Информационная безопасность. Отчет по лабораторной работе № 4

Вычисление наибольшего общего делителя

Мухамеджанов Исматулло Иззатуллоевич

Содержание

# 1 Цель работы

Освоить на практике применение вычисление Наибольшего Общего Делителя(НОД).

# 2 Указание к работе

Алгоритм Евклида

Бинарный алгоритм Евклида

Расширенный алгоритм Евклида

Расширенный бинарный алгоритм Евклида

# 3 Выполнение лабораторной работы

1. Алгоритм Евклида.

Вход. Целые числа n, b; 0 < b Е а. Выход.d -— НОД(n, b). ПОЛОЖИТЬ Р О, гу b, i ‹= 1. Найти остаток гдр рот деления r¡\_ наг¡. Если my = 0, то положить d +- r¡. В противном случае положить i +- i -1- 1 и вернуться на віаг 2. Результат: d. Бинарный алгоритм ЕвклиЬа является более быстрым при реализации на компьютере, поскольку использует двоичное представление чисел п и Ь. hинарный алгоритм Евклида основан па следутощих свойствах наиболыиего общего делитепя (считаем, что 0 < b й n): если оба числа n и b четнме, то Н0Д(n, b) —— 2 Н0Д(J, ); если число n — нечетное, число b — четное, то Н0Д(n, b) НОД(n,2) если оба числа n и b нечетные, n > b, то Н0Д(n, b) —— НОД(n — b,b),’ если n = b, то Н0Д(n, b) —— n.

1. Бинарный алгоритм 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[1]. Но это преимущество в скорости теряется с увеличением разницы между целыми числами более чем на несколько порядков, в результате чего число итераций вычитания (см. шаги 6, 7 в разделе Алгоритм) может многократно превышать число итераций обычного алгоритма, использующего сравнение по модулю. То есть скорость бинарных сдвигов дает эффект только для чисел близких друг другу.

Возможно, алгоритм был известен еще в Китае 1-го века[2], но опубликован был лишь в 1967 году израильским физиком и программистом Джозефом Стайном. Он основан на использовании следующих свойств НОД:

НОД(2m, 2n) = 2 НОД(m, n), НОД(2m, 2n+1) = НОД(m, 2n+1), НОД(-m, n) = НОД(m, n)

1. Расширенный алгоритм Евклида. Целые числа a,b: 0 < b <= a Выход НОД(a,b); такие числа x,y, что ax + by = d
2. Расширенный бинарный алгоритм Евклида. Целые числа a,b: 0 < b <= a Выход НОД(a,b) g = 1 a и b нечетные, a = a / 2 , b = b /2 , g = 2\*g пока a или b один из них не станет нечётным u = a, v = b, A = 1, B = 0, C = 0, D = 1 U != 0, u %2 == 0 : u = u / 2, A = A /2, B = B /2, A = (A + b) / 2, B = (B - a) / 2 v %2 == 0 : v = v / 2, C = C /2, D = D /2, C = (C + b) / 2, D = (D - a) / 2 u >= v, u = u - v, A = A - C, B = B - D, else v = v - u, C = C - A, D = D - B

