Лабораторна работа № 6 - Разложение чисел на множители

Покрас Илья Михайлович НФИмд-01-24

31 октября, 2024, Москва, Россия

Российский Университет Дружбы Народов Имени Патриса Лумумбы

Цель работы

Реализовать алгоритм разложения чисел на множители.

Задания

Реализовать алгоритм, реализующий ρ-метод Полларда.

ρ-метод Полларда - код

```julia
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. 1: Функция ρ-метода Полларда

ρ-метод Полларда - результат

```
6, 41, 1
41, 123939, 1
1686, 391594, 1
123939, 438157, 1
435426, 582738, 1
391594, 1144026, 1
1090062, 885749, 1181
Non-trivial factor of 1359331: 1181
```

Рис. 2: Результат выполнения кода

Вывод

Я реализовал алгоритм реализующий ρ-метод Полларда.

Спасибо за внимание