Fermat's Little Theorem.

Properties of Modular

1) $(a+b) \% M = \left(\underbrace{a \% M}_{[0, M-1]} + \underbrace{b \% M}_{[0, M-1]} \right) \% M$ $\quad [0, 2M-2]$

$a = 12$
$b = 8$

$(x \% M = [0, M-1])$

$(12+8) \% 7 = (12 \% 7 + 8 \% 7) \% 7$

$20 \% 7$

$= 6 = (5+1) \% 7 = 6 \% 7$

$= 6$

2) $(a \times b) \% M = ((a \% M) \times (b \% M)) \% M$

3) $(a-b) \% M = (a \% M - b \% M + M) \% M$

$[0, M-1] \quad [0, M-1]$

$x - y$

$[-(M-1), (M-1)]$

> $M \% M = 0$

Let, $A \,\%\, M = x$

then, $(A+M) \,\%\, M = (A \,\%\, M + M \,\%\, M) \,\%\, M$

$= (A \,\%\, M)$

$\Downarrow$

$[0, M-1]$

+s $2 \,\%\, 5 = 2$

+s $7 \,\%\, 5 = 2$

+s $12 \,\%\, 5 = 2$

+s $17 \,\%\, 5 = 2$

$\vdots$

$$A \,\%\, M = (A + xM) \,\%\, M$$

xM ↓ natural no.

4) $\left(\frac{a}{b}\right) \,\%\, M = \left(\frac{(a \,\%\, M)}{(b \,\%\, M)}\right) \,\%\, M.$

fractional no's, mod is not defined.

$$\left(\frac{a}{b}\right) \,\%\, M = (a \,\%\, M \times b^{-1} \,\%\, M) \,\%\, M$$

b^{-1} ↓ inverse mod of b w.r.t. M

(Only possible if $\gcd(b, m) = 1$)

$5 \Rightarrow (5)^{-1} = \frac{1}{5}$ — Multiplicative inverse.

$5 \times \frac{1}{5} = 1 \Rightarrow$ Multiplicative inverse.

Inverse mod of b wrt M

$(b^{-1} \,\%\, M) = x \Rightarrow$ +ve Integer

$(b \times x) \,\%\, M = 1$

$b = 5, \quad M = 7$

$5^{-1} \,\%\, 7 = x \quad (x = 3)$

$(5 \times x) \,\%\, 7 = 1$

$x = 1 \Rightarrow (5 \times 1) \,\%\, 7 = 5$ ✗

$x = 2 \Rightarrow (5 \times 2) \,\%\, 7 = 10 \,\%\, 7 = 3$ ✗

$x = 3 \Rightarrow (5 \times 3) \,\%\, 7 = 15 \,\%\, 7 = 1$ ✓

★ One answer of $(5^{-1} \,\%\, M)$ will be always found in the range $[1, m-1]$

given that gcd (5, m) = 1

Q Given two co-prime integers 5, m. And the value of $(5^{-1} \% m)$

Sol^n 1) Brute force

Iterate from i = 1 to m-1 & check if $((5 \times i) \% m == 1)$ then i is the ans,

break

T.C. = O(m)

