Отчёт по лабораторной работе 4

Вычисление наибольшего общего делителя

Гебриал Ибрам Есам Зекри НФИ-02-22

Содержание

# Цель работы

Реализация алгоритмов вычисления наибольшего общего делителя (Евклида).

# Теоретические сведения

Алгоритм Евклида — это способ нахождения наибольшего общего делителя (НОД) двух целых чисел. Оригинальная версия алгоритма, когда НОД находится вычитанием, была открыта Евклидом (III в. до н. э). В настоящее время чаще при вычислении НОД алгоритмом Евклида используют деление, так как данный метод эффективнее.

**Вычисление НОД делением**

Наибольший общий делитель пары чисел – это самое большое число, которое нацело делит оба числа пары. Пусть требуется вычислить НОД для чисел 108 и 72. Алгоритм вычисления делением будет таковым:

1. Разделим большее число (делимое) на меньшее (делитель): 108 / 72 = 1, остаток 36.
2. Поскольку остаток не был равен нулю, то сделаем делитель делимым, а остаток – делителем: 72 / 36 = 2, остаток 0.
3. Когда остаток равен нулю, то делитель является искомым НОД для пары заданных чисел. То есть НОД(108, 72) = 36. Действительно, 108 / 36 = 3 и 72 / 36 = 2.[1]

**Расширенный алгоритма Евклида**

Расширенным алгоритм называется не из-за более высокой скорости работы или более сложной реализации, а потому что он позволяет извлекать из входных данных дополнительную информацию.

Расширенный алгоритм также находит наибольший общий делитель, а ещё он определяет два коэффициента x и y, такие что:

ax + by = gcd(a,b), где gcd – это функция по нахождения НОД.

Иными словами, алгоритм находит наибольший делитель и его линейное представление.

gcd – это аббревиатура, которую часто используют для обозначения функции по назначению НОД:

g – Greatest (наибольший);

c – Common (общий);

d – Divisor (делитель).

**Бинарный алгоритм Евклида**

Суть бинарного алгоритма точно такая же — найти наибольший делитель. От классического он отличается только способом реализации.

Вместо классических арифметических операций, в бинарном алгоритме Евклида используются только битовые сдвиги влево и вправо, которые соответствуют умножению и делению на 2.[2]

# Выполнение лабораторной работы

1. Написал функцию evklid\_nod для вычисления алгоритма Евклида. (рис. 1)

Алгоритм нахождения НОД делением:

1. Большее число делим на меньшее.
2. Если делится без остатка, то меньшее число и есть НОД (следует выйти из цикла).
3. Если есть остаток, то большее число заменяем на остаток от деления.
4. Переходим к пункту 1.

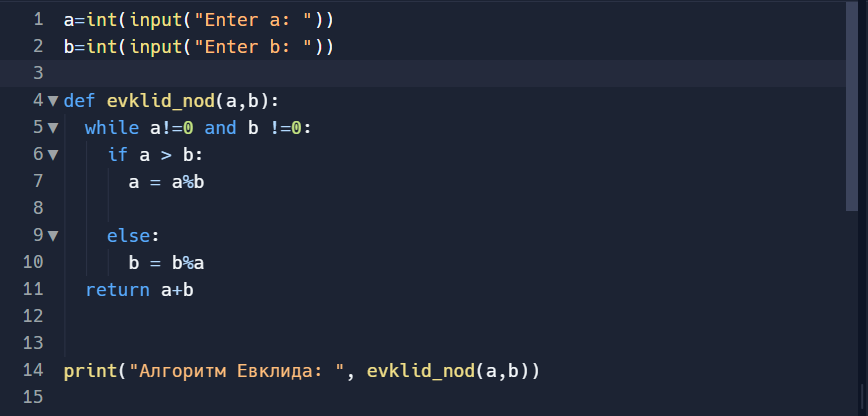


Figure 1: Функция для вычисления алгоритма Евклида

1. Написал функцию evklid\_binary для вычисления бинарного алгоритма Евклида. (рис. 2)
   1. Сначала положим g= 1
   2. Пока оба числа a и b четные, выполнить , , g= 2g до получения хотя одного нечетного значения a или b.
   3. Положим u=a, v=b
   4. Пока u :
      1. Пока u четное, полагать
      2. Пока v четное, полагать
      3. При u v положим u= u-v. В противном случае положим v=v-u
   5. Положим d=gv
   6. Получим результат d

