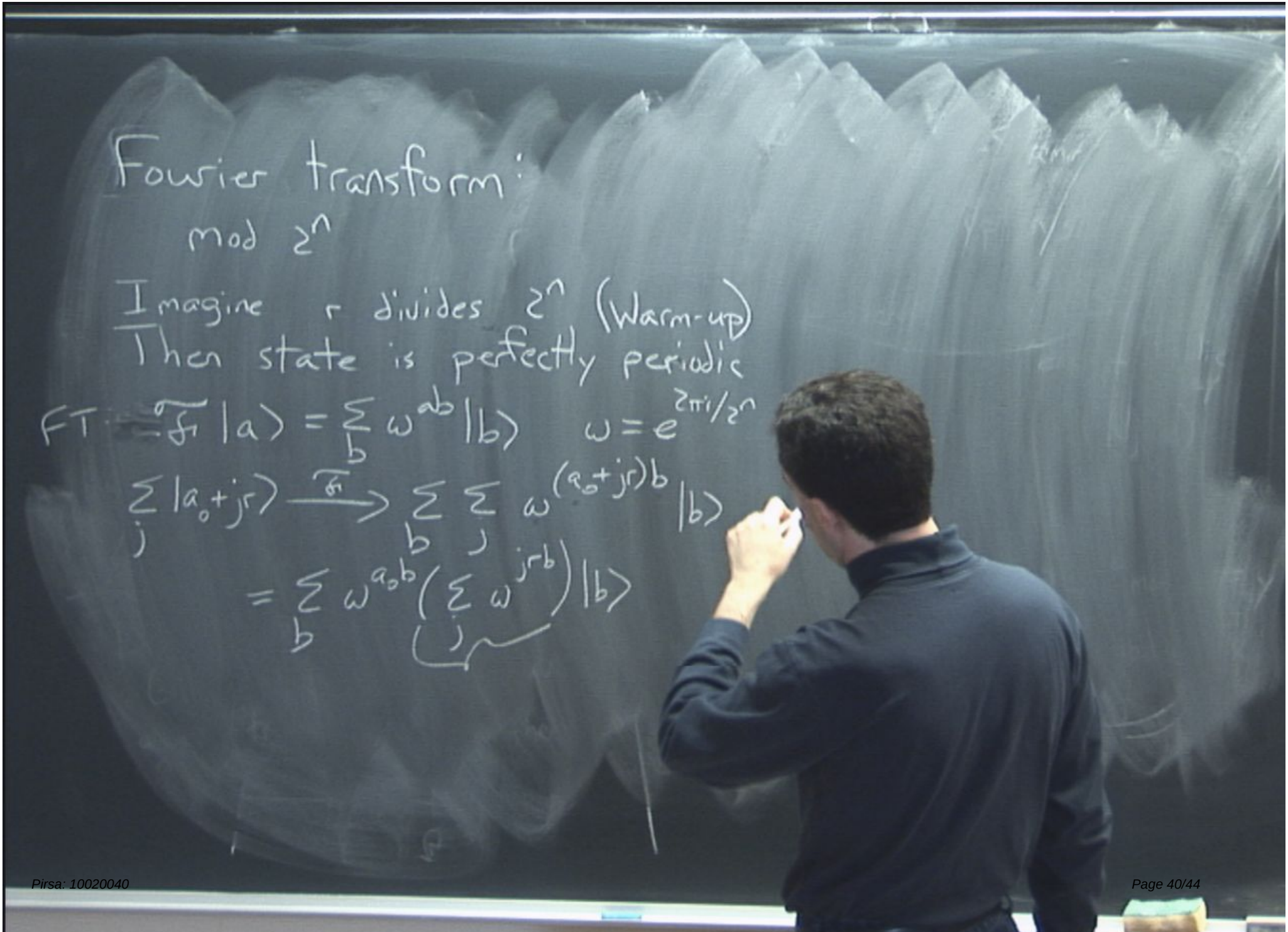
Fourier transform:

