

A  $\div$  B  $\Rightarrow$  Remainder left after dividing A by B

$$\begin{array}{r} 2 \rightarrow \text{Quotient} \\ 5 \overline{)14} \rightarrow \text{Dividend} \\ -10 \\ \hline \text{Divisor} \quad 4 \rightarrow \text{Remainder} \end{array}$$

$$\text{Dividend} = (\text{Divisor} \times \text{Quotient}) + \text{Remainder}$$

$$\text{Remainder} = \text{Dividend} - \text{Divisor} \times \text{Quotient}$$

$\Rightarrow$  largest multiple of divisor  $\leq$  dividend

Division is repeated subtraction

$$14 \div 5 = 14 - 5 = 9 - 5 = 4$$

↓  
2

< divisor

$$\begin{array}{r} 5 \times 2 = 10 \\ 5 \times 3 = 15 > 14 \times \end{array}$$

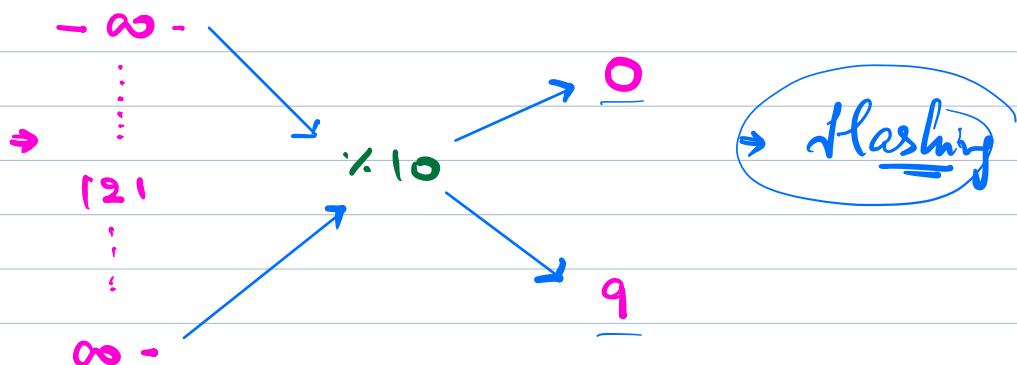
$$\begin{array}{rcl} 40 \div 6 & = & 40 - 6 \\ & & \checkmark \\ & & 34 - 6 \\ & & \checkmark \\ & & 28 - 6 \\ & & \checkmark \\ & & 22 - 6 \\ & & \checkmark \\ & & 16 - 6 \\ & & \checkmark \\ & & 10 - 6 \\ & & \checkmark \end{array}$$

$$\underline{\underline{4}} \Rightarrow$$

$$(5), 6 - 6 = \underline{\underline{0}}$$

$$\underline{\underline{40}} - \underline{\underline{(6 \times 6)}} = \underline{\underline{4}}$$

$$a \% \underline{\underline{m}} = [0, m-1]$$



$$\underline{\underline{0}} \quad -40 \% 7 \Rightarrow [0, 6]$$

$$-40 - ((7) \times \underline{\underline{\_}})$$

$$7 \Rightarrow 7, 14, 21, 28, 35 \dots \times (+ve)$$

$$7 \Rightarrow -7, -14, -21, -28, -35, \underline{\underline{-42}}, -49 \dots$$

$$\text{Ans} = -40 - (-42) = \underline{\underline{2}}$$

$$-\left(\frac{40}{\underline{-}} \cdot \frac{1}{\underline{7}}\right) = \left(-\frac{5}{\underline{-}} + \frac{3}{\underline{7}}\right) \cdot \frac{1}{\underline{7}}$$

[ $\frac{-}{\underline{-}}, \frac{0}{\underline{0}}$ ]
[ $\frac{\pm}{\underline{\pm}}, \frac{M}{\underline{M}}$ ]

$$2 \cdot \frac{1}{\underline{7}} = \frac{2}{\underline{1}}$$

## Modular Arithmetic $[0, \underline{M-1}]$

$$\textcircled{1} \quad \frac{(a+b)}{\underline{-}} \cdot \underline{M} = \left( \frac{a \cdot \underline{M}}{\underline{\downarrow}} + \frac{b \cdot \underline{M}}{\underline{\downarrow}} \right) \cdot \underline{M}$$

