

Разложение чисел на множители

Воробьев Александр Олегович

2023 Moscow, Russia

RUDN University, Moscow, Russian Federation

Цель работы

Реализация алгоритма, реализующий р-метод Полларда.


Задачи

1. Реализовать алгоритм, реализующий p -метод Полларда.

Реализация

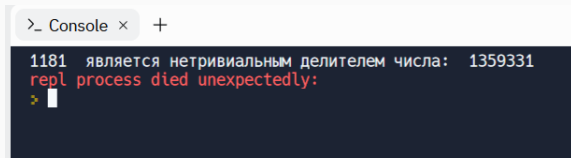
Реализация алгоритма Полларда

Функция pollarda для алгоритма полларда. (рис. -(fig:001?))



```
main.py × +
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(f(b,n),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)
```

Рис. 1: Функция для алгоритма полларда



A screenshot of a REPL console window. The window has a title bar with a prompt icon, the text ">_ Console", a close button (x), and a plus sign (+). The console area has a dark background. It displays the text "1181 является нетривиальным делителем числа: 1359331" in white. Below this, the text "repl process died unexpectedly:" is shown in red. At the bottom left of the console area, there is a yellow prompt character ">" followed by a white cursor block.

```
>_ Console × +  
1181 является нетривиальным делителем числа: 1359331  
repl process died unexpectedly:  
> █
```

Рис. 2: Результат алгоритма

Реализовал алгоритм, реализующий p -метод Полларда.

