Лабораторная работа №4

Математические основы защиты информации и информационной безопасности

Леонтьева Ксения Андреевна | НПМмд-02-23

Содержание

# 1 Цель работы

Реализовать на языке программирования алгоритмы Евклида для вычисления наибольшего общего делителя.

# 2 Теоретическое введение

Целое число называется **наибольшим общим делителем** целых чисел (обозначается НОД ), если выполняются следующие условия:

* каждое из чисел делится на ,
* если - другой общий делитель чисел , то делится на .

Ненулевые целые числа и называются **ассоциированными**, если делится на и делится на .

Для любых целых чисел существует наибольший общий делитель и его можно предствить в виде **линейной комбинации** этих чисел:

Целые числа называются **взаимно простыми в совокупности**, если НОД. Целые числа и называются **взаимно простыми**, если НОД.

Целые числа называются **попарно взаимно простыми**, если НОД для всех .

Для вычисления наибольшего общего делителя двух целых чисел применяется способ повторного деления с остатком, называемый **алгоритмом Евклида**.

**Бинарный алгоритм Евклида** основан на следующих свойствах наибольшего общего делителя (считаем, что ):

1. если оба числа и четные, то НОД НОД
2. если число - нечетное, число -четное, то НОД НОД
3. если оба числа и нечетные, , то НОД НОД
4. если , то НОД

Более подробно см. в [1].

# 3 Выполнение лабораторной работы

Алгоритм Евклида реализуем по следующей схеме:

На вход подаются целые числа и : .

1. Положить
2. Найти остаток от деления на
3. Если , то положить . В противном случае положить и вернуться на шаг 2
4. Результат

Код программы (рис. 1).

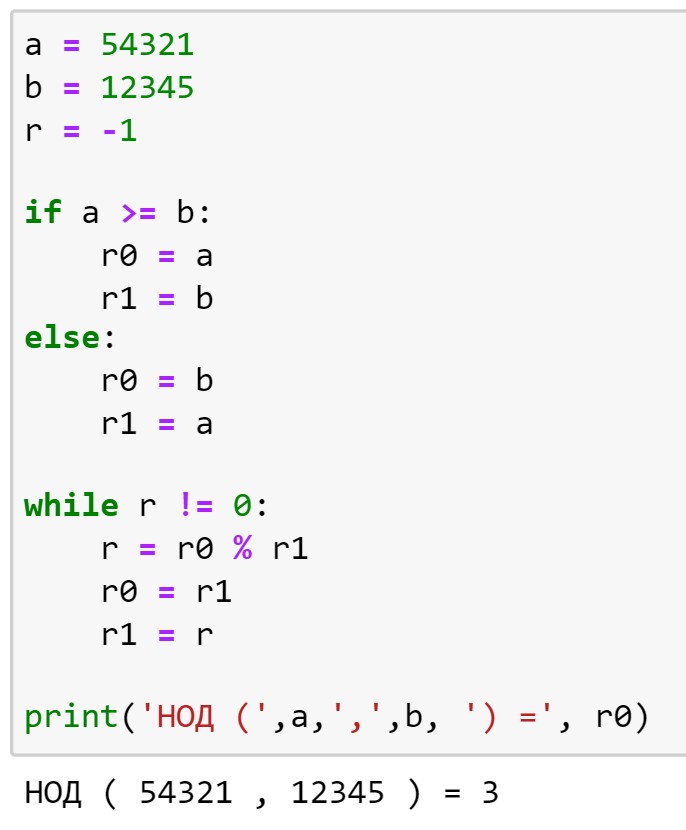


Рис. 1: Алгоритм Евклида

Бинарный алгоритм Евклида реализуем по следующей схеме:

На вход подаются целые числа и : .

1. Положить
2. Пока оба числа и четные, выполнять до получения хотя бы одного нечетного значения или
3. Положить
4. Пока выполнять следующие действия:

* 4.1. Пока четное, полагать
* 4.2. Пока четное, полагать
* 4.3. При положить . В противном случае положить

1. Положить
2. Результат

Код программы (рис. 2).