$[0, \underline{M-1}] \quad [0, \underline{M-1}]$

$$\begin{aligned}
 a &= 4, \quad b = 5, \quad M = 6 \\
 (4+5) \cdot 6 &= (4 \cdot 6 + 5 \cdot 6) \cdot \underline{6} \\
 &= 9 \cdot 1 \cdot 6 \\
 &= 3
 \end{aligned}
 \quad \left| \begin{array}{l} (\underline{4 \cdot 6} + \underline{5 \cdot 6}) \cdot \underline{6} \\ (\underline{4} + \underline{5}) \cdot \underline{6} \\ = \textcircled{9} \cdot \underline{1} \cdot \underline{6} \\ = 3 \end{array} \right.$$

$$\begin{aligned}
 \textcircled{2} \quad a \cdot \underline{M} &= (a+M) \cdot \underline{M} \\
 &= (a \cdot \underline{M} + M \cdot \cancel{\underline{M}}^0) \cdot \underline{M} \\
 21 \cdot \underline{5} &= (a \cdot \underline{M}) \cdot \underline{M} \\
 \frac{1 \cdot \underline{5}}{\underline{0, \underline{4}}} &= \textcircled{a \cdot \underline{M}}
 \end{aligned}$$

]

11.

$$3) \underline{\underline{(a * b)}} \cdot M = (\underline{a \cdot M} * \underline{b \cdot M}) \cdot M$$

$$4) \underline{\underline{(a - b)}} \cdot M = (\underline{a \cdot M} - \underline{b \cdot M}) \cdot M$$

$$a = 8, b = 4, M = 5$$

$$\begin{aligned} & \text{LHS} \\ & (8 - 4) \cdot 5 \\ &= \frac{4 \cdot 5}{4} \\ &= \underline{\underline{1}} \end{aligned}$$

$$\begin{aligned} & (8 \cdot 5 - 4 \cdot 5) \cdot 5 \\ &= (8 - 4) \cdot 5 \\ &= \underline{\underline{-1 \cdot 5}} = \underline{\underline{-1}} \end{aligned}$$

C/C++ / Java / C# / JS

$$\frac{-1 \cdot 5}{-1} = \underline{\underline{-1}}$$

Python

$$-1 \cdot 5 = \underline{\underline{4}}$$

Ans

$$\underline{\underline{(a - b)}} \cdot M = \left( \underbrace{a \cdot M}_{\text{+ve}} - \underbrace{b \cdot M}_{\text{+ve}} + \underline{\underline{M}} \right) \cdot M$$

[ 0, M-1 ]

Q

Given A, B,  $\underline{(A > B)}$

Find M s.t.  $\underline{\underline{A \cdot M}} = \underline{\underline{B \cdot M}}$ .

$$A = 16$$

$$B = 4$$

$$16 \cdot M = 4 \cdot M$$

$$M = 2, 3, 4, 6, 12$$

Q1 Can  $M > A$  ???

$$M = 17$$

$$A \cdot M = A$$

$$B \cdot M = B$$

$$16 \cdot 17 = 16$$

$$4 \cdot 17 = 4$$

## 2) Brute force

$\forall i$  from 1 to  $A$  check if  $A \cdot i = \underline{\underline{B \cdot i}}$

2)  $A \cdot M = B \cdot M$

$$\underline{A \cdot M - B \cdot M} = 0$$

Add  $M$  on both sides

$$A \cdot M - B \cdot M + M = M$$

Take  $\cdot M$  on both sides

$$(A \cdot M - B \cdot M + M) \cdot M = M \cdot M^0$$

$$\underline{(A-B) \cdot M = 0}$$

$(A-B)$  is a multiple of  $M$

$M$  is a factor of  $\underline{(A-B)}$

$$A = 16, B = 4$$

$$A - B = \underline{\underline{12}}$$

All factors of  $\underline{(A-B)}$  are one

Q2 Given  $N$  array elements.

