Modulo - Arithmetic

What is a % m ?

1) Remainder of a/m [0 ... m-1]
2) Repeated subtraction of m from a until we get a number less than m

30 % 7 => 23 % 7 => 16 % 7 => 9 % 7 = 2 % 7

a % m

31 % 6 => 1

20 % (7) = 6 (M-1)

a % m

→ Min value = 0

→ Max value = m - 1

A > B

A - B > 1

Question:

Given 2 numbers A, B such that |A - B| > 1

find M > 1 such that

A % M = B % M

Ex1 A = 10, B = 7

M = 3

10 % 3 = 1

7 % 3 = 1

Ex2 A = 2, B = 10

1) M = 2

2 % 2 = 0 , 10 % 2 = 0

2) M = 4

2 % 4 = 2 , 10 % 4 = 2

3) M = 8

2 % 8 = 2, 10 % 8 = 2

M = { 2, 4, 8 }

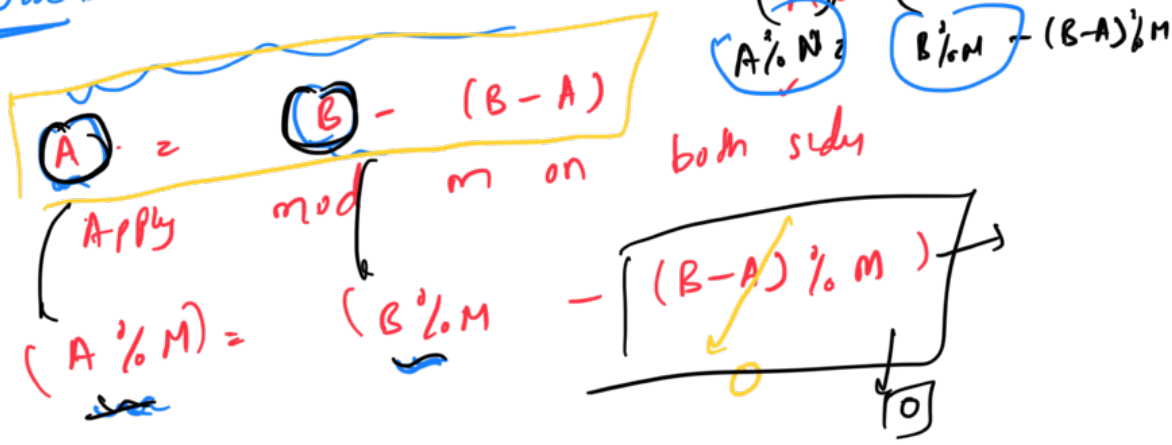
Brute-Force:

```
for (M=2; M<=...; M++) {
    if (A%M == B%M) {
        return M;
    }
}
```

$((B - (B-A)) \% M)$

$(A-B)\%M = (A\%M - B\%M + M)\%M$

Approach:



$(B-A)\%m = 0$

M has to be a factor of $(B-A)$

$m = (B-A)$

$(B-A)\%(B-A) = 0$

$M = B - A$

T.C: O(1)

→ Return the smallest factor / divisor of (B - A).

N = a x b

a ≤ √N , b ≥ √N

```
for(i = 2; i <= √N; i++) {
    if(N % i == 0) {
        // i is one factor
    }
}
```

T.C: O(√N)

A = B - (B - A)

A % M = ((B % M) - (B - A) % M + M) % M

A % M = B % M

A % M = B % M

(B - A) % M

(B - A) % M = 0

M has to be a factor of (B - A)

(B - A)

Proper fixes

1) (a + b) % m = (a % m + b % m) % m?

a = 7, b = 8, M = 11

LHS: 15 % 11 = 4

RHS: 7 % 11 + 8 % 11 = 15

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

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

(C++ compiler)

$(-2)\%7$, it returns a negative number

$[0 \dots M-1]$

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

$-2 \% 7 =$

$-2 = 7 \times (-1) + 5$

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

3) $(a \cdot b)\%m = (a\%m * b\%m)\%M$

4) $(a^b)\%m$

$(a \cdot b)\%m = (a\%m \times b\%m)\%M$

$b = a$

$(a^2)\%m = (a\%m \times a\%m)\%m$

$a^2\%m = (a\%m)^2\%m$ — (1)

