

# Отчёт по лабораторной работе №4.

## Вычисление наибольшего общего делителя

---

*Дисциплина: Математические основы защиты информации  
и информационной безопасности*

**Студент:** Майорова О.А., 1032212322

**Группа:** НФИмд-02-21

**Преподаватель:** д.ф.-м.н., Кулябов Д. С.

Москва, 2021

Цель: Ознакомиться с методами вычисления наибольшего общего делителя.

Задача: Программно реализовать алгоритмы вычисления наибольшего общего делителя для двух чисел: алгоритм Евклида, бинарный алгоритм Евклида, расширенный алгоритм Евклида, расширенный бинарный алгоритм Евклида.

Наибольшим общим делителем (НОД) двух чисел  $a$  и  $b$  называется наибольшее число, на которое  $a$  и  $b$  делятся без остатка  $\text{НОД}(a, b)$ .

НОД существует и однозначно определён, если хотя бы одно из чисел  $a$  или  $b$  не равно нулю.

Понятие наибольшего общего делителя естественным образом обобщается на наборы из более чем двух целых чисел.

# Алгоритм Евклида

Вход: целые числа  $a, b : 0 < b \leq a$

Выход:  $d = \text{НОД}(a, b)$

Проверка функции алгоритма Евклида:

```
1 Euclid(4269, 228)
```

3

```
1 Euclid(888888, 666)
```

222

# Бинарный алгоритм Евклида

Вход: целые числа  $a, b : 0 < b \leq a$

Выход:  $d = \text{НОД}(a, b)$

Проверка функции бинарного алгоритма Евклида:

```
1 BiEuclid(4269, 228)
```

3.0

```
1 BiEuclid(888888, 666)
```

222.0

# Расширенный алгоритм Евклида

Вход: целые числа  $a, b : 0 < b \leq a$

Выход:  $d = \text{НОД}(a, b)$ ,  $x, y$ , где  $x, y$  - такие целые числа, что  $ax + by = d$

Проверка функции расширенного алгоритма Евклида:

```
1 ExtEuclid(4269, 228)
```

```
(3, -29.0, 543.0)
```

```
1 ExtEuclid(888888, 666)
```

```
(222, -1.0, 1335.0)
```

# Расширенный бинарный алгоритм Евклида

Вход: целые числа  $a, b : 0 < b \leq a$

Выход:  $d = \text{НОД}(a, b)$ ,  $x, y$ , где  $x, y$  - такие целые числа, что  $ax + by = d$

Проверка ф-ии расширенного бинарного алгоритма Евклида:

```
1 ExtBiEuclid(4269, 228)
```

```
(3.0, 123.0, -2303.0)
```

```
1 ExtBiEuclid(888888, 666)
```

```
(222.0, -10.0, 13347.0)
```

Таким образом, была достигнута цель, поставленная в начале лабораторной работы. Было осуществлено знакомство с методами вычисления наибольшего общего делителя чисел: алгоритм Евклида, бинарный алгоритм Евклида, расширенный алгоритм Евклида, расширенный бинарный алгоритм Евклида. Также была получена реализация на языке Python рассмотренных алгоритмов для двух чисел.



**Спасибо за внимание**

---