Лабораторная работа №6

Разложение чисел на множители

Топонен Н. А.

18 ноября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Топонен Никита Андреевич
- студент Российского университет дружбы народов
- 1132236933@rudn.ru
- https://github.com/natoponen

Вводная часть

Цель работы

- Изучить алгоритм поиска нетривиального делителя числа.

Задание

Реализовать алгоритмы:

- Реализовать алгоритм, реализующий ρ-метод Полларда.

Теоретическое введение

ρ-алгоритм

- ρ-алгоритм — предложенный Джоном Поллардом в 1975 году алгоритм, служащий для факторизации (разложения на множители) целых чисел.
- В данной лабораторной работе рассматривается вариация ρ-алгоритма, предложенная Флойдом.

Выполнение лабораторной работы

Сжимающая функция f

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

Функция поиска НОД

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

Реализация ρ-метода

```
Long a = c;
Long b = c;
Long d = 1L;
```

Реализация ρ-метода

```
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", n));
    }
```

Результат работы алгоритма

```
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. 1: Результат работы алгоритма

Выводы

- Изучил и реализовал вероятностные алгоритм поиска нетривиального делителя числа, также известный как ρ-метод Полларда.