Modular Arithmetic

Jul 21, 2023

AGENDA

- Modulo operator (%)
- Modular Arithmetic
- Divisibility rules
- 1-2 interesting problems

% → Modulo operator

Binary operator (2 operands reqd.)

↳ a % b

→ Find the remainder.

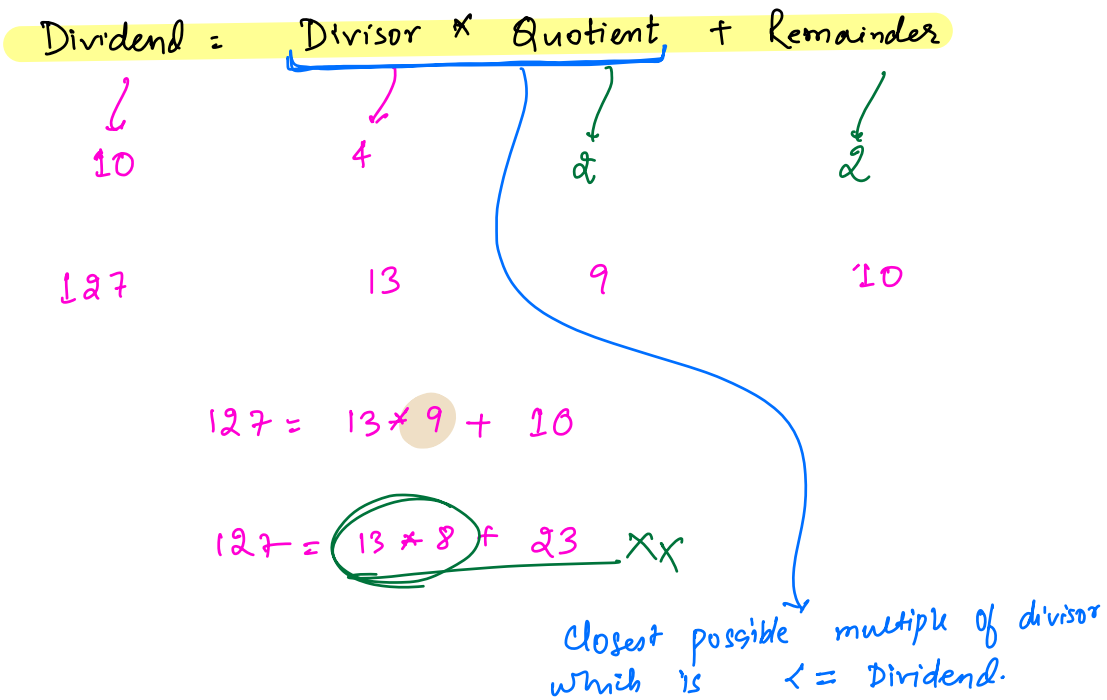
Real life use cases

↳ Cryptography

↳ Hashing (HashMap or Dictionary)

↳ Consistent Hashing (Load Balancer)

*



Remainder = Dividend − Divisor * Quotient

<= dividend

closest possible

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

$100 \% 7 = 100 - (7 * \frac{100}{7})$ → Integer division

$= 100 - (7 * 14)$

$= 100 - 98$

$= 2$

$150 \% 11 = 7$

$150 - (11 * 10) = 110$

$11 * 11 = 121$

$11 * 12 = 132$

$11 * 13 = 143$

$11 * 14 = 154$

```
11) 150 ( 13
    11
    ---
    40
    33
    ---
     7
```

$100 \% 7 = 100 - (7 * ?)$

$= 100 - 98$

$= 2$

$7 * 13 = 91$

$7 * 14 = 98$ (Closest possible)

$7 * 15 = 105$

Remainder = Dividend − Divisor * Quotient

<= dividend

closest possible

$-40 \% 7 = -40 - (7 * ?)$

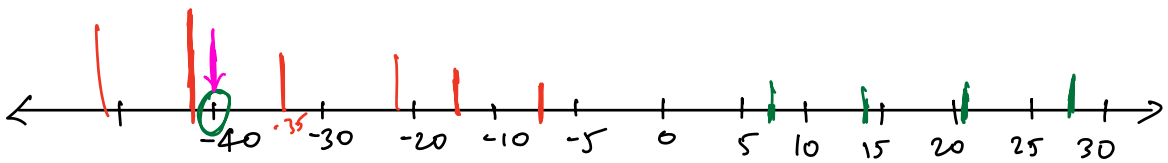
closest to -40

<= -40

$7*1 = 7$

$7*2 = 14$

$7*3 = 21$



Remainder = $-40 - (-42)$

= 2

$7*(-1) = -7$

$7*(-2) = -14$

$7*(-3) = -21$

$7*(-4) = -28$

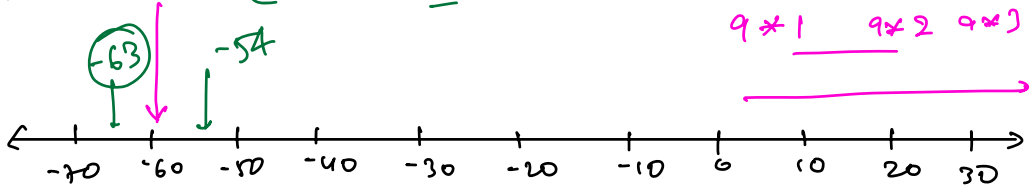
$7*(-5) = -35$

$7*(-6) = -42$

<= dividend

$7*(-7) = -49$

$-60 \% 9 =$ $-60 - (-63) = \underline{3}$



$9*1$ $9*2$ $9*3$

$9*-1 = -9$

$9*-2 =$

$9*-6 = -54$

$9*-7 = -63$

Observations

* Can remainder be negative?