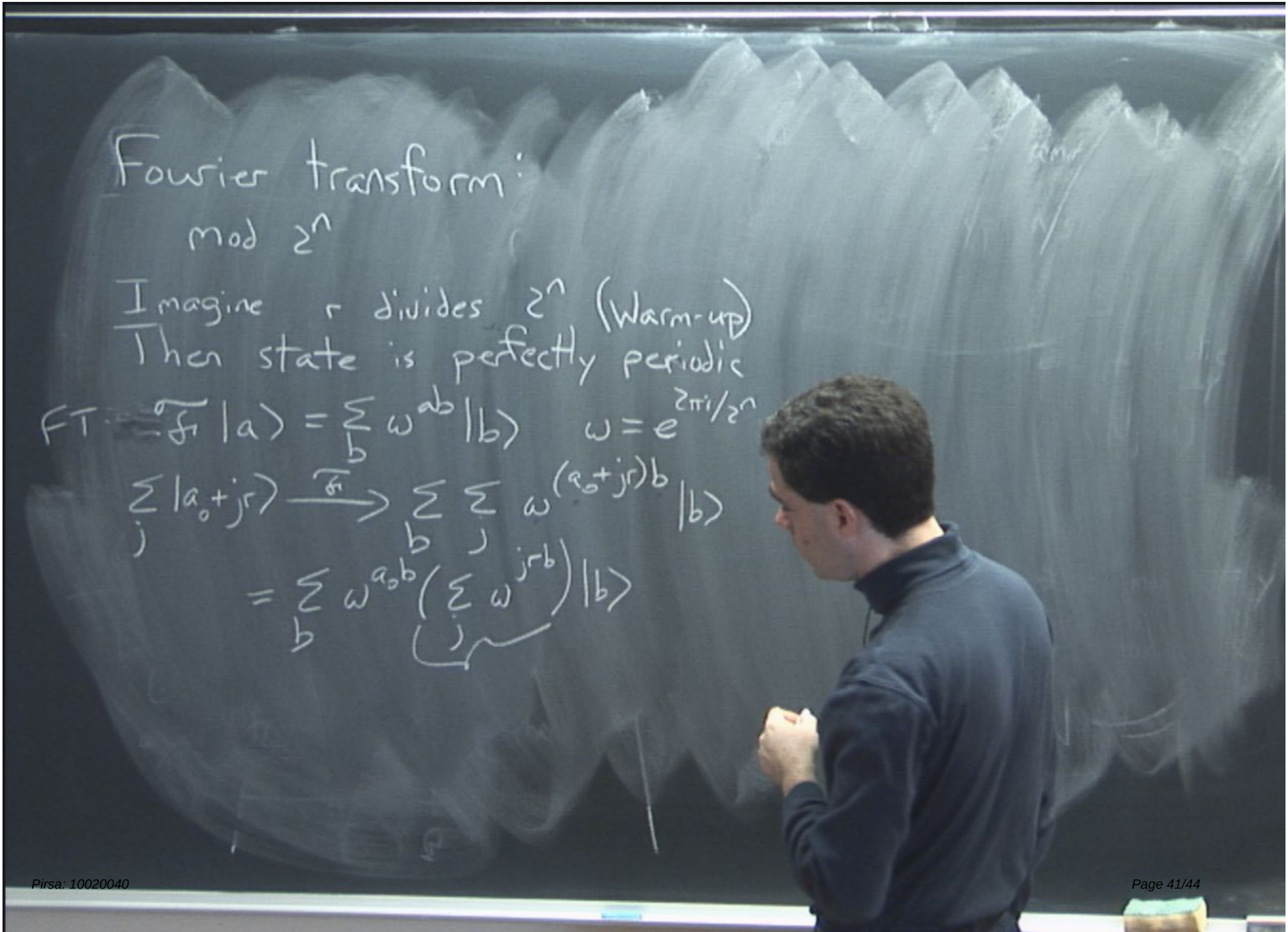
mod 2^n

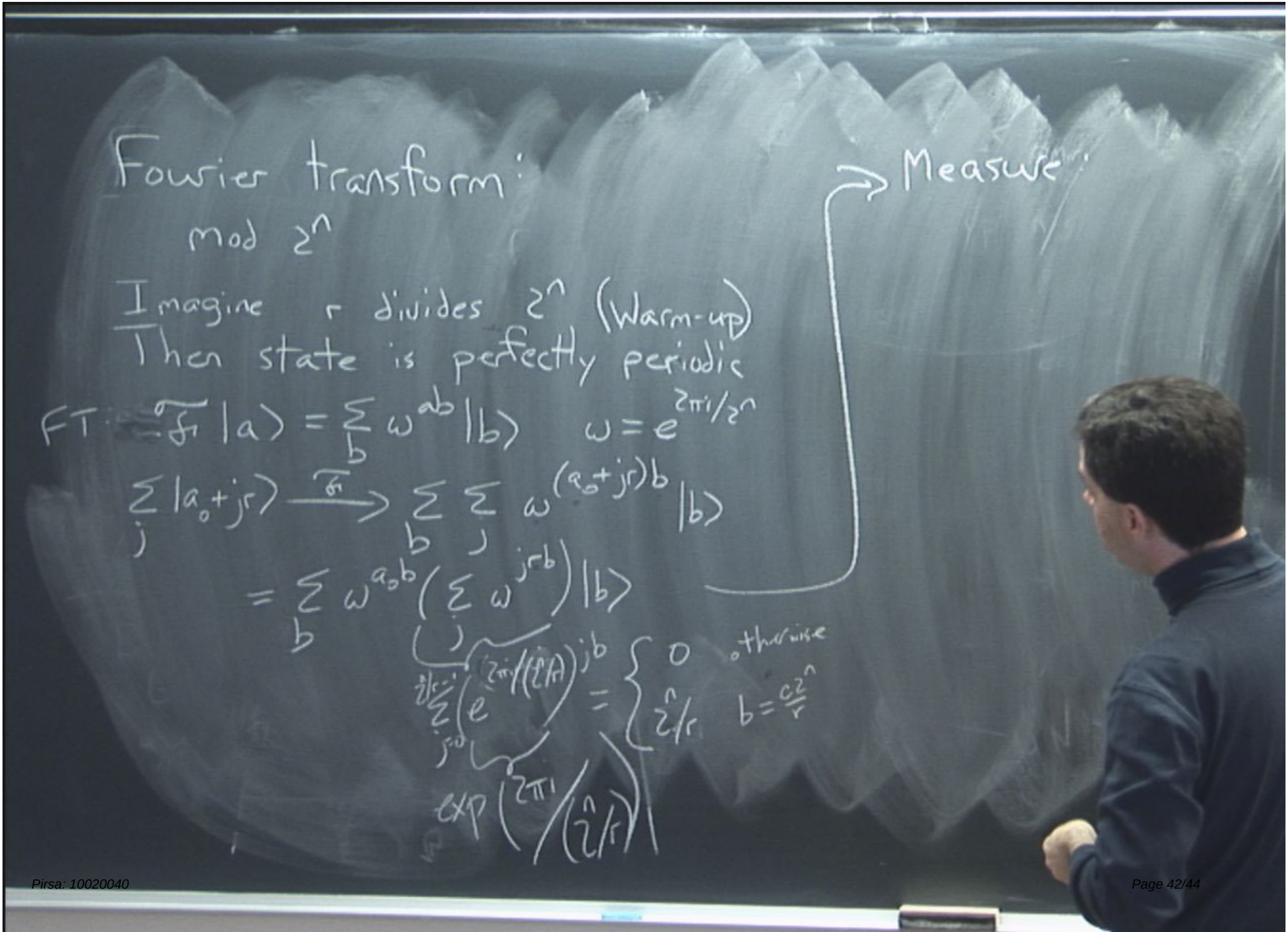
Imagine r divides 2^n (Warm-up)

