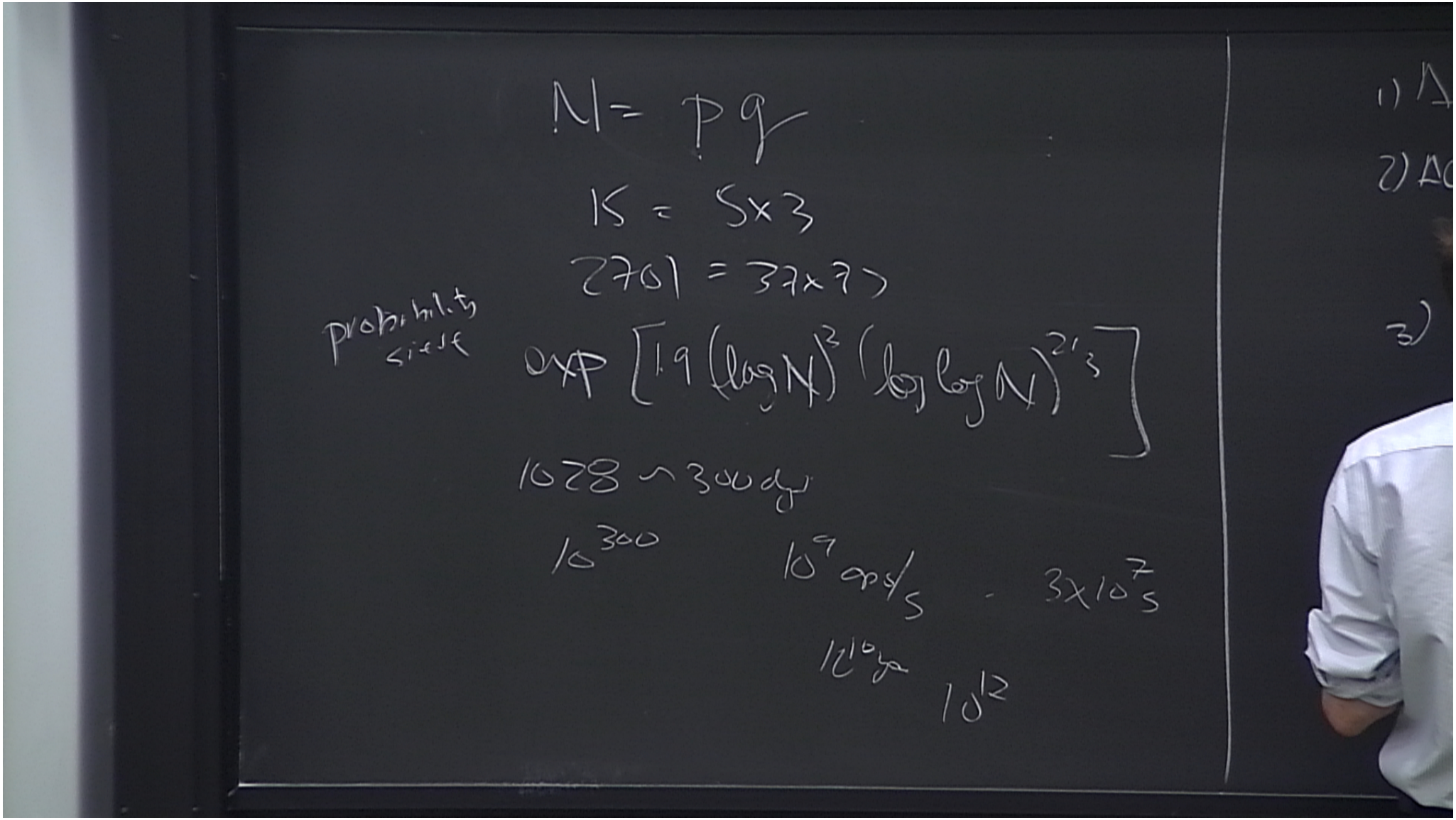
Title: PSI 2015/2016 Quantum Information - Lecture 9

Date: Mar 03, 2016 11:30 AM

URL: http://pirsa.org/16030056

Abstract:


N = pq
15 = 5x3
2701 = 37x73
probability sieve
exp [1.9 (log N)^{1/3} (log log N)^{2/3}]
1028 ~ 300 dg
10^300
10^9 ops/s
3x10^7 s
12^10 ya
10^12

1) Alice $(p,q) = n$. $(3,7) = 15$

2) Choose e $1 < e < \phi(n) = (p-1)(q-1) = 8$

$e = 7$

3) compute $d = e^{-1} \bmod \phi(n)$ $(e \cdot d = 1 \bmod \phi(n))$

$d = 7$ $\quad 7d = 1 \bmod 8$

$d = 7$

4) Public key (e,n) $\quad$ Private key (d,n)

$(7,15)$ $\quad (7,15)$

Encryption

(e,n), $(7,15)$

$m \in \mathbb{Z}_n \quad 3$

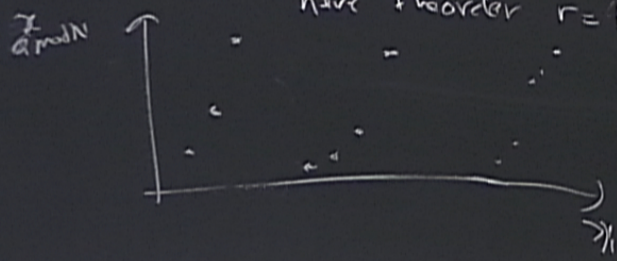
$C = m^e \bmod n$

factoring equivalent to order finding (Miller 70')

The order of an integer $a \bmod N$ is the smallest r such that $a^r \bmod N = 1$

