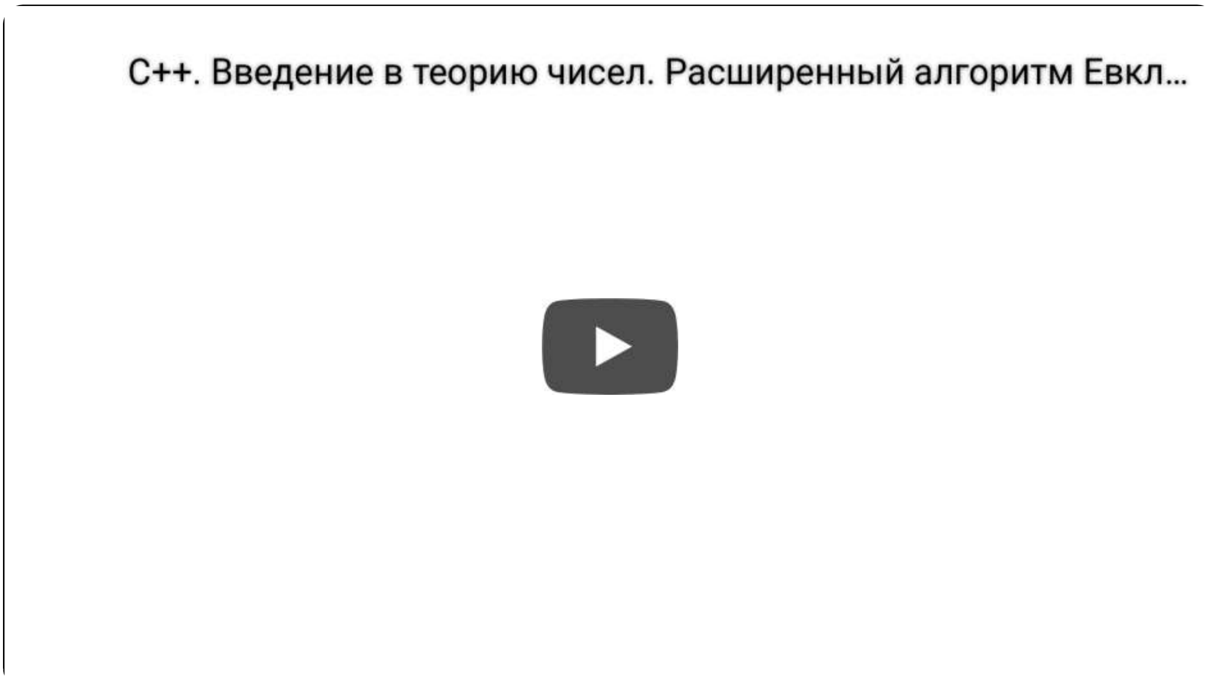
Расширенный алгоритм Евклида



Расширенный алгоритм Евклида

Рассмотрим следующее уравнение:

$ax + by = c$, где a, b и c – целые числа, $a \geq 0$, $b \geq 0$. Гарантируется, что $a \neq 0$ или $b \neq 0$. Необходимо найти все пары целых чисел x и y, которые являются решением уравнения.

Пусть $d = gcd(a, b)$. Если c не делится на d, то уравнение не имеет решений.

Рассмотрим уравнение:

$$ax_0 + by_0 = d$$

Пусть мы нашли решение уравнения

$$bx_1 + (a\%b)y_1 = d$$

Данное уравнение можно переписать в виде:

$$bx_1 + (a - \left\lfloor \frac{a}{b} \right\rfloor b)y_1 = d$$

Отсюда

$$ay_1 + b(x_1 - \left\lfloor \frac{a}{b} \right\rfloor y_1) = d$$

Следовательно

$$x_0 = y_1$$
$$y_0 = x_1 - \left\lfloor \frac{a}{b} \right\rfloor y_1$$

Таким образом, получаем соотношения для рекурсивного алгоритма поиска решения уравнения. Такой алгоритм называется расширенным алгоритмом Евклида.

Рекурсия в этом алгоритме будет прекращаться в тот момент, когда $b = 0$, так же, как и в обычном алгоритме Евклида.

Заметим, что алгоритм найдёт только одно решение уравнения — x_0 и y_0. Все остальные подходящие пары x и y связаны следующим свойством:

$$x = x_0 + \frac{b}{d}t$$
$$y = y_0 - \frac{a}{d}t,$$

где t — любое целое число.

Вернёмся к изначальному уравенению $ax + by = c$. Пусть x_0 и y_0 — решение уравнения $ax_0 + by_0 = d$, тогда

$$x = \frac{c}{d}x_0 + \frac{b}{d}t$$
$$y = \frac{c}{d}y_0 - \frac{a}{d}t,$$

где t — любое целое число.

Реализация расширенного алгоритма Евклида

```
int gcd_ext(int a, int b, int& x, int& y) {
    if (b == 0) {
        x = 1;
        y = 0;
        return a;
    }
    int d = gcd_ext(b, a % b, x, y);
    x -= (a / b) * y;
    swap(x, y);
    return d;
}
```