

# **Отчёт по лабораторной работе 8**

**Разложение чисел на множители. Алгоритм Полларда**

Аристова Арина Олеговна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Задание</b>	<b>5</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
3.1	Код реализации алгоритмов . . . . .	6
3.2	Проверка работы кода . . . . .	8
3.3	Вывод . . . . .	8
	<b>Список литературы</b>	<b>9</b>

# Список иллюстраций

3.1	Проверка работы кода для простого и составного чисел. . . . .	8
-----	---	---

# 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")
        end
    end
end
```

```

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

```

```

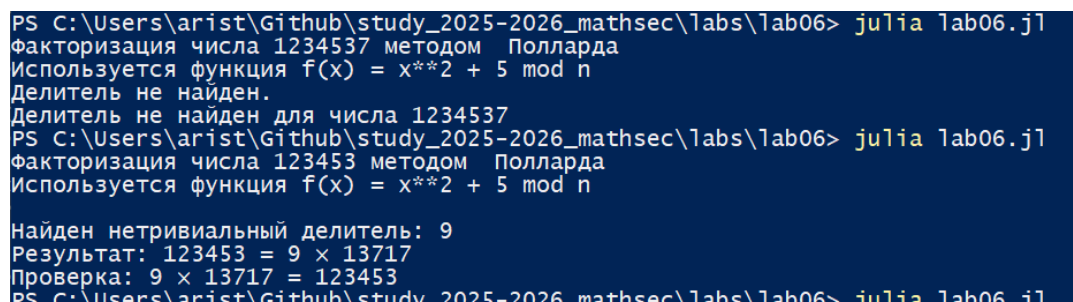
function main()
    if length(ARGS) > 0
        n = parse{Int, ARGS[1]}
    else
        n = 1234537
    end
    println("Факторизация числа $n методом Полларда")
    println("Используется функция  $f(x) = x^2 + 5 \bmod n$ ")
    result = pollard_rho(n)
    if result != nothing
        println("Результат:  $n = \text{result} \times (n \div \text{result})$ ")
        println("Проверка:  $\text{result} \times (n \div \text{result}) = (\text{result} * (n \div \text{result}))$ ")
    else
        println("Делитель не найден для числа $n")
    end
end
end

```

main()

## 3.2 Проверка работы кода

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



```
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab06> julia lab06.jl
факторизация числа 1234537 методом Полларда
Используется функция  $f(x) = x^2 + 5 \pmod n$ 
Делитель не найден.
Делитель не найден для числа 1234537
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab06> julia lab06.jl
факторизация числа 123453 методом Полларда
Используется функция  $f(x) = x^2 + 5 \pmod n$ 

Найден нетривиальный делитель: 9
Результат:  $123453 = 9 \times 13717$ 
Проверка:  $9 \times 13717 = 123453$ 
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab06> julia lab06.jl
```

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