Remainder = Dividend - Divisor * Quotient

* closest possible
* <= dividend.

Always >= 0

$20 \% 3 = \underline{2}$

$60 \% 9 = 60 - (9* \quad)$

$= 6$

$9, 18, 27, 36, 45, \underline{54}, 63$ | 60

$60 - 54 = 6$

$-60 \% 9 = -60 - (-63)$

$= -60 + 63$

$= \underline{3}$

$-9, -18, -27, -36, -45, \underline{-54}$ | -63 | -60

Obs 2: Can remainder be greater than divisor?

↓ (No)

I can get further close to dividend.

Conclusion ↳

N % m → [0, M-1] (Range)

↓

Remainder when divisor is m.

↓

1) >=0

2) less than divisor.

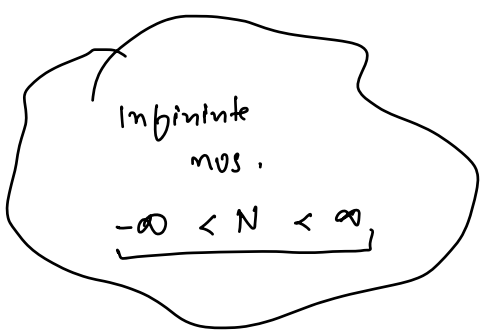
1,00,00,000 % M ↳ lie b/w [0, M-1]

Importance of modulo operator

↳ On applying % M on a no.

your space is truncated.

Limiting data



% M → [0, M-1]

* Modular Arithmetic

(*) $(a+b)\,\%\,M = (a\%M + b\%M)\,\%M$

$(9+20)\,\%\,7 = (9\%7 + 20\%7)\,\%M = 8\%7 = 1$

$9\%7 \to 2 \quad 20\%7 \to 6$

$(10^{10} + 10^{7})\,\%\,7 = (10^{10}\%7 + 10^{7}\%7)\,\%\,7$

10^{10} — Expensive

$10^{10}\%7 \to [0-6]$

$10^{7}\%7 \to [0-6]$

$(20+7)\,\%\,3 = (20\%3 + 7\%3)\,\%3$

$= (2+1)\%3$

$= 0$

* $(a\,\%M)\,\%M = a\%M$

$(20\%3)\,\%3$

$20\%3 \to 0, 1, 2$

$0, 1, 2$ $\%3$

* $(a * b)\%M = (a\%M * b\%M)\%M$

Modulus in languages,

	Actual remainder	Python	Java/C/C++/C#
$-40\%7$	2	2	-5

$-7 \quad -14 \quad -21 \quad -28 \quad -35 \quad -42$

$-40 - (-35)$

+ Divisor to get actual remainder.

Break till 8:15 AM

Divisibility rules

* By 3

3734689 → Sum of digits

If sum of digits is divisible by 3, no. is divisible by 3.

3+7+3+4+6+8+9

= 40

91731

9+1+7+3+1

= 21 → 21 % 3 = 0

∴ 91731 % 3 = 0 ✓

Why?

$(3\,5\,6\,3\,2)_{4\,3\,2\,1\,0}$ % 3

$= (3*10^4 + 5*10^3 + 6*10^2 + 3*10^1 + 2*10^0)$ % 3

$= [(3*10^4)\%3 + (5*10^3)\%3 + (6*10^2)\%3 + (1*10^1)\%3 + (2*10^0)\%3]\%3$

$= [(3\%3 * 10^4\%3)\%3 + (5\%3 * 10^3\%3)\%3 + (6\%3 * 10^2\%3)\%3 \ldots]\%3$

$= [(3\%3 * 1)\%3 + (5\%3 * 1)\%3 + (6\%3 * 1)\%3 \ldots]\%3$

$= (3\%3 + 5\%3 + 6\%3 + 3\%3 + 2\%3)\%3$

$= (3+5+6+3+2)\%3$

$10^i \%3 = 1$

$10^0 \%3 = 1$

$10^1 \%3 = 1$

$10^2 \%3 = 1$

$10^3 \%3 = 1$

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

$797 \% 3$

$= (7 * 100 + 9 * 10 + 7) \% 3$

$= ((7 * 100) \% 3 + (9 * 10) \% 3 + 7 \% 3) \% 3$

$= (7 \% 3 * 1) \% 3 + (9 \% 3 * 1) \% 3 + 7 \% 3) \% 3$

$= (7 \% 3 + 9 \% 3 + 7 \% 3) \% 3$

$= (7 + 9 + 7) \% 3$

Divisibility by 9

↳ If sum of digits is divisible by 9, no. is " .