$b = a^2$

$(a \cdot a^2)\%m = (a\%m \times a^2\%m)\%m$

$(a^3)\%m = [a\%m \times (a\%m)^2\%m]\%m$

$(a^3)\%m = [(a\%m)^3]\%m$

$$\boxed{(a^b)\%m = (a\%m)^b\%m}$$

3) $(a \cdot b)\%m = (a\%m \times b\%m)\%m$

$a = k_1 m + r_1$

$r_1 = a\%m$ $\quad r_1 \in [0 \dots m-1]$

$b = k_2 m + r_2$

$r_2 = b\%m$

$m = 7$

$58 = 7 \times 8 + 2$

$101 = 7 \times 14 + 3$

$(a \cdot b)\%m = [(k_1 m + r_1) \times (k_2 m + r_2)]\%m$

$= [(k_1 k_2 m^2) + k_1 m r_2 + k_2 r_1 m + r_1 r_2]\%m$

$(k_1 k_2 m^2)\%m = 0$, $k_1 m r_2 = 0$, $k_2 r_1 m = 0$

$(a \cdot b)\%m = [r_1 r_2]\%m$

$= [a\%m \times b\%m]\%m$

4) $(a^b)\%m = (a\%m)^b\%m$

$(a.c)\%m = (a\%m \cdot c\%m)\%m$

$\rightarrow c = a$

$(a^2)\%m = (a\%m \times a\%m)\%m$

$a^2\%m = (a\%m)^2\%m$ — (1)

$\rightarrow c = a^2$

$(a.a^2)\%m = (a\%m \cdot a^2\%m)\%m$

$(a^3)\%m = (a\%m \cdot (a\%m)^2\%m)\%m$

$(a^3)\%m = (a\%m)^3\%m$

$(a^b)\%m = (a\%m)^b\%m$

$(a\%m)^b$

$\rightarrow$ How to compute $(a^b)\%m$

$M = 10^9+7$

Brute - force

```
long pow(a, b, m) {
    long long ans = 1;
    for(i=1; i<=b; i++) {
        ans = ((ans * a)) % m;
    }
    return ans % m;
}
```

T-C: O(b)

i=1 to i=b

ans = 10^9 * $a = 10^9$

10^{18}

long long

a^b

(a x a x a ...) b times

% M

$(100)^{20} = 10^{40}$

```
ans = 1
for(i=1; i<=20; i++) {
    ans = ans * 100;
}
ans = (100)^20
```

int = 10^9

long long int = 10^{18}

INT(MAX)

$(10^9 \times 10^9)_2$

(10^{18})

long long int

long long int

$(\quad)$ % N

10^{14}

% $(10^9 + 7)$

(int)

(a^b) % m

O(b)

Can we do better?

$(a^b) \% M$

$3^{30} = (3^2)^{15}$

$3^{31} = 3 \cdot (3^2)^{15}$

3^{31} L $b=31$ $\quad 3 \cdot (3^2)^{\frac{31-1}{2}}$

a^b → $(a^2)^{b/2}$ if b is even

→ $(a \cdot (a^2)^{\frac{b-1}{2}}) \% n$ if b is odd

$(81)^5 \% 11 = (81 \% 11)^5 \% 11$

$(3^2)^{10}$ $\quad (b)$

$3^{20} \% 11$ → $(9)^{10} \% 11$ → $(81)^5 \% 11$ → $4^5 \% 11$

step1 → $(b/2)$ $\quad$ step2 $(b/4)$

$(a^b) \% m = (a \% m)^b \% m$

$16^2 \% 11 = (16 \% 11)^2 \% m$

$= 16^2 \% 11 = (16 \% 11)^2 \% 11$

$= (5)^2 \% 11$

$4 \cdot (16)^2 \% 11$ → step3 → $(b/8)$

$4 \cdot 5^2 \% 11$

$4 \cdot (25) \% 11$ → step4

$4 \cdot 3 \% 11$

$= 12 \% 11$ → step5

$25^3 \% 11 = 3$

5 steps ← 20 steps

Brute Force:

