Mod Arithmetic

- Intro & properties %[+,-,*]
- ⚠ Pair sum divide by $M = 0$
- Power & fast power with mad
- Inverse Mod & Fermat little theorem

$-5 \% 4$ | python $+3$

C/C++/C# -1

$-1+4=+3$

$21 \% 5 = 1$ remainder

Modular arithmatics

mod

$A \% B \rightarrow$ remainder when A/B

$\frac{21}{5} = 5 \times 4 + 1$

$n \% 1 = 0$ $n \% n = 0$

properties: if$(n<m)$ $n \% m = n$ $3 \% 7 = 3$ $3 \% 10 = 3$

$[0, m-1]$ $\underbrace{? \% 5}$ $0, 1, 2, 3, 4$

$A \% B < 0$

distribute mod over:

✓ $\oplus$ $(a+b) \% P = [(a \% P) + (b \% P)] \% P$

✓ $\circledast$ $(a*b) \% P = [(a \% P) * (b \% P)] \% P$

| a & $b >= 0$

$\ominus$

$\oslash$ ✓ $\ominus$ $a-b = a+(-b)$

$(a-b) \% P = (a+(-b)) \% P = [(a \% P + (-b) \% P)] \% P$

$(a \% P - \underbrace{(b \% P)}_{[0, P-1]} + P) \% P$ $[(a \% P) - (b \% P)] \% P$

$a[i] >= 0$

n

P1 Given an array of integers ($a[]$), and an int $m>0$

find the count of pairs (i,j) s.t $(A[i]+A[j]) \% m = 0$

$i<j$

ex $a = \{\overset{0}{1}, \overset{1}{4}, \overset{2}{3}, \overset{3}{8}\}$, $m=3$

ans = 2

$(1,3)$: $4+8=12 \% 3 = 0$ ✓

$(0,3)$: $1+8=9 \% 3 = 0$ ✓

ex $a = \{2_0, 7_1, 5_2, 10_3, 8_4, 4_5, 6_6, 11_7\}$, $m=5$ ans = 5

① ② ③ ④ ⑤

```
for i = 0 -> n-1
    for j = i+1 -> n-1
        ans += (a[i]+a[j]) % m == 0 ? 1 : 0
```

TC: $O(n^2)$

Contribution technique ⚠

Pay attention

not easy

count[i]	%5	
2	0 {5,10}	0
2	1 {6,11}	1
2	2 {2,7}	2
1	3 {8}	3
1	4 {4}	4

2, 3: (+) %5=0

1, 4: (+) %5=0

$(?+?') \% 5 = 0$

$(\underbrace{? \% 5}_{0,1,2,3,4} + \underbrace{?' \% 5}_{0,1,2,3,4}) \% 5 = 0$

① ④

6, 11 → 4

n 2

$C(n,k) = \frac{n(n-1)}{\boxed{2}}$

Quiz

pseudo code to populate the count of each group:

```
i = 0 -> n-1
    count[a[i] % m]++;
```

$O(n)$

ans = count[1]×count[4] + count[2]×count[3] + $\frac{count[0](count[0]-1)}{2}$

i $\qquad$ $m-i$

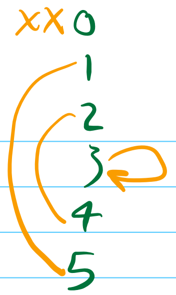
%6

$\lceil \frac{m}{2} \rceil$

ans = $C[1] \times C[5] +$
$C[2] \times C[4] +$
$C[3] \times (C[3]-1)/2 +$
$C[0] \times (C[0]-1)/2$

Quiz

$$\begin{cases} TC: O(n + \frac{m}{2}) \sim O(n+m) \\ SC: O(m) \end{cases}$$



floor

for($i=1$; $i < \lfloor \frac{m}{2} \rfloor$; i++)

...

special case 0

special case $\frac{m}{2}$ → only if m%2==0

assignment implementation

$(a^b)\%m$

$a=10 \quad b=50 \quad P=20$

$(a^b)\%P = (\underbrace{a \times a \times a \times \cdots \times a}_{b \text{ times}})\%P$

