তোমাকে যদি বলি, ৫ কে ৩ দ্বারা ভাগ করলে কত অবশিষ্ট থাকে, তুমি খুব সহজেই পারবে, তাই না? আর যদি ধরেও নিই, তুমি অঙ্কে অনেক কাঁচা (আমি বিশ্বাস করি, তুমি নও… ☺), তাও খাতা-কলম দিলেই পেরে যাবে। তুমি ক্লাস 1/2 তে যে ভাগ শিখেছ, সেটা করেই বলে দিবে, ৫ কে ৩ দিয়ে ভাগ করলে ২ অবশিষ্ট থাকে। এটাকে mathematically লিখা যায়,

```
৫ ≡ ২ (mod ৩)
```

“৫ কে ৩ দ্বারা ভাগ করলে কত অবশিষ্ট থাকে ? ” – এই প্রশ্নকেই অন্যভাবে বলা যায়, “৫ mod ৩ ≡ ?” এর মানে হল, ৫ কত এর equivalent, যখন কিনা ৩ দ্বারা ভাগ করে ভাগশেষ একই পাওয়া যায় ? এবার আমি যদি বলি, ২^৩ কে ৫ দ্বারা mod করলে কি পাব ? তখনও তুমি পারবে। ২^৩ মানে ৮। অর্থাৎ (৮ mod ৫) বের করতে বলা হয়েছে। উত্তর ৩। অর্থাৎ, (২^৩) mod ৫ ≡ ৩। তার মানে, যেকোন (a^p) mod m এর ভ্যালু তুমি বের করতে পার, তাই না? সত্যিই কি পারবে? যদি বলি, a & p হতে পারে ১০০০০০০০০, m হতে পারে ১০০০০০ কিংবা আরো বেশি, তখনো কি এত সহজে পারবে? হুম পারবে, আর এর জন্য যে এলগরিদম জানা লাগবে, সেটা হল, **Modular Exponentiation**, যাকে আমরা Big Mod নামেই বেশি চিনি। তোমার রিকার্শনের একদম বেসিক জ্ঞান থাকলে, এই এলগরিদম তোমার জন্য কোন ব্যাপারই না… ☺ এখন দেখব, এটি কিভাবে কাজ করে। এটি দেখার আগে কিছু ব্যাপার review করে নিই। ব্যাপারগুলো হয়ত আমরা জানি, তারপরও দেখা আর কি !!!

- (a*b)%m = ((a%m)*(b%m))%m
- (x^y)*(x^z) = x^(y+z)
- (x^y)^z = x^(yz)
- x^0 = 1

এখন, a=9, b=7, m=5 হলে (a*b)%m ≡ ((a%m)*(b%m))%m ⇒ (9*7)%5 ≡ ((9%5)*(7%5))%5 ⇒ (9*7)%5 ≡ (4*2)%5 ≡ 3 এবার কাজে আসা যাক। তোমাকে 3^10 বের করতে বললে, তুমি হয়ত লুপ চালিয়ে কিংবা pow() ব্যবহার করে linear complexity অর্থাৎ O(N) (এখানে N = সংখ্যার power) এ উত্তর বের করে ফেলতে পারবে। কিন্তু N যদি 10^9 বা তার বেশি হয়, তখন সেটা ভাল কোন solution না। এর পরিবর্তে আমরা log(N) complexity এর একটা solution দেখতে পারি। এখানে, log() বেস ২ এ। আমরা ক্যালকুলেটরে যেসব log() ভ্যালু পাই, সেগুলো বেস ১০ এ হিসাব করা হয়। বলা হয়েছিল, 3^10 বের করতে। 3^10 = $(3^5)^2$। এখন x = 3^5 হলে আমরা লিখতে পারি, 3^10 = x*x। তার মানে 3^10 বের করতে বললে 3^5 বের করলেই চলছে !!! 3^5 = 3*3^2*3^2। একটি বাড়তি ৩ গুণ করা প্রয়োজন হয়েছে, কারণ ৫ বিজোড়। 2 আর 2 যোগ করলে আমরা 4 পাই। এই বাড়তি ৩ গুণ করার কারণে বাম ও ডানপক্ষে ৩ এর power সমান হয়। 3^2 বের করতে বললে আমাকে জানতে হবে 3^1 কত। কারণ, 3^2 = 3^1*3^1। আর 3^1 বের করতে বললে আমাকে জানতে হবে 3^0 কত। আর সেটাতো আমরা জানিই !!! তাহলে দেখতে পারছি, 3^10 বের করতে বললে আমাকে 3^5, 3^2, 3^1 জানলেই চলছে !!! সাধারণভাবে লিখতে পারি,

```
x = a^(N/2);
```

যদি N জোড় হয়,

```
a = x*x
```

তা না হলে

```
a = x*x*a // N বিজোড় হলে বাড়তি a গুণ
```

এবার কোড দেখি...

```
int bmod(int a,int b,int m)

{

    if(b==0)

    return 1;

    int x=bmod(a,b/2,m);

    x=(x*x)%m;

    if(b%2==1)

    x=(x*a)%m;

    return x;

}
```

উপরের bmod() রিকার্সিব ফাংশনটি আমাকে (a^b)%m রিটার্ন করবে। রিকার্সনের প্রত্যেক স্টেটে x এ a^(N/2) সেভড হবে। আর যদি N বিজোড় হয়, তাহলে x এর সাথে আবার a গুণ হবে। উপরের উদহারণের জন্য, আমি b=10 নিয়ে bmod() এ যাব। এরপর b=5 এর জন্য আবার রিকার্সিবলি কল হবে। এভাবে, b=2, 1 ও 0 এর জন্য কল হবে। যখন b=0 হবে, তখন রিটার্ন করা শুরু হবে। m দিয়ে mod করার অর্থ কি? আমার উত্তর যাতে m থেকে ছোট ভ্যালু হয়। এখন, উপরের কোডে কোথায় কোথায় value m এর থেকে বেশি আসতে পারে ? দেখিঃ

```
x=(x*x)%m;
```

কিংবা

```
x=(x*a)%m;
```

তাই এই দুই ক্ষেত্রেই আমি m mod করেছি। যদি বুঝতে সমস্যা হয়, রিকার্সনের প্রতিটা স্টেট খাতা কলমে স্কেচ করার অনুরোধ রইল… ☺ আর reply option তো আছেই…… ☺ যদি পুরো পোস্টটি বুঝতে পারলে এই প্রবলেমগুলো করে দেখতে পার…

UVA 374

Spoj Short form of New Year