

Математические основы защиты информации и информационной безопасности. Лабораторная работа №6

Разложение чисел на множители

Студент: Масолова Анна Олеговна НФИмд-02-21

Преподаватель: Кулябов Дмитрий Сергеевич

Содержание

1	Цель работы	5
2	Задачи	6
3	Теоретические сведения	7
3.1	Р-метод Полларда	8
4	Выполнение работы	9
4.1	Реализация алгоритмов	9
4.2	Пример работы р-метода Полларда	10
5	Выводы	11
	Список литературы	12

List of Figures

3.1	Зацикливание числовой последовательности	8
4.1	Пример работы р-метода Полларда	10

List of Tables

1 Цель работы

Изучение алгоритма разложения составного числа на множители.

2 Задачи

Реализовать программно алгоритм, реализующий р-метод Полларда.

3 Теоретические сведения

Любое натуральное число $n > 1$ можно представить в виде произведения простых чисел. Это представление называется разложением числа n на простые множители. [1]

P-алгоритм Полларда строит числовую последовательность, элементы которой образуют цикл, начиная с некоторого номера n , что может быть проиллюстрировано, расположением чисел в виде греческой буквы p , что послужило названием семейству алгоритмов. Иллюстрацию этого алгоритма на плоскости можно увидеть на рис. 3.1

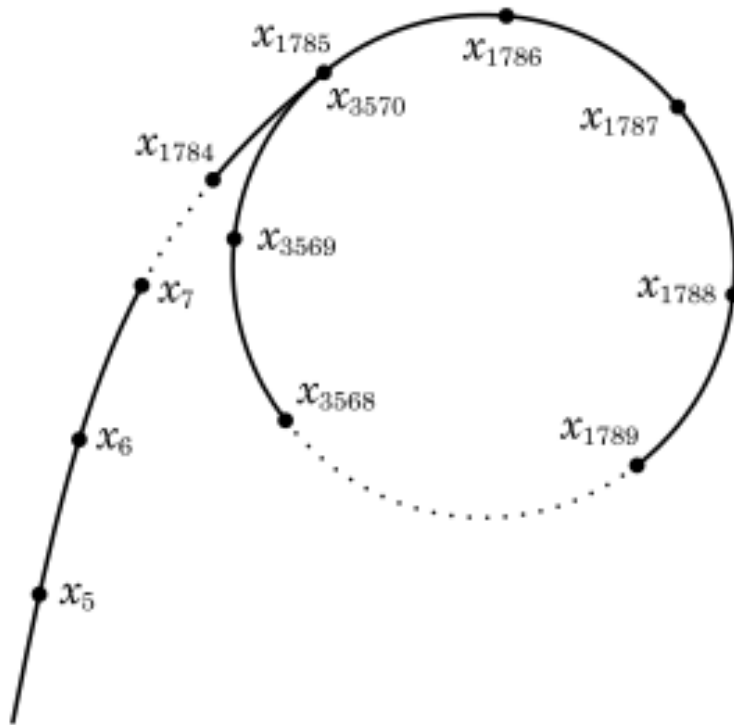


Figure 3.1: Зацикливание числовой последовательности

3.1 Р-метод Полларда

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

1. Положить $a = c, b = c$
2. Вычислить $a = f(a)(\text{mod } n), b = f(b)(\text{mod } n)$
3. Найти $d = (a - b, n)$
4. Если $1 < d < n$, то положить $p = d$ и результат: p . При $d = n$ результат: “Делитель не найден”; при $d = 1$ вернуться на шаг 2.

Подробнее об алгоритме: [2]

4 Выполнение работы

4.1 Реализация алгоритмов

```
def euclid(a, b):  
    r = []  
    r.append(a)  
    r.append(b)  
    i = 1  
    while True:  
        r.append(r[i - 1] % r[i])  
        if r[i + 1] == 0:  
            d = r[i]  
            return d  
        else:  
            i = i + 1
```

```
def pollard(n, c):  
    a = c  
    b = c  
    while True:  
        a = f(a, n) % n  
        b = f(f(b, n), n) % n
```

```

first = min(a - b, n)
second = max(a - b, n)
d = euclid(first, second)
if d > 1 and d < n:
    p = d
    return p
elif d == n:
    return -1
elif d == 1:
    continue

def f(x, n):
    return (x ** 2) + 5 % n

n = int(input("Введите число n: "))
c = int(input("Введите число c: "))
result = pollard(n, c)
print("Нетривиальный делитель числа n = {}".format(result))

```

4.2 Пример работы р-метода Полларда

На рис. 4.1 представлены результаты работы р-метода Полларда:

```

Введите число n: 1359331
Введите число c: 1
Нетривиальный делитель числа n = 1181

```

Figure 4.1: Пример работы р-метода Полларда

5 Выводы

В ходе выполнения работы был успешно изучен р-метод Полларда, а также был реализован программно программно на языке Python.

Список литературы

1. Разложение числа на множители онлайн [Электронный ресурс]. umath, 2021. URL: <https://umath.ru/calc/factorization/>.
2. Ро-алгоритм Полларда [Электронный ресурс]. Википедия, 2021. URL: https://ru.wikipedia.org/wiki/Ро-алгоритм_Полларда.