

Лабораторная работа №6.

Разложение чисел на множители

*Дисциплина: Математические основы защиты информации
и информационной безопасности*

Студент: Банникова Екатерина Алексеевна

Группа: НФИмд-02-23

2023, Москва

Цели и задачи работы

Целью данной лабораторной работы является ознакомление с алгоритмами для разложения чисел на множители.

1. Реализовать рассмотренный в инструкции к лабораторной работе алгоритм для разложения чисел на множители программно.
2. Разложить на множители данное в примере к лабораторной работе число.

Ход выполнения и результаты

```
n=1359331#ввели число n  
c=1#ввели начальное значение c
```

Figure 1: Входные данные для реализации алгоритма для разложения чисел на множители


Алгоритм, реализующий р-метод Полларда. Реализация

```
def f(x,n):  
    '''  
    ввод функции, обладающей сжимающими свойствами  
    '''  
    return (x**2+5)%n  
  
def algorithm_Evklida(a,b):  
    '''  
    Расписываем пункты 1-4 для алгоритма Евклида  
    '''  
    r=[]  
    r.append(a)  
    r.append(b)  
    i=1  
    while r[i]!=0:  
        i+=1  
        r.append(r[i-2]%r[i-1])  
    d=r[i-1]  
    return d
```

Figure 2: Реализация алгоритма р-метод Полларда

Алгоритм, реализующий р-метод Полларда. Реализация

```
def method_Pollarda(n,c):  
    #пункт 1  
    a=c  
    b=c  
    while True:  
        #пункт 2  
        a=f(a,n)%n  
        b=f(f(b,n),n)%n  
        #пункт 3  
        d=algorithm_Evklida(a-b,n)  
        #пункт 4  
        if 1<d<n:  
            p=d  
            return p  
        if d==n:  
            return 'Делитель не найден'  
method_Pollarda(n,c)
```

1181

Figure 4: Результат реализации алгоритма р-метод Полларда на примере

В результате выполнения данной лабораторной работы нам удалось осуществить программно алгоритм, рассмотренный в описании к лабораторной работе. А также получить ответ, совпадающий с ответом из инструкции.