Лабораторная работа №6

Математические основы защиты информации и информационной безопасности

Минов К. В., НПМмд-02-23 25 ноября 2023

Российский университет дружбы народов

Москва, Россия

Цель лабораторной работы

Реализовать на языке программирования р-метод Полларда

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

На практике необязательно находить каноническое разложение числа n. Достаточно найти его разложение на два нетривиальных сомножителя: $n = pq$, $1 \leq p \leq q < n$.

Теоретическое введение

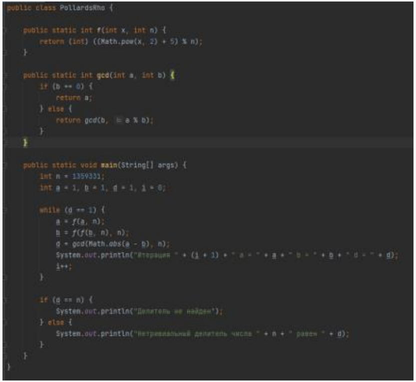
p- метод Полларда. Пусть n - нечетное составное число, $S = \{0, 1, ..., n - 1\}$ и $f : S \rightarrow S$ - случайное отображение, обладающее сжимающими свойствами, например, $f(x) \equiv (x^2 + 1)(mod\ n)$. Основная идея метода состоит в следующем. Выбираем случайный элемент $x_0 \in S$ и строим последовательность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

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

где $i \geq 0$, 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 $\{x_i\}$ будет состоять из "хвоста" $x_0, x_1, ..., x_{i-1}$ длины $O(\sqrt{\frac{\pi n}{8}})$ и цикла $x_i = x_j, x_{i+1}, ..., x_{j-1}$ той же длины.

Ход выполнения лабораторной работы

- Реализуем р-метод Полларда



```java
public class PollardsRho {

    public static int f(int x, int n) {
        return (int) ((Math.pow(x, 2) + 5) % n);
    }

    public static int gcd(int a, int b) {
        if (b == 0) {
            return a;
        } else {
            return gcd(b, a % b);
        }
    }

    public static void main(String[] args) {
        int n = 1359331;
        int a = 1, b = 1, d = 1, i = 0;

        while (d == 1) {
            a = f(a, n);
            b = f(f(b, n), n);
            d = gcd(Math.abs(a - b), n);
            System.out.println("Итерация " + (i + 1) + " a = " + a + " b = " + b + " d = " + d);
            i++;
        }

        if (d == n) {
            System.out.println("Делитель не найден");
        } else {
            System.out.println("Нетривиальный делитель числа " + n + " равен " + d);
        }
    }
}
```

Figure 1: Рис.1: р-метод Полларда

Вывод

- В ходе выполнения данной лабораторной работы был реализован p-метод Полларда