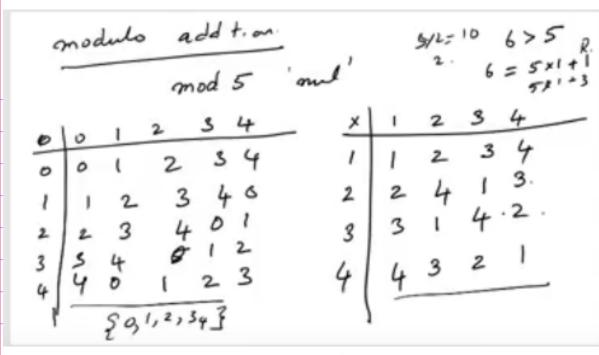
Shor's Algo	quantum state
	Cannot be
Two -> Alice & Bob	Copied,
Two -> Alice & Bob Msg: Encode & Devode	charlie will
Je cool	have to make
Charlie	a measurement.
$A \longleftrightarrow B$	
key o axb=EI	Josphic ky
	, d
Junat	2
IVOUP MEOVY	
Set.	
A B  key o axb = []  Set.  Set.  (a,b,c,d)  (x',','o') operation Ch-  a,beG thus	1 A , V >
(x): O' Toperation Ctr-	/X/+, mod T, mad =
(1) axb=C a, b∈G, they  Geometrican Closure	1 CEG
Gamponition Closure	
(2) 0*(p*c) = (0*p) * C	
(3) axl= exa=a	
(4) 0★b= b★ = 0	
2) $a + (b \times k) = (a + b) + c$ .  associations  association	
3) Heis Exist an identity element e	
3) There can a said an inverte.	
4) + claunt their exim	
a all the four propuets dough winder	
Gall he I'm Clorefee ton a	

	Rigsau on Loperations	
	Rines are con 2 Oberations	
	Ing sould be provided in	
	If a group are chosed under t	
	Ond of is semigroup under 'X'	
	⇒ Ruy Semigoup	
	C.P.	
	=> Ruy Semigroup C.p. Fields: Closed under both identity	
	mo inverse	
-+ - >		
RT- (0)	Brine numbers hield 1. addition	
	/ addition	
	Z mul	
	We don't have Commutation noutrand	
	We don't have Commutation groups and all etc.	
	Shor's Algorithm.	
	Rings 'O'z'   Field'ds	
	1) Closure and and	
	a) A fisher	
	3) idendity does not exist ofered in	
	4) invesse ]	
	4) 1	
	cloud #	



mod 4.

x | 1 2 3

1 | 1 | 2 3

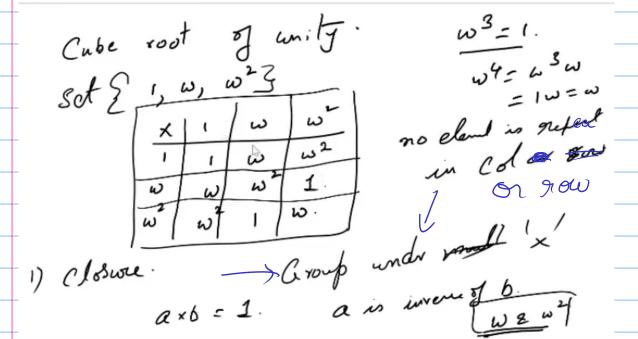
Only prime numbers

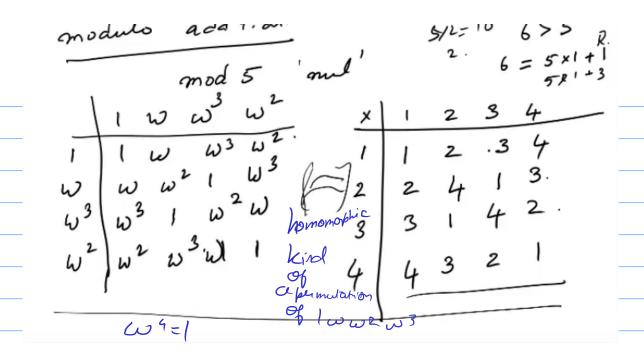
2 | 2 | 10 | 2

3 | 3 | 2 | 1

winder mod

mul





modulo add t. on 
$$\frac{matrices}{1}$$
 $e \left[ \begin{array}{c} 1 \\ 1 \\ 1 \end{array} \right]$ 
 $u = \left[ \begin{array}{c} 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right]$ 
 $u = \left[ \begin{array}{c} 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right]$ 
 $u = \left[ \begin{array}{c} 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right]$ 
 $u = \left[ \begin{array}{c} 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right]$ 
 $u = \left[ \begin{array}{c} 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right]$ 
 $u = \left[ \begin{array}{c} 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right]$ 
 $u = \left[ \begin{array}{c} 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right]$ 
 $u = \left[ \begin{array}{c} 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right]$ 
 $u = \left[ \begin{array}{c} 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right]$ 
 $u = \left[ \begin{array}{c} 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right]$ 
 $u = \left[ \begin{array}{c} 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right]$ 
 $u = \left[ \begin{array}{c} 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right]$ 
 $u = \left[ \begin{array}{c} 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right]$ 
 $u = \left[ \begin{array}{c} 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right]$ 
 $u = \left[ \begin{array}{c} 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right]$ 
 $u = \left[ \begin{array}{c} 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right]$ 
 $u = \left[ \begin{array}{c} 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right]$ 

Q= 9.6+97

n =amod b

879642. 8x10+1x6+9x10+6x10+4x10+2x10°=879642. Polynomial 8tr. 8x5+7x4+9x3+6x2+4x+2x°

querils &

cuite it is the form of the polynomial order of the field: # elements in field p: p-1 (for mod p)  $\alpha = \beta_1 k_1 p_2 k_3$   $Q^{b-1} = 1 \pmod{p}$ Enchid Q= a1b+n1 a, = a2 6 to 12 a2= a363+373 an = an-1 bn if and then its forine ab-1 = 1 mod p modulo add t. on. 5/1=10 6>5

11 14 . 2. 6=5x1+1

7x1+3 6 7 8 9 6 1 2 3 4 7 2 4 1 3 8 3 1 4 2 9 4 3 2 1 7 Ire beat