Today's Content :-

→ Modular operators
→ Modular arithematics
→ 1 Hard problem.

int range $\rightarrow$ $(-2*10^9$ to $2*10^9)$
long range $\rightarrow$ $(-8*10^{18}$ to $8*10^{18})$

% $\rightarrow$ modules / reminder,

Dividend = divisor * quotient + remainder.

$10 \% 4 \Rightarrow 10 = 4*\left(\frac{10}{4}\right) + r \Rightarrow 10 = 8 + r$
$\Rightarrow \underline{r = 2}.$

$13 \% 5 \Rightarrow 13 = 5*\left(\frac{13}{5}\right) + r \Rightarrow 13 = 10 + r \Rightarrow \underline{r = 3}.$

$100 \% 7 \Rightarrow 100 = 7*\left(\frac{100}{7}\right) + r \Rightarrow 98 + r = 100 \Rightarrow \underline{r = 2}.$

$150 \% 7 \Rightarrow 7*\left(\frac{150}{7}\right) + r \Rightarrow 147 + r \Rightarrow \underline{r = 3}.$

$-60 \% 9 \Rightarrow 9*\left(-\cancel{\frac{60}{9}}^{\,6}\right) + r \Rightarrow -54 + r = -60$
$\Rightarrow \underline{r = -6}.$

$$\left\{\begin{matrix}-\infty\\ \vdots \\ \infty\end{matrix}\right\} \; \% 10 \longrightarrow \underline{[0 \text{ to } 9]}$$

$$\left\{\begin{matrix}-\infty\\ \vdots \\ \infty\end{matrix}\right\} \; \underbrace{\% M}_{\text{limit range}} \longrightarrow [0 \text{ to } M-1]$$

- consistent hashing
- hashmap/dict
- cryptography

Conceptually :-

⇒ Dividend − divisor * quotient = remainder.

remainder = Dividend − (divisor * quotient)

greatest multiple of divisor <= dividend.

10 % 4 ⇒ 10 − 8 ⇒ 2.

13 % 5 ⇒ 13 − 10 ⇒ 3

100 % 7 ⇒ 100 − 98 ⇒ 2

150 % 7 ⇒ 150 − 147 = 3.

−60 % 9 ⇒ −60 − (greatest multiple of 9 which is less than or equal to −60)

⇒ −60 − (−63)

⇒ 3

63 ✗

−63

−54 ✗

9 ✗

$-40 \% 7 \Rightarrow -40 - $ (greatest multiple of 7 which is less than equal to -40)

$-40 - (-42)$

$\Rightarrow -40 + 42 \Rightarrow \underline{2}$.

As per your language → Not including python.

$-80 \% 9$ → language $\Rightarrow -8$

→ concept → $-80 - (-81) \Rightarrow 1$

$-40 \% 9$ → language $\Rightarrow -4$

→ concept $\Rightarrow -40 - (-45) \Rightarrow \underline{5}$

$-60 \% 9$ → language $\Rightarrow -6$

→ concept $\Rightarrow -60 - (-63) \Rightarrow \underline{3}$

```
if (x < 0) {
    (x % p + p)
}
```

→ only by adding p we can get expected ans

Modular arithmetic

① $(a+b)\%M \Rightarrow (\underbrace{a\%M}_{(0\ to\ M-1)} + \underbrace{b\%M}_{(0\ to\ M-1)})\%M$

$a=6,\ b=13,\ M=7$ $\Rightarrow (6\%7 + 13\%7)\%7$

$\Rightarrow (6+6)\%7$

$(13+6)\%7 \Rightarrow 5$ $\Rightarrow 12\%7$

$\Rightarrow 5$

② $(a*b)\%M \Rightarrow (\underbrace{a\%M}_{0\ to\ M-1} * \underbrace{b\%M}_{0\ to\ M-1})\%M$

$a=6,\ b=7,\ M=4$ $\Rightarrow (6\%4 * 7\%4)\%4$

$(2*3)\%4$

$(42)\%4$

$\Rightarrow 2$ $\Rightarrow 2$

③ $(a-b)\%M$

④ $(a/b)\%M$

advance.

