

Отчет по лабораторной работе №6

**Дисциплина: Математические основы защиты информации и
информационной безопасности**

Сапёров Максим Александрович, НПМмд-02-22

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
3.1	Шаг 1	7
3.2	Шаг 2	7
4	Выводы	9

List of Figures

3.1	Реализация алгоритма, реализующего р-метод Полларда	7
3.2	Разложение на множители	8

List of Tables

1 Цель работы

Ознакомится и реализовать алгоритм разложения чисел на множители.

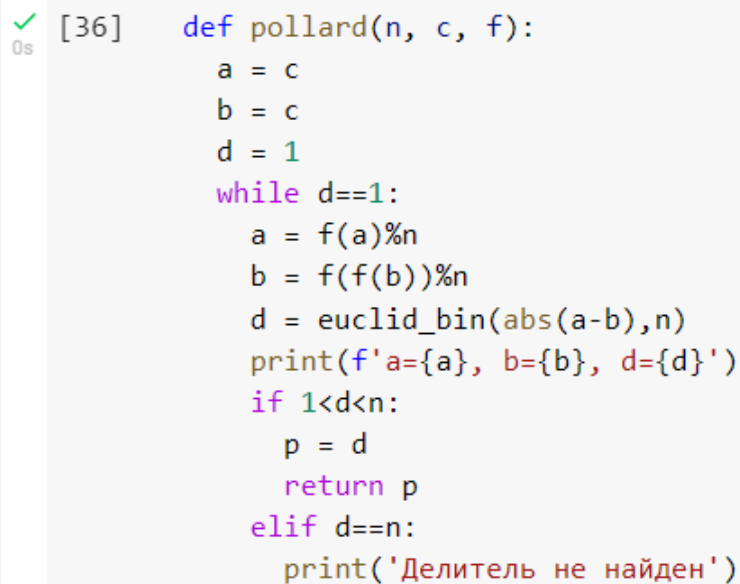
2 Задание

Реализовать программно алгоритм, реализующий р-метод Полларда.

3 Выполнение лабораторной работы

3.1 Шаг 1

Ознакомился с предоставленными теоретическими данными. Написал функцию Полларда



```
[36] def pollard(n, c, f):  
    a = c  
    b = c  
    d = 1  
    while d==1:  
        a = f(a)%n  
        b = f(f(b))%n  
        d = euclid_bin(abs(a-b),n)  
        print(f'a={a}, b={b}, d={d}')  
        if 1<d<n:  
            p = d  
            return p  
    elif d==n:  
        print('Делитель не найден')
```

Figure 3.1: Реализация алгоритма, реализующего р-метод Полларда

3.2 Шаг 2

Нашёл нетривиальный делитель

```
✓ [30] def test_f(x):  
0s      return x**2+5%1359331
```

```
✓ [37] pollard(1359331, 1, test_f)  
0s
```

```
a=6, b=41, d=1.0  
a=41, b=123939, d=1.0  
a=1686, b=391594, d=1.0  
a=123939, b=438157, d=1.0  
a=435426, b=582738, d=1.0  
a=391594, b=1144026, d=1.0  
a=1090062, b=885749, d=1181.0  
1181.0
```

Figure 3.2: Разложение на множители

4 Выводы

Ознакомился с алгоритмом, реализующем р-метод Полларда, и реализовал его программно.