

# Алгоритм Евклида

---

Константин Тохсыров

27 октября, 2023, Москва, Россия

Российский Университет Дружбы Народов

# Цели и задачи

---

# Цель лабораторной работы

Изучение алгоритма Евклида нахождения НОД и его вариаций.

# **Выполнение лабораторной работы**

---

# Наибольший общий делитель

Наибольший общий делитель (НОД) – это число, которое делит без остатка два числа и делится само без остатка на любой другой делитель данных двух чисел. Проще говоря, это самое большое число, на которое можно без остатка разделить два числа, для которых ищется НОД.

# Алгоритм Евклида

- Вход. Целые числа  $a, b$ ;  $0 < b < a$ .
  - Выход.  $d = \text{НОД}(a, b)$ .
1. Положить  $r_0 = a, r_1 = b, i = 1$ .
  2. Найти остаток  $r_{i-1} \bmod r_i$  от деления  $r_{i-1}$  на  $r_i$ .
  3. Если  $r_{i-1} \bmod r_i = 0$ , то положить  $d = r_i$ . В противном случае положить  $i = i + 1$  и вернуться на шаг 2.
  4. Результат:  $d$ .

## Бинарный алгоритм Евклида

- Вход. Целые числа  $a, b$ ;  $0 < b \leq a$ .
  - Выход.  $d = \text{НОД}(a, b)$ .
1. Положить  $g = 1$ .
  2. Пока оба числа  $a$  и  $b$  четные, выполнять  $a = a/2, b = b/2, g = 2g$  до получения хотя бы одного нечетного значения  $a$  или  $b$ .
  3. Положить  $u = a, v = b$ .
  4. Пока  $u \neq 0$ , выполнять следующие действия.
    - Пока  $u$  четное, полагать  $u = u/2$ .
    - Пока  $v$  четное, полагать  $v = v/2$ .
    - При  $u \geq v$  положить  $u = u - v$ . В противном случае положить  $v = v - u$ .
  5. Положить  $d = gv$ .
  6. Результат:  $d$

# Расширенный алгоритм Евклида

- Вход. Целые числа  $a, b$ ;  $0 < b \leq a$ .
- Выход:  $d = \text{НОД}(a, b)$ ; такие целые числа  $x, y$ , что  $ax + by = d$ .

1. Положить

$$r_0 = a, r_1 = b, x_0 = 1, x_1 = 0, y_0 = 0, y_1 = 1, i = 1$$

2. Разделить с остатком  $r_{i-1}$  на  $r_i$  :

$$r_{(i-1)} = q_i * r_i + r_{i+1}$$

3. Если  $r_{(i+1)} = 0$ , то положить  $d = r_i, x = x_i, y = y_i$ . В противном случае положить  $x_{(i+1)} = (x_{(i-1)} - q_i * x_i, y_{(i+1)} = (y_{(i-1)} - q_i * y_i, i = i + 1$  и вернуться на шаг 2.

4. Результат:  $d, x, y$ .



## Пример работы алгоритма

```
In [5]: 1 a = 7**15  
        2 b = 7**8
```

```
In [6]: 1 euklid_simply(a, b)
```

```
Out[6]: 5764801
```

```
In [7]: 1 euklid_ext(a, b)
```

```
Out[7]: (5764801, 0, 1)
```

```
In [8]: 1 euklid_bin(a, b)
```

```
Out[8]: 5764801
```

```
In [9]: 1 euklid_bin_ext(a, b)
```

```
Out[9]: (5764801, 0, 1)
```

## **Выводы**

---

Изучили алгоритм Евклида нахождения НОД.