Shor's Algo

Two → Alice ⟷ Bob

Msg: Encode & Decode

Charlie

Quantum state cannot be copied, Charlie will have to make a measurement.

A ⟷ B

key → 0

$a \times b =$ [E] → public key

↳ private

Group Theory

Set.

$\{a, b, c, d\}$

'*', '÷', 'o' → operation (+, −, ×, −÷, mod +, mod ÷, $\frac{d}{dx}$ etc)

(1) $a * b = c$ $\quad a, b \in G$ then $c \in G$

↳ composition Closure

(2) $a * (b * c) = (a * b) * c$

(3) $a * e = e * a = a$

(4) $a * b = b * a = e$

2) $a * (b * c) = (a * b) * c$. associative.

3) there Exist an identity element 'e'

$a * e = e * a = a$.

4) $\forall$ element there exist an inverse.

$a * b = b * a = e$.

G all the four properties a is closed under operation *

Rings: Groups are on 1 operation
Rings are on 2 operations

if a group G is closed under '+'
and G is semigroup under '×'
⇒ Ring

Fields: closed under both '+' and '×'

Semigroup
C.P.
identity
no inverse

R+-{0} Prime numbers field
% addition
% mul

We don't have Commutation groups and all etc.

Shor's Algorithm.

Groups '*'
1) Closure.
2) Associative
3) identity
4) inverse.

Closed *

Rings '⊙' '*'
1) closed under ⊙
2) Semigroup.
inverse.
does not exist

Field '⊙' '*'
closed under both operations.

modulo addition

mod 5 'add'

⊕	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\{0, 1, 2, 3, 4\}$

$5/2 = 10$ (2)

$6 > 5$

$6 = 5 \times 1 + 1$ (R)

$5 \times 1 = 3$

x	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

mod 4 is not a Group under multiplication

x	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

only prime numbers form groups under mod mul

Cube root of unity.

$w^3 = 1$.

$w^4 = w^3 w = 1w = w$

set $\{1, w, w^2\}$

x	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

no element is repeated in col or row

1) Closure → Group under 'x'

$a \times b = 1$. a is inverse of b.

w & w^2

modulo addition

mod 5 'mul'

	1	w	w^3	w^2
1	1	w	w^3	w^2
w	w	w^2	1	w^3
w^3	w^3	1	w^2	w
w^2	w^2	w^3	w	1

$w^4 = 1$

x	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

homomorphic kind of a permutation of $1\ w\ w^2\ w^3$

$5/2 = 10$ (2)

$6 > 5$

$6 = 5 \times 1 + 1$ (R.)

$5 \times 1 + 3$

modulo addition

matrices.

$e = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix}$

$w = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

$w^2 = \begin{bmatrix} & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & \end{bmatrix}$

$w^3 = \begin{bmatrix} & 1 & & \\ & & 1 & \\ & & & 1 \\ 1 & & & \end{bmatrix}$

	1	w^3	w^2	w
1	1	w^3	w^2	w
w	w	1	w^3	w^2
w^2	w^2	w	1	w^3
w^3	w^3	w^2	w	1

Representation in matrices

qubits ?

$a = q \cdot b + r$

$r = a \bmod b$

87964_2

$8 \times 10^4 + 7 \times 10^3 + 9 \times 10^2 + 6 \times 10^1 + 4 \times 10^0 + 2 \times 10^0 = 87964_2$

Polynomial str.

$8x^5 + 7x^4 + 9x^3 + 6x^2 + 4x + 2x^0$

10^{200} $\times 10^{200}$

write it in the form of the polynomial

order of the field: # elements in field

$p : p-1$ (for mod p)

$a = p_1^{k_1} p_2^{k_2} p_3^{k_3}$ $\quad a^{p-1} \equiv 1 \pmod p$

Euclid Algo

$a_0 = a_1 b + r_1$

$a_1 = a_2 b + r_2$

$a_2 = a_3 b 3 + r_3$

$\vdots$

$a_n = a_{n-1} b_n$ if $a_n = 1$ then it's prime

$\boxed{a^{p-1} \equiv 1 \mod p}$

modulo addition

	6	7	8	9
6	1	2	3	4
7	2	4	1	3
8	3	1	4	2
9	4	3	2	1

$5/2 = 10$ $\quad 6 > 5$

$6 = 5 \times 1 + 1$

$5 \times 1 + 3$

x	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

repeat