

Fermat's Little Theorem.

Properties of Modular

$$1) (a+b) \% M = \left(\begin{array}{c} \text{[0, 2M-2]} \\ a \% M + b \% M \\ \downarrow \quad \downarrow \\ \text{[0, M-1]} \quad \text{[0, M-1]} \end{array} \right) \% \underline{M}$$

$$a = 12 \quad \left(\begin{array}{c} x \% M = \text{[0, M-1]} \end{array} \right)$$

$$b = 8$$

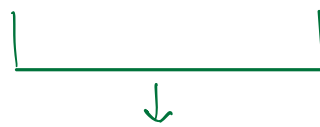
$$(12+8) \% 7 = (12 \% 7 + 8 \% 7) \% 7$$

$$\begin{array}{l} 20 \% 7 \\ = 6 \end{array} = \begin{array}{l} (5+1) \% 7 \\ = 6 \end{array} = 6 \% 7$$

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

$$3) (a-b) \% M = \left(\begin{array}{c} \underline{a \% M} - b \% M + M \\ \downarrow \quad \downarrow \\ \text{[0, M-1]} \quad \text{[0, M-1]} \end{array} \right) \% M$$

$x - y$



$$\text{[-(M-1), (M-1)]}$$

$$\triangleright M \% M = 0$$

$$\Downarrow$$

Let, $A \cdot \text{inv} M = x$

then, $(A + M) \cdot \text{inv} M = (A \cdot \text{inv} M + M \cdot \overset{0}{\text{inv} M}) \cdot \text{inv} M$

$$\begin{array}{l}
 +s \left(\begin{array}{l} 2 \cdot \text{inv} 5 = 2 \\ 7 \cdot \text{inv} 5 = 2 \\ 12 \cdot \text{inv} 5 = 2 \\ 17 \cdot \text{inv} 5 = 2 \\ \vdots \end{array} \right. \\
 \end{array}
 \qquad
 = \frac{(A \cdot \text{inv} M)}{\Downarrow}$$

$[0, M-1]$

$$A \cdot \text{inv} M = (A + \underset{\substack{\downarrow \\ \text{multiplier} \\ \text{no.}}}{xM}) \cdot \text{inv} M$$

~~$$4) \left(\frac{a}{b} \right) \cdot \text{inv} M = \left(\frac{(a \cdot \text{inv} M)}{(b \cdot \text{inv} M)} \right) \cdot \text{inv} M.$$~~

Fractional no's, mod is not defined.

$$\left(\frac{a}{b} \right) \cdot \text{inv} M = (a \cdot \text{inv} M \times \text{inv mod of } b \text{ w.r.t. } M) \cdot \text{inv} M$$

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

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

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

Inverse mod of b
wrt M

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

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

$$b = 5, \quad m = 7$$

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

$$(\underline{5 \times x}) \% 7 = 1$$

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

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

$$x = 3 \Rightarrow (5 \times 3) \% 7 = 15 \% 7 = 1 \quad \checkmark$$

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

given that $\gcd(b, m) = 1$

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

Solⁿ 1) Brute force

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

T.C. = $O(m)$

2) Fermat's Theorem

1) $\gcd(b, m) = 1$

2) M should be prime

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

multiply a^{-1} on both sides

log m

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

Question

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

- 1) a b c d
- 2) a b d c
- 3) a c b d
- 4) a c d b
- 5) a d b c
- 6) a d c b
- 7) b a c d
- 8) b a d c

6

$$\frac{a}{b} \quad \frac{3 \times 2 \times 1}{1} = 6$$

Diagram showing a sequence of operations: $\frac{a}{b}$, $\frac{1}{1} \times \frac{1}{1} = 1$, and a sequence of numbers 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100.

c b a d

a/b
c b a d

a a b c c d d d

(a, b, c)

c a b d
c a d b

b a c d (1)

$$\frac{3}{1} \Rightarrow \frac{2a, 2c, 3d}{7!}$$

Permutations with repeat

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

7!

(2!) (2!) (3!)

(7!) (1!) (1!) (2!) (3!)

$a_1 b a_2 a_3$

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

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

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

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

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

(freq)!