Calculate no. of pair  $(i, j)$  s.t.

$$(A[i] + A[j]) \cdot M = 0.$$

Note :  $i \neq j$  &  $(i, j) = (j, i)$

e.g.  $A: 4, 7, 6, 5, 5, 3, , M=3$

i            j

$$1 \quad 0 \quad 3 \quad \Rightarrow (4+5) \cdot 3 = 0$$

$$\begin{array}{cccc}
 2 & 0 & 4 & \Rightarrow 9 \cdot 1 \cdot 3 = 0 \\
 3 & 1 & 3 & \Rightarrow (7+5) \cdot 1 \cdot 3 = 0 \\
 4 & 1 & 4 & \Rightarrow (7+5) \cdot 1 \cdot 3 = 0 \\
 5 & 2 & 5 & \Rightarrow (6+3) \cdot 1 \cdot 3 = 0
 \end{array}$$

Anw = s

Solu

$$(A[ij] + A[ji]) \cdot M = 0$$

$$\left( \frac{A[ij] \cdot M}{\downarrow} + \frac{A[ji] \cdot M}{\downarrow} \right) \cdot M = 0$$

$x$        $y$

$[0, M-1]$        $[0, M-1]$

$$\left[ \frac{0, 2(M-1)}{0, M} \right] \cdot M = 0$$

$$M = 6$$

$$[0, 10] \Rightarrow 0, 6$$

$$0 \cdot 1 \cdot 6 = 0, \quad 6 \cdot 1 \cdot 6 = 0$$

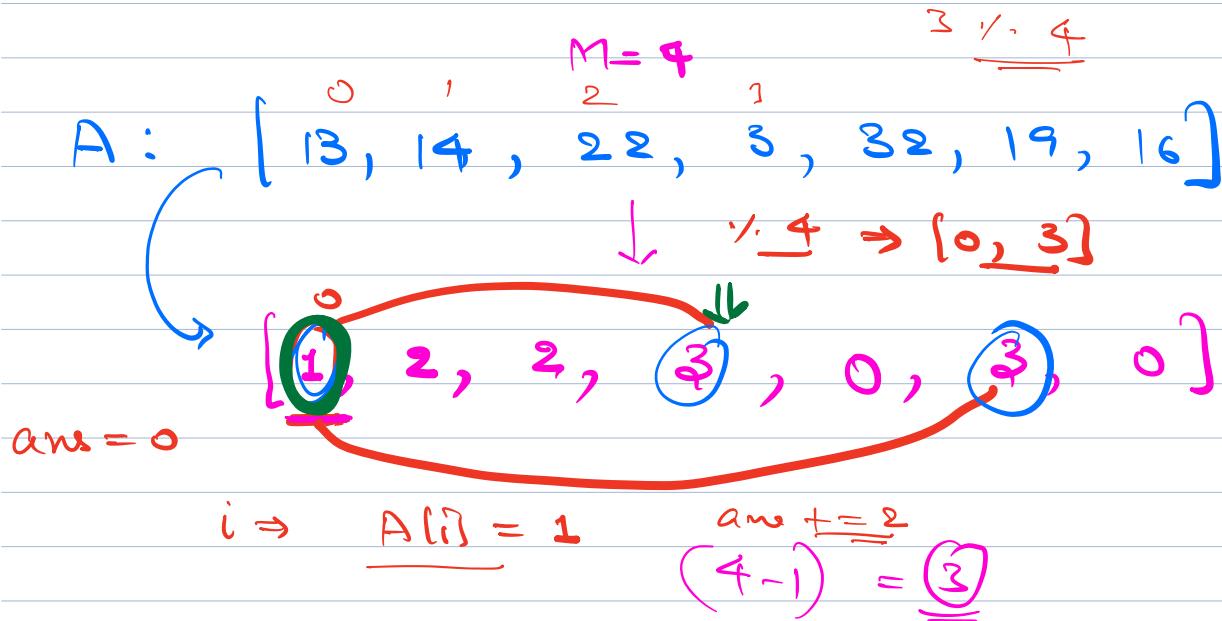
pairs s.t.