d = g\*v, x = C, y = D Вывод d,x,y

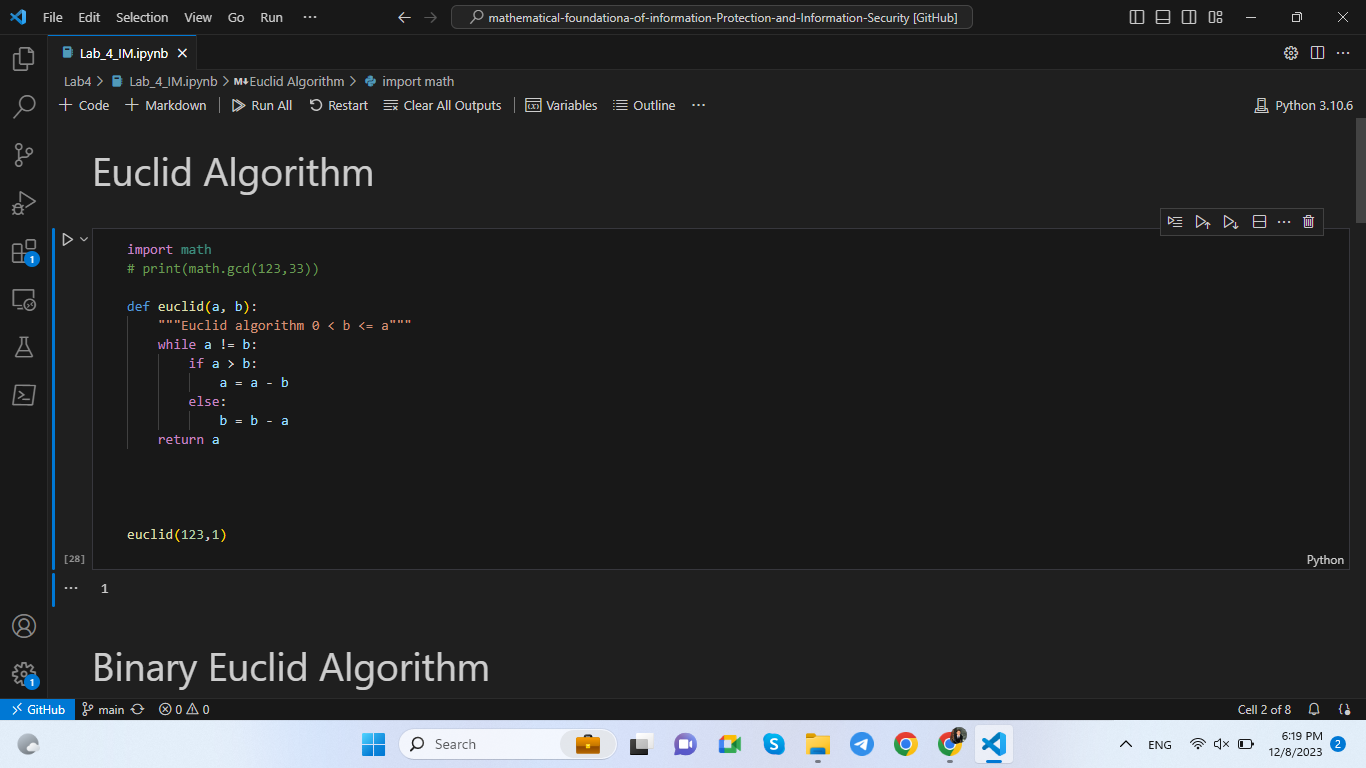


Figure 1: Программа (1)

