Лабораторная работа №4. Вычисление НОД.

Предмет: Математические основы защиты информации и информационной безопасности

Александр Сергеевич Баклашов

Содержание

# 1 Цель работы

Рассмотреть и реализовать алгоритмы нахождения НОД.

# 2 Задание

Реализовать следующие алгоритмы:

* Алгоритм Евклида;
* Бинарный алгоритм Евклида;
* Расширенный алгоритм Евклида;
* Расширенный бинарный алгоритм Евклида.

# 3 Теоретическое введение

## 3.1 Алгоритмы Евклида

Алгоритм 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.), который впервые описал его в VII и X книгах «Начал». 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 разницы между большим и меньшим числом. Процесс повторяется, пока числа не станут равными. Найденное число и есть наибольший общий делитель исходной пары. Евклид предложил алгоритм только для натуральных чисел и геометрических величин (длин, площадей, объёмов). Однако в XIX веке он был обобщён на другие типы математических объектов, включая целые числа Гаусса и полиномы от одной переменной. Это привело к появлению в современной общей алгебре такого понятия, как евклидово кольцо. Позже алгоритм Евклида был обобщён на другие математические структуры, такие как узлы и многомерные полиномы.

Для данного алгоритма существует множество теоретических и практических применений. В частности, он является основой для криптографического алгоритма с открытым ключом RSA, широко распространённого в электронной коммерции. Также алгоритм используется при решении линейных диофантовых уравнений, при построении непрерывных дробей, в методе Штурма. Алгоритм Евклида является основным инструментом для доказательства теорем в современной теории чисел, например таких как теорема Лагранжа о сумме четырёх квадратов и основная теорема арифметики.

# 4 Выполнение лабораторной работы

## 4.1 Алгоритм Евклида

### 4.1.1 Задача

Реализовать алгоритм Евклида

#### 4.1.1.1 Решение

Реализуем алгоритм Евклида (рис. [1](#fig:001))

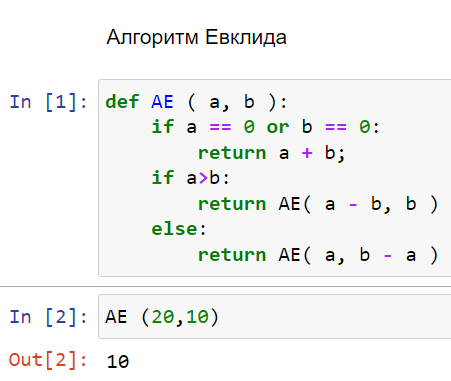


Figure 1: Алгоритм Евклида

## 4.2 Бинарный алгоритм Евклида

### 4.2.1 Задача

Реализовать бинарный алгоритм Евклида

#### 4.2.1.1 Решение

Реализуем бинарный алгоритм Евклида (рис. [2](#fig:002))



Figure 2: Бинарный алгоритм Евклида

## 4.3 Расширенный алгоритм Евклида

### 4.3.1 Задача

Реализуем расширенный алгоритм Евклида (рис. [3](#fig:003))

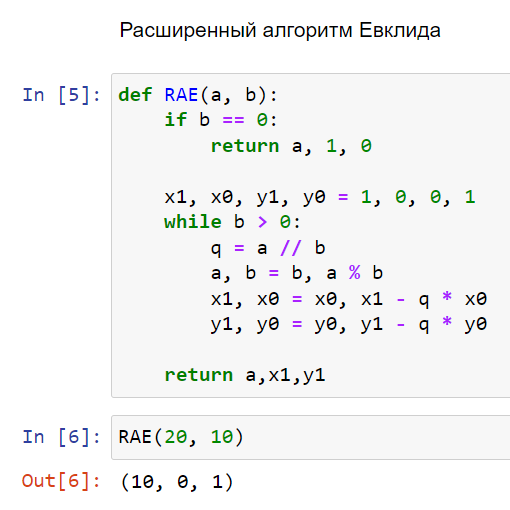


Figure 3: Расширенный алгоритм Евклида

## 4.4 Расширенный бинарный алгоритм Евклида

### 4.4.1 Задача

Реализуем расширенный бинарный алгоритм Евклида (рис. [4](#fig:004))

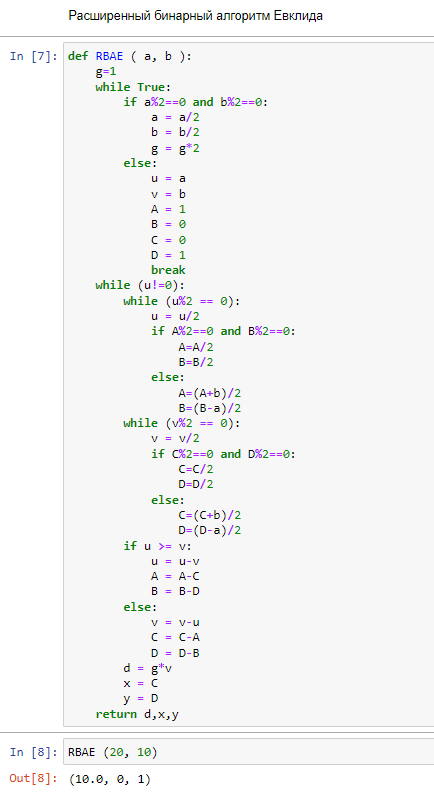


Figure 4: Расширенный бинарный алгоритм Евклида

# 5 Выводы

В ходе данной лабораторной работы я рассмотрел и реализовал следующие алгоритмы:

* Алгоритм Евклида;
* Бинарный алгоритм Евклида;
* Расширенный алгоритм Евклида;
* Расширенный бинарный алгоритм Евклида.

# 6 Библиография

1. Python documentation. [Электронный ресурс]. М. URL: [Python documentation](https://docs.python.org/3/index.html) (Дата обращения: 28.09.2023).
2. Лабораторная работа №4. Вычисление НОД. - 4 с. [Электронный ресурс]. М. URL: [Лабораторная работа №4. Вычисление НОД.](https://esystem.rudn.ru/pluginfile.php/2089804/mod_folder/content/0/lab04.pdf) (Дата обращения: 19.10.2023).