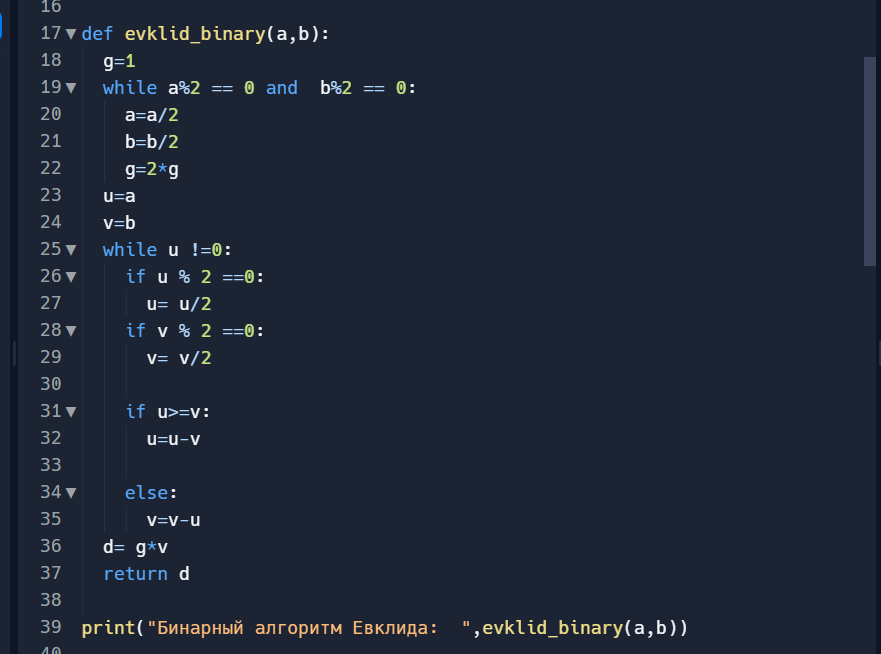


Figure 2: Функция для вычисления бинарного алгоритма Евклида

1. Написал функцию evklid\_extend для вычисления расширенного алгоритма Евклида. (рис. 3)

Сначала проверяется, равно ли первое число нулю, если это так, то второе число является делителем, а коэффициенты равны 0 и 1, так как «num1 \* x + num2 \* y = y» в том случае, если y = 1, а левое произведение равно нулю.

Функция возвращает три числа: делитель, коэффициент x и коэффициент y.

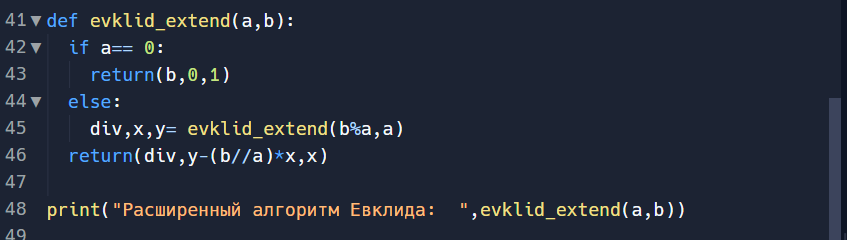


Figure 3: Функция для вычисления вычисления расширенного алгоритма Евклида.

1. Написал функцию evklid\_binary\_extend для вычисления расширенного бинарного алгоритма Евклида. (рис. 4) (рис. 5)
   1. Сначала положим g= 1
   2. Пока оба числа a и b четные, выполнить , , g= 2g до получения хотя одного нечетного значения a или b.
   3. Положим u=a, v=b, A=1, B= 0, C= 0, D=1.
   4. Пока u :
      1. Пока u четное, полагать
      2. Если оба числа A и B четные, полагать , . В противном случае положить ,
      3. Пока v четное, полагать
      4. Если оба числа C и D четные, полагать , . В противном случае положить ,
      5. При u v положим u= u-v, A= A-C, B = B-D. В противном случае положим v=v-u, C= C-A, D= D-B.
   5. Положим d=gv, x= C, y=D
   6. Получим результат d,x,y