2) Fermat's theorem

1) gcd (5, m) = 1
2) m should be prime

$$a^{M-1} \% M = 1 \% M$$

multiply a^{-1} on both sides

$$a^{M-2} \% M = a^{-1} \% M$$

log m

Question

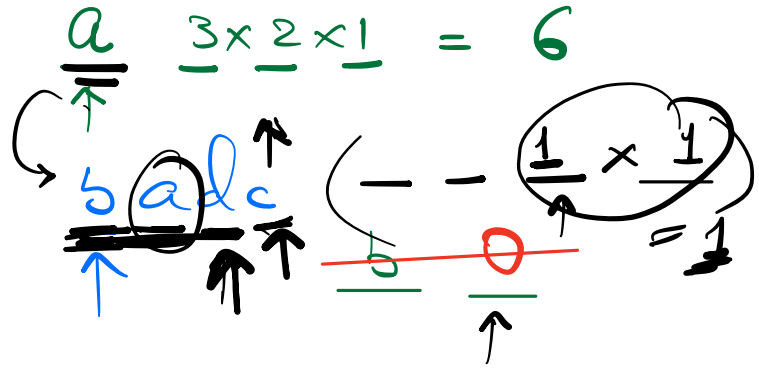
$a^{10} = a^5 \times a^5$

1) abcd
2) abdc
3) acbd
4) acdb
5) adbc
6) adcb

6

7) bacd
8) badc

⇒



cbad

a/b

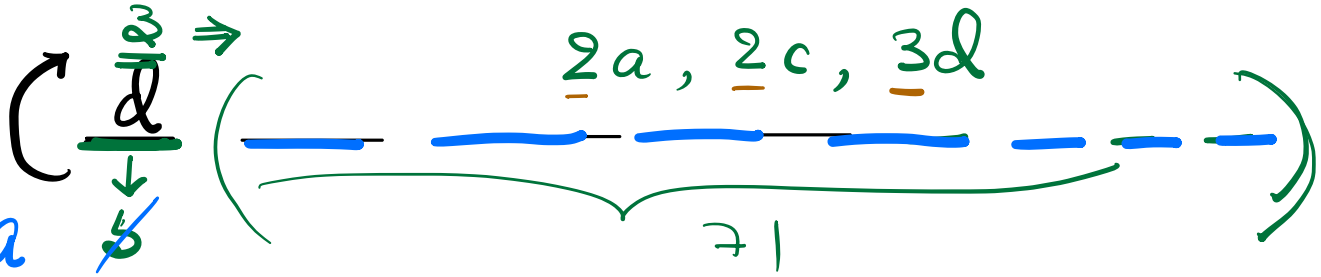
cbad

aabccddd

(a, b, c)

cabd
cadb

ba c d (1)



Permutations with repeat

(1a, 1b, 2c, 3d)

$\frac{7!}{(1!)(1!)(2!)(3!)}$

$\frac{7!}{(1!)(1!)(2!)\times 5!}$

a b a a

a_1 b a_2 a_3

$4! = 4 \times 3 \times 2 = 24$

a_1 b a_2 a_3
a_1 b a_3 a_2
a_1 a_2 b a_3
a_1 a_2 a_3 b
a_1 a_3 b a_2
a_1 a_3 a_2 b

a_2 b a_1 a_3
a_2 b a_3 a_1
a_2 a_1 b a_3
a_2 a_1 a_3 b
a_2 a_3 b a_1
a_2 a_3 a_1 b

a_1 b a_2 a_3
a_1 b a_3 a_2
a_1 a_2 b a_3
a_1 a_2 a_3 b
a_1 a_3 b a_2
a_1 a_3 a_2 b