$N = 15$, $a = 2$ $\quad 2^1 = 2$ $\quad 2^2 = 4$ $\quad 2^3 = 8$ $\quad 2^r = 2^4 = 1$

have the order $r = 4$



$(a^r - 1) \bmod N = 0$

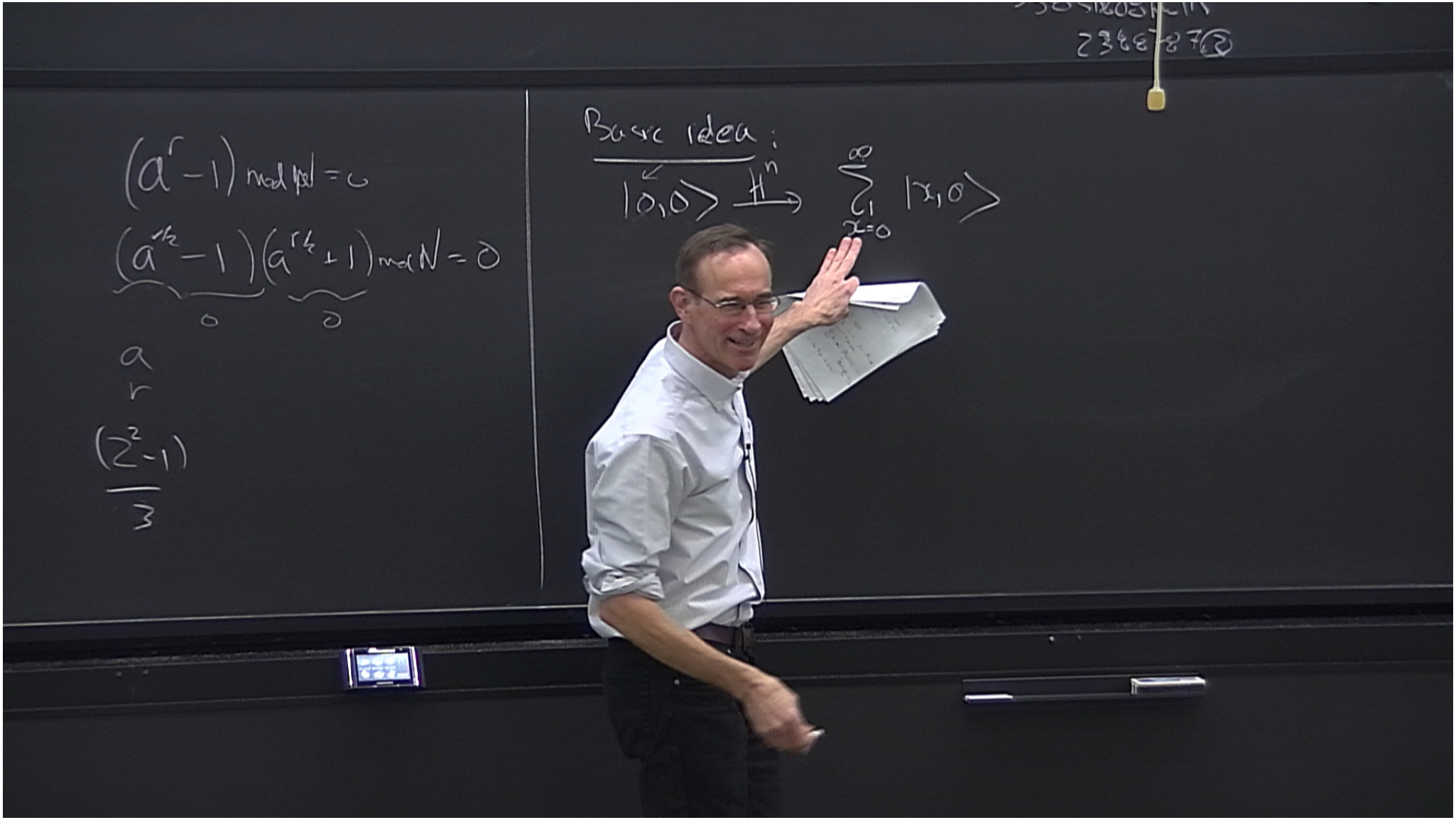
$(a^{r/2} - 1)(a^{r/2} + 1) \bmod N = 0$