$(10^{50})\%20 \rightarrow [0,19]$

$= (a\%P \times a\%P \times \cdots \times a\%P)\%P$

TC: $O(b)$

```
{ ans=1, a=a%P        (→ long)
  for i=1 → b{
     ans *= (a%P)  → (long)
     ans %= P
  }
  ret ans%P
}
```

b even

$(a^b)\%P = (a^{b/2} \times a^{b/2})\%P = \underline{(a^{b/2}\%P)} \times (a^{b/2}\%P)\%P$

V   X

$(V \times V)\%P$

$3^{20}\%P = (3^2\%P)^{10} = (3^4\%P)^5$

$$\text{I} \quad (a^b)\%P = \begin{cases} (a^2\%P)^{b/2}\%P, & b\%2=0 \quad \text{even} \\ a \times (a^2\%P)^{b/2}\%P, & b\%2=1 \quad \text{odd} \end{cases}$$

$$\boxed{\text{II} \quad (a^b)\%P = \begin{cases} (a^{b/2} \times a^{b/2})\%P & b\%2=0 \quad \text{even} \\ a \times (a^{b/2} \times a^{b/2})\%P & b\%2=1 \quad \text{odd} \end{cases}}$$

$a^b\%P$

```
int fastPower(a,b,P){
   if(b==0) return 1
   if (b%2==0){  //even
      ret fastPower(a×a%P, b/2, P)        (long)
   else{ //odd
      ret fastPower(a×a%P, b/2, P)×a%P
   }
}
```

assignment: Implement iterative version

$3 \% 2$ $\qquad$ $\frac{1}{4} \% 10$

$3.937 \% 7$ X

Inverse Mod

Condition: $GCD(b,P)=1$

① $(a/b)\%P = (a \times b^{-1})\%P = (a\%P \times \underbrace{b^{-1}\%P}_{?})\%P$

$a=10$, $b=4$ | $a=10$, $b=5$

$b^{-1}\%P = \frac{1}{b}\%P =$

$\frac{1}{5}\%3=2$

$2 = (\frac{10}{5}\%3) = (\underbrace{10\%3}_{1} \times \underbrace{\boxed{\frac{1}{5}\%3}}_{x})\%3$

$(1 \times x)\%3=2$ → 2

5

ans $3=5^{-1}\%7$

$\frac{1}{b}\%P$ $\qquad$ $\frac{b}{b}=1$ $\qquad$ $\frac{b}{b}\%P=1$

$=(b\%P \times \frac{1}{b}\%P)\%P=1$

$\frac{1}{5}\%7=?$

$(5 \times \frac{1}{5}\%7)=1 \Rightarrow (\underbrace{5\%7}_{5} \times \underbrace{\frac{1}{5}\%7}_{?})\%7=1$

$(5 \times ?)\%7=1$

Quiz

0 1 2 3 4 5 6

$(0 \times 5)\%7=0$ X

$(1 \times 5)\%7=5$ X

~~$(2 \times 5)\%7$~~ $=3$

$(3 \times 5)\%7=1$

Fermat "little" theorem

if P is a prime number

$a^P\%P = a\%P$ $\qquad$ $a^7\%7=a\%7$

⇒ $/a \Rightarrow a^{P-1}\%P=1 = \cancel{\frac{a}{a}}\%P$

1

P2 Find $3^{1002}\%11$ $\qquad$ $11-1$ $3^{10}\%11=1$

$(3^{1000} \times 3^2)\%11 = (3^{1000}\%11 \times 3^2\%11)\%11$

$((\underbrace{\overset{1}{\cancel{3^{10}\%11}} \times \overset{1}{\cancel{3^{10}\%11}} \times \cdots \times \overset{1}{\cancel{3^{10}\%11}}}_{100\ \text{times}}) \times \overset{9}{\cancel{3^2\%11}})\%11=9$ ← ans

$O(1)$

$1002\%10=2$

$$3+2=5$$

$$x+3=1 \longrightarrow x=-2$$

$$\underset{\substack{\searrow\\3}}{x}+2=5$$

$$5=\underbrace{\tfrac{1}{3}\,\%\,7}_{?} \longrightarrow \Big(3\times \underbrace{\tfrac{1}{3}\,\%\,7}_{?}\Big)\,\%\,7=1$$

$$=\Big(\underset{3}{\cancel{3\,\%\,7}}\times \underbrace{\tfrac{1}{3}\,\%\,7}_{\boxed{?}}\Big)\,\%\,7=\boxed{1}$$

0 1 2 3 4 5 6