Отчёт по лабораторной работе №6

Разложение чисел на множители

Милёхин Александр НПМмд-02-21

Содержание

List of Figures

1 Цель работы

Изучение задачи разложения на множители, изучение p-алгоритма Полларда.

2 Теоретические сведения

Разложение на множители — предмет непрерывного исследования в прошлом;и такие же исследования, вероятно, продолжатся в будущем. Разложение на множители играет очень важную роль в безопасности некоторых криптосистемс открытым ключом.

Согласно Основной теореме арифметики любое положительное целое числобольше единицы может быть уникально записано в следующей главной форме разложения на множители, где $p_1, p_2, \ldots, p_k$ — простые числа и $e_1, e_2, \ldots, e_k$ — положительные целые числа.

$$n = p_1^{e^1} * p_2^{e^2} * \ldots * p_k^{e^k}$$

Поиск эффективных алгоритмов для разложения на множители больших составных чисел ведется давно. К сожалению, совершенный алгоритм для этого пока не найден. Хотя есть несколько алгоритмов, которые могут разложить число на множители, ни один не способен провести разложение достаточно больших чисел в разумное время. Позже мы увидим, что это хорошо для криптографии, потому что современные криптографические системы полагаются на этот факт. В этой секции мы даем несколько простых алгоритмов, которые проводят разложение составного числа. Цель состоит в том, чтобы сделать процесс разложения на множители менее трудоёмким.

В 1974 г. Джон Поллард разработал метод, который находит разложение числа p на простые числа. Метод основан на условии, что p–1 не имеет сомножителя, большего, чем заранее определенное значение B, называемое границей.

Алгоритм Полларда показывает, что в этом случае

$$p = GCD(2^{B!} - 1, n)$$

Сложность. Заметим, что этот метод требует сделать $B-1$ операций возведения в степень $a = a^e mod n$. Есть быстрый алгоритм возведения в степень, который выполняет это за $2 * log_2 B$ операций. Метод также использует вычисления НОД, который требует n^3 операций. Мы можем сказать, что сложность — так или иначе больше, чем $O(B)$ или $O(2^n)$, где n_b — число битов в B. Другая проблема – этот алгоритм может заканчиваться сигналом об ошибке. Вероятность успеха очень мала, если B имеет значение, не очень близкое к величине $\sqrt{n}$.

2.1 p-алгоритм 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 $a = f(a)(mod n), b = f(b)(mod n)$
3. Найти $d = GCD(a - b, n)$
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.

3 Выполнение работы

3.1 Реализация алгоритмов на языке Python

```
from math import gcd


ag = 1
bg = 1


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


def method(n, a, b, d):
    a = f(a, n)%n
    b = f(f(b,n), n)%n
    d =  gcd(a-b,  n)
    if 1 < d < n:
        p = d
        print(p)
        exit()
    if d == n:
        print("Делитель не найден")
    if d == 1:
        global ag
```

```
        ag = b
        method(n, a, b, d)

def main():
    n = 1359331
    c = 1
    a = c
    b = c
    a  =  f(a,  n)%n
    b  =  f(a,  n)%n
    d = gcd(a-b, n)
    if 1 < d < n:
        p = d
        print(p)
        exit()
    if d == n:
        pass
    if d == 1:
        method(n, a, b, d)

main()
```

3.2 Контрольный пример

```python
            print("Делитель не найден")
        if d == 1:
            global ag
            ag = b
            method(n, a, b, d)

def main():
    n = 1359331
    c = 1
    a = c
    b = c
    a = f(a, n)%n
    b = f(a, n)%n
    d = gcd(a-b, n)
    if 1 < d < n:
        p = d
        print(p)
        exit()
    if d == n:
        pass
    if d == 1:
        method(n, a, b, d)
```

```
In [2]: main()

1181
```

Figure 3.1: Пример работы алгоритма

Таким образом, число 1181 является нетривиальным делителем числа 1359331.

4 Выводы

Я изучил задачу разложения на множители и p-алгоритм Полларда, а также реализовал данный алгоритм программнона языке Python.

Список литературы

1. Алгоритмы тестирования на простоту и факторизации
2. Р-метод Полларда