New Method For Finding Modular Inverse

6

I was aware of using **a^(mod-2)%mod** and **extended euclidean** for finding modular inverse. But today, while solving CNTWAYS, I came across another method for finding modular inverse. The previous two methods were too slow and apparently this method is much faster.

This is what I found in the Tester's solution:

```
/* calculate all inverses of 1..8000000 mod MOD */
inv[1] = 1;
REP(i,2,800010) inv[i] = MOD - ((MOD/i)*inv[MOD%i]%MOD);
```

I found it interesting. So anybody has any idea how this code is actually working. Exactly what is this? I have never seen it before.

modular number-theory algorithm

asked **14 Jul '14, 13:00**

4★ forthright
[566]●4●12●17
accept rate: 10%

vai ami o kisu bujlam na. onek time pass korlam but still don't know how it works. @forthright

2★ robinmbstu12 (14 Jul '14, 14:52)

One Answer: oldest answers newest answers popular answers

4

There are three common ways of computing modular inverses. They have all been explained here: http://e-maxx.ru/algo/reverse_element It's a Russian website, so translate it to English, if needed.

link

answered **26 Jul '14, 18:43**

4★ aakashc31
[221]●3●4
accept rate: 27%

Thank you. I was looking for the proof.

4★ forthright (29 Jul '14, 14:02)