Лабораторная работа №6

Дисциплина: Математические основы защиты информации и информационной безопасности

Аветисян Давид Артурович

Содержание

# 1 Цель работы

Реализовать алгоритм, реализующий p-метод Полларда.

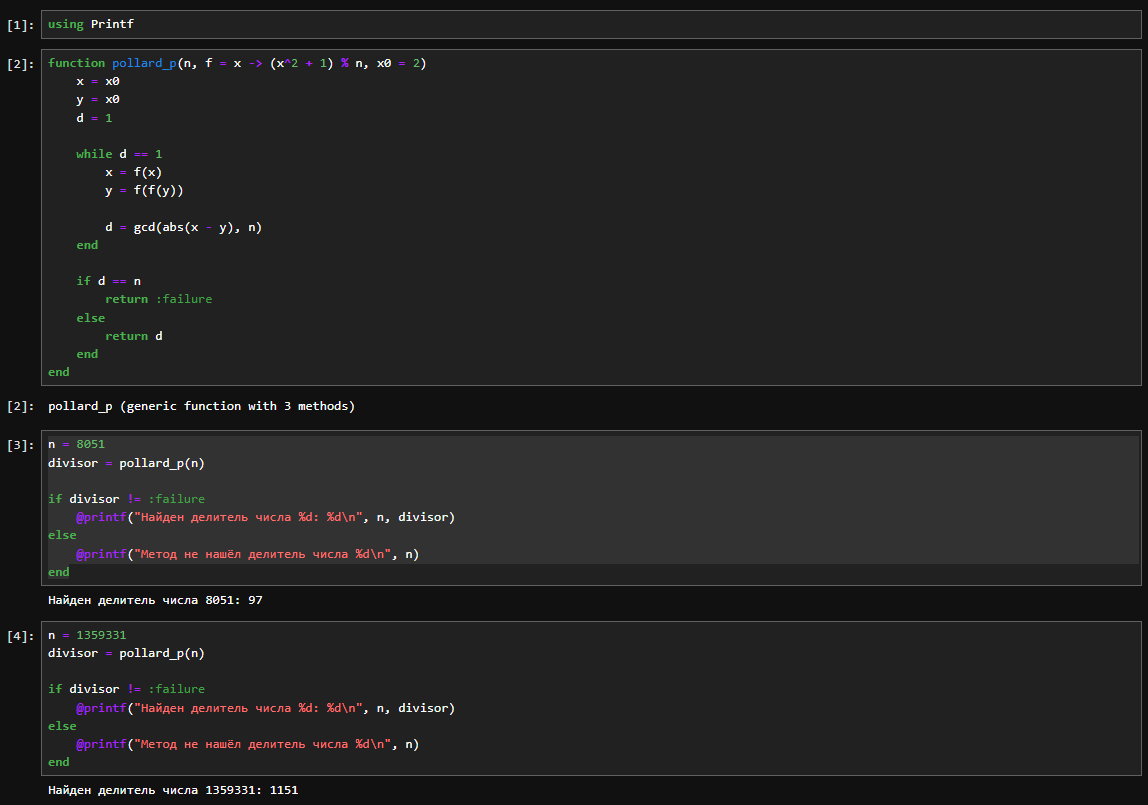
# 2 Задание

1. Реализовать алгоритм, реализующий p-метод Полларда.
2. Разложить на множители данное преподавателем число.

# 3 Выполнение лабораторной работы

Данная работа была выполнена на языке Julia.

Для реализации алгоритм, реализующего p-метод Полларда, была написана следующая программа.



Алгоритм, реализующий p-метод Полларда, на языке Julia

В данной программе:  
- 1-й блок. Импорт необходимых модулей  
- 2-й блок. Реализация самого алгоритма: Задаются начальные значения и и НОД . С помощью цикла вычисляется медленный и быстрый шаги и . Затем они сравниваются, чтобы найти НОД. В конце проверяется результат выполнения алгоритма.  
- 3-й блок. Задаётся значение , для которого нужно найти делитель и вызывается функция, описанная выше.  
- 4-й блок. Вывод ответа в зависмости от результат выполнения алгоритма.

Мы можем видеть результат для чисел 8051 и 1359331 (данное преподавателем число) на рисунке выше. Программа работает верно.

# 4 Выводы

Я реализовал алгоритм, реализующий p-метод Полларда.