

# РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

## ОТЧЕТ ПО

### ЛАБОРАТОРНОЙ РАБОТЕ №6

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

Студент: Хиссен Али Уэддей

Группа: НПМмд-02-20

Ст. билет № 1032209306

## Цель работы

Изучение алгоритм разложение чисел на множители..

## Теоретическая часть

---

Алгоритм, реализующий р-метод Полларда.

Вход. Число  $n$ , начальное значение  $s$ , функция  $f$ , обладающая сжимающими свойствами. Выход. Нетривиальный делитель числа  $n$ .

1. Положить  $a \leftarrow s$ ,  $b \leftarrow C$ .
2. Вычислить  $a \leftarrow f(a) \pmod n$ ,  $b \leftarrow f(b) \pmod n$
3. Найти  $d \leftarrow \text{НОД}(a - b, n)$ .
4. Если  $1 < d < n$ , то положить  $p \leftarrow d$  и результат:  $p$ . При  $d = n$  результат:  $\langle \langle \text{Делитель не найден} \rangle \rangle$ ; при  $d = 1$  вернуться на шаг 2.

Например : найти р-методом Полларда нетривиальный делитель числа  $n=1359331$ . Положим  $s = 1$  и  $f(x) = x^2 + 5 \pmod n$ .

## Метод квадратов. (Теорема Ферма о разложении)

Для любого положительного нечетного числа  $n$  существует взаимно однозначное соответствие между множеством делителей числа  $n$ , не меньших, чем  $\sqrt{n}$ , и множеством пар  $\{s, t\}$  таких неотрицательных целых чисел, что  $n = s^2 - t^2$ . Например . У числа 15 два делителя, не меньших, чем  $\sqrt{15}$ , — это числа 5 и 15. Тогда получаем два представления:

1.  $15 = pq = 3 \cdot 5$ , откуда  $s = 4$ , откуда  $t = 1$  и  $15 = 4^2 - 1^2$ ;
2.  $15 = pq = 1 \cdot 15$ , откуда  $s = 8$ , откуда  $t = 7$  и  $15 = 8^2 - 7^2$ .

## программная часть

---

1. Реализуем рассмотренный алгоритм программно.
2. Разложим на множители данное преподавателем число.

##Для начала импортируем функцию для вычисления наибольшего общего делителя двух целых чисел

**тут показано результат вызова функции**

```
: 1 #from AlorithmEuclidien
  2 from calcul_nod import*
  3 import math
```

```
: 1 AlorithmEuclidien(10,20)
```

НОД(a,b) = 10

```
: 10
```

введем функцию f(x) для дальнейшего вычисления

```
1 def Fonction_fx(x ,n):
  2     resultat=x**2 + 5%n
  3     return resultat
```

```
1 Fonction_fx(2,10)
```

9

**результата вызова функцию при заданом некоторый аргумент**

Альгоритм, реализующий р-метод Полларда

```
1 def AlgorithmPollard():
2     n = int(input('Введите n: '))
3     c = int(input('Введите c: '))
4     a=c
5     b=c
6
7     check=True
8
9     while(check):
10
11         a=Fonction_fx(a,n)%n
12
13         b=Fonction_fx(Fonction_fx(b,n),n)%n
14
15         d=AlgorithmEuclidien(a-b,n)
16
17         print ("a= ",a ,"b= ",b ,"d= ",d)
18
19         if d>1 and d<n:
20
21             p=d
22
23             print("Нетривиальный делитель равно\n",p)
24             check=False
25
26         elif d == n:
27
28             print(" делитель не найден")
29             break
30
31         else :
32
33             continue
34
```

результата вызова функцию, реализующая р-метод Полларда

Тогда пр  $n = 1359331$ , его нетривиальный делитель равно 1181

1	AlgorithmPollard()
---	--------------------

```
Введите n: 1359331
Введите c: 1
НОД(a,b) = 1
a= 6 b= 41 d= 1
НОД(a,b) = 1
a= 41 b= 123939 d= 1
НОД(a,b) = 1
a= 1686 b= 391594 d= 1
НОД(a,b) = 1
a= 123939 b= 438157 d= 1
НОД(a,b) = 1
a= 435426 b= 582738 d= 1
НОД(a,b) = 1
a= 391594 b= 1144026 d= 1
НОД(a,b) = 1181
a= 1090062 b= 885749 d= 1181
Нетривиальный делитель равно
1181
```

Алгоритм, реализующий метод Квадратов

```
n = int(input('Введите нечетное число n: '))
a=1
list=[]
while(a<=n):

    if(n%a==0):

        list.append(a)

    a+=2

k=0

for i in list:

    if i>math.sqrt(n):

        k+=1

print("тогда получаем {}".format(k),"представление")

for i in range(len(list)):

    for j in range(len(list)):

        if list[i]*list[j]==n:

            if list[i]>list[j]:

                s=int((list[i] + list[j])/2)

                t=int((list[i] - list[j])/2)

                print("{} можно преставит в виде {} -{}".format(n,s**2,t**2))
```

результат работы метода

```
33
34         print("{} можно преставит в виде {} -{}".format(n,s**2,t**2))
35
```

Введите нечетное число n: 75  
тогда получаем 3 представление  
75 можно преставит в виде 100 -25  
75 можно преставит в виде 196 -121  
75 можно преставит в виде 1444 -1369

**вывод** Мы изучали алгоритм для разложния чисел на множители..