Отчёт по лабораторной работе №4  
Математические основы защиты информации и информационной безопасности

Вычисление наибольшего общего делителя

Выполнил: Махорин Иван Сергеевич,  
НФИмд-02-21, 1032259380

Содержание

# 1 Цель работы

Изучить алгоритмы нахождения наибольшего общего делителя и научиться их реализовывать.

# 2 Выполнение лабораторной работы

## 2.1 Реализация алгоритма Евклида

Алгоритм Евклида — эффективный алгоритм для нахождения наибольшего общего делителя двух целых чисел (или общей меры двух отрезков). Алгоритм назван в честь греческого математика Евклида (III век до н. э.), который впервые описал его в VII и X книгах «Начал».

Выполним реализацию этого алгоритма на языке Julia (рис. 1) и (рис. 2):

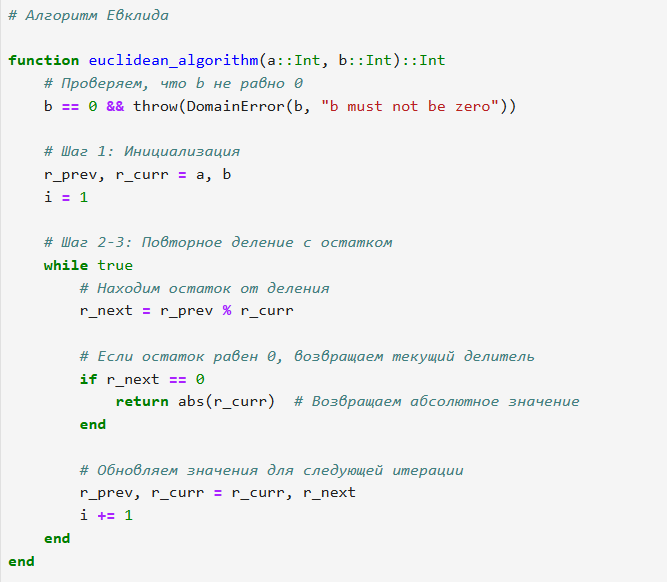


Рис. 1: Реализация алгоритма Евклида

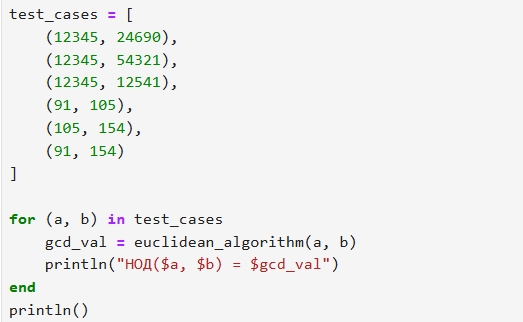


Рис. 2: Реализация алгоритма Евклида

Проверим работу алгоритма (рис. 3):

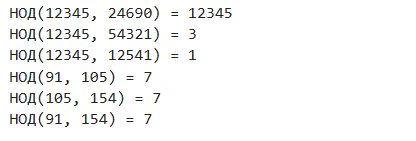


Рис. 3: Проверка

## 2.2 Реализация бинарного алгоритма Евклида

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.

Выполним реализацию этого алгоритма на языке Julia (рис. 4) и (рис. 5):



Рис. 4: Реализация бинарного алгоритма Евклида



Рис. 5: Реализация бинарного алгоритма Евклида

Проверим работу алгоритма (рис. 6):

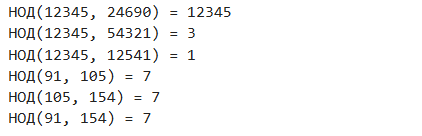


Рис. 6: Проверка

## 2.3 Реализация расширенного алгоритма Евклида

Расширенный алгоритм Евклида — модификация алгоритма Евклида, вычисляющая, кроме наибольшего общего делителя (НОД) целых чисел и , ещё и коэффициенты соотношения Безу, то есть такие целые и , что НОД(a , b).

