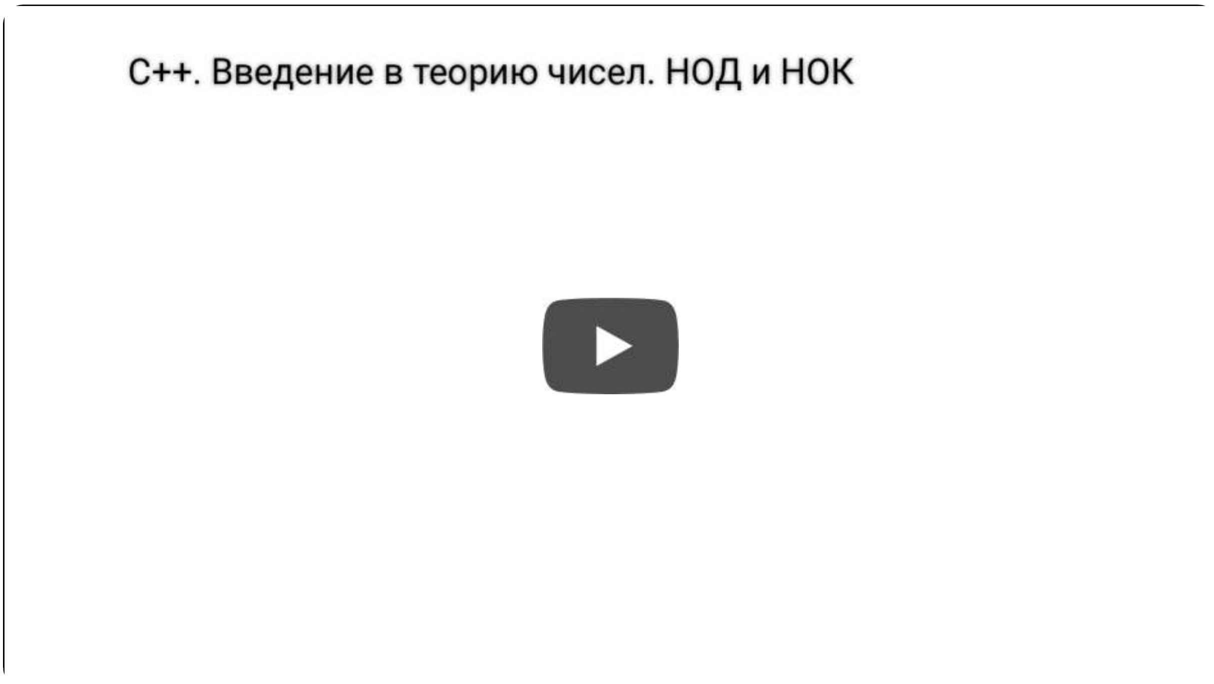
НОД и НОК



Наибольший общий делитель (НОД) двух целых чисел a и b, $a \neq 0$ или $b \neq 0$, – наибольшее целое число, которое является делителем a и b одновременно. В дальнейшем наибольший общий делитель будем обозначать gcd (от английского "greatest common divisor").

Для наибольшего общего делителя верны следующие свойства:

- $gcd(a, 0) = a$, при $a > 0$
- $gcd(a, b) = gcd(a - b, b)$, при $a \geq b > 0$
- $gcd(a, b) = gcd(a \% b, b)$, при $a \geq b > 0$

На основе последнего свойства можно написать алгоритм для поиска наибольшего общего делителя. Такой алгоритм называют алгоритмом Евклида. Его вычислительная сложность – $O(\log \min(a, b))$.

Рекурсивная реализация алгоритма Евклида

```
int gcd(int a, int b) {
    if (b == 0)
        return a;
    return gcd(b, a % b);
}
```

Нерекурсивная реализация алгоритма Евклида

```
int gcd(int a, int b) {
    while (b > 0) {
        a %= b;
        swap(a, b);
    }
    return a;
}
```

Наименьшее общее кратное (НОК) двух целых чисел a и b, $a \neq 0$ и $b \neq 0$, – наименьшее натуральное число, которое делится на a и b одновременно. В дальнейшем наименьшее общее кратное будем обозначать lcm (от английского "least common multiple").

Наибольший общий делитель и наименьшее общее кратное связаны между собой следующим свойством:

$$gcd(a,b) \cdot lcm(a,b) = a \cdot b$$

С помощью этого свойства мы можем найти наименьшее общее кратное двух чисел, пользуясь алгоритмом Евклида.

Основная теорема арифметики

Пусть дано натуральное число $n > 1$. Тогда существует и единственно представление n в виде $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, где $p_1 < p_2 < \dots < p_s$ — простые числа, а $\alpha_1, \alpha_2, \dots, \alpha_s$ — натуральные числа.

Воспользуемся этой теоремой, чтобы выписать формулы для НОД и НОК через разложения чисел на простые. Пусть нам даны два натуральных числа a и b. Выпишем их разложения на простые числа по основной теореме арифметики. Наборы простых в разложениях чисел a и b могут отличаться, поэтому объединим эти наборы в одно множество, в итоге получим:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_s^{\alpha_s},\ \alpha_i \geq 0$$

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_s^{\beta_s},\ \beta_i \geq 0$$

Тогда для НОД и НОК чисел a и b верны следующие формулы:

$$gcd(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdots p_s^{\min(\alpha_s, \beta_s)}$$

$$lcm(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \cdots p_s^{\max(\alpha_s, \beta_s)}$$