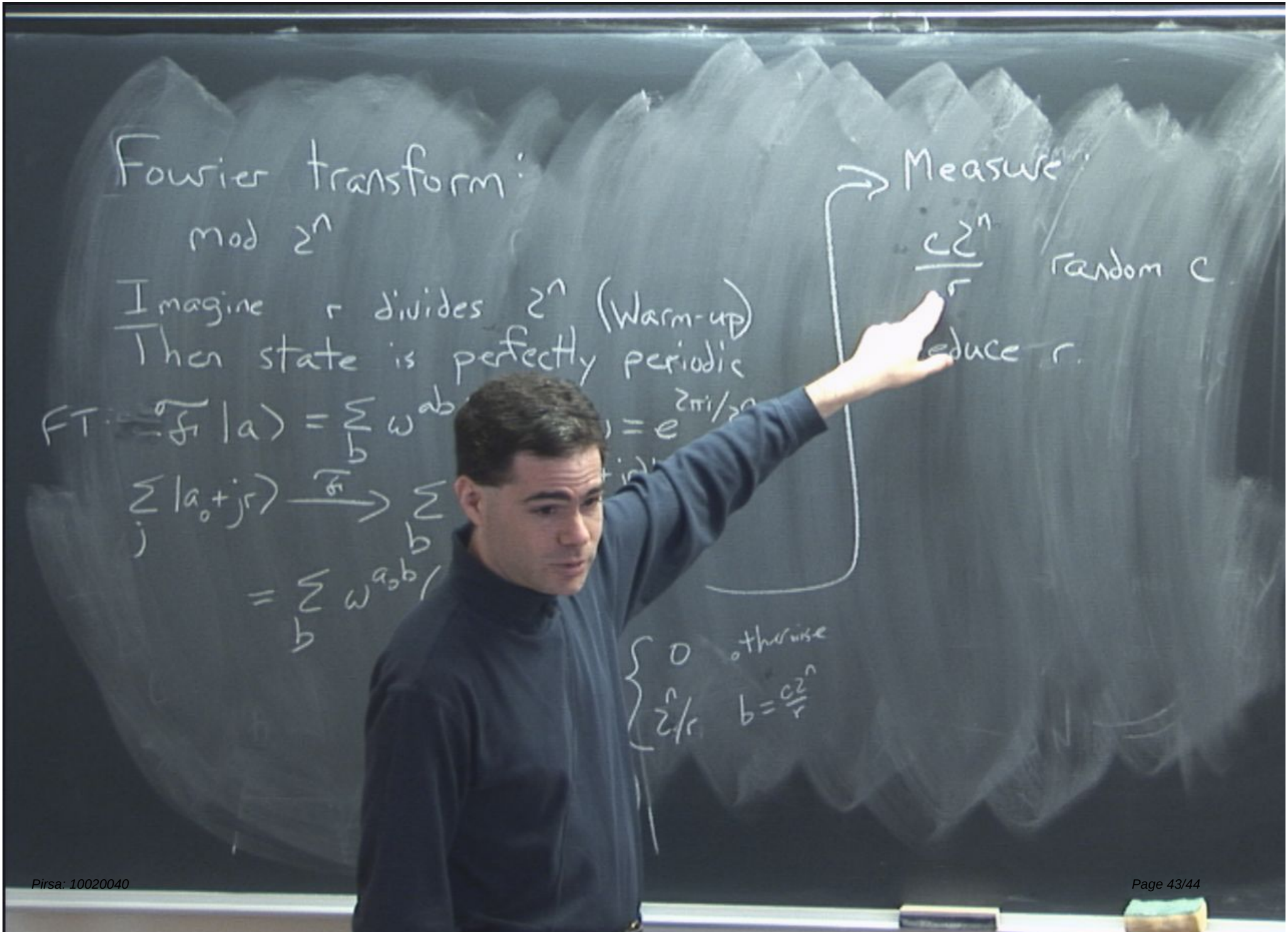
Then state is perfectly periodic

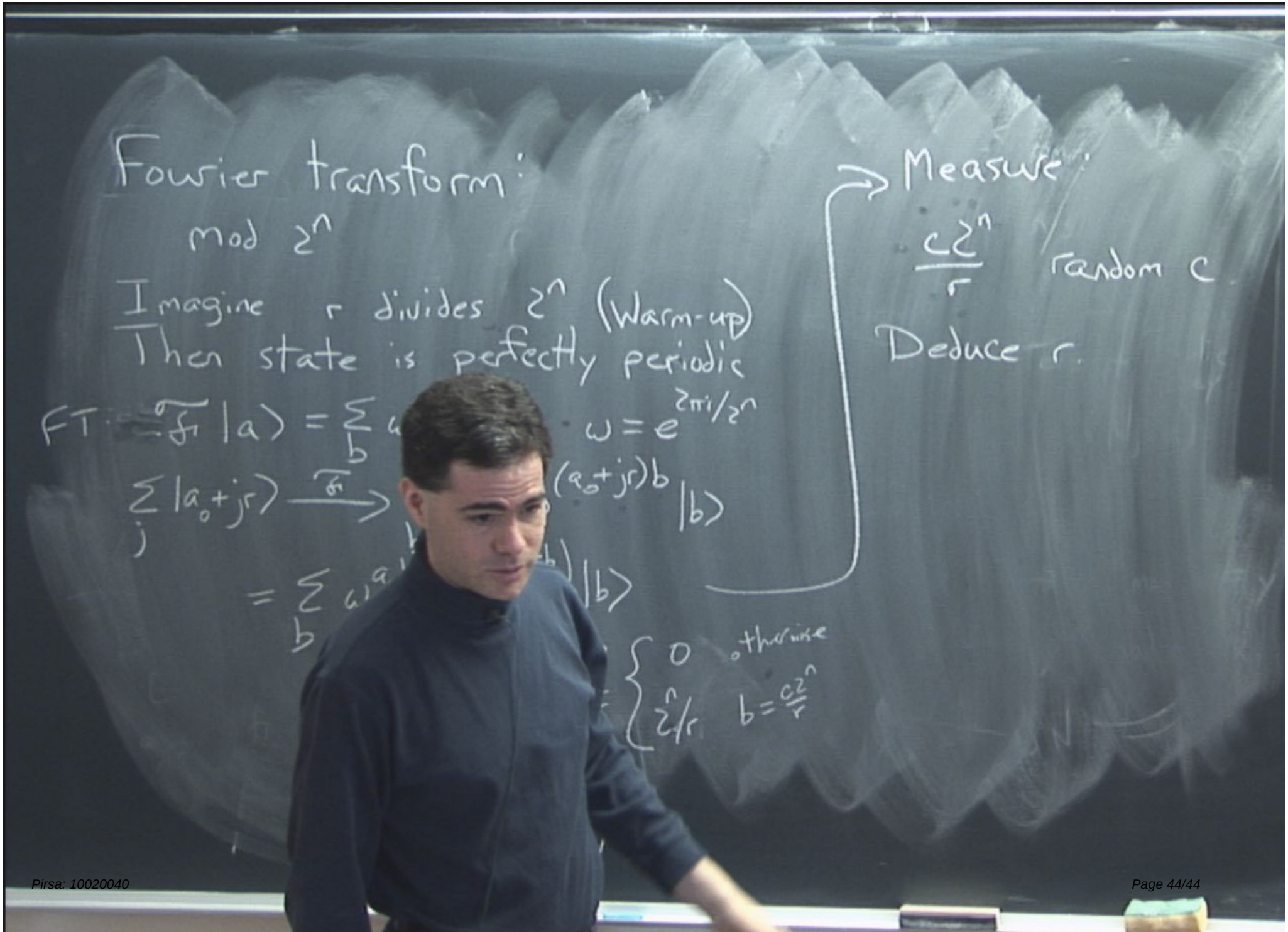
FT: $\frac{1}{\sqrt{r}} \sum_b \omega^{ab} |b\rangle \quad \omega = e^{2\pi i / 2^n}$


