Математические основы защиты информации и информационной безопасности

Супонина Анастасия Павловна

23 Ноября 2024

РУДН, Москва, Россия

Лабораторная работа 6

Цель работы

Изучить p-метод Полларда и научиться его программно реализовывать.

Задание

Программно реализовать на языке Julia p-метод Полларда

1. Реализовать алгоритм программно.
2. Разложить на множители данное преподавателем число.

Расширенный алгоритм Евклида

```
function euclid(n, number1)
    r_array = [number1, n]
    x_array = Float64[1, 0]
    y_array = Float64[0, 1]
    i = 1
    while r_array[i+1] != 0
        q = div(r_array[i], r_array[i+1])
        push!(r_array, r_array[i] % r_array[i+1])
        push!(x_array, x_array[i] - q * x_array[i+1])
        push!(y_array, y_array[i] - q * y_array[i+1])
        i += 1
    end

    return r_array[i]
end
```

Функция f

```
function f(a, n)
    a = (a^2 + 5) % n
    return a
end
```

Рис. 2: Функция f

```
n = 1359331
c = 1
a = c
b = c
d = 1
```

Рис. 3: Входные данные

```
function pollard(d, n, a, b)
    while true
        if d > 1 && d < n
            return d
        elseif d == n
            return "Делитель не найден"
        elseif d == 1
            a = f(a, n)
            b = f(f(b, n), n)
            d = euclid(n, a-b)
            if d < 0
                d *= -1
            end
        end
    end
end
```

```
res = pollard(d, n, a, b)
println(res)
```

Рис. 5: Запуск функции и вывод результата

Отображение результата

```
function pollard(d, n, a, b)
    while true
        if d > 1 && d < n
            return d
        elseif d == n
            return "Делитель не найден"
        elseif d == 1
            a = f(a, n)
            b = f(f(b, n), n)
            d = euclid(n, a-b)
            if d < 0
                d *= -1
            end
        end
    end
end
```

Выводы

Выводы

В процессе выполнения работы, я реализовала разложение на множители для заданного числа, а именно реализовала p-алгоритм Полланда на языке программирования Julia.

Спасибо за внимание!