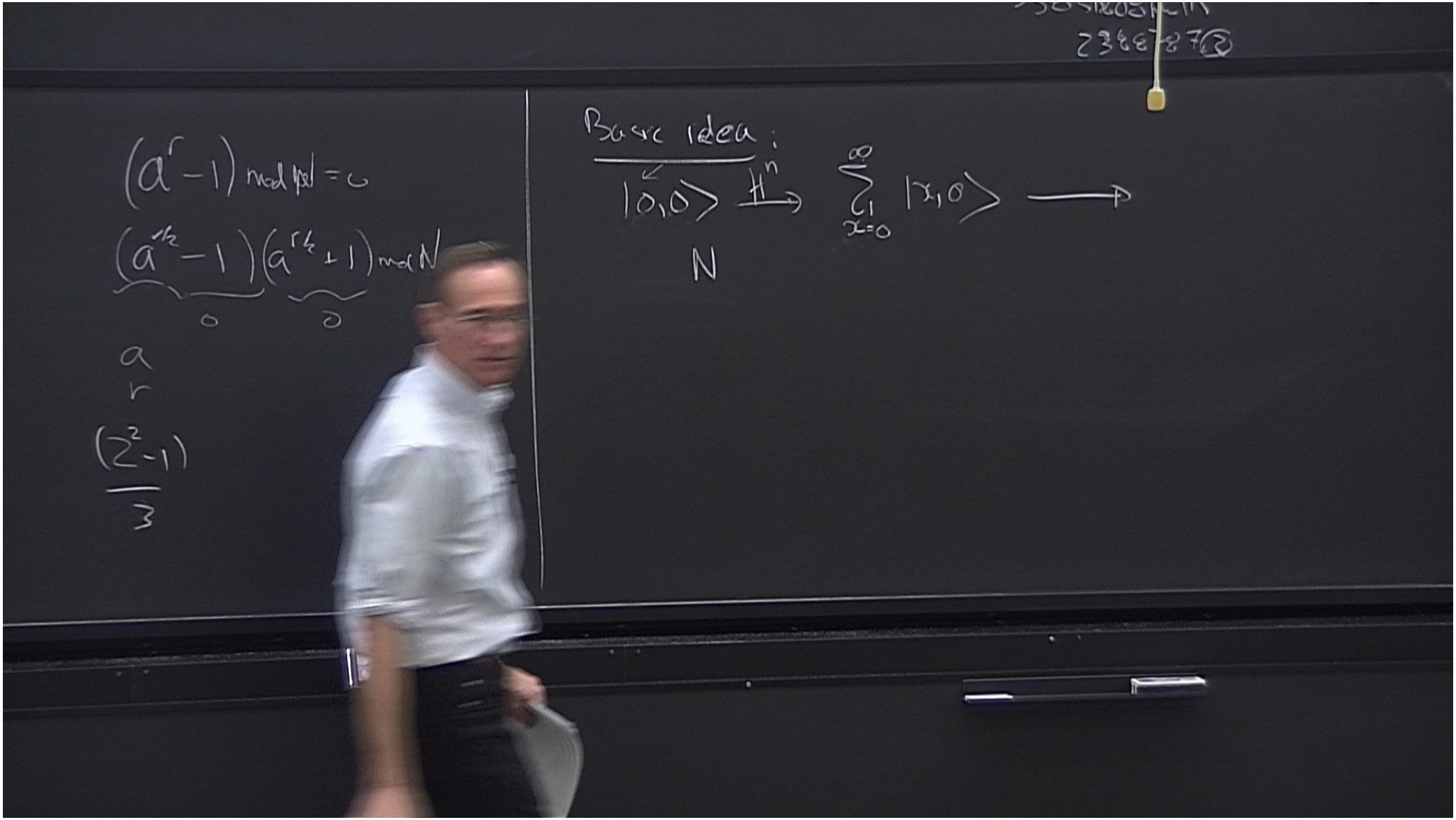
a

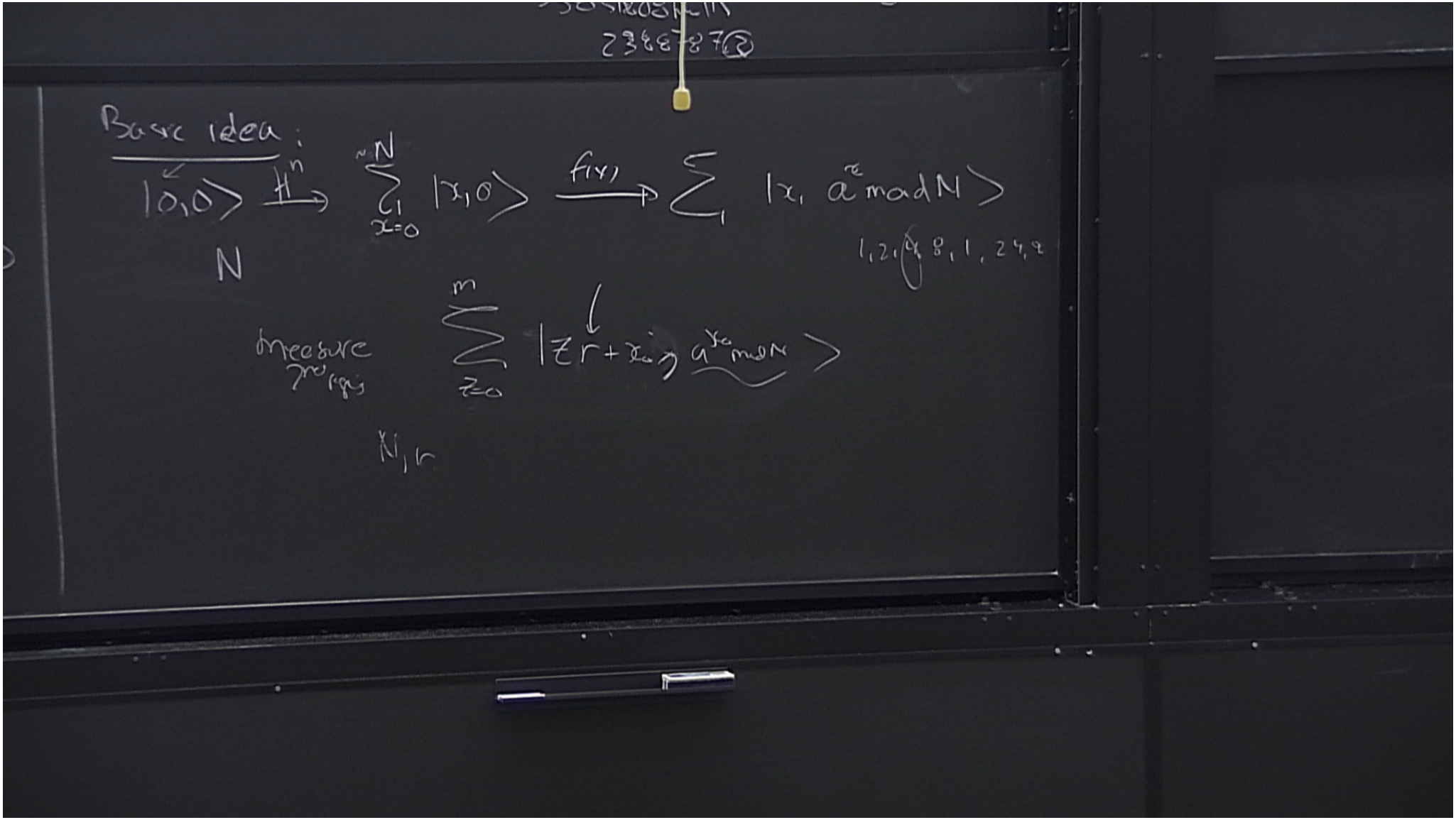
r

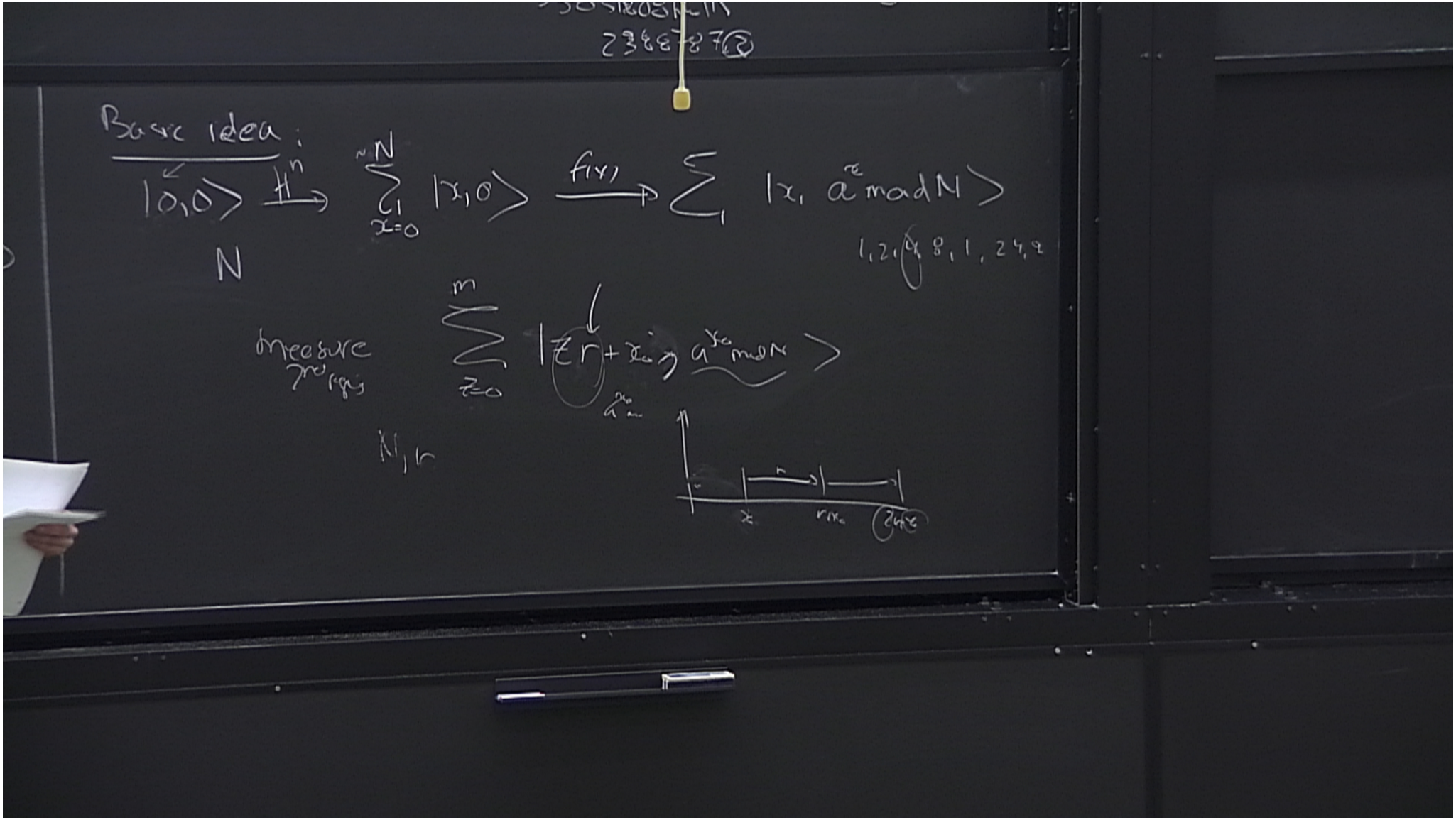