$(91736) \% 9$

$= (9 * 10^4 + 1 * 10^3 + 7 * 10^2 + 3 * 10^1 + 6 * 10^0) \% 9$

$= (9 \% 9 * 1 \% 9 + 7 \% 9 + 3 \% 9 + 6 \% 9) \% 9$

$= (9 + 1 + 7 + 3 + 6) \% 9$

$10^0 \% 9 = 1$
$10^1 \% 9 = 1$
$10^2 \% 9 = 1$
$10^3 \% 9 = 1$
⋮

Divisibility by 4

↳ If last 2 digits is divisible by 4, no. is divisible by 4.

$7368924 \,\%\, 4$

$(91736) \,\%\, 4$

$= (9*10^4 + 1*10^3 + 7*10^2 + 3*10^1 + 6*10^0) \,\%\, 4$

$= 9\%4*0 + 1\%4*0 + 7\%4*0 + (3*10^1+6*10^0)\%4$

$= (3*10^1 + 6*10^0)\%4$

$= 36\%4$

$10^0 \%4 = 1$

$10^1 \%4 = 2$

$10^2 \%4 = 0$

$10^3 \%4 = 0$

$10^4 \%4 = 0$

$\vdots$

$10^{5/6/7} \%4 = 0$

Q: Given a, n, p, find $a^n \% p$ without using inbuilt functions.

$1 <= a <= 10^9$

$1 <= p <= 10^9$

$1 <= n <= 10^5$

$a^n \% p$ → 0 to $p-1$ → max value = 10^9 → int ✓

$n = 10$

$(10^9)^{10}$

10^{90}

$(a * b) \% M = (a\%M * b\%M) \% M$

Code (B.F.)

```
ans = 1
for(int i = 0; i < n; i++)
 {
        ans = ans * a      ← overflow
 }
return ans % p
```

```
ans = 1
for(int i = 0; i < n; i++)
 {
        ans = (ans % p * a % p) % p
 }
return ans
```

$a = 3$

$n = 10$

$p = 7$

ans = 3 (1)

ans = 9 2

ans = 2 * 3 = 6

ans = 6 * 3 = 18 4

ans = 4 * 3 = 12 5

$a^n \% p$

$= (a * a * a * a * a * \cdots) \% p$

$= ((a\%p * a\%p) \% p * a\%p) \% p$

Q. Given a very large no in form of an array. Find num % p.

No. of elements in array = no. of digits in no.

$1 <= N <= 10^5$

$0 <= arr[i] <= 9$

$2 <= p <= 10^7$

[6, 2, 3, 4, 3] p = 49

62343 % 49 = ? ✓

[2, 3, 4, 7] p = 16

2347 % 16 = ? ✓

How to create a no. from an array?

3 2 1 0
[2, 3, 4, 7]

$7*10^0 + 4*10^1 + 3*10^2 + 2*10^3$

arr[] = [7, 0, 8] (2 1 0) → represents no. 708

int a = 708

$7*10^2 + 0*10^1 + 8*10^0$

3 2 1 0

[2, 3, 4, 7] % 16

ans = 0

ans += (7 * 10^0) % 16 = 7

ans += 4 * 10^1 [7 + 40 = 47 % 16 = 15]

ans += 3 * 10^2 [15 + 300 = 315 % 16 = 11]

ans += 2 * 10^3 [11 + 2000 = 2011 % 16 = ...]

13 12 11 10 9 8 7 6 5 4 3 2 1 0

[1, 7, 3, 6, 2, 4, 8, 9, 0, 7, 2, 6, 3, 4, 5] % 7

[1 * 10^{14} + 7 * 10^{13} + 3 * 10^{12} + 6 * 10^{11} + ...]

5 * 10^0 = 5 + 4 * 10^1 % 7 = 12 % 7 = 3

4 % 7 * 10 % 7

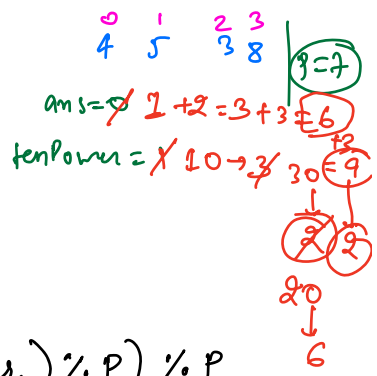
12

Code.

```
ans=0
tenPower=  1      // 10^0
for(int i=n-1; i>=0; i--)
{
        ans =(ans + (arr[i] * tenPower)%p)%p
        tenPower = (tenPower * 10)%p
}
return ans.
```

ans=2

10^0 10^1 10^2



4538%7 = 2

7)4538(648

42

33

28

58

56

2

%.M

ans%M

%.M

%.M

%. 10^9+7

ans += ans *= a

arr = [7, 3, 6, 8, 9]

return an int. 7389

```
ans = 0
tenPower = 1
for(int i = n-1; i >= 0; i--)
{
    ans += (arr[i] % p * tenPower % p) % p
    tenPower = (tenPower * 10) % p
}
return ans % p
```