Problem :-

given $a, n, p \rightarrow$ calculate $a^n \% p$.

a	n	p
3	4	7

$\Rightarrow (3^4) \% 7 \Rightarrow 81 \% 7 \Rightarrow 4.$

```
power (int a, int n, int p) {
    // no overflow.
    for (i=1; i<=n; i++) {
        a = a * a
    }
    return a%p
}
```

wrong.

given, $a, n=5$,

$a^5 \% p$

i		
		a^1
1	$a = a * a \Rightarrow$	a^2
2	$a = a * a \Rightarrow$	a^4
3	$a = a * a \Rightarrow$	a^8

```
power (int a, int n, int p) {
        // no overflow .
    int ans = 1;
    for (i=1; i<=N; i++) {
            ans = a * a
    }
    return ans % p
}
```

wrong answer .

```
power (int a, int n, int p) {
①      long ans = 1;
②      for (i=1; i<=N; i++) {
③          ans = (ans * a) % p
④      }
⑤
⑥      return ans
}
```

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

$$\underbrace{ans \% p}_{10^9 - 1} \qquad \underbrace{a \% p}_{10^9 - 1}$$

i = 1 :-

Constraints :-

$1 <= N <= 10^5$

$1 <= a <= 10^9$

$1 <= p <= 10^9$

$$(a^n) \% p$$

$$(\overset{100}{a} \times \underbrace{a \times a \times a \cdots}_{n}) \% p \Rightarrow ?.$$

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

$\underbrace{\qquad\qquad\qquad}_{n}$

$7^5 \to 16807$

$(7^5) \% 9 \Rightarrow \text{0 to 8}$, 100

$(7 * 7 * 7 * 7 * 7) \% 9$

$((7 * 7) \% 9 * (7 * 7) \% 9 * 7 \% 9) \% 9$

$(4 * 4 * 7) \% 9$

$((4 * 4) \% 9 * 7 \% 9)$

$16 \% 9 \times 7 \% 9$

$(7 * 7) \% 9$

$\Rightarrow 4$

$10^{10} \% 7 \Rightarrow 4$

$(10^5 * 10^5) \% 7 \Rightarrow \text{0 to 6}$.

$$(10^5 \% 7 * 10^5 \% 7) \% 7$$

$$(5 * 5) \% 7$$

4

Break

10:11 : 10:21 pm

Divisibility of 3 :- Sum of its digits are divisible by 3.

$(789) \% 3 \rightarrow$ ✓ $(8215) \% 3$ ✗

$10 \% 3 \Rightarrow 1$

$10^2 \% 3 \Rightarrow 1$

$10^3 \% 3 \Rightarrow 1$

$10^4 \% 3 \Rightarrow 1$

if $((3458) \% 3 == 0)$

$\Rightarrow (3 * 10^3 + 4 * 10^2 + 5 * 10^1 + 8 * 10^0) \% 3$

$\Rightarrow \left(\underbrace{(3 * 10^3) \% 3}_{} + \underbrace{(4 * 10^2) \% 3}_{} + \underbrace{(5 * 10^1) \% 3}_{} + (8 * 10^0) \% 3 \right) \% 3$

$\rightarrow (8 \% 3 + 4 \% 3 + 5 \% 3 + 8 \% 3) \% 3$

$\rightarrow (3 + 4 + 5 + 8) \% 3$

(*) Divisibility of $\underline{4}$:- (last 2 digits % 4)

if $((a_3 a_2 a_1 a_0) \% 4 == 0)$

$\downarrow$

$(a_3 * 10^3 + a_2 * 10^2 + a_1 a_0) \% 4$

$((a_3 * 10^3) \% 4 + (a_2 * 10^2) \% 4 + a_1 a_0 \% 4) \% 4$

$(0 + 0 + a_1 a_0 \% 4) \% 4$

$\Rightarrow a_1 a_0 \% 4$

Ques) Given 1 number in arr[], calc number % p.

$\underline{N = 5}$

	0	1	2	3	4
arr[5] =	7	8	9	6	2

$p = 5$

$(7 8 9 6 2) \% 5$.

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

Constraints :-

$1 <= N <= 10^5$

$1 <= P <= 10^9$

$N=3.\quad 999 : 10^3-1$

$N=5 : 99999 : 10^5-1$

$N=10 : 10^{10}-1 \rightarrow$ int.

$N=20 : 10^{20}-1 \rightarrow$ long.

