Отчет по лабораторной работе №6

Разложение чисел на множители

Арам Грачьяевич Саргсян

Содержание

# 1 Цель работы

Изучить вероятностные алгоритмы проверки чисел на простоту.

# 2 Выполнение лабораторной работы

1. Я реализовал метод Полларда на языке julia.

using Random  
using StatsBase  
  
# Функция для вычисления НОД  
function gcd(a::Int, b::Int)  
 while b != 0  
 a, b = b, a % b  
 end  
 return a  
end  
  
function pollards\_rho(n::Int, c::Int, f::Function)  
 a = c  
 b = c  
  
 while true  
 # Вычисление следующего значения a и b  
 a = f(a) % n  
 b = f(f(b) % n) % n  
  
 # Вычисление НОД  
 d = gcd(abs(a - b), n)  
  
 # Проверка условия завершения  
 if d > 1 && d < n  
 return d # Нетривиальный делитель найден  
 elseif d == n  
 return "Делитель не найден"  
 end  
 end  
end  
  
# Пример использования:  
n = 1359331 # Число, для которого ищем делитель  
c = 1 # Начальное значение  
f(x) = x^2 + 5 # Пример сжимающей функции  
  
result = pollards\_rho(n, c, f)  
println("Найденный делитель: $result")

Найденный делитель: 1181

# 3 Выводы

Я реализовал алгоритм разложения чисел на множители.