$$x + y = 0$$

or

$$x + y = M$$

Step 1  $\Rightarrow \forall i \quad A[i] = A[i] \cdot i \cdot M$



freq of 3 was important

Create a freq array

$A : [ ] \Rightarrow A[i] \cdot M \Rightarrow [0, \frac{M-1}{\downarrow}]$

Array of size  $M$

$i \Rightarrow A[i] \cdot M = i \quad (S+IS) \cdot 10$

$A = \{29, 11, 21, 17, 2, 5, 4, 6, 23, 13, 26, 14, 18, 15\}$

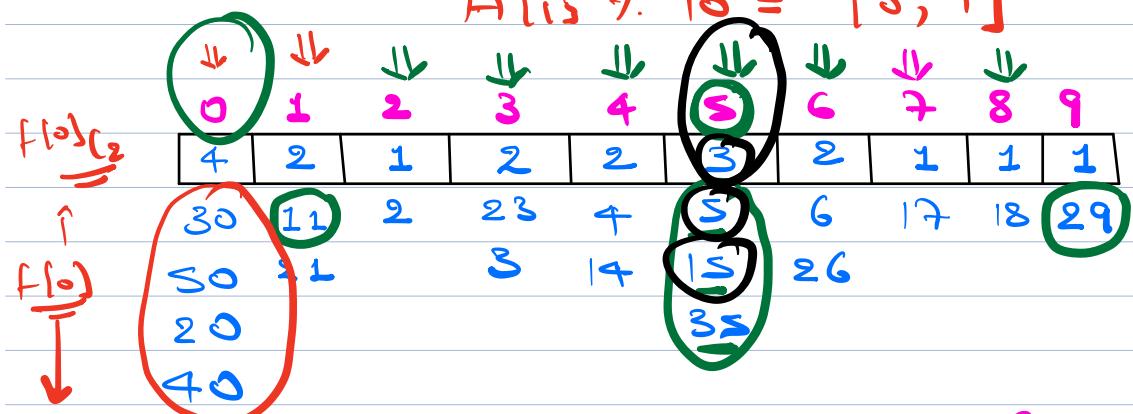
$\underline{30}, \underline{35}, \underline{50}, \underline{20}, \underline{40}\}$

$$S + S = 10$$

$$\underline{\underline{M = 10}}$$

$$\begin{array}{l} M=9 \\ M=11 \end{array}$$

$$A[13 \times 10] = [0, 9]$$



$$S \cdot C = O(M)$$

$$2 \times 1 \quad (\text{Count } 1) \times (\text{Count } 9)$$

$$1 \times 1 \quad (\text{Count } 2) \times (\text{Count } 8) \quad i \Rightarrow \underline{m-i}$$

$$2 \times 2 \quad (\text{Count } 3) \times (\text{Count } 7)$$

$$2 \times 2 \quad (\text{Count } 4) \times (\text{Count } 6)$$

$$(\text{Count } 5) + (\text{Count } 5) C_2$$

$$N_{C_2} = \frac{(N)(N-1)}{2}$$

$$\frac{(\text{Count } 5) \times (\text{Count } 5 - 1)}{2} = 10$$

+

$$(\text{Count } 0) C_2$$

$$\left( \begin{array}{l} M=9 \\ \hline \hline 11 \end{array} \right)$$

## Code

Even

Time to create freq array =  $O(N)$

f  $\Rightarrow$  freq array // M

ans = 0 ;

$f[0] = 0$

$$\underline{\underline{\text{ans}}} + \underline{\underline{=}} \frac{f[0] \times (f[0] - 1)}{2} // \underline{\underline{0}}$$

i = 1 ; j = M-1 ;

$\Rightarrow$  while ( $i < j$ )  $\leftarrow$  (M)

$$\text{ans} + = f[i] \times f[j] ;$$

i++;  
j--;  
b

if ( $M - 1 \cdot 2 = 0$ )  $\leftarrow$

$$\text{ans} + = \frac{f[M/2] \times (f[M/2] - 1)}{2}$$

b

return ans;

$$T.C. = O(N + M)$$

$$S.C. = O(\underline{M})$$

11: 13

$$\cancel{4 \cdot \cancel{-3}} \Rightarrow \text{Not defined}$$

$$4) \frac{\underline{a/b}}{\underline{\underline{M}}} \cdot \underline{M} = \left( \frac{\underline{\underline{(a \cdot \underline{M})}}}{\underline{\underline{b \cdot \underline{M}}}} \right) \cdot \underline{M} \quad \times$$

$$a = 16, b = 4$$

$$M = s$$

$$(16/4) \cdot s$$

$$(4 \cdot s) = \underline{\underline{4}}$$

$$\left( \frac{(16 \cdot s)}{(4 \cdot s)} \right) \cdot s$$

$$= \left( \frac{4}{4} \right) \cdot s$$

$$= (0) \cdot s = \underline{\underline{0}}$$

$$(a/b) \cdot M = (a \times b^{-1}) \cdot M$$

$$= ((a \cdot M) \times \underbrace{(b^{-1} \cdot M)}_{\downarrow}) \cdot M$$

Inverse mod of b  
w.r.t M

O

1 1 1

# Inverse Mod

Given  $b, M$

two integers  $a$  and  $b$  are coprime, relatively prime or mutually prime if the only positive integer that is a divisor of both of them is 1.

