

```
long long f(long long x,long long c,long long n)
{
    return ((long long)x*x+c)%n;
}

long long PollardRho(long long x)
{
    long long s=0,t=0;
    long long c=rand()%(x-1)+1;
    long long val=1;
    int goal;
    for(goal=1;;goal<=1,s=t,val=1)
    {
        int step;
        for(step=1;step<=goal;++step)
        {
            t=f(t,c,x);
            val=val*abs(t-s)%x;
            if((step%127)==0)
            {
                long long d=gcd(val,x);
                if(d>1)
                {
                    return d;
                }
            }
        }
        long long d=gcd(val,x);
        if(d>1)
        {
            return d;
        }
    }
}
```

From:
<https://wiki.cvbbacm.com/> - CVBB ACM Team

Permanent link:
<https://wiki.cvbbacm.com/doku.php?id=2020-2021:teams:namespace:pollardrho%E7%AE%97%E6%B3%95%E6%9D%BF%E5%AD%90>

Last update: 2021/01/28 12:22