$(2^2 - 1)$

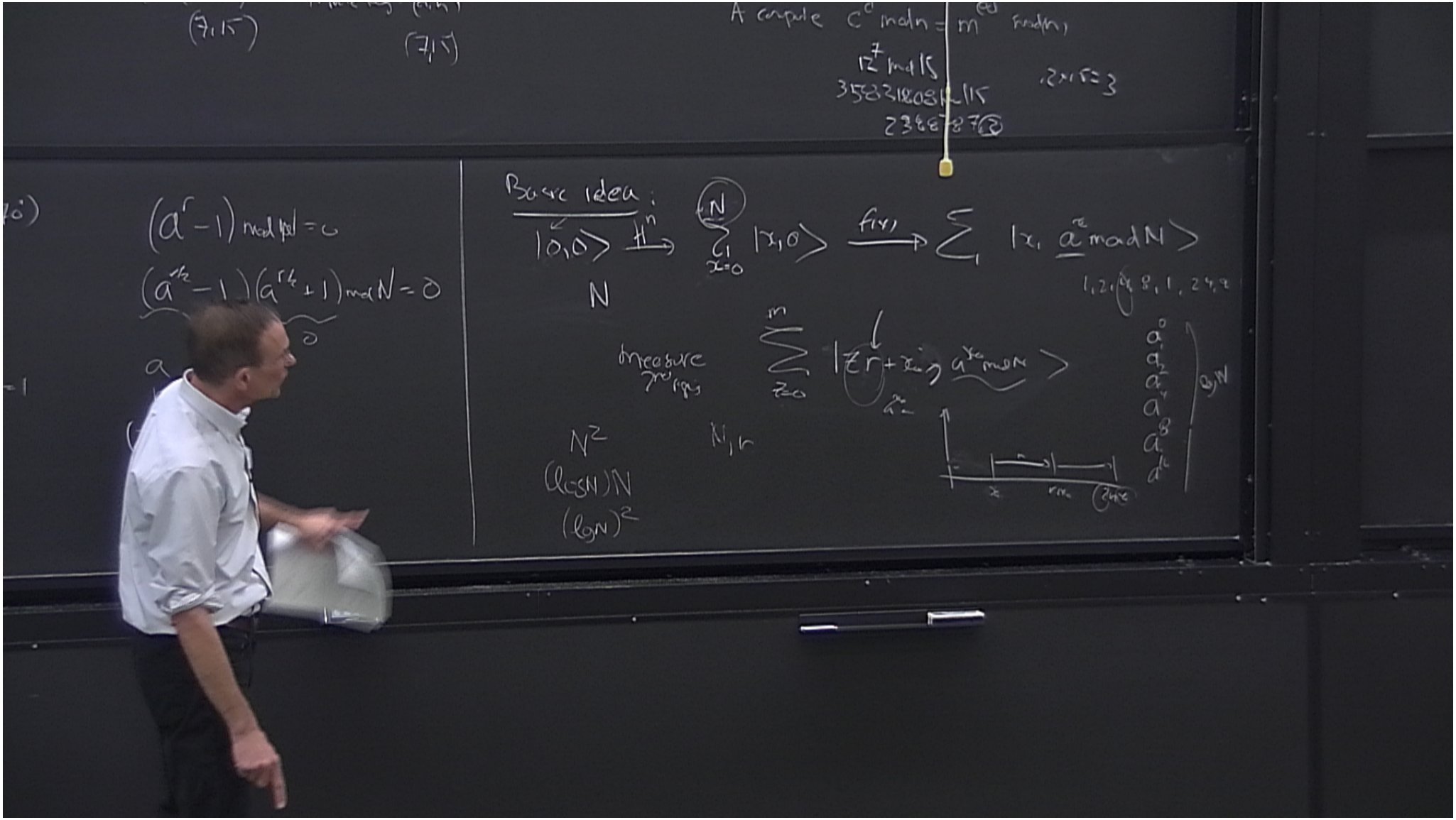
3

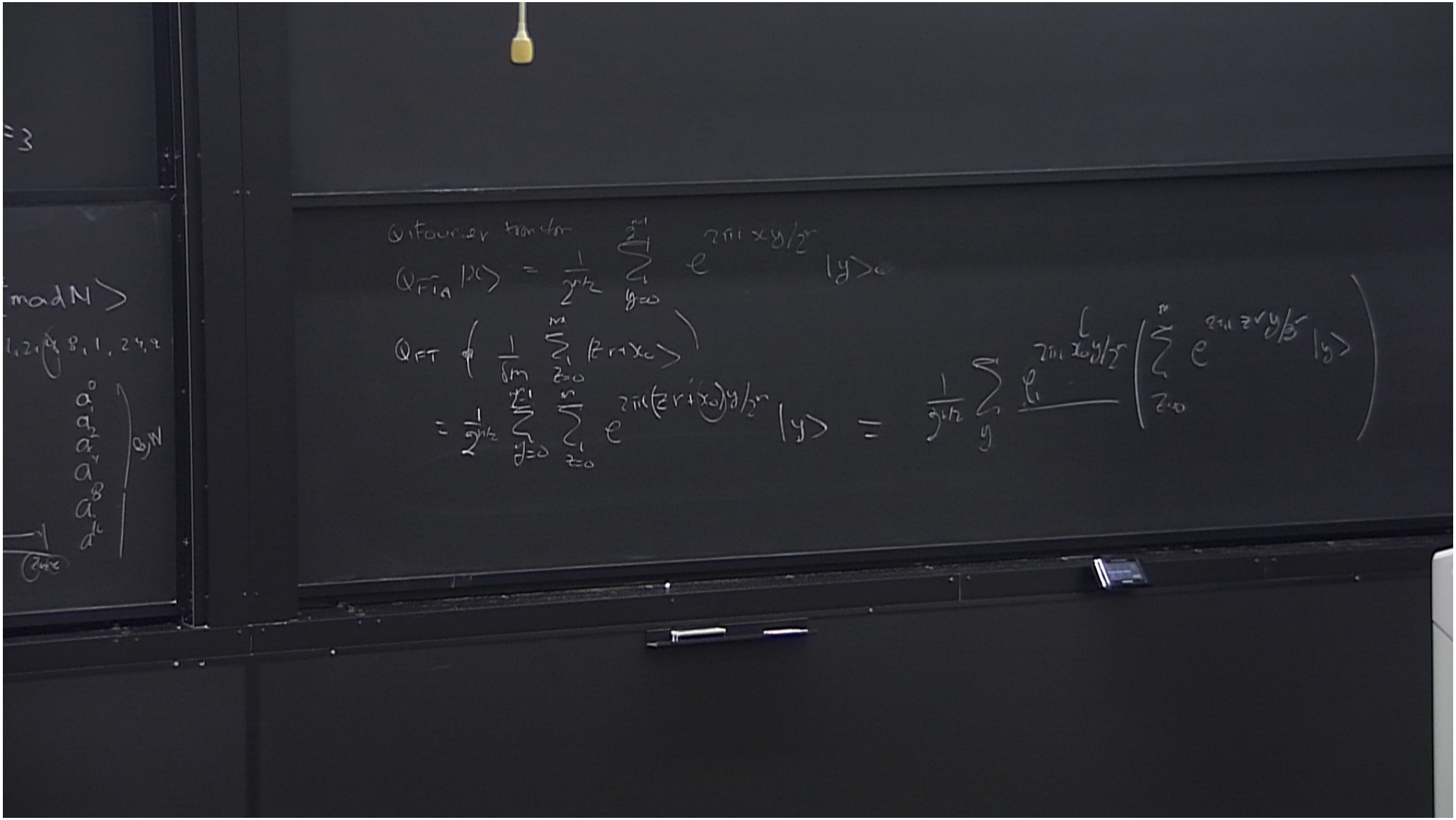

$(a^r - 1) \bmod N = 0$
$(a^{r/2} - 1)(a^{r/2} + 1) \bmod N = 0$
0
0
a
r
$(2^2 - 1)$
3
Basic idea:
$|0,0\rangle \xrightarrow{H^n} \sum_{x=0}^{\infty} |x,0\rangle$

