РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ПРЕЗЕНТАЦИЯ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 6

дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Пиняева Анна Андреевна

Группа: НПИмд-01-24

МОСКВА

2025

Цель работы

Знакомство и реализация алгоритма разложения числа на множители.

Ход работы

1. Бинарный алгоритм Евклида

```
function evklidBin(a, b)
    if a == 0 || b == 0
        return 0
    elseif a == b
        return a
    elseif a < 0
        a *= -1
    elseif b < 0
        b *= -1
    end
    g = 1
    u = a; v = b
    while u > 0
        if u % 2 == 0 && v % 2 == 0
            g *= 2
            u = round(Int, u/2)
            v = round(Int, v/2)
        elseif u % 2 == 0
            u = round(Int, u/2)
        elseif v % 2 == 0
            v = round(Int, v/2)
        elseif u >= v
            u = u - v
        else
            v = v - u
        end
    end
    g *= v
    return g
end
```

2. p-метод Полларда

```
function metodPollarda(n, c, any_func::Function)
    if n % 2 == 0
        return 2, round(Int, n/2)
    end
    a = c; b = c
    i = 0
    p = 0
    while p == 0 && i < 100
        a = any_func(a)
        b = any_func(any_func(b))
        d = evklidBin(a-b, n)
        if d > 1
            return d, round(Int, n/d)
        end
        i += 1
    end
    return "Делитель не найден"
end
```

3. Тестирование

```
n = 222
c = 1
metodPollarda(n, c, x -> (x^2 + 5) % n)
```

Результат тестирования представлен на рис.1

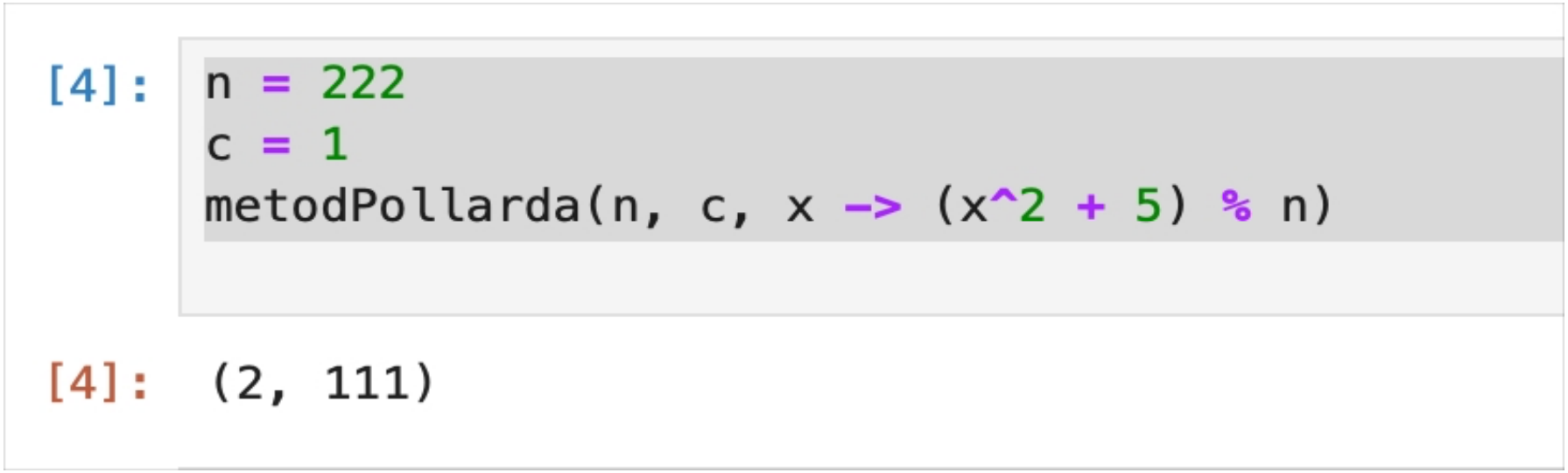

Рис. 1 Тестирование:

Вывод:

В ходе данной работы мной были изучен и реализован p-метод Полларда для разложения числа на множетели. Написан программный код на языке Julia и протестирован.