Fourier transform:
mod 2^n
Imagine r divides 2^n (Warm-up)
Then state is perfectly periodic
FT $|a\rangle = \sum_b \omega^{ab} |b\rangle$ $\omega = e^{2\pi i/2^n}$
$\sum_j |a_0 + jr\rangle \xrightarrow{FT} \sum_b \sum_j \omega^{(a_0+jr)b} |b\rangle$
$= \sum_b \omega^{a_0 b} \left(\sum_j \omega^{jrb} \right) |b\rangle$


Fourier transform:
mod 2^n
Imagine r divides 2^n (Warm-up)
Then state is perfectly periodic
FT $|a\rangle = \sum_b \omega^{ab} |b\rangle$ $\omega = e^{2\pi i/2^n}$
$\sum_j |a_0 + jr\rangle \xrightarrow{FT} \sum_b \sum_j \omega^{(a_0+jr)b} |b\rangle$
$= \sum_b \omega^{a_0 b} \left(\sum_j \omega^{jrb} \right) |b\rangle$


Fourier transform:
mod 2^n
Measure!
Imagine r divides 2^n (Warm-up)
Then state is perfectly periodic
FT: $\mathcal{F}_r|a\rangle = \sum_b \omega^{ab}|b\rangle \quad \omega = e^{2\pi i/2^n}$
$\sum_j |a_0 + jr\rangle \xrightarrow{\mathcal{F}} \sum_b \sum_j \omega^{(a_0+jr)b}|b\rangle$
$= \sum_b \omega^{a_0 b}\left(\sum_j \omega^{jrb}\right)|b\rangle$
$\sum_{j=0}^{2^n/r} e^{2\pi i/(2^n/r)\, jb} = \begin{cases} 0 & \text{otherwise} \\ 2^n/r & b = c\frac{2^n}{r} \end{cases}$
$\exp\left(2\pi i/(2^n/r)\right)$


Fourier transform:
mod 2^n
Imagine r divides 2^n (Warm-up)
Then state is perfectly periodic
Measure
$\frac{c2^n}{r}$
random c
educe r.
otherwise
$b = \frac{c2^n}{r}$


Fourier transform:
mod 2^n
Imagine r divides 2^n (Warm-up)
Then state is perfectly periodic
$\omega = e^{2\pi i/2^n}$
$\sum_j |a_0 + jr\rangle \xrightarrow{FT} \sum_b \omega^{(a_0+jr)b} |b\rangle$
$= \sum_b c_b |b\rangle$
$\begin{cases} 0 & \text{otherwise} \\ r & b = \frac{c2^n}{r} \end{cases}$
Measure
$\frac{c2^n}{r}$ random c
Deduce r.