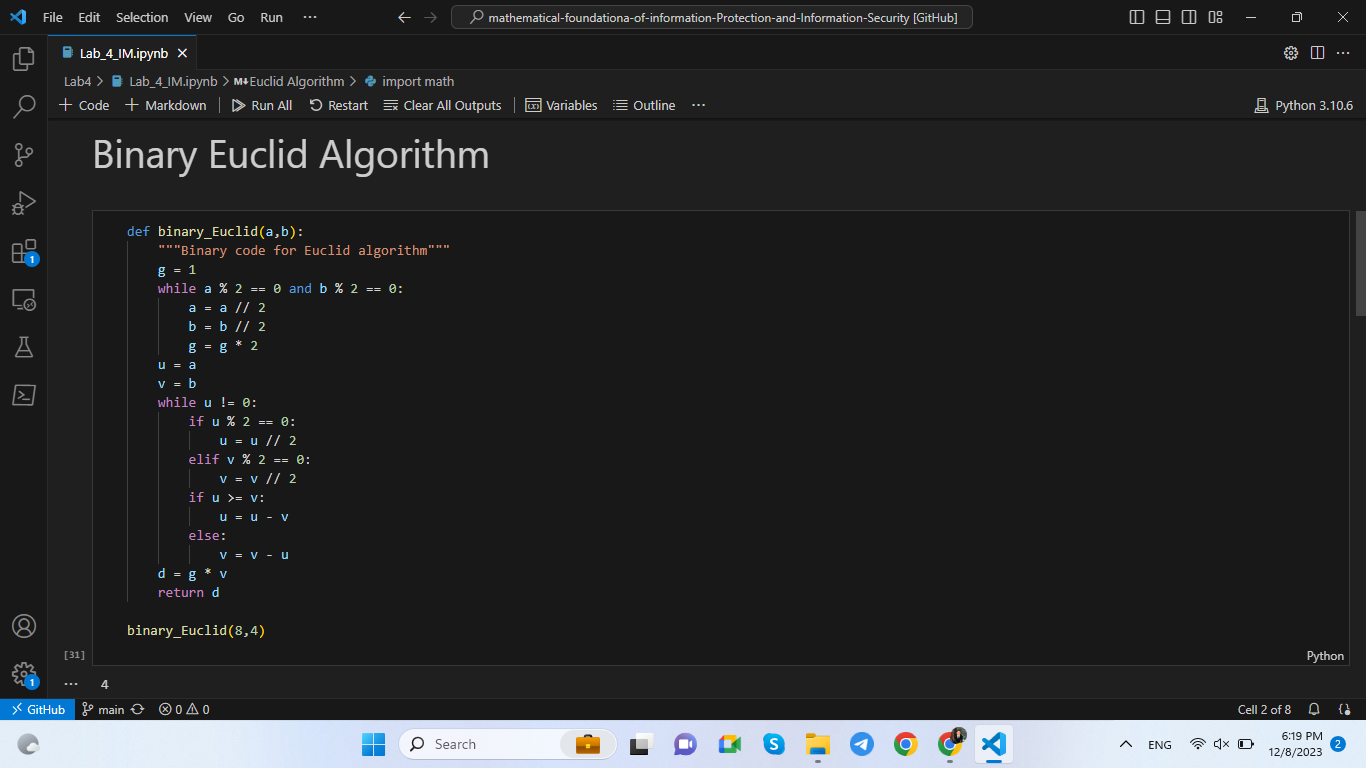


Figure 2: Программа (2)

