Лабораторная работа №4

Математические основы защиты информации и информационной безопасности

Дарижапов Тимур Андреевич

Содержание

# Цель работы

Познакомиться с алгоритмами вычисления наибольшего общего делителя и практическая реализация алгоритмов.

# Задание

Реализовать алгоритмы вычисления наибольшего общего делителя, рассмотренные в лабораторной работе.

# Выполнение лабораторной работы

Данная работа была выполнена на языке Julia.

Для реализации алгоритма Евклида была написана следующая программа (рис. 1 ) :

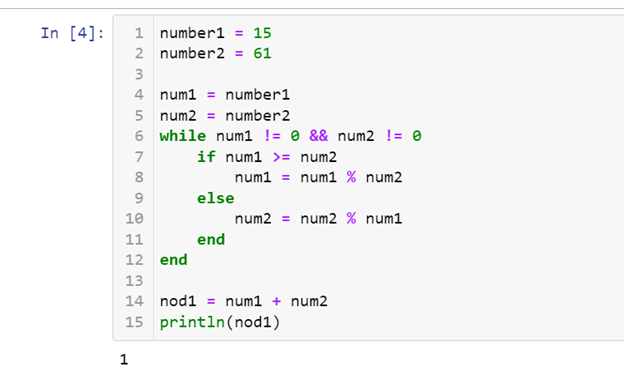


Figure 1: Программа реализации алгоритма Евклида

В данной программе:

1-5 строки: задание чисел, НОД которого ищем.

6-12: реализация самого алгоритма Евклида: делим наибольшее число на наименьшее и записываем остаток до тех пор, пока одно из них не обнулится.

14: запись НОД в переменную.

15: вывод результата

Мы можем видеть результат на (рис. 1 ) . Программа работает верно.

Для реализации бинарного алгоритма Евклида была написана следующая программа (рис. 2 )

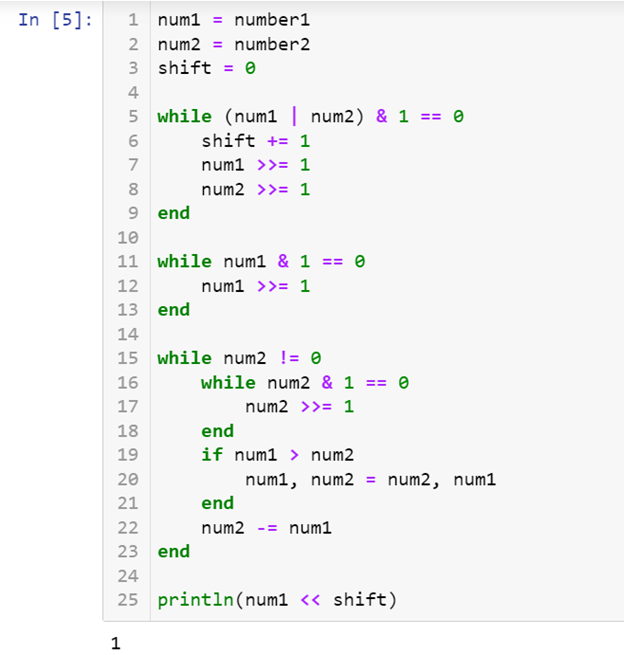


Figure 2: Программа реализации бинарного алгоритма Евклида

В данной программе:

1-3 строки: задание чисел, НОД которого ищем, обнуление “сдвига”

5-23: реализация самого бинарного алгоритма Евклида: смотрим на четность получающихся чисел и записываем насколько нам необходимо “сдвинуть” число, чтобы получить НОД

25: сдвиг влево и вывод получившегося НОД.

Для реализации расширенного алгоритма Евклида была написана следующая программа (рис. 3 )

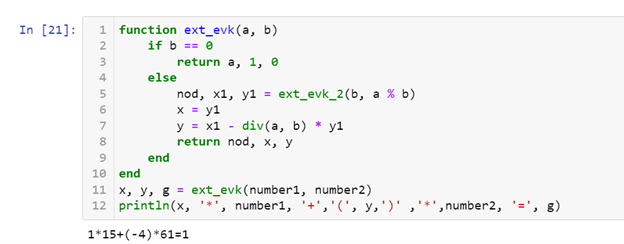


Figure 3: Программа расширенного алгоритма Евклида

1 строка: зададим рекурсивную функцию

2-3: если второе число равно нулю, возвращаем ответ из трёх чисел

5-7: в ином случае запускаем рекурсию, а затем выводим ответ согласно формуле на строке 7.

8: возвращаем вывод в качестве получившегося НОД, числа, что нужно домножить на первую цифру и на вторую, чтобы получить НОД.

11: вывоз функции и сохранение данных в переменные

12: вывод на экран.

Для реализации расширенного бинарного алгоритма Евклида была написана следующая программа (рис. 4 )

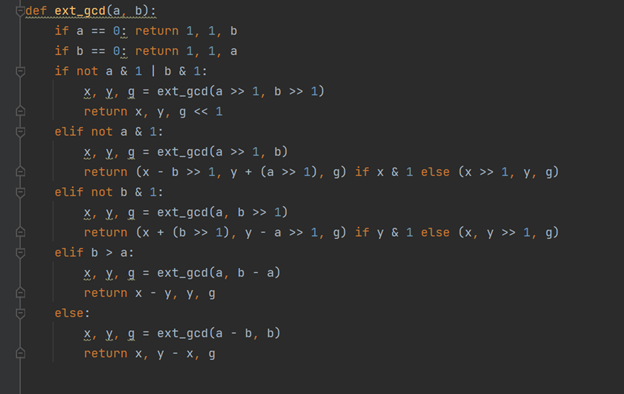


Figure 4: Программа расширенного бинарного алгоритма Евклида

Данная программа также работает рекурсивно, рассматривая 4 случая: 1) а четное 2) а нечетное и b четное 3) а нечетное и b нечетное, b > a 4) а нечетное и b нечетное , b < a

Каждая рекурсия сдвигает биты в цифрах, формируя окончательный ответ.

В итоге выводит три значения: НОД, число, что нужно домножить на первую цифру и на вторую, чтобы получить НОД.

Выводы всех программ (рис. 5 )

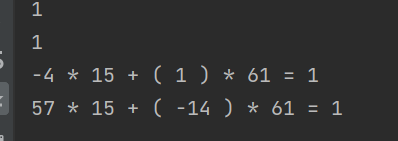


Figure 5: Результаты работы всех программ

Необходимо обратить внимание, что расширенные алгоритмы выводят разные множители, однако оба ответа верны и дают верный НОД.

# Выводы

Я познакомился с алгоритмами вычисления наибольшего общего делителя и практически реализовал алгоритмы.

# Список литературы

Лабораторная работа №4

Вычисление наибольшего общего делителя [Электронный ресурс]. URL: https://esystem.rudn.ru/mod/folder/view.php?id=1150974