$b, \frac{b}{2}, \frac{b}{4}, \frac{b}{8}, \ldots, \frac{b}{2^k}$

$\frac{b}{2^0}, \frac{b}{2^1}, \frac{b}{2^2}, \frac{b}{2^3}$

$\frac{b}{2^k} = 1$

$b = 2^k$

No. of step = $k = \log_2^b$

$(a^b) \% m$

T.C: $O(\log b)$

Fast Exponentiation / Binary Exponentiation

Recursive Approach

$a^0 \% m$

(ans % M)

```
long fast (a, b, m) {
    if(b == 0) return 1;

    if(b % 2 == 0) {          // b is even
        return fast((a*a)%m, b/2, m)
    }
    else if(b % 2 == 1) {     // b is odd
        return (a * fast((a*a)%m, (b-1)/2, m))%m
    }
}
```

Congruent Modulo Notation

$a \equiv b \mod n$

↓ Congrent

$a \% n = b \% n$

1) a and b have the same remainder when divided by n

2) $(a-b) \% n = 0$

n divides $(a-b)$

$10 \equiv 14 \mod 4$

$10 \% 4 = 2$

$14 \% 4 = 2$

1) $10 \equiv 14 \mod 4$ ✓

2) $2 \equiv 10 \mod 4$ ✓

3) $20 \equiv 44 \mod 4$ ✓

A, B, C

$44 \% 4 = 0$

$20 \% 4 = 0$

% 4

$10 \equiv 14 \mod 4$

$10 \equiv (3 \times 4 + 2) \mod 4$

$10 \equiv 2 \mod 4$

$14 = K \times 4 + 2$

$K = 3$

$(10 + x) \equiv (2 + x) \mod 4$ ✓

$10 \% 4 = 2 \% 4$

$(10+n) \% 4 = (10\%4 + n\%4) \% 4$ — ①

$(2+n) \% 4 = (2\%4 + n\%4) \% 4$ — ②

① = ②

$\Rightarrow (10+n) \equiv (2+n) \bmod 4$

∴ if $A \equiv B \bmod N$

$A \equiv (B + k \cdot N) \bmod N$

$k \cdot N$ → Multiple of N

k can multiple of N.

Fermat's Little Theorem

If p is a prime number, then for any integer a,

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

$\Rightarrow (a^{p-1}) \% p = 1 \% p$

$\therefore \boxed{a^{p-1} \% p = 1}$

Fermat

$\gcd(a, p) = 1$

Co-prime

$a \equiv b \bmod p$

$a \% p = b \% m$

$p = 17, \quad a = 2$

$2^{17-1} \equiv 1 \bmod 17$

$2^{16} \equiv 1 \bmod 17 \Rightarrow \boxed{2^{16} \% 17 = 1}$

$(2^{16} - 1) \% 17 = 0$

$(2^{16}-1)$ is a multiple of 11

Property - 5

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

LHS: $(100/4)\%11 = 25\%11 = 3$

$[0 \ldots M-1]$

RHS: $(100\%11 / 4\%11)\%11$

$= (1/4)\%11$

$\Rightarrow (0.25)\%11$

Modular - Inverse

$(a/b)\%m = ((a\%m) \times (b^{-1}\%m))\%m$

$b^{-1}\%m \Rightarrow$ Inverse mod of b w.r.t m

Modular Inverse

If there is an x such that,

if $(b \times x)\%m = 1$

then x is the modular Inverse of b w.r.t m

$b = 6, \quad m = 23$

$x = 4$

$(6 \times 4)\%23 = 1$

$\left(\frac{1}{b}\right) < 1$

$b^{-1} = 4$

$b = 5, \quad m = 8$

$x = b^{-1} = 5$

$(5 \cdot x) \% 8 = 1$

$(25) \% 8 = 1$

$b = 7, \quad m = 4$

$b^{-1} = 3$

$(7 \times 3) \% 4 = 1$

$(7 \times 7) \% 4 = 1$

$\vdots$

$[3, 7, 11, 11+4, 15th \ldots]$

Does b^{-1} always exist:?

Modulo Inverse of b wrt m exists only if.