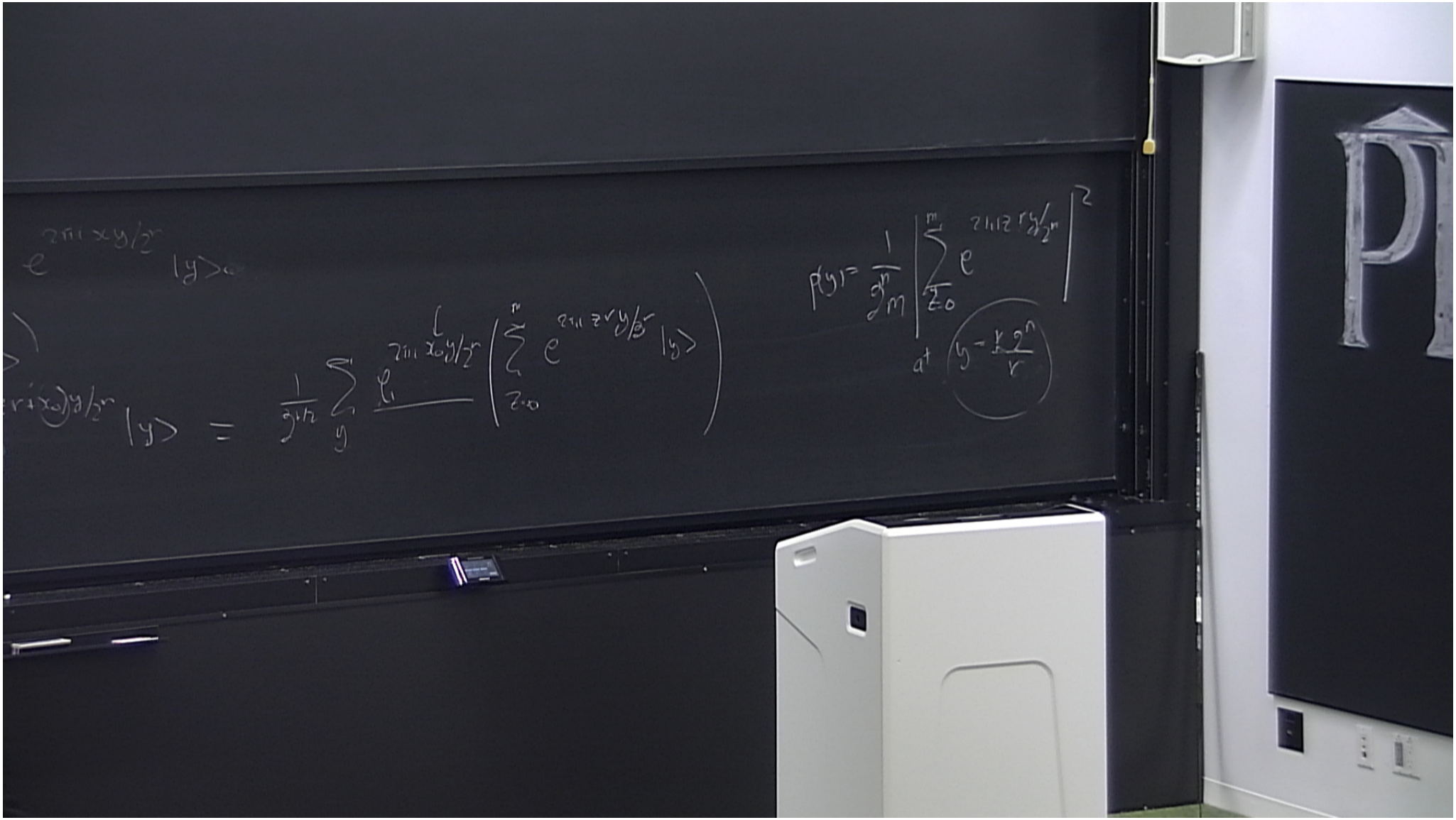

$(a^r - 1) \bmod N = 0$
$(a^{r/2} - 1)(a^{r/2} + 1) \bmod N$
0
0
a
r
$(2^2 - 1)$
3
Basic idea:
$|0,0\rangle \xrightarrow{H^n} \sum_{x=0}^{\infty} c_x |x,0\rangle \longrightarrow$
N

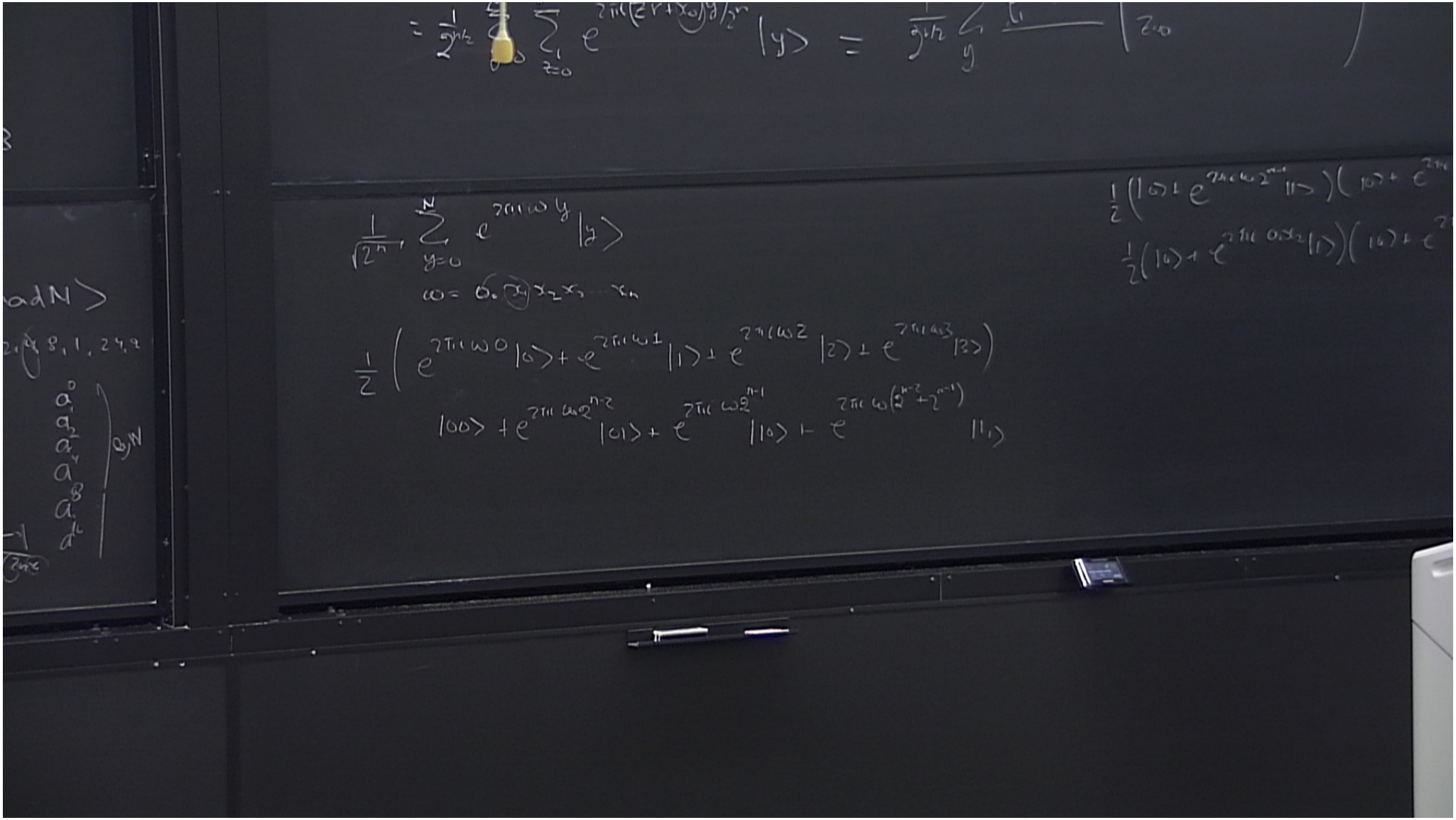

Basic idea:
$|0,0\rangle$
H^n
$\sum_{x=0}^{N} |x,0\rangle$
$f(x)$
$\sum |x, a^x \bmod N\rangle$
N
1, 2, 4, 8, 1, 2, 4, 8
measure
$\sum_{z=0}^{m} |zr + x_0\rangle |a^{x_0} \bmod N\rangle$
N, r


