

Элементы теории чисел

Лектор профессор Ю.В. Нестеренко
механико-математический факультет МГУ
1 поток 1 курса, осень 2026г.

Лекция 3: Показатели $\nu_p(n)$ и их свойства. НОД и НОК нескольких чисел. Формулы для кратности вхождения простого числа в $n!$ и в наименьшее общее кратное всех натуральных чисел до заданной границы.

Алгоритм Евклида

Теорема 5

- 1. Уравнение $ax + by = c$ разрешимо в целых числах x, y тогда и только тогда, когда $(a, b) | c$.*
- 2. В случае разрешимости множество решений бесконечно. Все они имеют вид*

$$x = x_0 + \frac{b}{(a, b)}t, \quad y = y_0 - \frac{a}{(a, b)}t, \quad (1)$$

где пара чисел x_0, y_0 есть какое-либо фиксированное решение, а t – произвольное целое число.

Расширенный алгоритм Евклида.

- Натуральное число называется *составным*, если его можно представить в виде произведения двух меньших натуральных чисел.
- Натуральное число, отличное от 1, называется *простым*, если его нельзя представить в виде произведения меньших множителей.

Следствие 1

Каждое целое число $N > 1$ имеет простой делитель.

Теорема 6 (Теорема Евклида)

Множество простых чисел бесконечно.

Решето Эратосфена.

Теорема 7 (Основная теорема арифметики)

Каждое целое число, большее единицы, раскладывается в произведение простых чисел и притом единственным способом, если не учитывать порядок сомножителей.

§2.3. Показатели $\nu_p(n)$ и их свойства. НОД и НОК нескольких чисел.

Среди простых сомножителей, присутствующих в разложении $n = p_1 \cdots p_r$ могут быть и одинаковые. Например, $25 = 5 \cdot 5 = 5^2$. Их можно объединить вместе, воспользовавшись операцией возведения в степень. Кроме того, простые сомножители можно упорядочить по величине. В результате получается разложение

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad p_1 < p_2 < \dots < p_k.$$

- Такое представление числа называется *каноническим разложением* на простые сомножители. Например, каноническое представление числа 2520 имеет вид $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$.
- Набор различных простых чисел, а также набор показателей степени α_j определяются по числу n единственным способом.

Для кратности вхождения простого числа p в каноническое разложение числа n будет использоваться обозначение $\nu_p(n)$.

Если n не делится на простое p , будем считать $\nu_p(n) = 0$.

Например, $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$,

$$\nu_2(2520) = 3, \quad \nu_3(2520) = 2, \quad \nu_{11}(2520) = 0.$$

При таком определении справедливо представление

$$n = \prod_{p|n} p^{\nu_p(n)}. \quad (2)$$

Дальше будут использоваться подобные выражения с указанием под знаком произведения тех или иных условий на входящие в него простые числа.

- Иногда удобно бывает формально записывать и бесконечные произведения, если лишь конечное количество, входящих в них сомножителей отлично от единицы. Например, см. (2),

$$n = \prod_p p^{\nu_p(n)},$$

$$n = \prod_p p^{\nu_p(n)},$$

где произведение берется по бесконечному множеству всех простых чисел. В этом произведении лишь конечное количество сомножителей отлично от единицы, ведь $\nu_p(n) \neq 0$ лишь для простых делителей p числа n , а это множество конечно.

- При умножении степеней с одинаковым основанием показатели степени складываются, поэтому

1. *для любых двух целых чисел a, b и простого числа p выполняется равенство*

$$\nu_p(ab) = \nu_p(a) + \nu_p(b). \quad (3)$$

$$\nu_p(ab) = \nu_p(a) + \nu_p(b).$$

- Отсюда, в частности следует, что

2. *целое число n делится на число d в том и только том случае, когда для любого простого числа p выполняются неравенства*

$$\nu_p(d) \leq \nu_p(n). \quad (4)$$

- Действительно, равенство $n = d \cdot u$ в силу последнего равенства и неравенства $\nu_p(u) \geq 0$ приводит к (4).
- Если же наоборот, для любого простого числа p выполняется неравенство (4), то целое число

$$u = \prod_p p^{\nu_p(n) - \nu_p(d)}$$

удовлетворяет равенству $n = du$ и, значит, $d|n$.

Ещё одно простое, но полезное свойство будет использоваться в дальнейшем.

3. Если a и b – натуральные числа, причем для каждого простого числа p выполнено равенство $\nu_p(a) = \nu_p(b)$, то $a = b$.

- Действительно, из условия следует, что для любого простого числа p выполняются неравенства $\nu_p(a) \leq \nu_p(b)$ и $\nu_p(a) \geq \nu_p(b)$. Первые неравенства означают, что $a|b$, а вторые, что $b|a$. Теперь, учитывая, что a и b положительны, заключаем, что $a = b$.

