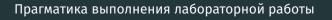
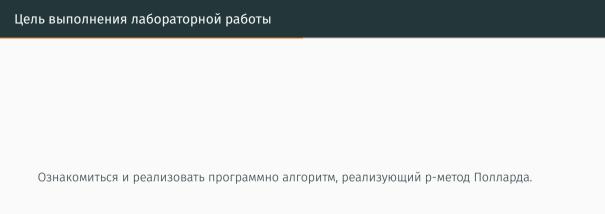
## Отчет по лабораторной работе 6

Дисциплина: Математические основы защиты информации и информационной безопасности

Сапёров Максим Александрович - студент группы НПМмд-02-22 08.01.2022



Приобретение практических навыков разложения чисел на множители.



## Задачи выполнения лабораторной работы

Реализовать программно алгоритм, реализующий р-метод 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 1cden:
                p = d
                return p
              elif d==n:
                print('Делитель не найден')
```

Figure 1: Реализация алгоритма, реализующего р-метод Полларда

## Задачи выполнения лабораторной работы

## Разложить число на множители

```
✓ [30] def test_f(x):
           return x**2+5%1359331
✓ [37] pollard(1359331, 1, test f)
       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
```



Результатом выполнения работы стала реализация алгоритма нахождения нетривиального делителя, что можно использовать для разложения числа на множители.