

# Отчёт по лабораторной работе 6

---

Хамбалеев Булат Галимович

26 ноября, 2022

Реализовать алгоритм р-метода Полларда.

Задание подразумевает реализацию алгоритма р-метода Полларда.

# **Выполнение лабораторной работы**

---

# Выполнение лабораторной работы

## 1. Реализуем функцию алгоритма Евклида.

```
Ввод [13]: def Eucllead(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 1:** рис.1. Евклид.

## 2. Реализуем алгоритм р-метода Полларда.

```
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 = Eucllead(a-b,n)
                if 1<d<n:
                    p=d
                    return p
                elif d == n:
                    return 'Делитель не найден'
                elif d == 1:
                    goto .begin
```

**Figure 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:** рис.3. Проверка.

**Спасибо за внимание**