Лабораторная работа №4

Математические основы защиты информации и информационной безопасности

Данилова Анастасия Сергеевна

Содержание

[Цель работы 1](#_Toc180861416)

[Задание 1](#_Toc180861417)

[Теоретическое введение 1](#_Toc180861418)

[Выполнение лабораторной работы 2](#_Toc180861419)

[Выводы 2](#_Toc180861420)

[Список литературы 2](#_Toc180861421)

# Цель работы

Изучить различные вариации алгоритма Евклида и реализовать их программно на языке Julia.

# Задание

* Изучить теоретическую часть о способах нахождения НОД
* Реализовать алгоритм Евклида, бинарный алгоритм Евклида, а также их расширенные варианты

# Теоретическое введение

**НОД** (наибольший общий делитель) – это наибольшее натуральное целое число, на которое эти числа делятся без остатка.

*Алгоритм Евклида*

Для нахождения наибольшего общего делителя двух чисел нужно заменить большее из чисел на остаток от деления его на меньшее и для полученной пары повторять эту процедуру, пока одно из чисел не станет равно нулю. Тогда второе число будет равно наибольшему общему делителю исходных чисел.

*Бинарный Алгоритм Евклида*

Метод нахождения наибольшего общего делителя двух целых чисел. Данный алгоритм «быстрее» обычного алгоритма Евклида, так как вместо медленных операций деления и умножения используются сдвиги. Но это преимущество в скорости теряется с увеличением разницы между целыми числами более чем на несколько порядков, в результате чего число итераций вычитания может многократно превышать число итераций обычного алгоритма, использующего сравнение по модулю. То есть скорость бинарных сдвигов даёт эффект только для чисел, близких друг к другу.

*Расширенный Алгоритм Евклида*

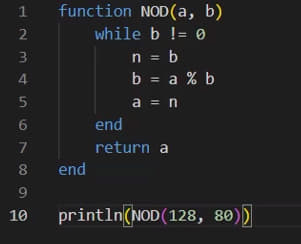
Расширенный алгоритм возвращает не только НОД(a, b), но и коэффициенты x и y. Коэффициенты можно получить, используя рекурсивное свойство алгоритма Евклида. Уравнение Безу: a⋅x+b⋅y=gcd(a,b)

*Расширенный бинарный Алгоритм Евклида*

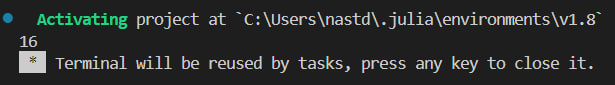
Расширенный бинарный алгоритм Евклида находит наибольший общий делитель (НОД) двух чисел и определяет два коэффициента x и y, такие что НОД = ax + by. Иными словами, алгоритм находит наибольший делитель и его линейное представление.

# Выполнение лабораторной работы

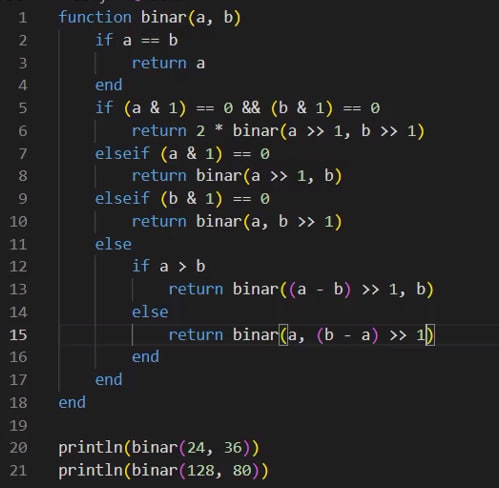
**Алгоритм Евклида**



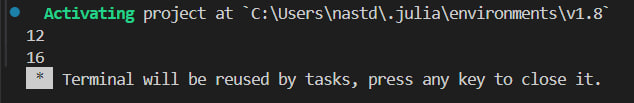
Код для Алгоритма Евклида



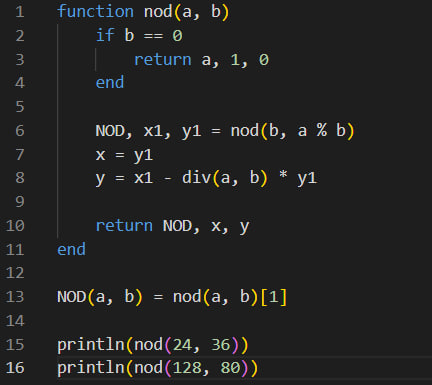
Результат



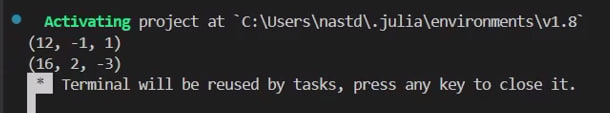
Код для бинарного Алгоритма Евклида



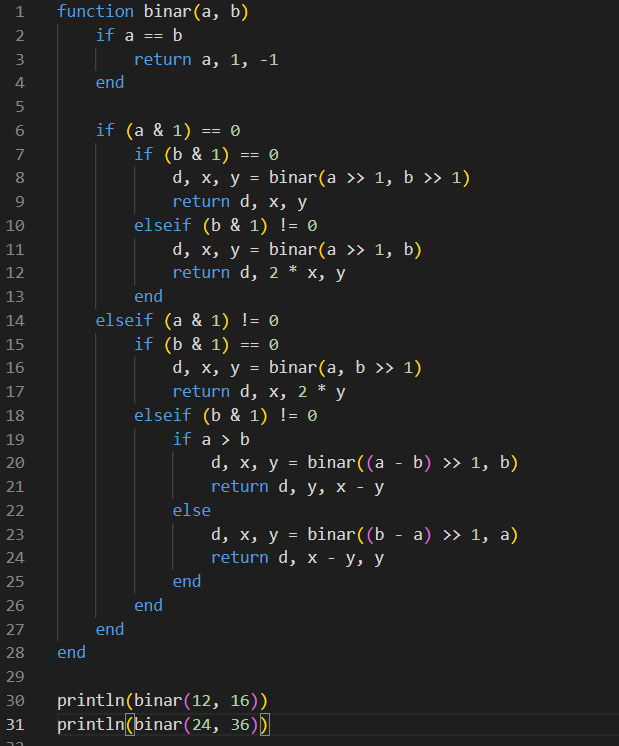
Результат



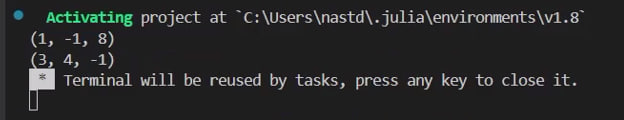
Код для расширенного Алгоритма Евклида



Результат



Код для расширенного бинарного Алгоритма Евклида



Результат

# Выводы

Мы изучили различные вариации алгоритма Евклида и реализовали их программно на языке Julia.

# Список литературы

1. Mathematics // Julia URL: https://docs.julialang.org/en/v1/base/math/