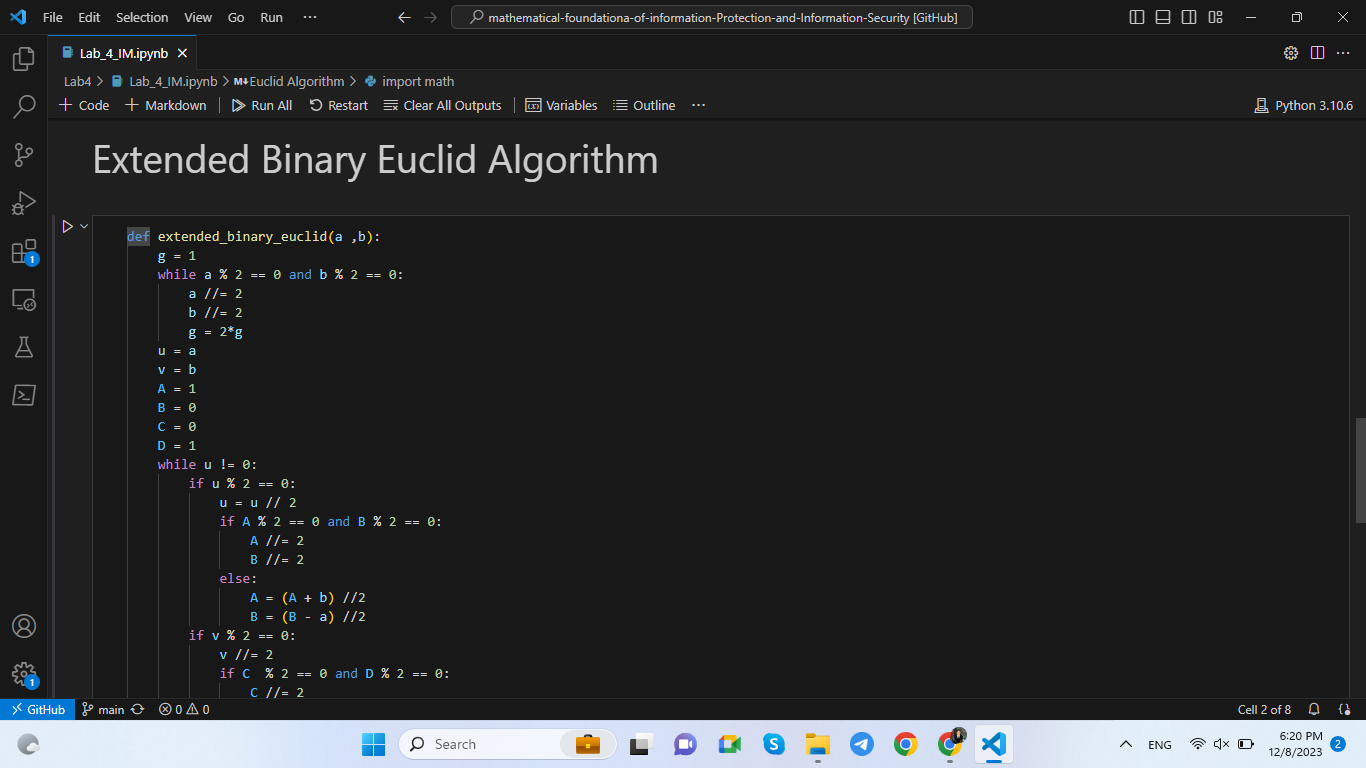


Figure 3: Программа (3)

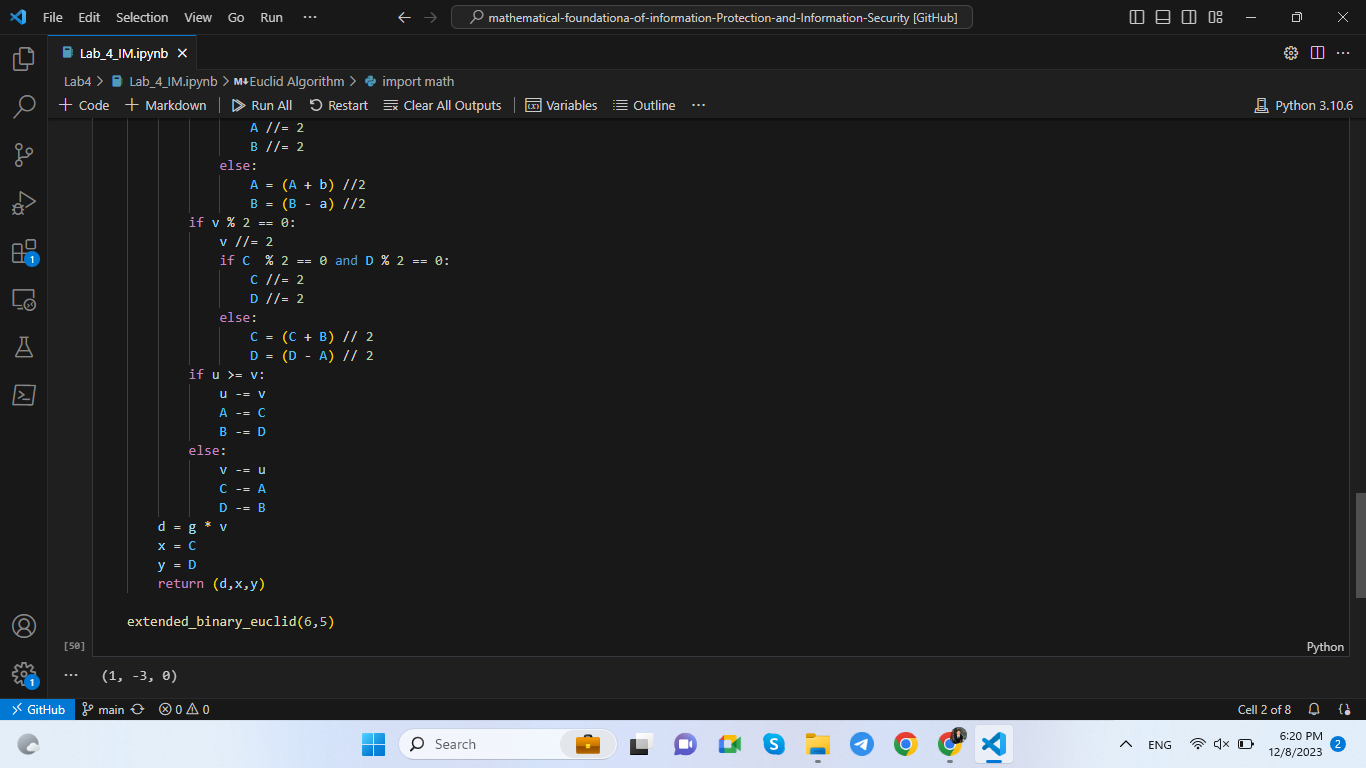


Figure 4: Программа (4)