Basic idea:
|0,0⟩
H^n
N
Σ_{x=0}^{N-1} |x,0⟩
f(x)
Σ |x, a^x mod N⟩
1, 2, 4, 8, 1, 2, 4, 8
measure
Σ_{x=0}^{m} |x_0 + jr⟩ a^{x_0} mod N⟩
N, r
x
r
2^m


Basic idea:
f(x)
measure
N^2
(log N) N
(log N)^2


Quantum Fourier transform
$Q_{FT}|x\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{2\pi i xy/2^n} |y\rangle$
$Q_{FT}\left(\frac{1}{\sqrt{m}} \sum_{r=0}^{m-1} |x_0 + rs\rangle\right)$
$= \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} \sum_{r=0}^{m-1} e^{2\pi i (x_0 + rs)y/2^n} |y\rangle = \frac{1}{2^{n/2}} \sum_y e^{2\pi i x_0 y/2^n} \left(\sum_{r=0}^{m-1} e^{2\pi i rsy/2^n} |y\rangle \right)$


Pr

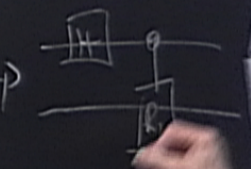

$\frac{1}{\sqrt{2^n}} \sum_{y=0}^{N} e^{2\pi i \omega y} |y\rangle$
$\omega = 0.x_1 x_2 x_3 \ldots x_n$
$\frac{1}{2}\left(e^{2\pi i \omega 0}|0\rangle + e^{2\pi i \omega 1}|1\rangle + e^{2\pi i \omega 2}|2\rangle + e^{2\pi i \omega 3}|3\rangle \right)$
$|00\rangle + e^{2\pi i \omega 2^{n-2}}|01\rangle + e^{2\pi i \omega 2^{n-1}}|10\rangle + e^{2\pi i \omega (2^{n-1}+2^{n-2})}|11\rangle$
$\frac{1}{2}\left(|0\rangle + e^{2\pi i \omega 2^{n-1}}|1\rangle\right)\left(|0\rangle + e^{2\pi i \omega 2}|1\rangle\right)\left(|0\rangle + e^{2\pi i}\right.$
B/W

$$\frac{1}{\sqrt{2^n}} \sum_{y=0}^{N} e^{2\pi i \omega y} |y\rangle$$

$$\omega = 0.x_1 x_2 x_3 \cdots x_n$$

$$\frac{1}{2}\left(e^{2\pi i \omega 0}|0\rangle + e^{2\pi i \omega 1}|1\rangle + e^{2\pi i \omega 2}|2\rangle + e^{2\pi i \omega 3}|3\rangle \right)$$

$$|00\rangle + e^{2\pi i \omega 2^{n-2}}|01\rangle + e^{2\pi i \omega 2^{n-1}}|10\rangle + e^{2\pi i \omega (2^{n-2}+2^{n-1})}|11\rangle$$



$$\frac{1}{\sqrt{2^n}} \sum_{y=0}^{N} e^{2\pi i \omega y} |y\rangle$$

$$\omega = 0.x_1 x_2 x_3 \cdots x_n$$

$$\frac{1}{2}\left(e^{2\pi i \omega 0}|0\rangle + e^{2\pi i \omega 1}|1\rangle + e^{2\pi i \omega 2}|2\rangle + e^{2\pi i \omega 3}|3\rangle \right)$$

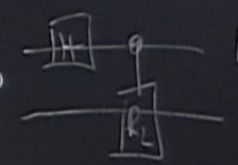
$$|00\rangle + e^{2\pi i \omega 2^{n-2}}|01\rangle + e^{2\pi i \omega 2^{n-1}}|10\rangle + e^{2\pi i \omega (2^{n-2}+2^{n-1})}|11\rangle$$

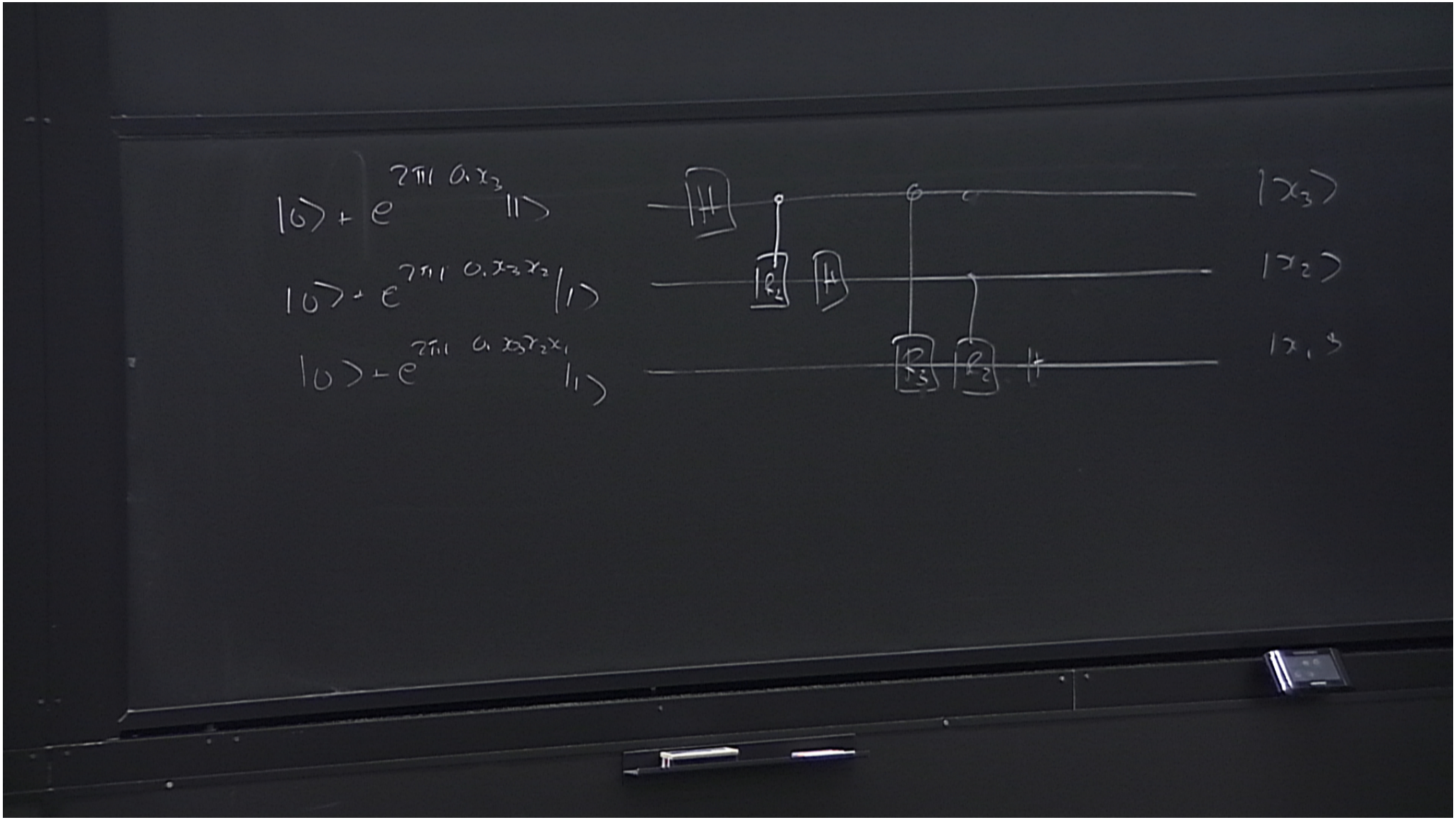
$$\frac{1}{2}\left(|0\rangle + e^{2\pi i \omega}$$