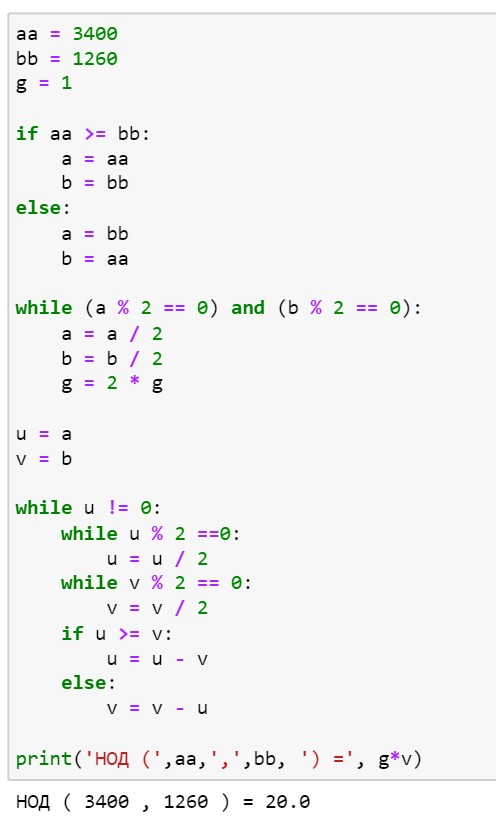


Рис. 2: Бинарный алгоритм Евклида

Расширенный алгоритм Евклида реализуем по следующей схеме:

На вход подаются целые числа и : .

1. Положить
2. Разделить с остатком на :
3. Если , то положить . В противном случае положить и вернуться на шаг 2
4. Результат

Код программы (рис. 3).

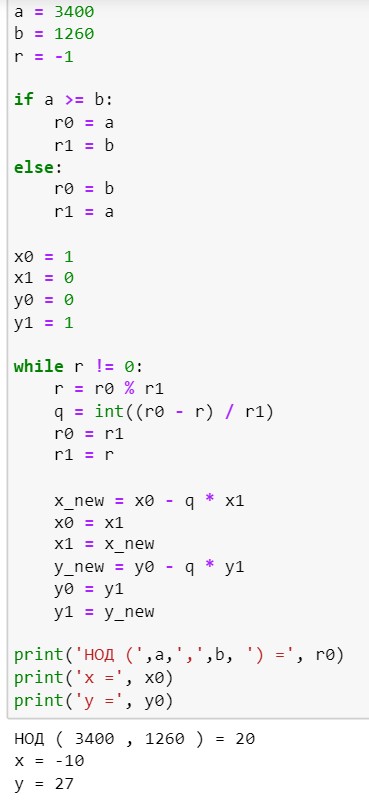


Рис. 3: Расширенный алгоритм Евклида

Расширенный бинарный алгоритм Евклида реализуем по следующей схеме:

На вход подаются целые числа и : .

1. Положить
2. Пока числа и четные, выполнять до получения хотя бы одного нечетного значения или
3. Положить
4. Пока выполнять следующие действия:

* 4.1. Пока четное:
* 4.1.1. Положить
* 4.1.2. Если оба числа и четные, то положить . В противном случае положить
* 4.2. Пока четное:
* 4.2.1. Положить
* 4.2.2. Если оба числа и четные, то положить . В противном случае положить
* 4.3. При положить . В противном случае положить

1. Положить
2. Результат

Код программы (рис. 4).

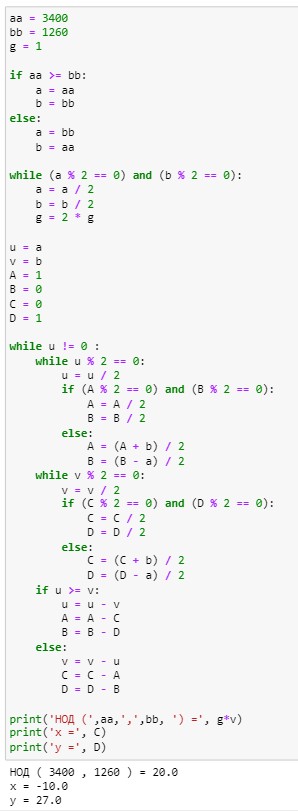


Рис. 4: Расширенный бинарный алгоритм Евклида

# 4 Выводы

В ходе выполнения данной лабораторной работы были реализованы алгоритмы Евклида для вычисления наибольшего общего делителя.

# Список литературы

1. Наибольший общий делитель [Электронный ресурс]. URL: <http://www.cleverstudents.ru/divisibility/nod.html>.