

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

Разложение чисел на множители

Лесков Данила Валерьевич: НФИмд-02-21

Преподаватель: Кулябов Дмитрий Сергеевич

11 декабря, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритма разложения составного числа на множители.

Реализовать программно алгоритм, реализующий р-метод Полларда

Выполнение лабораторной работы

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

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.

Иллюстрация р-алгоритма Полларда

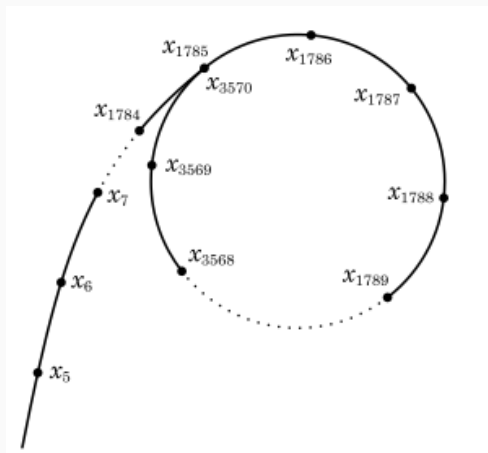


Figure 1: Зацикливание числовой последовательности

- 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.

Пример работы р-алгоритма Полларда

```
C:\Users\afsb\AppData\Local\Programs\Python\Python37\python.exe
Введите число n: 1359331
Введите число c: 1
Нетривиальный делитель числа n = 1181
Process finished with exit code 0
```

Figure 2: Пример работы р-алгоритма Полларда

Выводы

Результаты выполнения лабораторной работы

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