$b^{-1} \cdot M$  exists only if  $\text{gcd}(b, M) = 1$   
 $b \not\equiv m$  are  
co-prime.

$$b = \frac{2}{1}, M = \frac{5}{1} \quad \checkmark$$

$$\textcircled{1}, 2 \quad \textcircled{1} \leftarrow$$

$$b = \frac{32}{1} \quad M = \frac{9}{1} \quad \checkmark$$

$$\textcircled{1}, 2, 4, 8, 16, 32 \quad \textcircled{1}, 3, 9$$

$$\left( \frac{1}{2} \right) \cdot \cancel{5} \\ \left( 2^{-1} \right) \cdot \cancel{5} =$$

$$b = \frac{96}{1} \quad M = \frac{9}{1} \quad \times$$

$$1, 2, \textcircled{3} \dots \quad 1, \textcircled{3}, 9$$

$$b \times \frac{1}{b} = 1$$

$$\left( b \times \frac{1}{b} \right) \cdot M = 1$$

$$1 \cdot M = 1 \quad \begin{cases} M > 1 \\ M = 1 \end{cases}$$

$$(b \cdot M) \times (b^{-1} \cdot M) = 1$$

$$(b \cdot M) \times (b^{-1} \cdot M) \cdot M = 1$$

( = - ' ) = ↑

Ans. will always be present in  $[1, M-1]$

no need  
for proof

$$b^{-1} \cdot M \Rightarrow [1, M-1]$$

for ( $i=1$ ;  $i < M$ ;  $i++$ ) {

$$\text{if } ((b \cdot M) \times i) \cdot M == 1 \text{ } \}$$

return  $i$ ;

b

$$T.C. = O(M)$$

Eg

$$b = 10, M = 7$$

$$\frac{b^{-1} \cdot 7}{x} \rightarrow [1, 6]$$

$$((\underline{b-1} \cdot 7) \times x) \cdot 7 = 1$$

$$((10 \cdot 7) \times x) \cdot 7 = 1$$

$$(3 \times x) \cdot 7 = 1$$

$$1 = 3 \cdot 7 \equiv 1$$

$$2 = 3 \times 2 = 6 \not\equiv 1 \pmod{7}$$

$$3 \times 3 \not\equiv 1 \pmod{7}$$

$$4 \times 4 \not\equiv 1 \pmod{7}$$

$$5 = 3 \times 5 = 15 \not\equiv 1 \pmod{7}$$

$$10^{-1} \pmod{7} = 5$$

## Fermat's Little Theorem ✓

$$b^{-1} \pmod{m} \rightarrow \text{if } m \text{ is prime}$$

$$a^p \equiv a \pmod{p} \rightarrow a^p \cdot p = a \cdot p$$

$$b^m \equiv b \pmod{m} \Rightarrow b^m \cdot m = b \cdot m$$

$$b^{m-1} \equiv 1 \pmod{m}$$

$= b^{-1} \pmod{m}$  on both sides

$$\boxed{b^{m-1} \pmod{m} = b^{-1} \pmod{m}}$$

IGNORE THE ABOVE STEPS  
FOCUS ON THIS EQUATION ONLY

if  $m$  is prime

$\underline{m \geq 2}$

$(\underline{b^M} \cdot M) \Rightarrow$  fast power

$$a^p \Rightarrow a^{p/2} \times a^{p/2} \Rightarrow \log(p)$$

$$\log(M-2) = O(\underline{\log(M)})$$

$$3 \cong 6 \% 3 = 3 \% 3 = 6 \% 3$$

$$a \cong b \pmod{m} \Rightarrow a \% m = b \% m$$

$$b^M \% M = b \% M$$

$b^{-2} \% M$  on both sides

$$(b^M \% M) \times (b^{-2} \% M) = \cancel{b \% M} \times b^{-2} \% M$$

Take  $\% M$  on both sides

$$\frac{((b^M \% M) \times (b^{-2} \% M)) \% M}{((b \% M) \times \cancel{(b^{-2} \% M)}) \% M}$$

$$(b^M \times b^{-2}) \% M = (b \times b^{-2}) \% M$$

$$\underbrace{\left(b^{\frac{M-2}{2}}\right) \cdot 1 \cdot M}_{\Downarrow} = \underbrace{\left(b^{\frac{-2}{2}}\right) \cdot 1 \cdot M}$$

$\log(M)$  time

Divide integers  $\Rightarrow$  H.w.