

Защита лабораторной работы №6

Разложение чисел на множители

Асеинова Елизавета

23 ноября 2023

Российский университет дружбы народов, Москва, Россия

- Освоение *p-метода Полларда*, который является одним из алгоритмом разложения составного числа на множители
- Программная реализация представленного алгоритма разложения заданного числа на множители

Задача разложения на множители - одна из первых задач, использованных для построения криптосистем с открытым ключом.

Задача разложения составного числа на множители: для данного положительного целого числа n найти его разложение на два нетривиальных сомножителя:

$$n = pq, 1 \leq p \leq q < n$$

Алгоритм, реализующий р-метод Полларда

Вход. Число n , начальное значение c , функция f , обладающая сжимающими свойствами.

Выход. Нетривиальный делитель числа n .

- положить $a \leftarrow c, b \leftarrow c$
- вычислить $a \leftarrow f(a)(\text{mod } n), b \leftarrow f(b)(\text{mod } n)$
- найти $d \leftarrow (a - b, n)$
- если $1 < d < n$, то положить $p \leftarrow d$ и результат: p . При $d = n$ результат: “Делитель не найден”; при $d = 1$ вернуться на шаг 2

Постановка задачи:

- Реализовать алгоритм разложения числа на множители с помощью р-метода Полларда
- Разложить на множители заданное число

Результат выполнения лабораторной работы


Алгоритм, реализующий р-метод Полларда:

```
[ ] from math import gcd
    def add_func(x, n):
        return (x**2 + 5) % n

[ ] def Pollard(n, a, b, d):
    a = add_func(a,n)
    b = add_func(add_func(b, n), n)
    d = gcd(a-b, n)
    if 1 < d < n:
        print(d)
        exit()
    if d == n:
        print("Делитель не найден")
    if d == 1:
        Pollard(n, a, b, d)
```

Результат выполнения лабораторной работы

Пример реализации алгоритма:



```
#пример
def example():
    n = 1359331
    c = 1
    a = add_func(c, n)
    b = add_func(a, n)
    d = gcd(a-b, n)
    if 1 < d < n:
        print(d)
        exit()
    if d == n:
        pass
    if d == 1:
        Pollard(n,a,b,d)
```

```
[ ] example()
```

Выводы

1. Изучили метод Полларда разложения чисел на множители
2. Программно реализовали представленный алгоритм разложения чисел на множители
3. Разложили на множители заданное число