# Отчёт по лабораторной работе 6

**Разложение чисел на множители. Алгоритм Полларда**

Аристова Арина Олеговна

# Содержание

# Список иллюстраций

# 1 Цель работы

Изучить алгоритм Полларда для разложения составного числа на множители, реализовать его на языке Julia.

# 2 Задание

- Реализовать программно алгоритм Полларда
- Найти наименьший делитель числа с помощью реализованного алгоритма или сделать вывод об отсутствии нетривиальных делителей

# 3 Выполнение лабораторной работы

## 3.1 Код реализации алгоритмов

Код, реализующий алгоритм Поллардавыглядит следующим образом.

Функция main() “вытаскивает” из запроса командной строки число, которое будем проверять, поданное в качестве аргумента, в противном случае (если на вход не подано число) проверяем какое-то число по умолчанию.

```
function pollard_rho(n, c=1, f=x -> (x^2 + 5) % n, max_iterations=10000)
    if n % 2 == 0
        return 2
    end

    a = c
    b = c
    for i in 1:max_iterations
        a = f(a)
        b = f(f(b))

        d = gcd(abs(a-b), n)
        # println("Итерация $i: a = $a, b = $b, d = $d")

        if 1 < d < n
            println("Найден нетривиальный делитель: $d")
```

```
            return d
        elseif d == n
            println("Делитель не найден.")
            return nothing
        end
    end
    println("Достигнуто максимальное кол-во итераций")
    return nothing
end


function main()
    if length(ARGS) > 0
        n = parse(Int, ARGS[1])
    else
        n = 1234537
    end
    println("Факторизация числа $n методом  Полларда")
    println("Используется функция f(x) = x**2 + 5 mod n")
    result = pollard_rho(n)
    if result !== nothing
        println("Результат: $n = $result × $(n ÷ result)")
     println("Проверка: $result × $(n ÷ result) = $(result * (n ÷ result))")
    else
        println("Делитель не найден для числа $n")
    end
end
```

```
main()
```

## 3.2 Проверка работы кода

Проверяю работу кода. Рассматриваем разные числа: простое число, не имеющее делителей, и составное число

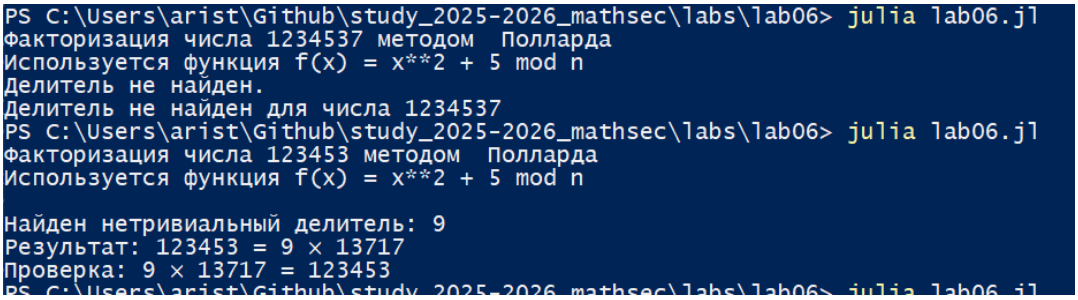


Рис. 3.1: Проверка работы кода для простого и составного чисел.

## 3.3 Вывод

В ходе выполнения лабораторной работы мною было реализовано программное решение алгоритма поиска нетривиального делителя составного числа методом Полларда.

# Список литературы


- Описание лабораторной работы