Отчёт по лабораторной работе №4

Дисциплина: Математические основы защиты информации и информационной безопасности

Дэнэилэ Александр Дмитриевич, НПМмд-02-23

Содержание

# Цель работы

Изучить алгоритмы вычисления наибольшего общего делителя.

# Задание

1. Реализовать алгоритм Евклида.
2. Реализовать бинарный алгоритм Евклида
3. Реализовать расширенный алгоритм Евклида
4. Реализовать расширенный бинарный алгоритм Евклида

# Теоретическое введение

Пусть числа и целые и . Разделить на с остатком - значит представить в виде , где и . Число называется неполным частным, число - неполным остатком от деления на .

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

1. Каждое из чисел делится на ;
2. Если - другой общий делитель чисел , то делится на .

Например, НОД(12345, 24690) = 12345, НОД(12345, 54321) = 3, НОД(12345, 12541) = 1.

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

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

Например, НОД чисел 91, 105, 154 равен 7. В качестве линейного представления можно взять

либо

Целые числа называются *взаимно простыми в совокупности*, если НОД() = 1. Целые числа и называются *взаимно* простыми, если НОД(*a, b*) = 1.

Целые числа называются *попарно взаимно простыми*, если НОД() = 1 для всех .

# Выполнение лабораторной работы

1. Реализация алгоритма Евклида нахождения наименьшего общего делителя (рис. [1](#fig:001)).

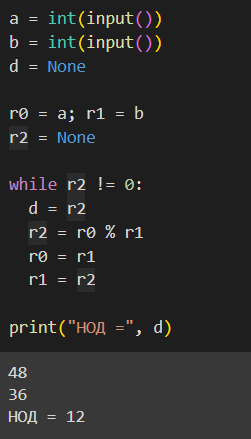


Figure 1: Алгоритм Евклида

1. Реализация бинарного алгоритма Евклида нахождения наименьшего общего делителя (рис. [2](#fig:002)).

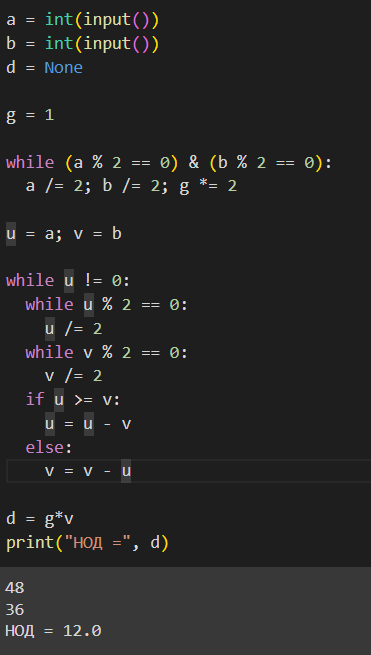


Figure 2: Бинарный алгоритм Евклида

1. Реализация расширенного алгоритм Евклида нахождения наименьшего общего делителя и представление его в виде линейной комбинации чисел и (рис. [3](#fig:003)).

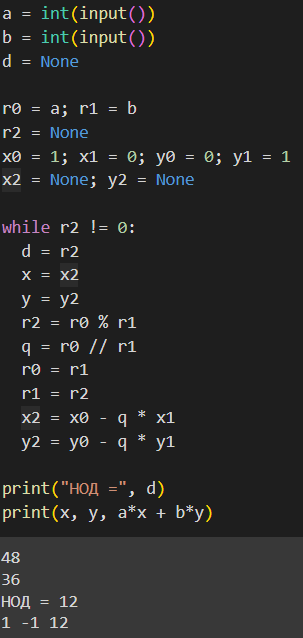


Figure 3: Расширенный алгоритм Евклида

1. Реализация расширенного бинарного алгоритма Евклида нахождения наименьшего общего делителя и представление его в виде линейной комбинации чисел и (рис. [4](#fig:004)).

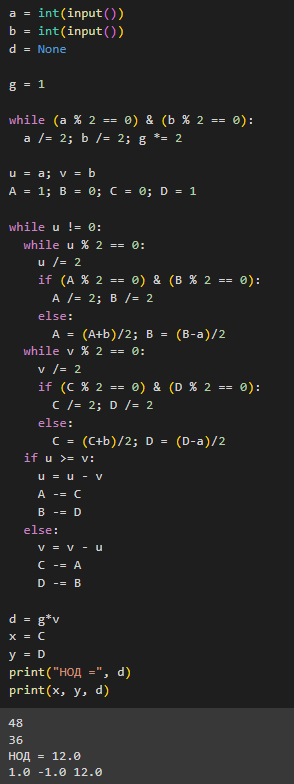


Figure 4: Расширенный бинарный алгоритм Евклида

# Выводы

Ознакомился с различными вариациями реализации алгоритмов нахождения наименьшего общего делителя.

# Список литературы