$\gcd(b, m) = 1$

Extended Euclidean Algorithm

Brute Force:

B^{-1}

$(B \cdot x) \% m = 1$

$B^{-1} : [1, M-1]$

Try all values of x

```
for (x = 1; x <= M - 1; x++) {
    if ( B . x % m == 1)
        return x;
}
```

T.C: $O(m)$

If B^{-1} exists, then it is in

Claim: % the range [1, M-1]

Lets assume, we have B^{-1} in [M, 2M-1]

Proof by contradiction.

$x = B^{-1} = (M + K)$ where $0 \le K \le M-1$

$K = 0$, $M+0 = M$

$K = M-1$, $M + M-1 = 2M-1$

$(B \cdot x) \% m = 1$

$B \cdot (M+K) \% m = 1$

$(B \cdot M) \% m + (B \cdot K) \% m = 1$

$0 \Rightarrow (B \cdot K) \% m = 1$

$K \in [0, m-1]$

Approach 2:

$b^{p-1} \equiv 1 \bmod p$ ✓ (p is prime)

$b \cdot b^{p-2} \equiv 1 \bmod p$

$\{b^{p-1} = b \cdot b^{p-2}\}$

$(b \cdot b^{p-2}) \% p = 1$

$x = b^{p-2}$

$(b \cdot x) \% p = 1$

$a \equiv b \bmod p$

$a \% p = b \% p$

$b^{-1} = x = (b^{p-2})$ Modular inverse

$(b^{p-2} \% p)$ → Fast Exponent.

$\Rightarrow (b \cdot x) \% p = 1$ $O(\log p)$

Find x such that

$(b \cdot x) \% p = 1$

p is prime

$b^{p-1} \equiv 1 \bmod p$

$b \cdot b^{p-2} \equiv 1 \bmod p$

$(b \cdot b^{p-2}) \% p = 1 \% p = 1$

$(b \cdot b^{p-2}) \% p = 1$

Find x such that

$(b \cdot x) \% p = 1$

$a \equiv b \bmod p$

$a \% p = b \% p$

$b^{-1} = x = b^{p-2}$

$m = 10^9 + 7$

Fast Exponentiation

$O(\log p)$

5) $(a/b) \% m = ((a \% m) \times (b^{-1} \% m)) \% m$

$(a/b) \% m = ((a \% m) \times (b^{m-2} \% m)) \% m$

→ ✓ only when m is a prime number

→ $\gcd(b, m) = 1$ (fermat's Little)

Problem: Very large Power

Given A, B

Compute $(A^B) \% M$

$M = 10^9 + 7$

$A, B \leq 10^5$

$[0 \ldots M-1]$

Brute force

1) Compute $(B!) \Rightarrow O(b)$

2) $(A^{B!}) \Rightarrow$ Fast Exponentiation $\Rightarrow O(\log b!)$

$(A^B) \Rightarrow \log B$

Fermat's Little theorem

$a^{p-1} \equiv 1 \bmod p$ (1) where p is prime.

$us = 7 \times 6 + 5$ (5)

(p)

$N = k \times p + r$, $[0 \ldots p-1]$

N/p

$a^{b!}$

$b! = k(p-1) + r$ — (1)

$r = b! \,\%\, (p-1)$ — (2) $\Rightarrow O(b)$

$N \% p = (kp + r) \% p$

$N \% p = ((kp) \% p + r \% p) \% p$

$\Rightarrow a^{b!} = a^{k(p-1)+r}$

$(a^{b!}) \% p = (a^{p-1} \cdot a^{p-1} \cdot a^{p-1} \cdot \_ \_ \times a^r) \% p$

k times

$(a^{b!}) \% p = (a^{p-1} \% p) \cdot (a^{p-1} \% p) \cdot 1 \cdot 1 \times (a^r) \% p$

k times

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

$(a^{p-1}) \% p = 1$

$a^{b!} \% p = (a^{r}) \% p$

$r = b! \% (p-1) \Rightarrow O(b)$

T.C: $O(b) + O(\log(b! \% p-1))$ (log a) → $O(\log p)$

$a^b \Rightarrow$ Fast Exponentiation. T.C: $O(\log b)$

$a^{b!} \Rightarrow$ T.C: $O(\log b!)$

$r = b! \% p-1$

```
ans = 1
for(i = 1; i <= b; i++)
    ans = (ans * i) % p-1
```

