Modular Multiplicative Inverse

october 1, 2014, posted in algorithm, big mod, modular multiplicative inverse

তুমি **Big Mod** সম্পর্কে জেনে থাকলে এই পোস্টটি continue করতে পারো।

তুমি (a*b) কে mod করতে পার। যদি বলি, (a/b) কে m দিয়ে mod করতে ? তখন তোমাকে প্রথমে (b mod m) এর **Modular Multiplicative Inverse** বের করতে হবে। তারপর সেই ভ্যালুকে a এর সাথে modular multiplicative এর নিয়ম অনুযায়ী গুণ করতে হবে। অর্থাৎ, x=Modular Multiplicative Inverse of (b mod m) হলে,

```
(a/b)%m = ((a%m)*(x%m))%m
```

এই পোস্টে আমি বুঝানোর চেষ্টা করব, কিভাবে একটি নাম্বারের Modular Multiplicative Inverse বের করতে হয়।

ধরি, আমি (y mod m) এর Modular Multiplicative Inverse বের করব এবং তা হল x। তাহলে, লিখতে পারি,

$y \equiv x \pmod m$

একে আবার লিখা যায়,

```
yx = 1 (mod m)
```

অর্থাৎ, x তখনই (y mod m) এর Modular Multiplicative Inverse হবে, যখন $yx \equiv 1 \pmod m$ হবে।

এখন ব্যাপার হল, x কিভাবে বের করব। এই জন্য আমাদের **Fermat's Little Theorem** নামে একটা Theorem জানা লাগবে। এই Theorem অনুযায়ী,

যদি p একটি প্রাইম নাম্বার, a যেকোন integer হয় এবং a যদি p দিয়ে বিভাজ্য না হয়, তাহলে লিখা যায়,

```
a^(p-1) = 1 (mod p)
```

এটাকে আবার আমরা লিখতে পারি,

```
a*a^(p-2) = 1 (mod p)
```

অর্থাৎ, আমরা বলতে পারি, a এর Modular Multiplicative Inverse হচ্ছে a^(p-2)।

এখানেই লাগছে, Big Mod এর concept। আমরা যখন Modular Multiplicative Inverse এর কোন প্রবলেম সল্ভ করার চেষ্টা করি, তখন ছোট কোন প্রাইম নিই না (কারণ কি ?)। যার কারণে, (p-2) আসলে মোটামুটি বড় একটি নাম্বার (আমি চেষ্টা করি, p = 1000000007 রাখার)। এখন, a এর ভ্যালু ১ থেকে বড় যাই হোক, আমার (a^(p-2))%m বের করতে হলে, Big Mod ছাড়া আর কোন পথ নাই। 😉

এবার আসি কোড কেমন হবে...

যদি আমাকে (a/b)%m বের করতে বলে, আমাকে (b mod m) এর Modular Multiplicative Inverse বের করতে হবে। x=Modular Multiplicative Inverse of (b mod m) হলে, আমি bigMod() ফাংশনে পাঠাব,

```
b, p-2, m
```

যেখানে, b হচ্ছে যে নাম্বারের Modular Multiplicative Inverse বের করতে চাচ্ছি, p-2 হচ্ছে আমার সিলেক্ট করা প্রাইম থেকে ২ বিয়োগ করে যে সংখ্যা আসে তা আর m হচ্ছে যা দিয়ে mod করছি। এই ফাংশন আমাকে যা রিটার্ন করবে, তাই হচ্ছে Modular Multiplicative Inverse of (b mod m)।

```
int bigMod(int a,int b,int m) {
    if(b==0)
        return 1;
    int x=bigMod(a,b/2,m);
    x=(x*x)%m;
    if(b%2==1)
        x=(x*a)%m;
    return x;
}
```

যদি পুরা পোস্ট বুঝতে পারো, নিচের প্রবলেমটি করে ফেল।

Combinations

SHARE THIS:

Twitter Facebook LinkedIn Reddit WhatsApp Skype

Loading...

tagged algorithm, big-mod, modular-multiplicative-inverse

PREVIOUS POST
Big Mod

NEXT POST
UVA 106 : Fermat vs. Pythagoras

7 THOUGHTS ON "MODULAR MULTIPLICATIVE INVERSE"

sajib Khan
october1, 2014 at 4:54 pm

int x=bmod(a,b/2);
Is this line is right???

Reply

mukitmkbs
october2, 2014 at 2:09 am

Thanks...
Now, it's ok.. 😀

Reply

Pingback: বাংলায় প্রোগ্রামিং রিসোর্সসমূহ - Aditta Chakraborty

Pingback: বাংলায় প্রোগ্রামিং রিসোর্সসমূহ - Binary-Geek

Pingback: বাংলায় প্রোগ্রামিং রিসোর্সসমূহ - CSEian.com

Pingback: বাংলায় প্রোগ্রামিং রিসোর্সসমূহ ! - azomTech

Pingback: বাংলা প্রোগ্রামিং রিসোর্স- জেনে রাখা ভালো | প্রোগ্রামিং গরুসাফ

LEAVE A REPLY

Enter your comment here...

Algorithm Big-Mod Binary-Search BitSet C Codeforces Database GCD Java LeetCode Modular-Multiplicative-Inverse Number-Theory OOP Stream UVA

Select Language
Powered by Google Translate

BLOG STATISTICS

14,343 hits

Type your em SUBSCRIBE