

Презентация к лабораторной работе 4

Математические основы защиты информации и информационной безопасности

Аристова Арина Олеговна

07 октября 2025

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

- Аристова Арина Олеговна
- студентка группы НФИмд-01-25
- Российский университет дружбы народов имени Патриса Лумумбы
- 1032259382@rudn.ru
- <https://github.com/aoaristova>



Изучить алгоритм Евклида для нахождения НОД (наибольшего общего делителя), бинарный алгоритм Евклида, а также расширенные их версии, которые находят также коэффициенты соотношения Безу: $\text{НОД} = x * a + y * b$, где a, b - рассматриваемые числа.

Реализовать программный код для:

- алгоритма Евклида
- бинарного алгоритма Евклида
- расширенного алгоритма Евклида
- расширенного бинарного алгоритма Евклида

Выполнение лабораторной работы

Последовательно заменяем числа (a, b) на $(b, a \% b)$ до тех пор, пока $b \neq 0$.
Последнее ненулевое число — это НОД.

Базовый алгоритм

```
function evclid(a::Int, b::Int)
    while b != 0
        a, b = b, a % b
    end
    return abs(a)
end
```

```
function bin_evclid(a::Int, b::Int)
    if a == 0
        return abs(b)
    end
    if b == 0
        return abs(a)
    end
    shift = 0
    while iseven(a) && iseven(b)
        a >>= 1
        b >>= 1
        shift += 1
    end
end
```

Бинарный алгоритм Евклида

```
while a != b
  if iseven(a)
    a >>= 1
  elseif iseven(b)
    b >>= 1
  elseif a > b
    a = a - b
  else
    b = b - a
  end
end
return a << shift
end
```

Решение задачи. Расширенный алгоритм Евклида

Классический алгоритм, дополненный тем, что находит также числа x и y , такие что выполняется линейная комбинация: $(a, b) = a * x + b * y$

```
function extended_evclid(a::Int, b::Int)
    old_r, r = a, b
    old_x, x = 1, 0
    old_y, y = 0, 1
    while r != 0
        quotient = div(old_r, r)
        old_r, r = r, old_r - quotient*r
        old_x, x = x, old_x - quotient*x
        old_y, y = y, old_y - quotient*y
    end
    return old_r, old_x, old_y
end
```

Проверяю работу кода. Результаты для каждого из вариантов алгоритмов получились идентичными.

```
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab04> julia .\evclid.jl
4
4
(4, 2, -1)
(4, 2, -1)
```

Рис. 1: Результат работы программы

В ходе выполнения данной лабораторной работы мною были получены знания о нахождении НОД с помощью различных вариантов алгоритма Евклида, а также написана программа, реализующая каждый из них.

Расширенные алгоритмы позволяют вычислить коэффициенты x и y , удовлетворяющие формуле: $(a, b) = a * x + b * y$.