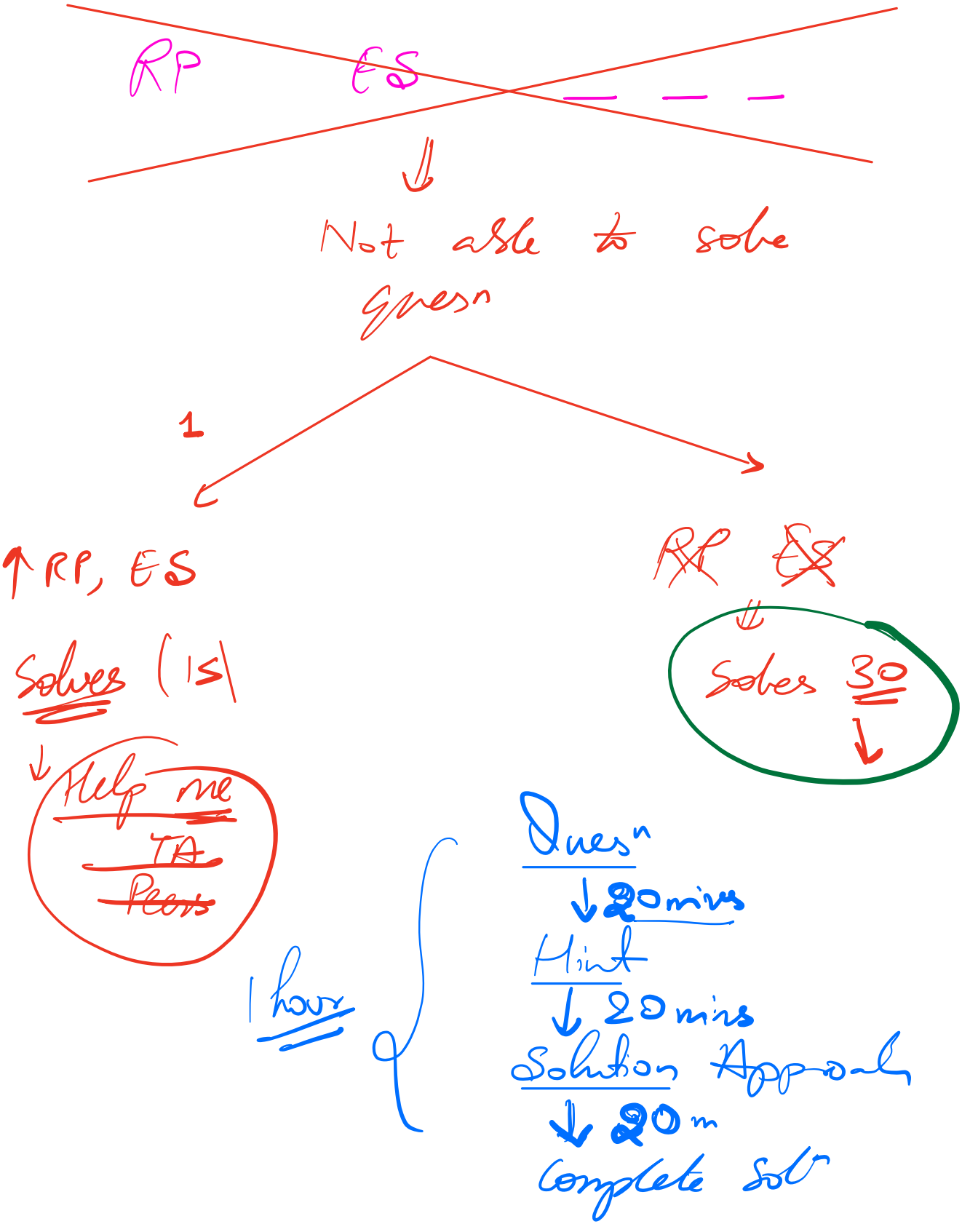
a_1 b a_2 a_3
a_1 b a_3 a_2
a_1 a_2 b a_3
a_1 a_2 a_3 b
a_1 a_3 b a_2
a_1 a_3 a_2 b

(freq)!

Array ⇒ $C_1 \Rightarrow \gamma_1$, $C_2 \Rightarrow \gamma_2$, $C_3 \Rightarrow \gamma_3$, ⋮

Total size = N

$$\frac{N!}{(\gamma_1)! \times (\gamma_2)! \times (\gamma_3)! \ldots}$$



A[] ⇒ B

return the no. of pairs in A

whose sum is divisible by m.

