Лабораторна работа № 6

Разложение чисел на множители

Покрас Илья Михайлович

Содержание

Список иллюстраций

1 Цель работы

Реализовать алгоритм разложения чисел на множители.

2 Задание

Реализовать алгоритм, реализующий ρ-метод Полларда.

3 Теоретическое введение

ρ-алгоритм Полларда — предложенный Джоном Поллардом в 1975 году алгоритм, служащий для факторизации (разложения на множители) целых чисел. ρ-алгоритм строит числовую последовательность, элементы которой образуют цикл, начиная с некоторого номера n, что может быть проиллюстрировано, расположением чисел в виде греческой буквы , что послужило названием семейству алгоритмов

4 Выполнение лабораторной работы

Я создал функцию алгоритма, реализующего ρ-метод Полларда, принимающий число для разложения n и начальное значение c. Далее я задал число для разложения множителей, вызвал функцию и вывел полученные данные (рис. 4.1).

```
function pollard_rho(n, c)
    f(x)=(x^2+5) % n
    a = c
    b = c

    while true
        a = f(a)
        b = f(f(b))
        d = gcd(a - b, n)
        println("$a, $b, $d")

        if 1 < d < n
            return d
        elseif d == n
            return "Error"
        end
    end
end

n = 1359331
factor = pollard_rho(n, 1)
println("Non-trivial factor of $n: $factor")
```

Рис. 4.1: Функция ρ-метода Полларда

И получил следующий результат (рис. 4.2).

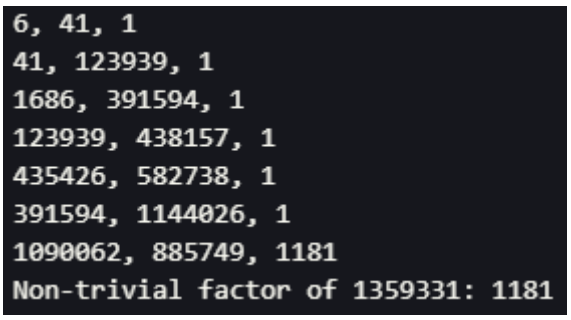

Рис. 4.2: Результат выполнения кода

Здесь выведены значения a, b и n на каждой итерации и финальный резльутат.

5 Выводы

Я реализовал алгоритм реализующий ρ-метод Полларда.

Список Литературы

1. Julia - Control Flow
2. Julia - Mathematical Operations
3. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone - Handbook of Applied Cryptography