Array \Rightarrow
 ↓
 Total size
 $= N$

$C_1 \Rightarrow r_1$
 $C_2 \Rightarrow r_2$
 $C_3 \Rightarrow r_3$
 \vdots

$$\frac{N!}{(r_1)! \times (r_2)! \times (r_3)! \times \dots}$$

RP

ES



Not able to solve
quesn

1

↑ RP, ES

Solves (15)

↓
Help me
TA
Peers

1 hour

~~RP~~ ~~ES~~

↓
Solves 30
↓

Quesn

↓ 20 mins

Hint

↓ 20 mins

Solution Approach

↓ 20 m

Complete soln

A[] ⇒ B

return the no. of pairs in A

where sum is divisible by m .

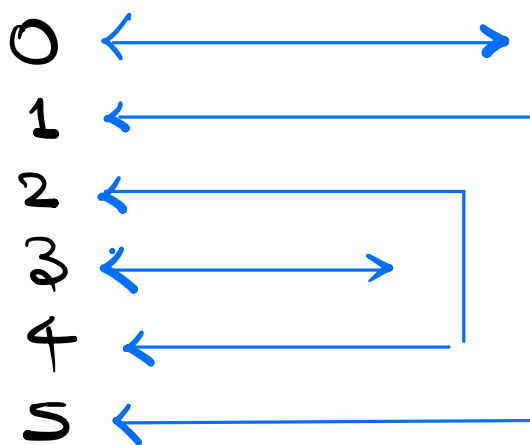
$$A = [11, 7, 23, 13, 12, 9, 15, 21]$$

$$B = 6$$

$$x \cdot \frac{1}{B} = \frac{0, B-1}{(c)}$$

$$(A[i] + A[j]) \cdot \frac{1}{B} = 0$$

$$\left((A[i] \cdot B) + (A[j] \cdot B) \right) \cdot \frac{1}{B} = 0$$



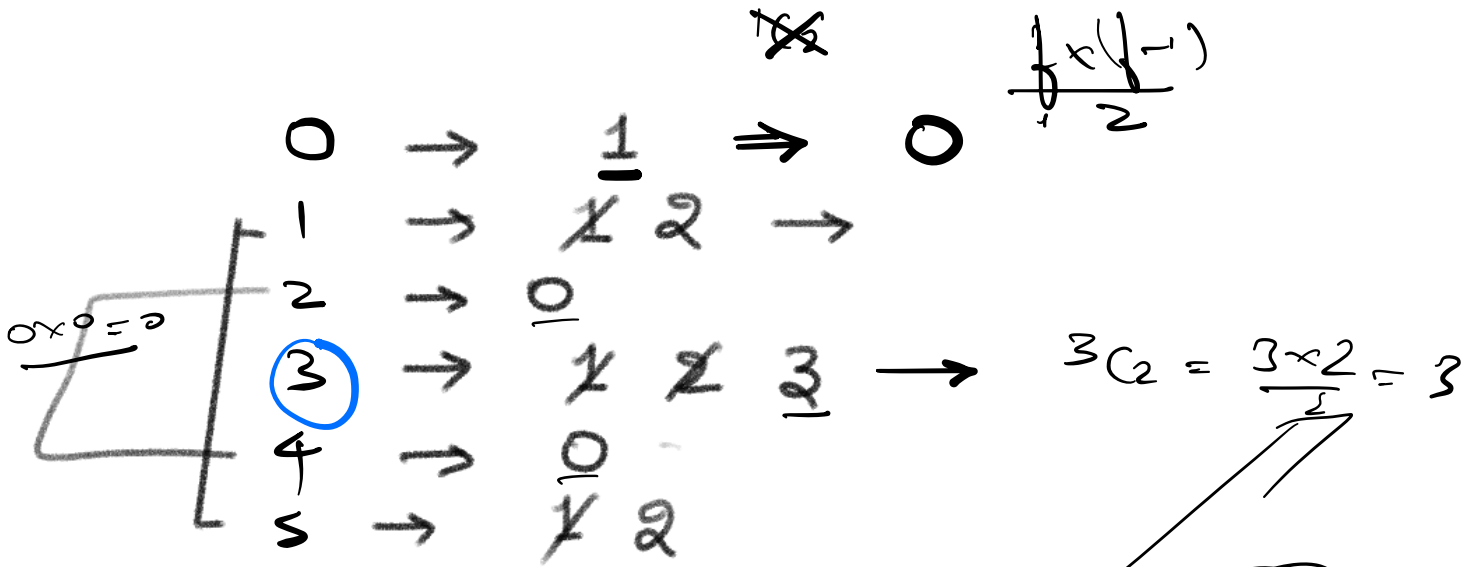
$$\frac{A[i] + A[j]}{6}$$

$$A[i] \cdot \frac{1}{6} = (6)(7) + r_1$$

$$A[j] \cdot \frac{1}{6} = (6)(3) + r_2$$

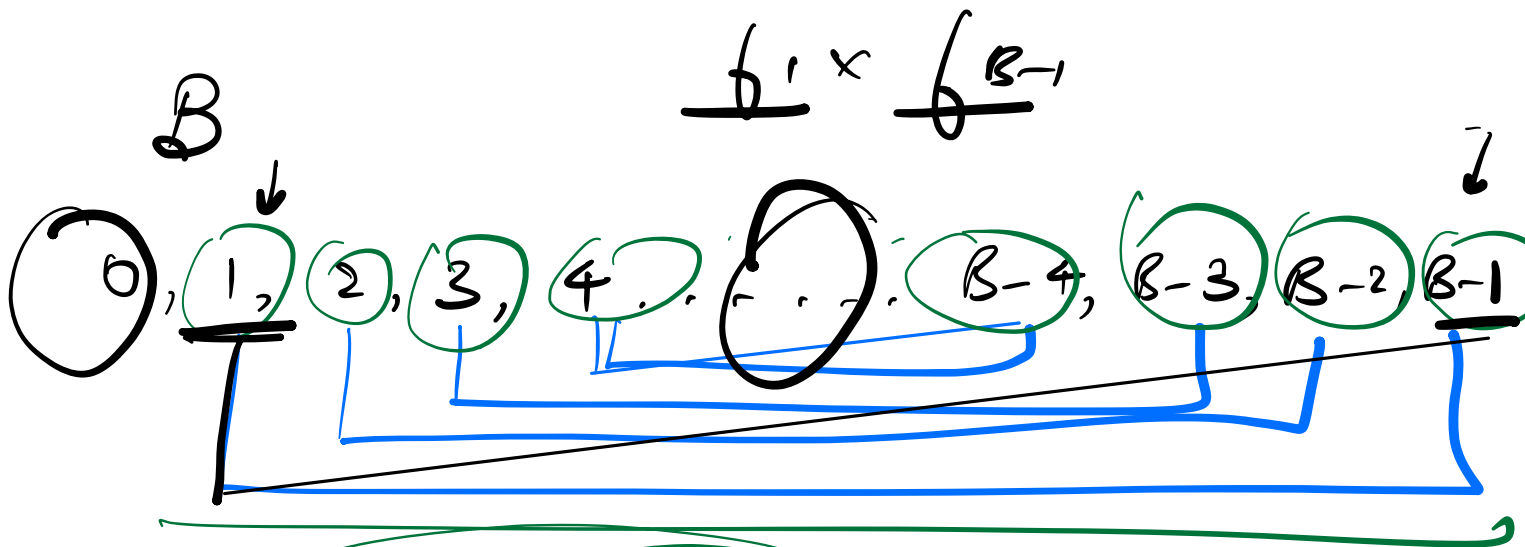
$$\frac{(r_1 + r_2)}{6}$$

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



2 \times 2 = 4

7



B is an even

$\frac{B}{2} \Rightarrow \frac{f(f-1)}{2}$

✓ 0 ⇒ $\frac{f(f-1)}{2}$

$$0 \Rightarrow \textcircled{fl_2}$$



$$\text{then} \Rightarrow B/2 \Rightarrow \textcircled{fl_2}$$

$$7 \Rightarrow \textcircled{1, 5, 2}$$

$$0 \Rightarrow \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{matrix}$$

$$B = 6$$

$$\begin{matrix} 0 \\ 1 \\ 2 \\ 3 \end{matrix}$$

Diagram showing a sequence of operations: $3+3$ (circled) and 3 (circled) with arrows indicating a flow. A large blue arrow points from the list of numbers to the right.

Tuesday 9:00 PM ??



- 1) K^{th} Symbol
- 2) $A^{\wedge B}!$
- 3) Rearrange array
- 4) Compute $\underline{n(x \% M)} \Rightarrow \underline{\underline{Remainder}}$

↓

$$n(r)M = \binom{n-1}{r-1} x_m + \binom{n-1}{r} x_{n-1} \Big)_{1 \leq m}$$

5) Encl column File

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