$N=10^5 : 10^{10^5}-1$

$$\begin{array}{lccccc} & 0 & 1 & 2 & 3 & 4 \\ arr[5] = & 3, & 2, & 6, & 4, & 9 \end{array} \;\%P \longrightarrow 32649$$

$$\left(9*10^0 + 4*10^1 + 6*10^2 + 2*10^3 + 3*10^4 \right) \;\%\; P$$

Pseudocode :-

```
//given arr[N] & P.
   long fans = 0;
   long powerOfT = 1

for (i=N-1; i>=0; i--) {
    fans = fans + {(arr[i] % P) *
                        (powerofT % P)} % P

      powerofT = (powerofT * 10) % P
    }

return fans % P;
```

0	1	2	3	4
3	2	6	4	9

arr [5] = arr[0], arr[1], arr[2], arr[3], arr[4]

arr[4] * 10^0

arr [3] * 10^1

arr [2] * 10^2

arr [1] * 10^3

(arr [0] * 10^4)

$$\Rightarrow \big(\,(arr[0] * 10^4) + (arr[1] * 10^3) + (arr[2] * 10^2) + (arr[3] * 10^1) + arr[4] * 10^0\,\big) \% p$$

$$\Rightarrow \big(\,(arr[0] * 10^4) \% p + (arr[1] * 10^3) \% p + (arr[2] * 10^2) + (arr[3] * 10^1) \% p + arr[4] * 10^0\,\big) \% p$$

$$(arr[0] \% p * 10^4 \% p)$$

Remainder = dividend − div * quotient.

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

$$\underset{a}{100} \,\%\, \underset{b}{7} \Rightarrow 100 - 7 * \left(\cancel{\frac{100}{7}}^{\,14}\right) \to (a/b)$$

$$100 - (7 * 14) \Rightarrow 100 - 98 = 2$$

$$-40 \,\%\, 7 \Rightarrow -40 - 7 * \left(\cancel{\frac{-40}{7}}^{\,-5}\right) \Rightarrow -40 + 35 = -5.$$

$$-60 \,\%\, 9 \Rightarrow -60 - 9 * \left(\cancel{\frac{-60}{9}}^{\,-6}\right) \Rightarrow -60 + 54 \Rightarrow \underline{-6}.$$

Python :-

(a/b)

Remainder = dividend − div * quotient.

$\downarrow$

$floor\left(\frac{a}{b}\right)$

$floor(14.2)$

$$100 \,\%\, 7 \Rightarrow 100 - 7 \left(\frac{100}{7}\right)$$

$$\Rightarrow 100 - 7 * 14 \Rightarrow \underline{2}.$$

$floor(-5.76)$

$-40 \% 7 \Rightarrow -40 - 7 \left(\cancel{\frac{-40}{7}} \right)$

$\Rightarrow -40 - 7(-6)$

$\Rightarrow -40 + 42 \Rightarrow \underline{2}$.

$$\text{floor}(-6.66) \Rightarrow -7$$

$-60 \% 9 \Rightarrow -60 - 9 * \left(\cancel{\frac{-60}{9}} \right)$

$-60 - 9 * -7 \Rightarrow -60 + 63 \Rightarrow \underline{3}$

$l = 31, \quad r = 0$

while $(\underline{l} < \underline{r})$ {

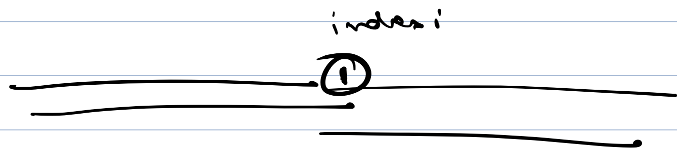
$\_\_\_\_ \quad \_\_\_\_$

}

17

$0 \xrightarrow{+1} 1 \to 2 \to 4 \to 8 \to 16 \xrightarrow{+1} 17 \to$

1 0 0 0 1



$$(a/b) \% m \Rightarrow (a * b^{-1}) \% m$$

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

$b^{-1} \% m$ → This will exist $\gcd(b, m) = 1$ → why?

$$(a * b) \% m \Rightarrow 1$$

→ b is inverse of a.

$$\underbrace{(a \% m)}_{0 \text{ to } m-1} * \underbrace{(b \% m)}_{(1 \text{ to } m-1}$$

$a = 7$, $m = 10$. $(a^{-1} \% m)$.

$\gcd(a, m) = 1$.

$(a^{-1} \% m) \Rightarrow$ 1 to 9.

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

$(1 * 7) \% 10 \neq 1$ 5
$(2 * 7 \% 10) \neq 1$ 6
$(3 * 7 \% 10) = 1$ 7
4 8
9

fermat's theorem :- if m is prime.

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