Modular Arithmetic

> The first step to achieving your goal, is to take a moment to respect your goal. Know what it means to you to achieve it.
>
> DWAYNE JOHNSON

Good Morning

Today's content

→ Modular arithmetic & properties

→ Fermat theorem

→ No. of pairs such that

(arr[i] + arr[j]) % m = 0

A % B → remainder when A is divided by B.

Dividend = Divisor * quotient + remainder

remainder = Dividend − divisor * quotient

↓

largest multiple of divisor ≤ dividend

10 % 4 = 10 − 8 (largest mul of 4 ≤ 10) = 2

13 % 5 = 13 − 10 (largest mul of 5 ≤ 13) = 3

−40 % 7 = −40 − (−42) (largest mul of 7 ≤ −40) = 2

−60 % 9 = −60 − (−63) (largest mul of 9 ≤ −60) = 3

−51 % 2 = −51 − (−52) (largest mul of 2 ≤ −51) = 1

x % m = min ans: 0 , max ans: m − 1

12 % 6 = 0
13 % 6 = 1
14 % 6 = 2
15 % 6 = 3

16 % 6 = 4
17 % 6 = 5
18 % 6 = 0
19 % 6 = 1

Issues with some programming languages (C++, Java, C#)

Integer

print (-40 % 7) = -5 + 7 = 2 (correct)

print (-60 % 9) = -6 + 9 = 3

if (A ≥ 0) ⟶ return A % B

if (A < 0) ⟶ return A % B + B

* Why % M ?

→ Restricting the output

→ limit our output in a particular range

$$\left.\begin{matrix} -\infty \\ \vdots \\ \infty \end{matrix}\right\} \% M = \{0 \quad M-1\}$$

Ans

$M = 10^9 + 7$ ⟶ prime no.

↳ HashMap implementation

* Modular Arithmetic → % + {+, −, *, /}

01. $(a+b)\%m = (a\%m + b\%m)\%m$

a	b	m
13	9	5

limit = 20

$(13+9)\%5$

$\Rightarrow 22\%5$

$\Rightarrow 2$

$= (13\%5 + 9\%5)\%5$

$= (3+4)\%5$

$= 7\%5$

$= 2$

02. $(a*b)\%m = (a\%m * b\%m)\%m$

a	b	m
13	9	5

limit = 20

$(13*9)\%5$

$\Rightarrow 117\%5$

$\Rightarrow 2$

$= (13\%5 * 9\%5)\%5$

$= (3*4)\%5$

$= 12\%5$

$= 2$

03. $(a-b)\%m = (a\%m - b\%m)\%m$

$(13-9)\%5 = (13\%5 - 9\%5)\%5$

$4\%5 = (3-4)\%5$

$= 4 = -1\%5 = -1$

$(a-b)\%m = (a\%m - b\%m)\%m + 0$

$= (a\%m - b\%m)\%m + \underline{m}\%m$

$$(a-b)\%m = (a\%m - b\%m + m)\%m$$

a	b	m
-9	13	5

limit = -20 to 20

$(-9-13)\%5 = (\underline{-9\%5} - 13\%5 + 5)\%5$

$\rightarrow -22\%5 = (-4 - 3 + 5)\%5$

$\rightarrow -2 = (-7+5)\%5 \Rightarrow -2\%5 = -2$

$= -2$

04. $(a \% m) \% m = a \% m$

05 $a^n \% m$

$$a^n = \underbrace{a * a * a * \ldots * a}_{a^{n-1}} * a$$

→ fastpow fn

```
long powmod (int a, int n, int m)
{
    if (n==0) return 1

    long t = powmod(a, n/2, m)

    if (n%2 == 0)
    {
        return (t * t) % m
    }
    else
    {
        return ((t * t) % m * a % m) % m
    }
}
```

TC: O(log n)

* $(a/b) \% m = (a \% m / b \% m) \% m$

$b \% m = 0 \rightarrow$ not a valid expression

$(a/b) \% m = (a \% m * b^{-1} \% m) \% m$ → prime, $gcd(b, m) = 1$

$b^{-1} \% m$ → inverse modulo of b wrt m

* $\Rightarrow \frac{b}{b} \% m = (b * \frac{1}{b}) \% m$

$= (b * b^{-1}) \% m$

$= 1$

In general $(x * inv(x)) \% m = 1$ → $gcd(x, m) = 1$

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

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

$(5 * 5^{-1}) \% 7 = 1$ → equivalent to 3

$(5 * 1) \% 7 = 5$ ✗

$(5 * 2) \% 7 = 3$ ✗

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

* $3^{-1} \% 13 = ?$

* $(3 * \boxed{3^{-1}}) \% 13 = 1$ → equivalent to 9

01. $(3*1) \% 13 = 3$

02. $(3*2) \% 13 = 6$

03. $(3*3) \% 13 = 9$

04. $(3*4) \% 13 = 12$

05. $(3*5) \% 13 = 2$

06. $(3*6) \% 13 = 5$

07. $(3*7) \% 13 = 8$

08 $(3*8) \% 13 = 11$

09. $(3*9) \% 13 = 1$

* Fermat theorem

$$a^{m-1} \equiv 1 \bmod m$$

m → prime no.