Выполним реализацию этого алгоритма на языке Julia (рис. 7) и (рис. 8):

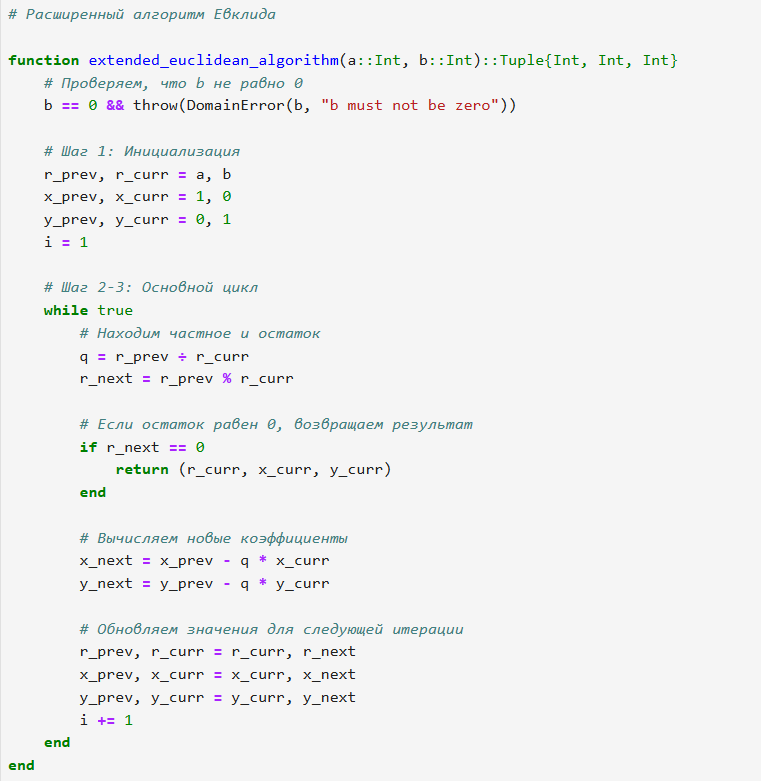


Рис. 7: Реализация расширенного алгоритма Евклида

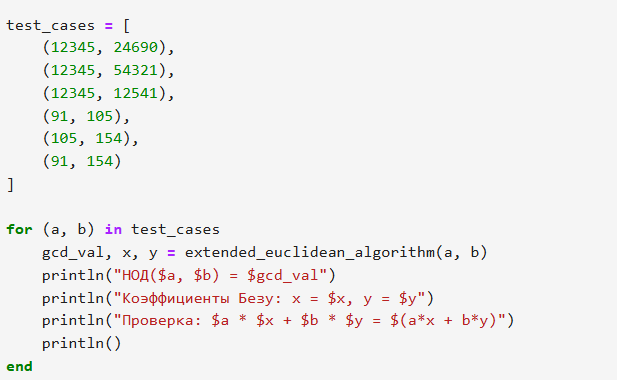


Рис. 8: Реализация расширенного алгоритма Евклида

Проверим работу алгоритма (рис. 9):

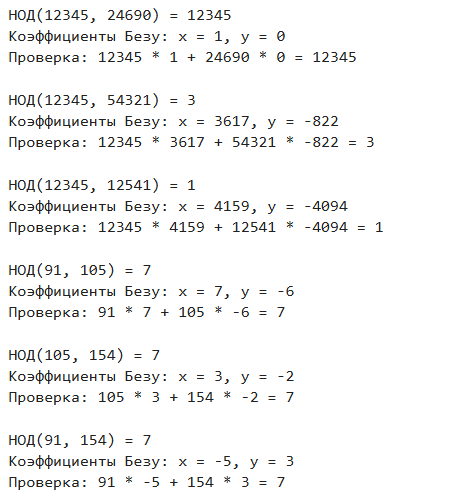


Рис. 9: Проверка

## 2.4 Реализация расширенного бинарного алгоритма Евклида

Выполним реализацию этого алгоритма на языке Julia (рис. 10 - рис. 12):