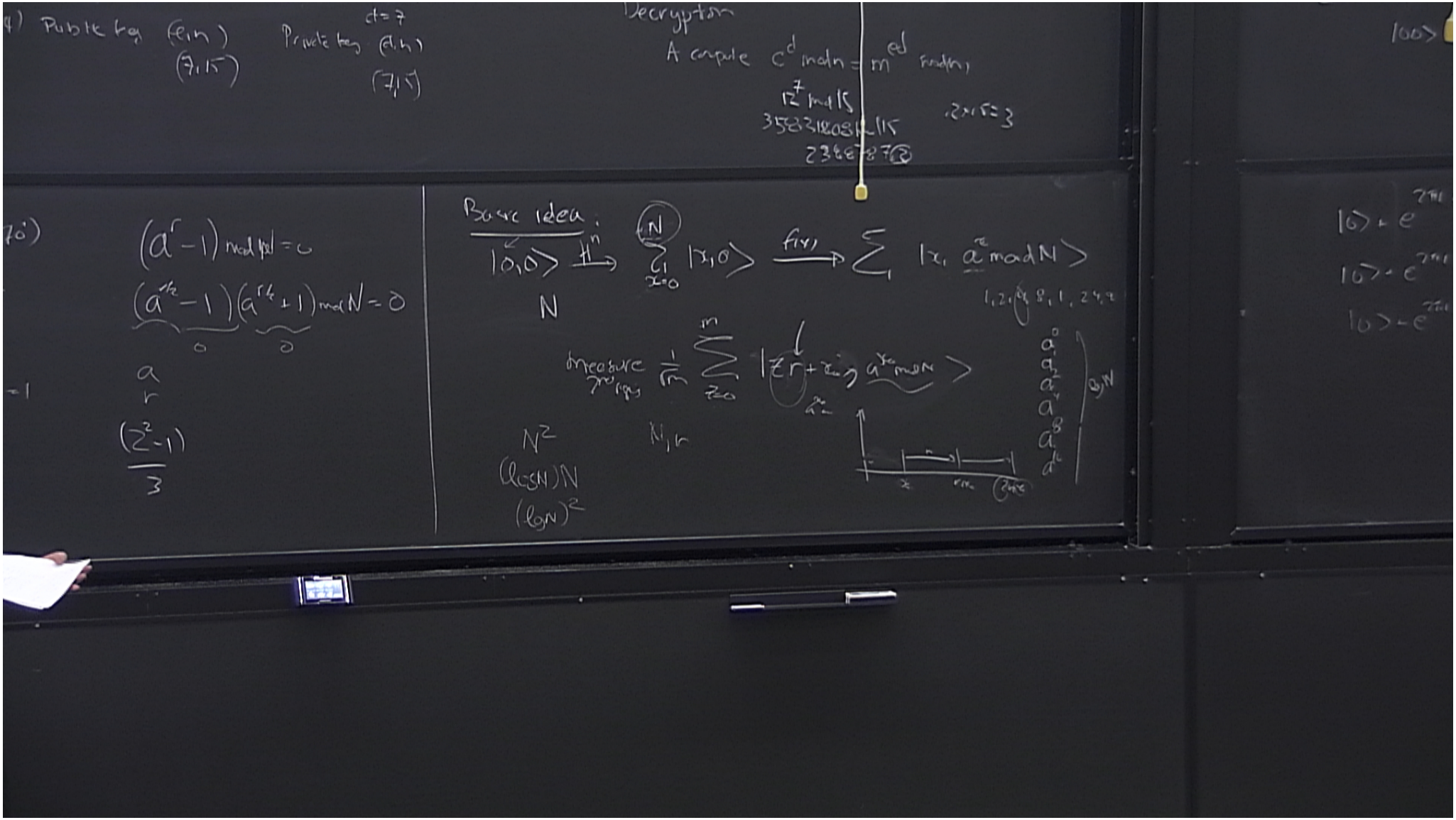
$$\frac{1}{2}\left(|0\rangle + e^{2\pi i}$$

$x_2 = 0$

$x_2 = 1$




$|0\rangle + e^{2\pi i\, 0.x_3}|1\rangle$
$|0\rangle + e^{2\pi i\, 0.x_3x_2}|1\rangle$
$|0\rangle + e^{2\pi i\, 0.x_3x_2x_1}|1\rangle$
H
R_2
H
R_3
R_2
H
$|x_3\rangle$
$|x_2\rangle$
$|x_1\rangle$


Public key (e,n) (7,15)
Private key (d,n) (7,15)
Decryption
Basic idea:
$(a^r-1) \bmod N = 0$
$(a^{r/2}-1)(a^{r/2}+1) \bmod N = 0$
$\frac{(2^2-1)}{3}$
N^2
$(\log N) N$
$(\log N)^2$