Лабораторна работа № 4

Вычисление наибольшего общего делителя

Покрас Илья Михайлович

Содержание

# 1 Цель работы

Реализовать алгоритмы нахождения наибольшего общего делителя (НОД)

# 2 Задание

* Реализовать алгоритм Евклида;
* Реализовать расширенный алгоритм Евклида;
* Реализовать бинарный алгоритм Евклида;
* Реализовать бинарный расширенный алгоритм Евклида;

# 3 Теоретическое введение

Алгори́тм 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.). Это один из старейших численных алгоритмов, используемых в наше время. В самом простом случае алгоритм Евклида применяется к паре положительных целых чисел и формирует новую пару, которая состоит из меньшего числа и остатка от деления большего числа на меньшее. Процесс повторяется, пока числа не станут равными. Найденное число и есть наибольший общий делитель исходной пары.

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.

Расширенные алгоритмы Евклида — модификации алгоритмы Евклида, вычисляющая, кроме наибольшего общего делителя (НОД) целых чисел a и b, ещё и коэффициенты соотношения Безу, то есть такие целые x и y, что ax+by=НОД(a,b)

# 4 Выполнение лабораторной работы

## 4.1 Алогритм Евклида

Я создал функцию алгоритма Евклида, принимающую числа a и b, находящую через рекурсию НОД и возращающую его (рис. 1).

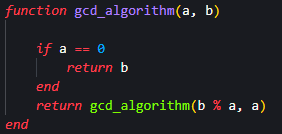


Рис. 1: Функция алгоритма Евклида

## 4.2 Расширенный алогритм Евклида

Далее я создал расширенный алгоритм Евклида для нахождения и возврата НОД и коэффициентов соотношения Безу x и y (рис. 2).

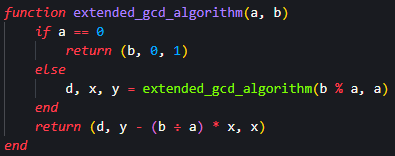


Рис. 2: Функция расширенного алгоритма Евклида

Я создал блок инициализации переменных a и b и вызов функций с входными переменными (рис. 3).

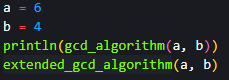


Рис. 3: Инициализация переменных и вызов функций(1)

И получил следующие значения (рис. 4).

Результат выполнения(1)

Рис. 4: Результат выполнения(1)

## 4.3 Бинарный алогритм Евклида

Я создал функцию бинарного алгоритма Евклида, принимающую числа a и b, находящую с помощью сдвигов и возращающую НОД (рис. 5).

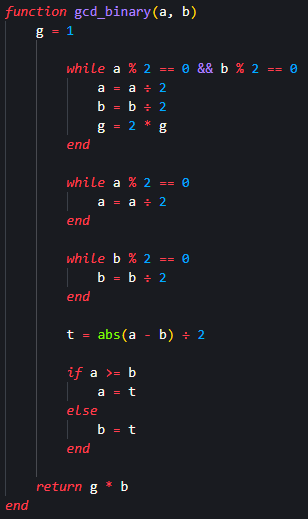


Рис. 5: Функция бинарного алгоритма Евклида

## 4.4 Расширенный бинарный алогритм Евклида

Далее я создал расширенный бинарный алгоритм Евклида для нахождения коэффициентов и возврата НОД и соотношения Безу x и y (рис. 6).

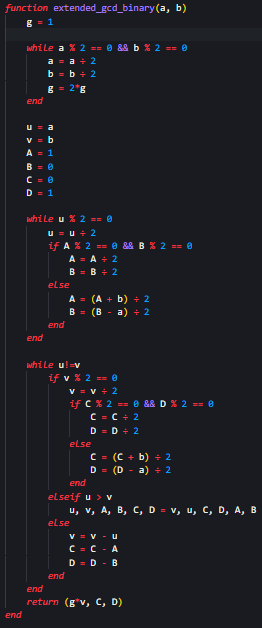


Рис. 6: Функция расширенного алгоритма Евклида

Я создал блок инициализации переменных a и b и вызов функций с входными переменными (рис. 7).

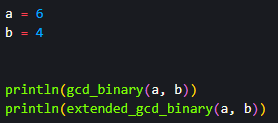


Рис. 7: Инициализация переменных и вызов функций(2)

И получил следующие значения (рис. 8).

Результат выполнения(2)

Рис. 8: Результат выполнения(2)

# 5 Выводы

Я реализовал алгоритмы нахождения НОД.

# Список Литературы

1. [Julia - Control Flow](https://docs.julialang.org/en/v1/manual/control-flow/)
2. [Julia - Mathematical Operations](https://docs.julialang.org/en/v1/manual/mathematical-operations/)
3. [Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone - Handbook of Applied Cryptography](https://cacr.uwaterloo.ca/hac/)