Primitive Root Modulo n

Leave a reply

Hey folks,
Today we are going to talk about the concept of *primitive root modulo n* and a codeforces problem on it.

Definition
x is a primitive root modulo of a number *n* if
for all 'a' such that 'a' is coprime to 'n' there exist a 'k' for which the following condition holds true.

x^k = a (mod n)

Actually the above condition can also be written in simpler words like :

let A is a set of all numbers coprime to 'n' and are less than 'n'
then for every 'x' in A if *multiplicative order* of 'x' is equal to the euler_totient_function(n) then 'x' is primitive root modulo 'n'.

Example:

Search

RECENT POSTS

Running Median
Diameter of a Tree
Range Minimum Query
Bridges a.k.a. Cut Edges
Articulation Points a.k.a. Cut Vertices

ARCHIVES

June 2014
September 2013
July 2013
June 2013
May 2013
March 2013

Example:
if n=14 then A= {1,3,5,9,11,13}

```
x x, x2, x3, ... (mod 14)
1 : 1
3 : 3, 9, 13, 11, 5, 1
5 : 5, 11, 13, 9, 3, 1
9 : 9, 11, 1
11 : 11, 9, 1
13 : 13, 1
```

only 'x' = 3 and 5 satisfied the given condition so they are primitive root modulo 'n'.

Note : It is possible that there is no primitive root modulo 'n' for example there is no primitive root modulo 'n' for 15.

Finally , the no of primitive root modulo 'n' of a give number are
euler_totient_function(euler_totient_function(n))

the problem on codeforces is also the same in which we have to calculate the no of primitive root modulo 'n'.

External Links:
My Solution
primitive root modulo
euler totient function
multiplicative order

return 42;

May 2012

CATEGORIES

Algorithms
Interview Questions
Linux

BLOG TO SHARE

Error: Not a valid Facebook Page url.

META

Register
Log in
Entries RSS
Comments RSS
WordPress.com

Share this:

Twitter Facebook

Like

Be the first to like this.

Related

Computing nCr
In "Algorithms"

Diameter of a Tree
In "Algorithms"

Josephus problem
In "Algorithms"

This entry was posted in Algorithms on March 18, 2013.

« Josephus problem

Computing nCr »

Leave a Reply

Enter your comment here...