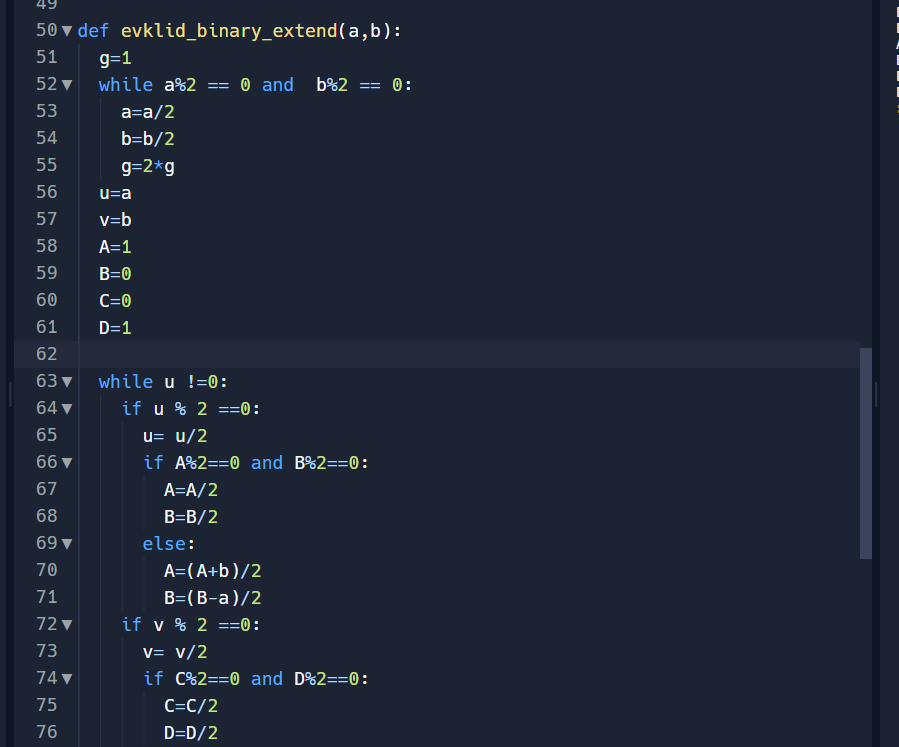


Figure 4: Функция для вычисления расширенного бинарного алгоритма Евклида. Первая часть

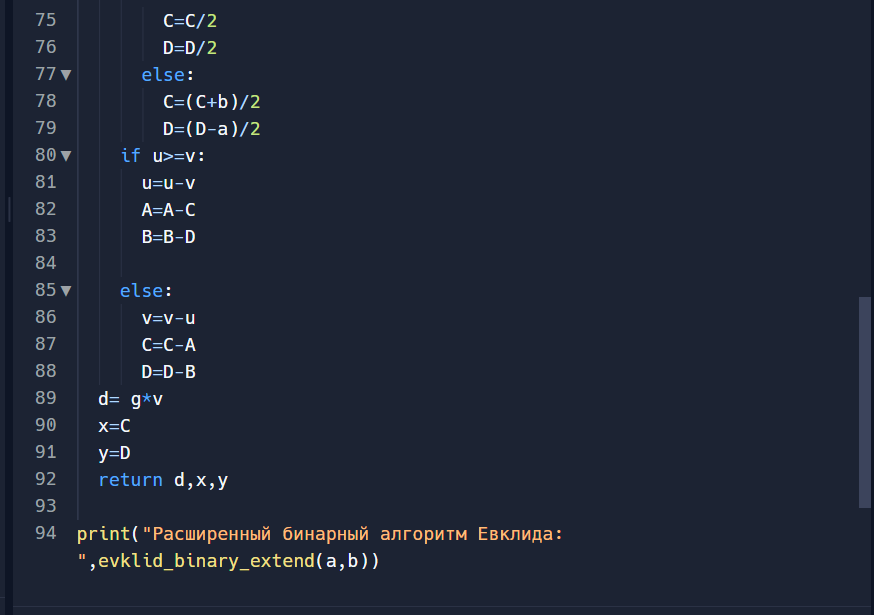


Figure 5: Функция для вычисления расширенного бинарного алгоритма Евклида. Вторая часть

1. Получил результат (рис. 6)

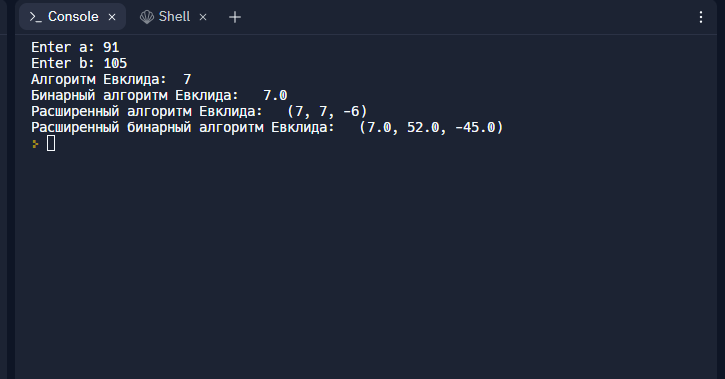


Figure 6: Результат алгоритмов

# Выводы

Реализовал алгоритм вычисления наибольшего общего делителя (Евклида).

# Список литературы

1. Алгоритм Евклида [Электронный ресурс] - Режим доступа: https://scienceland.info/

algebra8/euclid-algorithm

1. Бинарный алгоритм вычисления НОД [Электронный ресурс] - Режим доступа: https://intellect.icu/binarnyj-algoritm-vychisleniya-nod-4394