НОД и НОК нескольких чисел.

Определим канонические разложения НОК и НОД нескольких натуральных чисел.

Следствие 2

Для любых натуральных чисел $a_1, \dots, a_m$ и любого простого числа p справедливы равенства

$$\nu_p([a_1, \dots, a_m]) = \max\{\nu_p(a_1), \dots, \nu_p(a_m)\} \quad (5)$$

$$\nu_p((a_1, \dots, a_m)) = \min\{\nu_p(a_1), \dots, \nu_p(a_m)\} \quad (6)$$

Доказательство следствия 2.

Определим целое число M равенством

$$M = \prod_p p^{\max\{\nu_p(a_1), \dots, \nu_p(a_m)\}}.$$

Из неравенств $\nu_p(M) \geq \nu_p(a_j)$ следует $a_j | M$, т.е. M – общее кратное чисел $a_1, \dots, a_m$. Если K – какое-нибудь общее кратное этих чисел, то при любом простом p должны выполняться неравенства

$$\begin{aligned}\nu_p(K) &\geq \nu_p(a_j), & j = 1, \dots, m, \\ \nu_p(K) &\geq \max\{\nu_p(a_1), \dots, \nu_p(a_m)\} = \nu_p(M).\end{aligned}$$

Следовательно, $M | K$ и $M \leq K$. Это доказывает, что M есть НОК данных чисел, а также равенство (5).

Равенство (6) доказывается аналогично.

Равенства (5) и (6) могут использоваться для вычисления наименьшего кратного и наибольшего общего делителя нескольких чисел. Так имеем

$$2737 = 7 \cdot 17 \cdot 23, \quad 9163 = 7^2 \cdot 11 \cdot 17, \quad 9639 = 3^4 \cdot 7 \cdot 17$$

и, значит,

$$\begin{aligned} [2737, 9163, 9639] &= 3^4 \cdot 7^2 \cdot 11 \cdot 17 \cdot 23 = 17070669, \\ (2737, 9163, 9639) &= 7 \cdot 17 = 119. \end{aligned}$$

Этот способ, однако, применим лишь, если числа сравнительно невелики.

Разложение на простые сомножители больших чисел – очень трудоёмкая задача.

- В таком случае для нахождения НОД и НОК нескольких чисел $a_1, a_2, \dots, a_n$ удобнее использовать равенства

$$(a_1, \dots, a_n) = (a_1, \dots, a_{n-2}, (a_{n-1}, a_n)), \quad (7)$$

$$[a_1, \dots, a_n] = [a_1, \dots, a_{n-2}, [a_{n-1}, a_n]], \quad (8)$$

легко выводимые из следствия 2.

Действительно, $\min\{\nu_p(a_{n-1}), \nu_p(a_n)\} = \nu_p((a_{n-1}, a_n))$ и для $D = (a_1, \dots, a_n)$ имеем

$$\nu_p(D) = \min_{1 \leq k \leq n} \nu_p(a_k) = \min\{\nu_p(a_1), \dots, \nu_p(a_{n-2}), \nu_p((a_{n-1}, a_n))\}$$

- Пользуясь алгоритмом Евклида для вычисления НОД и НОК двух чисел, а также равенствами (7) и (8), можно вычислять НОД и НОК нескольких чисел. Например,

$$(2737, 9163, 9639) = (2737, (9163, 9639)) = (2737, 476) = 119.$$

Целая часть числа.

- Целой частью действительного числа x называется наибольшее целое число k , удовлетворяющее неравенству $k \leq x$. Обозначается эта функция $[x]$.
- **Пример:** $[2, 5] = 2$, $[\pi] = 3$, $[-1, 3] = -1$.
- Складывая неравенства $[x] \leq x$ и $[y] \leq y$, получаем $[x] + [y] \leq x + y$, и, по определению $[x] + [y] \leq [x + y]$. Это неравенство справедливо и при любом количестве слагаемых, что легко доказать с помощью индукции. Из определения следует, что
- при любом x справедливы неравенства $[x] \leq x < [x] + 1$. Из них для любого $n \in \mathbb{Z}$ находим
- $[x] + n \leq x + n < [x] + n + 1$ и согласно определению целой части $[x + n] = [x] + n$.

При любом действительном x и любом натуральном a выполняется равенство

$$\left[\frac{[x]}{a} \right] = \left[\frac{x}{a} \right], \quad (9)$$

- Действительно, обозначим $q = \left[\frac{x}{a} \right]$. Тогда $aq \leq x < a(q+1)$ и

$$aq \leq [x] \leq x < a(q+1).$$

- Разделив эти неравенства на a , получаем

$$q \leq \frac{[x]}{a} < q+1,$$

что и доказывает (9).