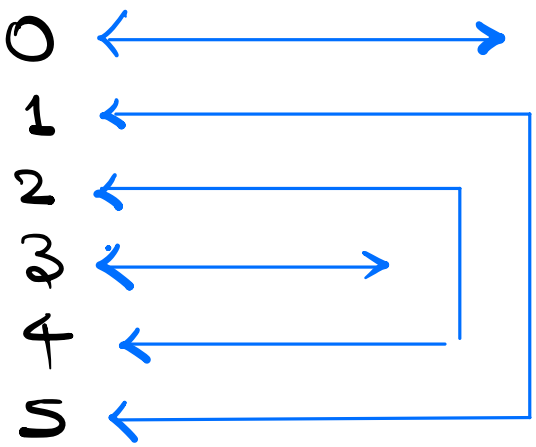
A = [11, 7, 23, 13, 12, 9, 15, 21]

B = 6

$x \,\%\, B = [0, 5]$ (0, B-1)

$(A[i] + A[j]) \,\%\, B == 0$

$((A[i] \,\%\, B) + (A[j] \,\%\, B)) \,\%\, B == 0$



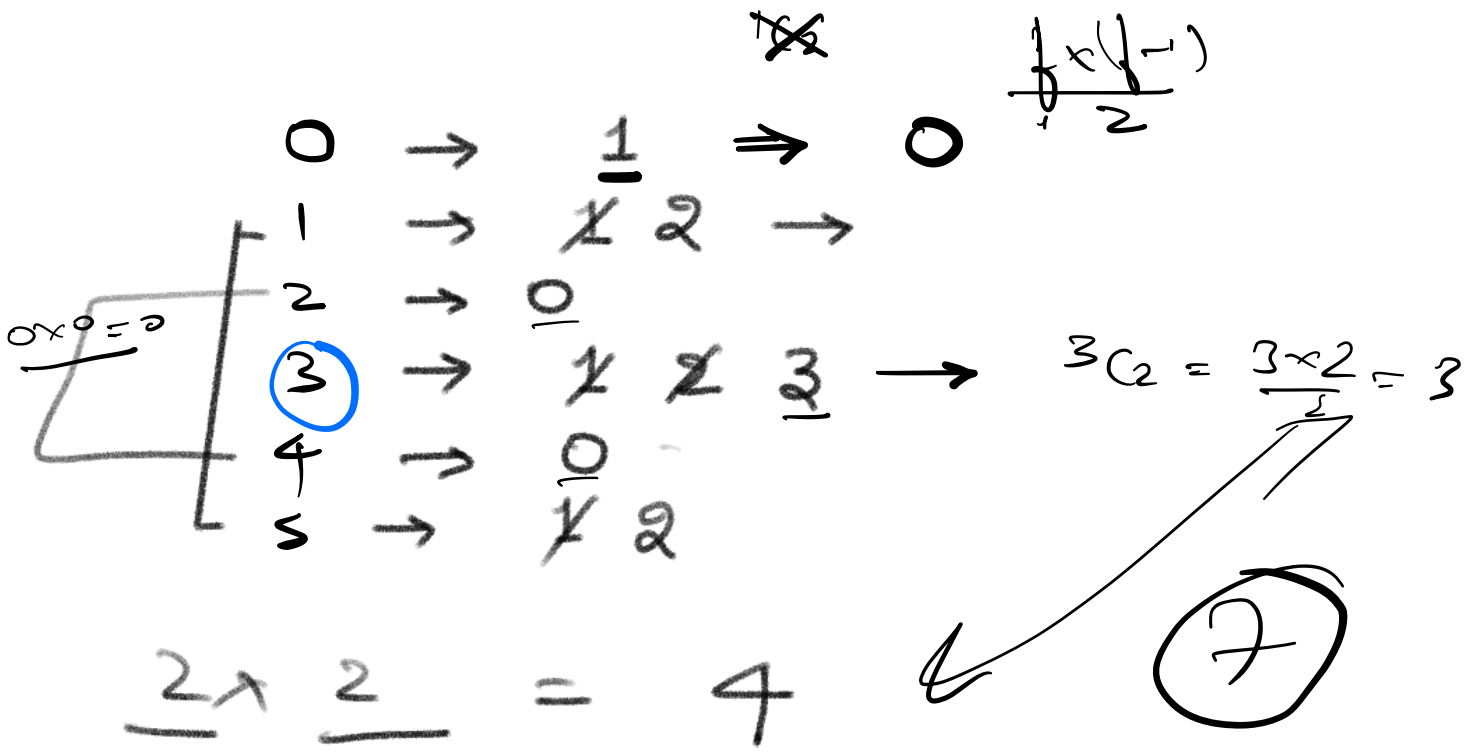
$\frac{A[i]+A[j]}{6}$

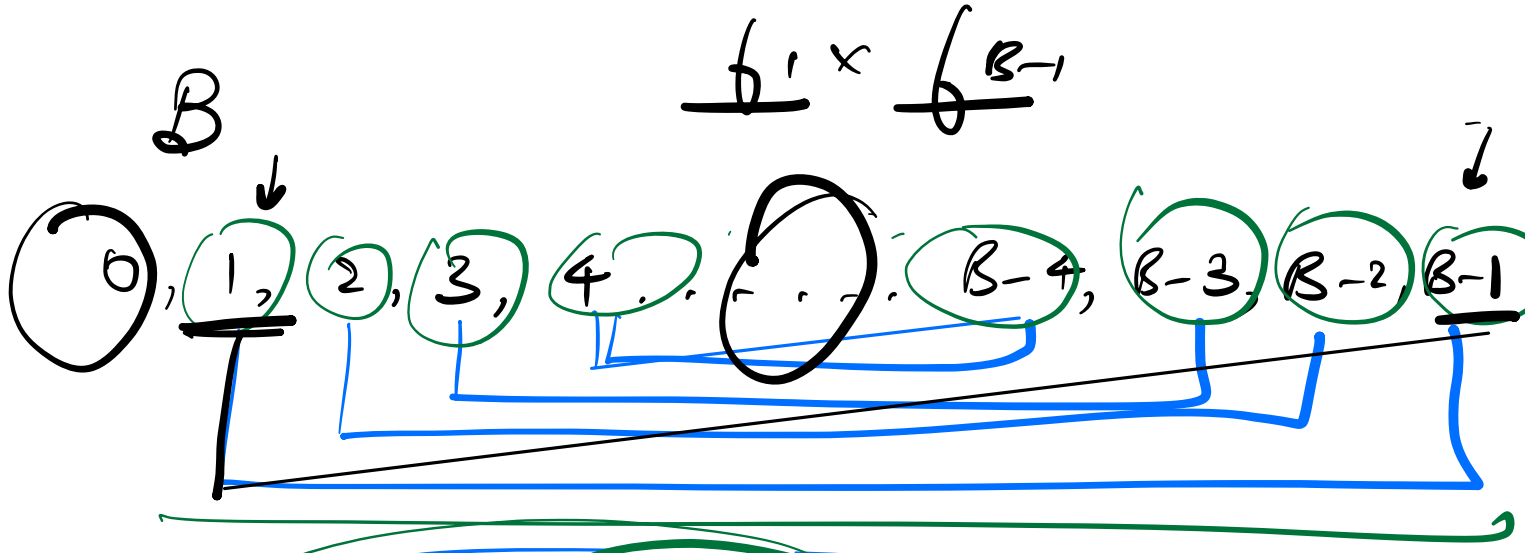
$A[i] \,\%\, 6 = (6)(y) + r_1$

$A[j] \,\%\, 6 = (6)(j) + r_2$

$\frac{(r_1+r_2)}{6}$

A- [11, 7, 23, 13, 19, 9, 15, 21]

