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

Лабораторная работа №6. Разложение чисел на множители

Никита Андреевич Топонен

Содержание

# 1 Цель работы

Цель работы — изучить алгоритм поиска нетривиального делителя числа.

# 2 Задание

* Реализовать алгоритм, реализующий p-метод Полларда.

# 3 Теоретическое введение

p-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

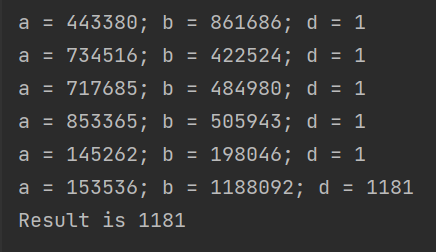
## 4.1 Алгоритм, реализующий p-метод Полларда

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", n));  
 }  
 }  
  
 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:



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 p-метод Полларда.

# Список литературы