Дробная часть числа

Функция $\{x\} = x - [x]$ называется *дробной частью* числа x .
Она удовлетворяет неравенствам $0 \leq \{x\} < 1$ и имеет период 1.
Действительно, $\{x + 1\} = x + 1 - [x + 1] = x - [x] = \{x\}$.
Например,

$$\{-1, 3\} = \{-1, 3 + 2\} = \{0, 7\} = 0, 7.$$

Каноническое разложение для НОК всех $n \leq x$.

Обозначим для каждого действительного числа $x \geq 1$ символом $K(x)$ наименьшее общее кратное всех натуральных чисел, не превосходящих x .

Лемма 1

Для любого действительного $x \geq 1$ имеем

$$K(x) = \prod_{p \leq x} p^{\left[\frac{\ln x}{\ln p} \right]}.$$

Доказательство леммы 1.

$$K(x) = \prod_{p \leq x} p^{\left\lfloor \frac{\ln x}{\ln p} \right\rfloor} \quad ?$$

Для каждого простого числа p с помощью (5) имеем $\nu_p(K(x)) = \max_{1 \leq u \leq x} \nu_p(u)$. Если $k = \nu_p(u)$ для некоторого $u \leq x$, то $p^k | u$ и $p^k \leq u \leq x$. Значит, $k \leq \frac{\ln x}{\ln p}$. Но тогда $\nu_p(u) = k \leq \left\lfloor \frac{\ln x}{\ln p} \right\rfloor$. Эта оценка и неравенство

$$p^{\left\lfloor \frac{\ln x}{\ln p} \right\rfloor} \leq p^{\frac{\ln x}{\ln p}} = x$$

доказывают, что

$$\max_{1 \leq u \leq x} \nu_p(u) = \left\lfloor \frac{\ln x}{\ln p} \right\rfloor$$

и при $p > x$ выполняется $\nu_p(K(x)) = 0$. Лемма доказана.

Формулы для кратности вхождения простого числа в $n!$

Далее символом $n!$ обозначается произведение всех целых чисел от 1 до n , т.е. $n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n$.

Лемма 2

Для каждого натурального числа n имеем

$$\nu_p(n!) = \left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \dots = \sum_{k \geq 1} \left[\frac{n}{p^k} \right]. \quad (10)$$

Сумма в действительности конечна, так как при $p^k > n$, т.е. при $k > \frac{\ln n}{\ln p}$ слагаемые равны нулю.

Доказательство леммы 2.

Среди чисел $1, 2, \dots, n$ на простое p делятся лишь $p, 2p, 3p, \dots, mp$, где m есть наибольшее целое число, удовлетворяющее неравенству $mp \leq n$, т.е. $m = \left[\frac{n}{p} \right]$. Поэтому

$$\nu_p(n!) = \nu_p(p \cdot 2p \cdots mp) = \nu_p(p^m \cdot m!) = m + \nu_p(m!). \quad (11)$$

Докажем теперь нужное равенство с помощью индукции.

При $n < p$ обе части равенства (10) равны нулю, и оно, конечно, выполняется. Предположим теперь, что $n \geq p$ и это равенство справедливо для любого натурального числа, меньшего n . Тогда из (11) и (9), поскольку $m < n$, находим

$$\nu_p(n!) = m + \sum_{\ell \geq 1} \left[\frac{m}{p^\ell} \right] = \left[\frac{n}{p} \right] + \sum_{\ell \geq 1} \left[\frac{\left[\frac{n}{p} \right]}{p^\ell} \right] = \left[\frac{n}{p} \right] + \sum_{\ell \geq 1} \left[\frac{n}{p^{\ell+1}} \right],$$

что и завершает доказательство леммы 2.

Пример. Докажем, что при любых целых числах $n \geq k \geq 0$ дробь $S = \frac{n!}{k!(n-k)!}$ есть целое число.

Пусть p – простое число. Тогда

$$\nu_p(S) = \nu_p\left(\frac{n!}{k!(n-k)!}\right) = \nu_p(n!) - \nu_p(k!) - \nu_p((n-k)!) = \sum_{\ell \geq 1} \left(\left[\frac{n}{p^\ell} \right] - \left[\frac{k}{p^\ell} \right] - \left[\frac{n-k}{p^\ell} \right] \right). \quad (12)$$

Учитывая, что

$$\left[\frac{k}{p^\ell} \right] + \left[\frac{n-k}{p^\ell} \right] \leq \left[\frac{k + (n-k)}{p^\ell} \right] = \left[\frac{n}{p^\ell} \right]$$

закключаем, что все слагаемые в сумме (12) неотрицательны. Поэтому $\nu_p(S) \geq 0$ для любого простого числа p и, значит, S – целое число.

Задача. Докажите, что для любого целого числа $n \geq 0$ дробь

$$\frac{(6n)!n!}{(3n)!(2n)!(2n)!}$$

есть целое число.

Конец 3-й лекции