

Отчет по лабораторной работе номер 6

Хамбалеев Булат Галимович

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение работы	7
4	Библиография	9
5	Выводы	10

List of Tables

List of Figures

3.1	рис.1. Евклид.	7
3.2	рис.2. Поллард.	7
3.3	рис.3. Проверка.	8

1 Цель работы

Реализовать алгоритм р-метода Полларда.

2 Задание

Задание подразумевает реализацию алгоритма р-метода Полларда.

3 Выполнение работы

1. Реализуем функцию алгоритма Евклида.(рис. 1)

```
Ввод [13]: def Euclead(a,b):  
    r = []  
    d = 0  
    if a>b:  
        r.append(a)  
        r.append(b)  
    else:  
        r.append(b)  
        r.append(a)  
    i=0  
    while True:  
        r.append(r[i]%r[i+1])  
        if r[-1]==0:  
            d=r[i+1]  
            break  
        i+=1  
    return d
```

Figure 3.1: рис.1. Евклид.

2. Реализуем алгоритм р-метода Полларда. (рис. 2)

```
Ввод [12]: from goto import with_goto  
from goto import goto, label  
@with_goto  
def Pollard(n,c,f):  
    a = c  
    b = c  
    label .begin  
    a = f(a)%n  
    b = f(b)%n  
    d = Euclead(a-b,n)  
    if 1<d<n:  
        p=d  
        return p  
    elif d == n:  
        return 'Делитель не найден'  
    elif d == 1:  
        goto .begin
```

Figure 3.2: рис.2. Поллард.

3. Проверим работу алгоритма.

```
Ввод [15]: def f(x):  
            return x**2 + 5%1359331  
            c = 1  
            Pollard(1359331,c,f)  
  
Out[15]: 1181  
  
Ввод [ ]:
```

Figure 3.3: рис.3. Проверка.

4 Библиография

1. ТУИС РУДН

5 Выводы

Во время выполнения лабораторной работы я на практике реализовал алгоритм р-метода Полларда.