$b! \Rightarrow O(b)$

}

$10^8 = (10^9 \times 10^9) \% M \quad (10^9 \% M \times 10^9 \% M)$

$(10^9 \times 10^9)$

$M = 10^{9+7}$

$M \geq 10^9+7$ $< M$

→ $(10^9 \% M) = 10^9$

2) $(10^{20} \times 10^{20}) \%$

$M \geq 10^9+7$

3) $(10^9)^{20}$

→

$M \geq 10^9+7$

```
ans = 1
for(i = 1; i <= 20; i++){
    ans = (ans x 10^9) % M
}
```

Steps

1) ans = $(1 \times 10^9) \% M$
   = 10^9

2) ans = $(10^9 \times 10^9) \% M$
   = $(10^{18} \% M)$
   ↓
   $[0 \ldots M-1]$

yahnit.sirineni_1@scaler.com

$N = K \cdot P + r$

$r \in [0 \ldots P-1]$

value of r

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

we want

$N \% P = (KP + r) \% P$

$= (KP \% P + r \% P) \% P$

$k \cdot p$ $\%$ p $\quad r \in [0 \ldots p-1]$

$N \% p = (r \% p) \% p$

$r = N \% p$

$N = k \times p + r$

$(N \% p)$

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

$-2 \% 7 =$

$a \% m \Rightarrow$ Remainder when a/m divide by $[0 \ldots m-1]$

$-2 = (-1) \times 7 + 5$

$(-2 \% 7) = 5$

$-13 \% 7 =$

$-13 = (-2) \times 7 + 1$

k

$-13 \% 7 = 1$

$(0-2) \% 7 \Rightarrow$

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

$(0-2) \% M = [0 \% m - 2 \% m + m) \% m$

$m) \% M = 0$

(a-b) %

Aptitude

Finance / Banks

Assignments / HWs

27 steps

test

$p = 10^9 + 7$

$O(b)+$

$O(\log(b! \% p-1))$

$b = 10^6$

$\log(k)$

$k = \frac{b! \% p - 1}{(p-2)}$

$= 10^9$

$\log(10^9)$

$9 \times \log(10)$

$9 \times 3 =$ 27 steps

10^8 ops

$(a-b) \% M$

if $(a = b)$

$0 \% M =$ 0

Modulo Inverse of b wrt m only

if $gcd(b, m) = 1$

10^7

$10^9 + 7$

$10^7 + 3$

int : 2×10^9 ☺ Less no. of collision

ans % M ⇒ [0 .... M-1]

ans % M

ans % 10^7

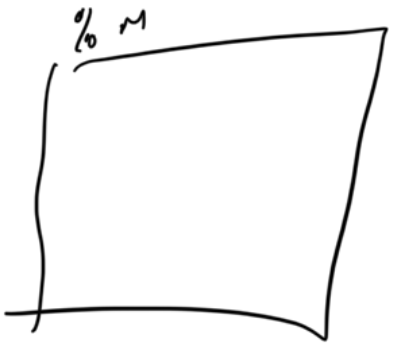
ans % 10^9

$10^9 + 7$

→ $(a+b)\%M = (a\%M + b\%M)\%M$

$(a-b)\%M$

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

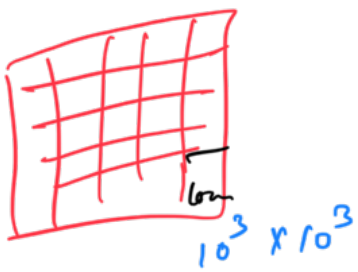


10^9 ⇒ 10^{10}

$1 \le N, M \le 1000$

⇒ $M = 10^3 \times 10^3$

$-10^5 \le A[i][j] \le 10^5$



10^6 element.

$10^6 \times 10^3 = 10^9$ → int?

$M = 10^9 + 7$ → $[0, M-1]$

$(a \cdot b) \% m = [a \% m \times b \% m) \% m$

$10^9 \times 10^9$

2) $(10^{18}) \% m$ → $[0, M-1]$

$(a \cdot b) \% M$

$M = 10^9 + 7$

$(a \times b) \% m$

$(100!) \% M$

```
long long ans = 1
for(i = 1; i <= 100; i++) {
    ans = (ans * i) % M;
}
```

long long int;

int ans — 32 bit

32 bit