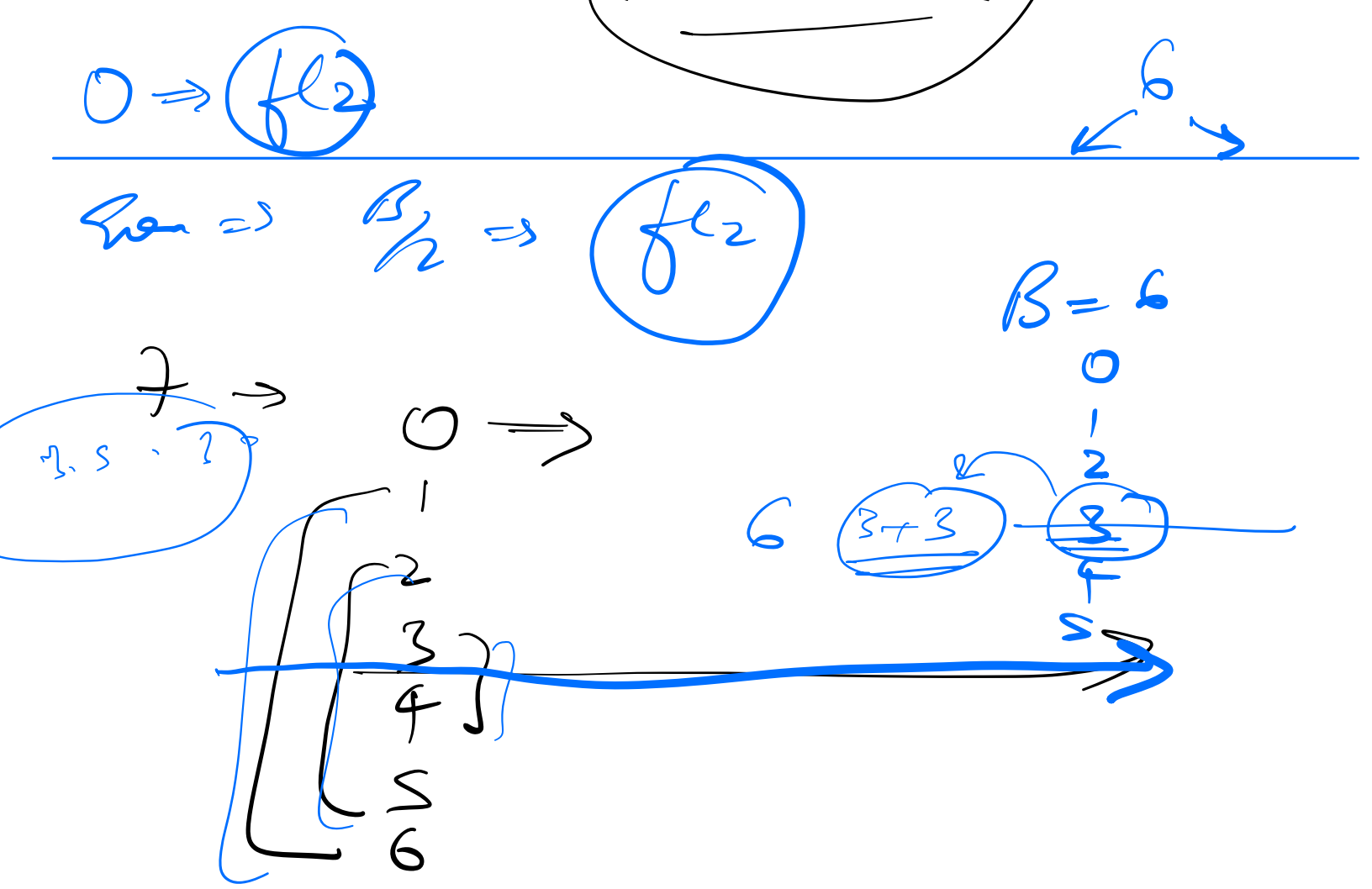




B is an even

B/2 ⇒ (f) (f-1) / 2

0 ⇒ (f) (f-1) / 2



Tuesday 9:00PM ??

1) Kth Symbol
2) A^B!
3) Reorange array
4) Compute nCr % M ⇒ Recursion

$n(r \pm M = \left(\binom{n-1}{r-1} \times m + \binom{n-1}{r} \times 1 \right) \times m$

5) Excel Colum Title

6) Distance b/w 2 adjacent 1 in a BE of an integer