Отчет по лабораторной работе по предмету Математические основы защиты информации и информационной безопасности

Лабораторная работа №6. Разложение чисел на множители

Никита Андреевич Топонен

Содержание

Список иллюстраций

1 Цель работы

Цель работы — изучить алгоритм поиска нетривиального делителя числа.

2 Задание

- Реализовать алгоритм, реализующий p-метод Полларда.

3 Теоретическое введение

ρ-алгоритм — предложенный Джоном Поллардом в 1975 году алгоритм, служащий для факторизации (разложения на множители) целых чисел. Данный алгоритм основывается на алгоритме Флойда поиска длины цикла в последовательности и некоторых следствиях из парадокса дней рождения. Алгоритм наиболее эффективен при факторизации составных чисел с достаточно малыми множителями в разложении.

4 Выполнение лабораторной работы

4.1 Алгоритм, реализующий p-метод Полларда

В рамках данной лабораторной работы я реализовал алгоритм p-метода Полларда на языке Java. Ниже приведен код:

```
private static Long pMethod(Long n, Long c) {
    Long a = c;
    Long b = c;
    Long d = 1L;

    while (d.equals(1L)) {
        a = f(a) % n;
        b = f(f(b)) % n;
        if (b < 0) b += n;
        d = GCD(abs(a - b), n);

        System.out.printf("a = %s; b = %s; d = %s%n", a, b, d);

        if (1 < d && d < n) {
            return d;
        } else if (d.equals(n)) {
            throw new RuntimeException(String.format("Divider for %s not found",
        }
```

```
        }

        return 0L;
    }

    private static Long f(Long x) {
        return x*x + 5;
    }

    private static Long GCD(Long a, Long b) {
        if (b == 0) {
            return a;
        }
        return GCD(b, a % b);
    }
```

4.2 Проверка работы

С помощью алгоритма нашел нетривиальный делитель числа 1359331, равный 1181:

```
a = 443380; b = 861686; d = 1
a = 734516; b = 422524; d = 1
a = 717685; b = 484980; d = 1
a = 853365; b = 505943; d = 1
a = 145262; b = 198046; d = 1
a = 153536; b = 1188092; d = 1181
Result is 1181
```

Рис. 4.1: Результат работы программы

5 Выводы

В рамках данной лабораторной работы я изучил и реализовал на языке Java алгоритм поиска нетривиального делителя числа, также известный как ρ-метод Полларда.

Список литературы