Защита лабораторной работы №6

Разложение чисел на множители

Бурдина К. П.

23 ноября 2023

Российский университет дружбы народов, Москва, Россия

Докладчик

* Бурдина Ксения Павловна
* студентка группы НФИмд-02-23
* студ. билет № 1132236896
* Российский университет дружбы народов
* 1132236896@rudn.ru

Вводная часть

Цель выполнения лабораторной работы

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

Теоретические сведения

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*:

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

Алгоритм, реализующий p-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 $a \leftarrow f(a)(mod\, n)$, $b \leftarrow f(b)(mod\, n)$
- 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

Найти нетривиальный делитель числа $n = 1359331$, если $c = 1$ и $f(x) = x^2 + 5(mod\, n)$. Работа алгоритма иллюстрируется следующей таблицей:

i	*a*	*b*	*d* = НОД(*a* - *b*, *n*)
	1	1	
2	6	41	1
2	41	123939	1
3	1686	391594	1
4	123939	438157	1
5	435426	582738	1
6	391594	1144026	1
7	[illegible]	[illegible]	[illegible]

Результат выполнения лабораторной работы

Результат выполнения лабораторной работы

Постановка задачи:

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

Алгоритм, реализующий р-метод Полларда:

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

```
def Pollard(n, a, b, d):
    a = f(a, n)
    b = f(f(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)
```

Рис. 2: р-метод Полларда

Пример реализации алгоритма:

```
def prim():
    n = 1359331
    c = 1
    a = f(c, n)
    b = f(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)
```

```
prim()
```

```
1181
```

Рис. 3: Пример реализации

Выводы

Выводы

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