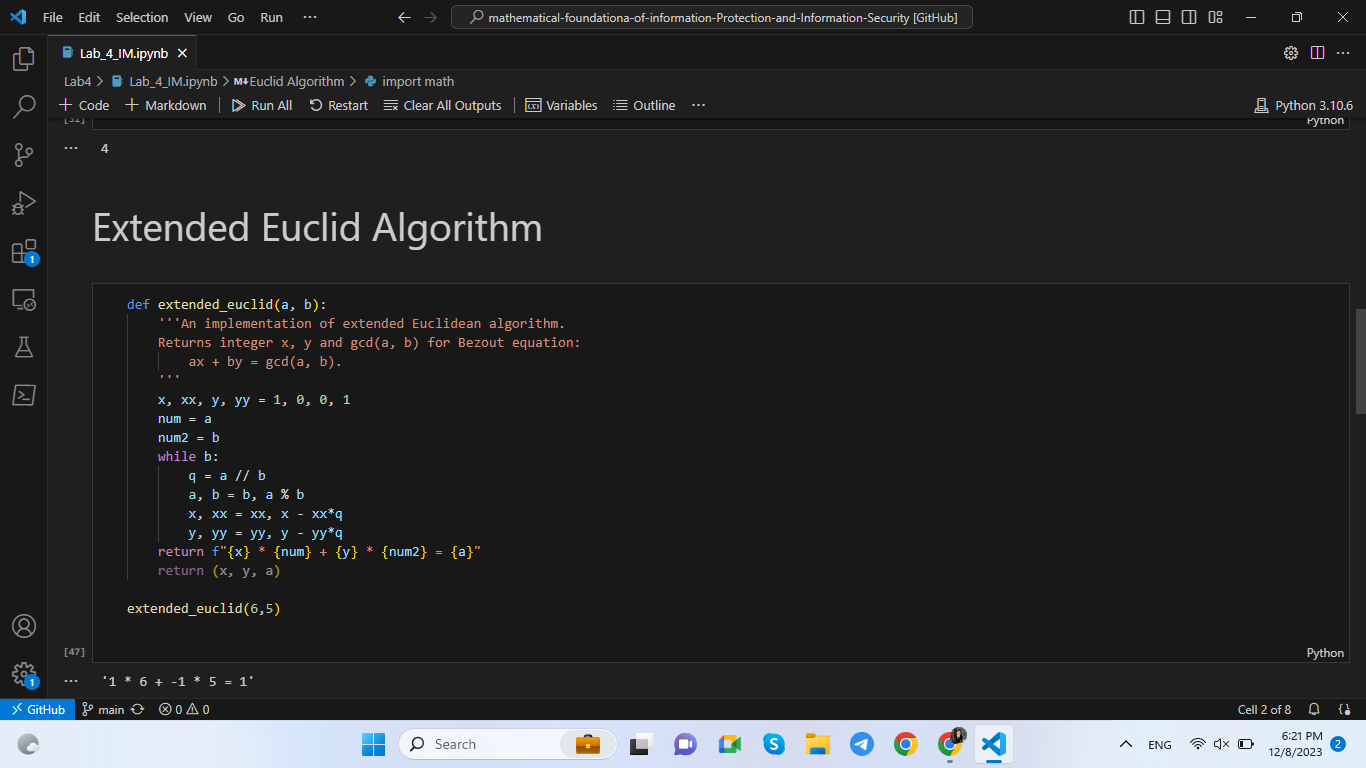


Figure 5: Программа (5)

# 4 Выводы

Освоены методы определения НОД

# 5 Список литературы

1. Методические материалы курса
2. Википедия