

Разложение чисел на множители

Гаджиев Нурсултан Тофик оглы

2022 Moscow, Russia

RUDN University, Moscow, Russian Federation

Цель работы

Реализация алгоритма, реализующий р-метод Полларда.

Задачи

1. Реализовать алгоритм, реализующий p -метод Полларда.

Реализация

Функция pollarda для алгоритма полларда. (рис. 1)

```
main.py x +  
1  from math import gcd  
2  
3  def f(x,n):  
4      return (x*x +5)%n  
5  
6  def pollarda (n,a,b):  
7      a=f(a,n)%n  
8      b=f(b,n)%n  
9      d=gcd(a-b,n)  
10     if 1<d<n:  
11         p=d  
12         print(p, " является нетривиальным делителем числа: ",n)  
13         exit()  
14     if d==n:  
15         print("Делитель не найден")  
16     if d==1:  
17         pollarda(n,a,b)  
18  
19 c=1  
20 a=c  
21 b=c  
22  
23 pollarda(1359331,a,b)
```

Figure 1: Функция для алгоритма полларда

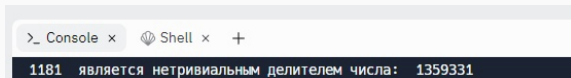


Figure 2: Результат алгоритма

Реализовал алгоритм, реализующий p -метод Полларда.

Спасибо за внимание