Отчёт по лабораторной работе №4

Дисциплина: Математические основы защиты информации и информационной безопасности

Полиенко Анастасия Николаевна, НПМмд-02-23

Содержание

# 1 Цель работы

Изучить алгоритмы вычисления наибольшего общего делителя.

# 2 Задание

Реализовать алгоритм Евклида в четырёх его вариациях:

1. Алгоритм Евклида
2. Бинарный алгоритм Евклида
3. Расширенный алгоритм Евклида
4. Расширенный бинарный алгоритм Евклида

# 3 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

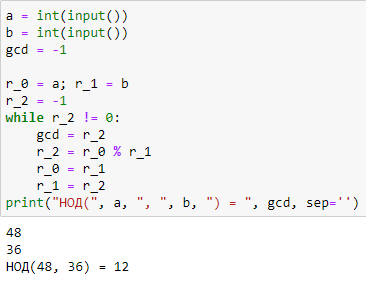
Целые числа называются *взаимно простыми в совокупности*, если НОД() = 1. Целые числа и называются *взаимно* простыми, если НОД(*a, b*) = 1.

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

Более подробно см. в [1–6].

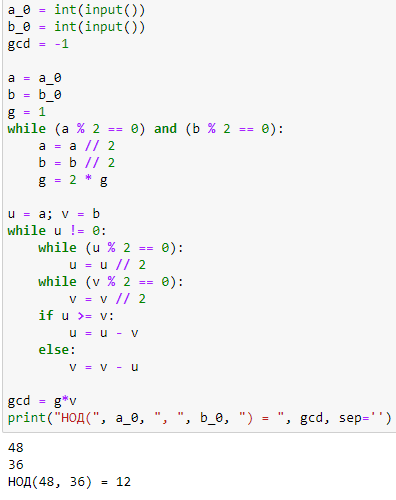
# 4 Выполнение лабораторной работы

1. Реализуем алгоритм Евклида нахождения наименьшего общего делителя (рис. ??).



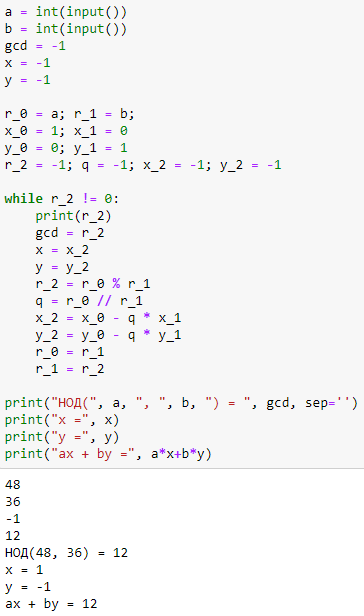
Алгоритм Евклида

1. Реализуем бинарный алгоритм Евклида нахождения наименьшего общего делителя (рис. ??).



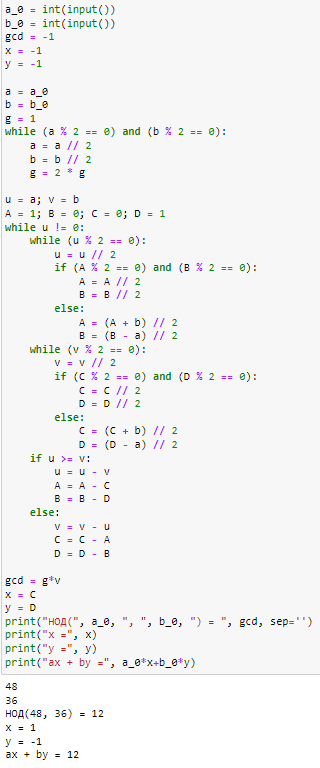
Бинарный алгоритм Евклида

1. Реализуем расширенный алгоритм Евклида нахождения наименьшего общего делителя и представления его в виде линейной комбинации чисел и (рис. ??).



Расширенный алгоритм Евклида

1. Реализуем расширенный бинарный алгоритм Евклида нахождения наименьшего общего делителя и представления его в виде линейной комбинации чисел и (рис. ??).



Расширенный бинарный алгоритм Евклида

# 5 Выводы

Изучила алгоритмы нахождения наименьшего общего делителя.

# Список литературы

1. GNU Bash Manual [Электронный ресурс]. Free Software Foundation, 2016. URL: <https://www.gnu.org/software/bash/manual/>.

2. Newham C. [Learning the bash Shell: Unix Shell Programming](http://www.amazon.com/Learning-bash-Shell-Programming-Nutshell/dp/0596009658). O’Reilly Media, 2005. 354 с.

3. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.

4. Robbins A. [Bash Pocket Reference](https://www.ncbi.nlm.nih.gov/pubmed/25246403). O’Reilly Media, 2016. 156 с.

5. Таненбаум Э. Архитектура компьютера. 6-е изд. СПб.: Питер, 2013. 874 с.

6. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.