Search: Go

Not logged in

Forum General C++ Programming Pollard's rho algorithm register log in

C++
Information
Tutorials
Reference
Articles
Forum

Forum
Beginners
Windows Programming
UNIX/Linux Programming
General C++ Programming
Lounge
Jobs

Pollard's rho algorithm

menopaws (25) Jan 29, 2012 at 4:23pm

Hi!

Trying to implement Polards Algorithm:
http://en.wikipedia.org/wiki/Pollard's_rho_algorithm

Cant really get it right tho,i get my "X" values right,but not "Y"´s..

```
#include <iostream>
#include <math.h>
#include <ctime>
using namespace std;
long long gcd(long long a,long long b)
{
return b==0?
a:gcd(b,a%b);
}
```

```
 1 int main()
 2 {
 3 
 4         long long n=115;
 5         long long y=2;
 6         long long x=2;
 7 
 8         long long d=1;
 9 
10 
11         //for(int i=0;i<3;i++)
12         //{
13         //      x=(x*x+1)%n;
14         //      y=(x*x+1)%n;
15 
16         //      d=gcd(n,x-y);
17 
18         //      cout<<"==========""turn "<<i<<endl;
19         //      cout<<"x: "<<x<<endl;
20         //      cout<<"y: "<<y<<endl;
21         //      cout<<"D: "<<d<<endl;
22 
23         //}
24         while(d>1&&d<n)
25         {
26                 x=(x*x+1)%n;
27                 y=(x*x+1)%n;
28                 d=gcd(n,x-y);
29         }
30         cout<<"Divisor:"<<d<<endl;
31 
32         return 0;
33 }
```

The outcommented for loop is just me checking X and Y values.
X values seem to be right,but X´s is off. "D" should be 5,with n=115.

Hope someone can help me out,thanks in advance!

Peter87 (4875) Jan 29, 2012 at 4:32pm

If you are implementing the algorithm in the wikipeida page you are doing a few things wrong.

Line 24 should be `while(d == 1)`

Line 27 is probably wrong. Note that they use f(f(y)) and not f(y).

line 28 you should use the absolute value of x-y.

menopaws (25) Jan 29, 2012 at 4:44pm

Yeah,i know it says d==1 on the wiki page,i was using my declaration cause it worked even when d is negative(because of my gcd function).

But using absolute value should take care of that:)

```
        while(d==1)
        {
                x=(x*x+1)%n;
                y=(x*x+1)%n;
                d=gcd(n,abs(x)-abs(y));
        }
```

Still dont know tho what i should about the Y value tho..

Last edited on Jan 29, 2012 at 4:46pm

Peter87 (4875) Jan 29, 2012 at 4:49pm

I think this is how it should be

```
while(d==1)
{
        x=(x*x+1)%n;
        y=((y*y+1) * (y*y+1) + 1)%n;
        gcd(n,abs(x - y));
}
```

It is probably more readable if you define the function f (name it whatever you want) and use that in your code.

menopaws (25) Jan 29, 2012 at 5:01pm

Dosent work:(

Oh well,gonna try it again later on..

menopaws (25) Jan 29, 2012 at 5:04pm

Actually it does,i get 23 as divisor,115/23=5.

Topic archived. No new replies allowed.

Home page | Privacy policy

Spotted an error? contact us