Отчет по лабораторной работе №6

Разложение чисел на множители

Бармина Ольга Константиновна

2024 September 7th

Содержание

1 Цель работы **4**

2 Задание **5**

3 Теоретическое введение **6**

4 Выполнение лабораторной работы **7**

5 Выводы **9**

6 Список литературы **10**

List of Figures

4.1 Реализация метода Полларда 8

1 Цель работы

Целью данной работы является освоение *p-метода Полларда*, который является одним из алгоритмом разложения составного числа на множители.

2 Задание

1. Изучить алгоритм разложения чисел на множители.
2. Реализовать представленный алгоритм и разложить на множители заданное число.

3 Теоретическое введение

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

Задача разложения составного числа на множители формулируется следующим образом: для данного положительного целого числа *n* найти его каноническое разложение $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_s^{\alpha_s}$, где p_i - попарно различные простые числа, $\alpha_i \geqslant 1$.

На практике не обязательно находить каноническое разложение числа *n*. Достаточно найти его разложение на два *нетривиальных сомножителя*: $n = pq, 1 \leqslant p \leqslant q < n$. Далее будем понимать задачу разложения именно в этом смысле.

p-Метод Полларда. Пусть *n* - нечетное составное число, $S = 0, 1, ..., n-1$ и $f : S \to S$ - случайное отображение. обладающее сжимающими свойствами. например. $f(x) \equiv x^2 + 1 \ (mod\ n)$. Основная идея метода состоит в следующем. Выбираем случайный элемент $x_0 \in S$ и строим последовательность $x_0, x_1, x_2, ...$, определяемую рекуррентным соотношением

$$x_{i+1} = f(x_i),$$

где $i \geqslant 0$, до тех пор, пока не найдем такие числа i, j, что $i < j$ и $x_i = x_j$. Поскольку множество S конечно, такие индексы i, j существуют (последовательность “зацикливается”) [2]. Последовательность $\{x_i\}$ будет состоять из “хваста” $x_0, x_1, ..., x_{i-1}$ длины $O\left(\sqrt{\frac{\pi n}{8}}\right)$ и цикла $x_i = x_j, x_{i+1}, ..., x_{j-1}$ той же длины.

4 Выполнение лабораторной работы

Для реализации рассмотренного алгоритма разложения чисел на множители используется среда Google Colab.

1. Запишем алгоритм, реализующий *p-метод Полларда*. Проверим корректность работы алгоритма для заданных сведений. Для этого запишем условие примера с помощью следующей функции:

При вызове данной функции видим, что получаем то же число, что было описано в примере. То есть 1181 является нетривиальным делителем числа 1359331.

```python
n = 1359331
c = 1
def f(x, n):
    return (x**2 + 5)%n
```

```python
def pollard(n, a, b, f):
    a = f(a, n)
    b = f(f(b, n), n)

    c = a - b
    d = n
    if c < 0:
        d1 = 0
    else:
        while c!=0 and d!=0:
            if c>=d:
                c = c%d
            else:
                d = d%c
        d1 = c or d
    print(a, b, d1)

    if 1 < d1 < n:
        return d1
    elif d1 == n:
        return 'делитель не найден'
    else:
        pollard(n, a, b, f)
```

```python
pollard(n, c, c, f)
```

```
6 41 0
41 123939 0
1686 391594 0
123939 438157 0
435426 582738 0
391594 1144026 0
1090062 885749 1181
```

Figure 4.1: Реализация метода Полларда

5 Выводы

В ходе работы мы изучили и реализовали вероятностные алгоритмы проверки чисел на простоту.

6 Список литературы

1. Фороузан Б. А. Криптография и безопасность сетей. - М.: Интернет-Университет Информационных Технологий : БИНОМ. Лаборатория знаний, 2010. - 784 с. [1]

2. Методические материалы курса [2]