$$x \equiv y \bmod m$$

$$x \% m = y \% m$$

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

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

Multiply both the sides with a^{-1}

$a^{-1} * a^{m-1} \% m = a^{-1} * 1 \% m$

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

resolve by using powmod function

inv modulo

$TC = O(\log(m-2)) \approx (\log m)$

* Find $3^{1002} \% 11$

$a^{m-1} \% m = 1 \% m$ Fermat theorem

$3^{11-1} \% 11 = 1 \% 11$

$3^{10} \% 11 = 1$

$3^{1002} \% 11 = (3^{10} * 3^{10} * 3^{10} + \cdots * 3^{10} * 3^2) \% 11$

$= (3^{10} \% 11 * 3^{10} \% 11 * \cdots * 3^2 \% 11) \% 11$

$= (9 \% 11) \% 11 \Rightarrow 9$

12:27 pm → 12:37 pm

Q Given ar[N], m, Calculate no. of pairs i, j such that $\{ar[i] + ar[j]\} \% m = 0$

Note: $i != j$ and pair (i,j) is same as pair(j,i)

Ex: ar[6] = { 4 7 6 5 5 3 } m=3 (indices: 0 1 2 3 4 5)

i	j	ar[i]	ar[j]	(ar[i]+ar[j])%m
0	3	4	5	(4+5)%3 = 0
0	4	4	5	(4+5)%3 = 0
1	3	7	5	(7+5)%3 = 0
1	4	7	5	(7+5)%3 = 0
2	5	6	3	(6+3)%3 = 0

Ans = 5

* Brute force → check for every possible pair if

$$(ar[i] + ar[j]) \% m == 0$$

TC : $O(n^2)$

SC : $O(1)$

Idea 2

$$(ar[i] + ar[j]) \% m = 0$$

$$(ar[i] \% m + ar[j] \% m) \% m = 0$$

$[0 \quad m-1]$ $[0 \quad m-1]$

$0 + 0$

$1 + (m-1)$

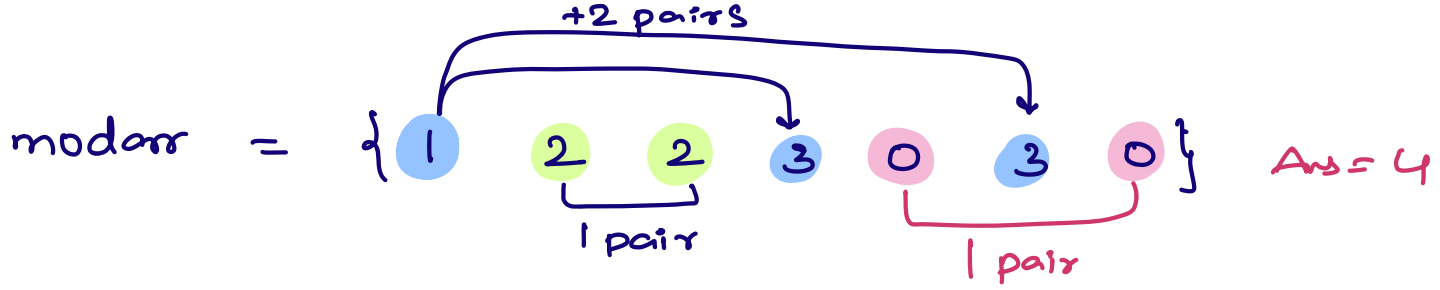
$2 + (m-2)$

$3 + (m-3)$

$\vdots$

$K + (m-K)$

arr[ ] = {13 14 22 3 32 19 16} m = 4



arr[12] =

0	1	2	3	4	5	6	7	8	9	10	11
6	7	5	11	19	20	9	15	14	13	12	23

, m = 5

marr =

0	1	2	3	4	5	6	7	8	9	10	11
1	2	0	1	4	0	4	0	4	3	2	3

range of remainder = { 3 2 2 2 3 }

0 1 2 3 4

1 & 4 = 2 * 3 = 6 { (6,19) (6,9) (6,14) (11,19) (11,9) (11,14) }

2 & 3 = 2 * 2 = 4 { (7,13) (7,23) (12,13) (12,23) }

0 & 0 = $^3C_2$ = 3 { (5,20) (5,15) (15,20) }

Ans = 13

$$^nC_2 = \frac{n * (n-1)}{2}$$

m = 10

ar[ ] =

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
29	11	21	17	2	5	4	6	23	13	26	14	18	15	30	35	50	20	40	9

marr =

9	1	1	7	2	5	4	6	3	3	6	4	8	5	0	5	0	0	0	9

cnt [10] =

0	1	2	3	4	5	6	7	8	9
4	2	1	2	2	3	2	1	1	2

ar[i] % 10 ar[j] % 10 = 0

cnt [0] ⟶ $^4C_2$ pairs

cnt [1] * cnt [9] = 4 pairs

cnt [2] * cnt [8] = 1 pair

cnt [3] * cnt [7] = 2 pairs

cnt [4] * cnt [6] = 4 pairs

cnt [5] ⟶ $^3C_2$ pairs

```
int countPairs(int[] ar, int m)
```

01. Store freq of remainders

```
int[] cnt = new int[m]
for(i=0; i<n; i++){
    int rem = ar[i] % m
    cnt[rem]++;
}
```

```
ans = 0
```

02 Handle Edge case

```
int a = cnt[0]
```

$$ans = ans + \frac{a * (a-1)}{2}$$

```
if(m % 2 == 0){
    int b = cnt[m/2]
```

$$ans = ans + \frac{b * (b-1)}{2}$$

```
}
```

03. get all the remaining pairs

```
i = 1    j = m-1
```

```
    while (i < j){
        ans = ans + cnt[i] * cnt[j];
        i = i+1;
        j = j-1;
    }
    return ans;
}
```

TC: O(n+m)

SC: O(m)