Лабораторная работа №6

Математические основы защиты информации и информационной безопасности

Минов Кирилл Вячеславович | НПМмд-02-23

Содержание

1 Цель работы

Реализовать на языке программирования p-метод Полларда.

2 Теоретическое введение

Задача разложения составного числа на множители формулируется следующим образом: для данного положительного целого числа n найти его каноническое разложение $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, 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:* $n = pq, 1 \leq p \leq q < n$.

3 Выполнение лабораторной работы

Реализуем метод Полларда:

На вход подается число n, начальное значение c, функция f, обладающая сжимающими свойствами.

1. Положить $a \leftarrow c, b \leftarrow c$.
2. Создать функцию $f(x, n) = (x^2 + 5)(mod\ n)$
3. Вычислить $a \leftarrow f(a, n), b \leftarrow f(f(b, n), n)$.
4. Найти $d \leftarrow$ НОД $(a - b, n)$
5. Если $1 < d < n$, то положить $p \leftarrow d$ и результат: p. При $d = n$ результат: “Делитель не найден”; при $d = 1$ вернуться на шаг 2.

Код программы (рис. 1).

```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,  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);
        }
    }
}
```

Рис. 1: p-метод Полларда

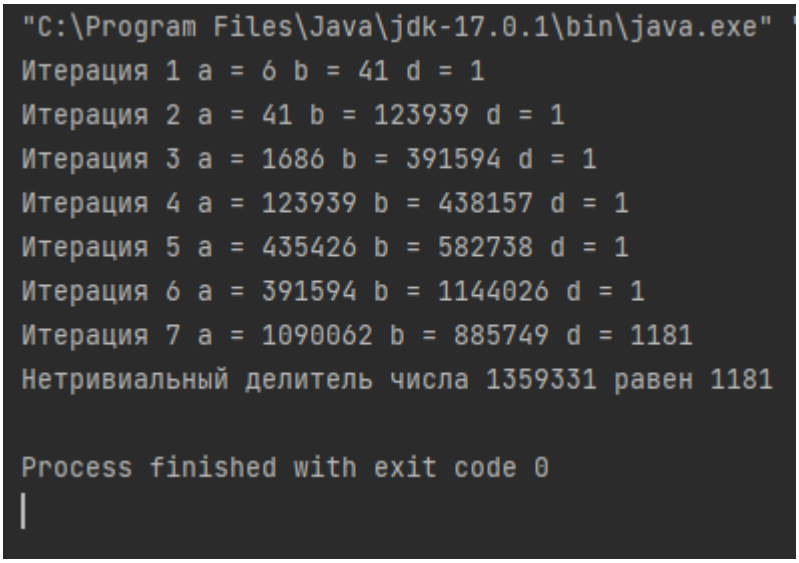

Рис. 2: p-метод Полларда

4 Выводы

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

Список литературы

1. p-метод Полларда [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Pollard%27s_rho_algorithm.