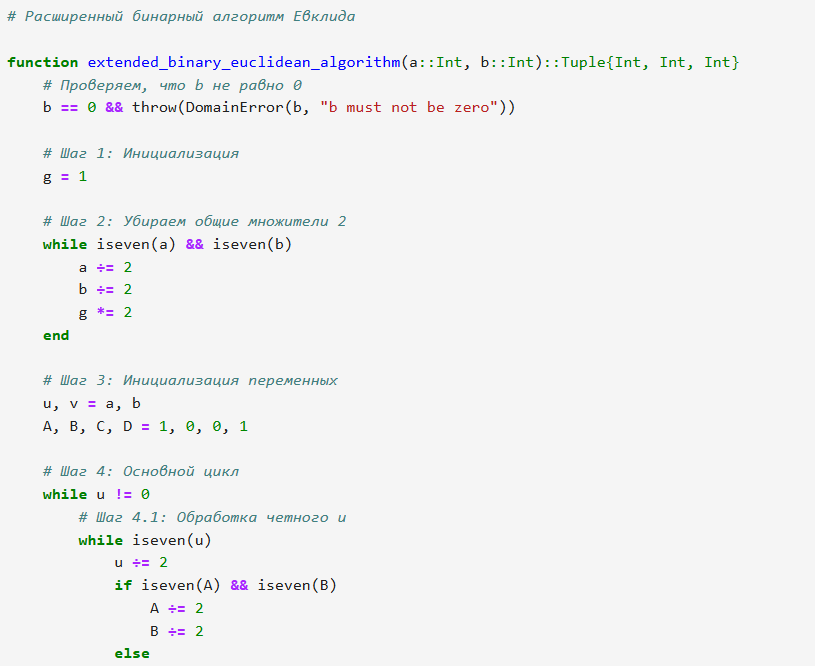


Рис. 10: Реализация расширенного бинарного алгоритма Евклида

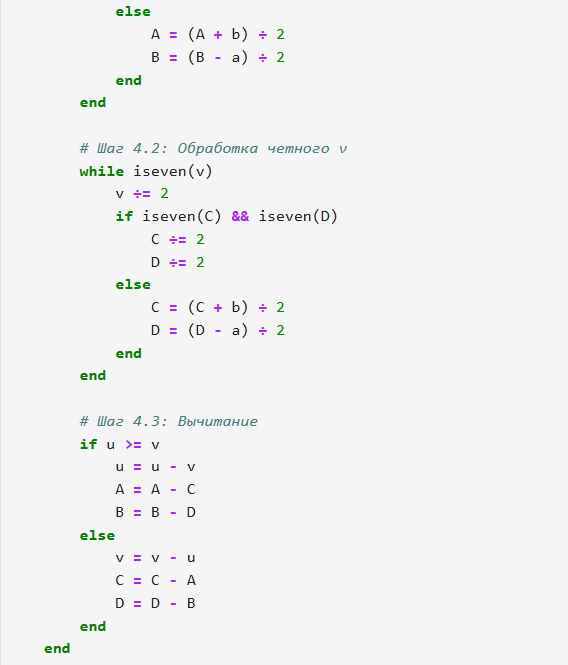


Рис. 11: Реализация расширенного бинарного алгоритма Евклида

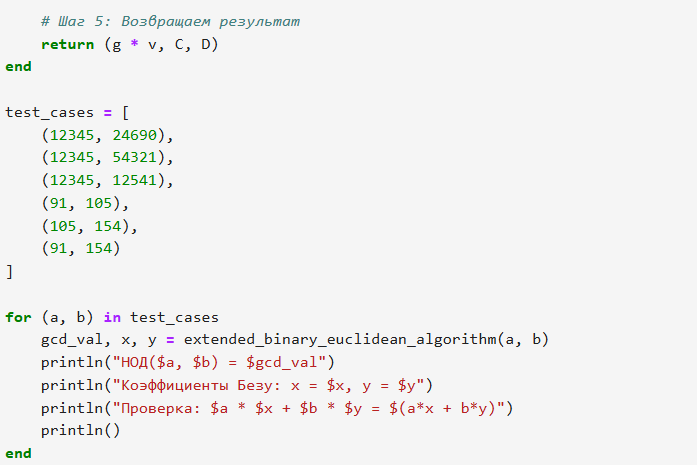


Рис. 12: Реализация расширенного бинарного алгоритма Евклида

Проверим работу алгоритма (рис. 13):

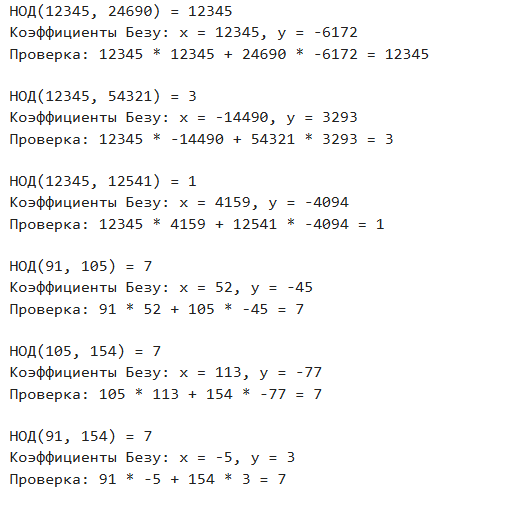


Рис. 13: Проверка

# 3 Список литературы. Библиография

[1] Julia: https://docs.julialang.org/en/v1/