

Отчёт по лабораторной работе 6

Разложение чисел на множители

Гебриал Ибрам Есам Зекри НФИ-02-22

Содержание

1	Цель работы	5
2	Теоретические сведения	6
3	Выполнение лабораторной работы	7
4	Выводы	8
5	Список литературы	9

List of Tables

List of Figures

3.1	Функция для алгоритма полларда	7
3.2	Результат алгоритма	7

1 Цель работы

Реализация алгоритма, реализующий р-метод Полларда.

2 Теоретические сведения

Один из простейших способов разложить число на простые множители – это проверить, делится ли данное число на 2, 3, 5, ... и т.д., т.е. проверить, делится ли число на ряд простых чисел. Если число n не делится ни на какое простое число до s , то данное число является простым, т.к. если число составное, то имеет по крайней мере два множителя и оба они не могут быть больше s .

Представим алгоритм разложения числа n на простые множители. Подготовим заранее таблицу простых чисел до s . Обозначим ряд простых чисел через p_1, p_2, \dots, p_k [1].

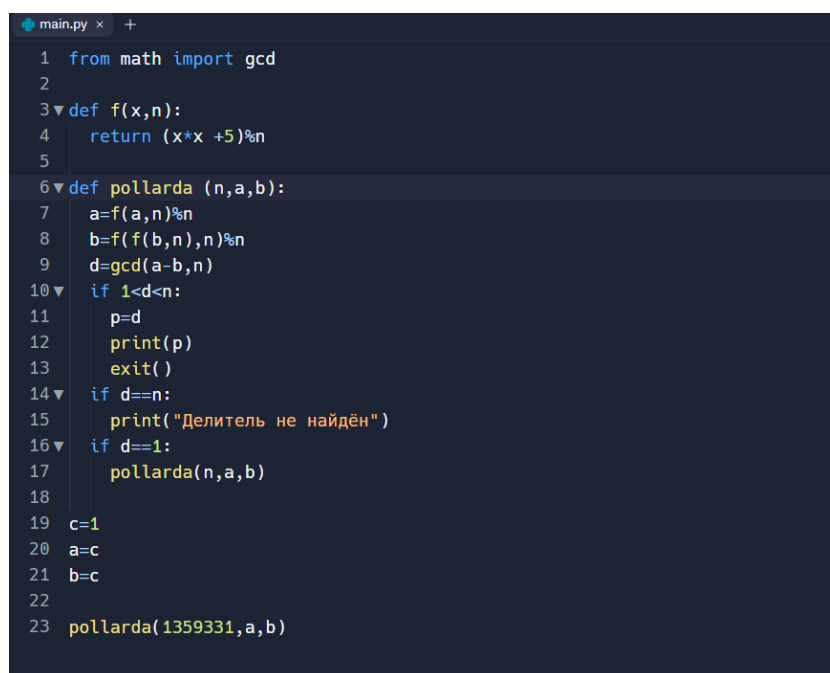
p-алгоритм Поллрада

- Вход. Число n , начальное значение c , функция f , обладающая сжимающими свойствами.
- Выход. Нетривиальный делитель числа n .

1. Положить $a = c, b = c$
2. Вычислить $a = f(a)(\text{mod } n), b = f(b)(\text{mod } n)$
3. Найти $d = \text{GCD}(a - b, n)$
4. Если $1 < d < n$, то положить $p = d$ и результат: p . При $d = n$ результат: ДЕЛИТЕЛЬ НЕ НАЙДЕН. При $d = 1$ вернуться на шаг 2.

3 Выполнение лабораторной работы

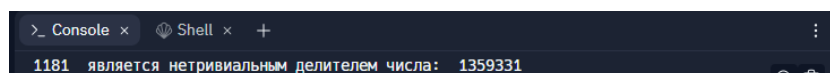
1. Написал функцию pollarda для алгоритма полларда. (рис. 3.1)



```
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)
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 3.1: Функция для алгоритма полларда

6. Получил результат (рис. 3.2)



```
>_ Console x Shell x +
1181 является нетривиальным делителем числа: 1359331
```

Figure 3.2: Результат алгоритма

4 Выводы

Реализовал алгоритм, реализующий р-метод Полларда.

5 Список литературы

1. Разложение числа на простые множители онлайн [Электронный ресурс] -
Режим доступа: <https://matworld.ru/teorija-chisel/razlozhenie-chisel.php>