

Элементы теории чисел. Теория сравнений.

Ученик 10-4 класса Оконешников Д.Д. по лекции к.ф.-м.н. Протопоповой Т.В.

от 12 января 2021 г.

1 Лекция №12

Определение. $a \in Z$ и $b \in Z \setminus \{0\}$ определена операция деления с остатком: разделить целое a на целое $b (\neq 0)$ с остатком, означает найти такие целые $q, r \in Z$, что $a = b * q + r, 0 \leq r < |b|$.

Определение. Если при делении с остатком $r = 0$, то число a делится на b ($a:b$). Число b при этом называется делителем числа a .

Пример. -7 на 5 $-7 = 5 * (-2) + 3$

1.1 Свойства делимости (нацело). ОТА

(1) Если $a:c$ и $b:c$, то $(a \pm b):c$

$\begin{matrix} a = cq_1 \\ b = cq_2 \end{matrix} \Rightarrow (a \pm b) = c(q_1 \pm q_2) \Rightarrow (a \pm b):c \downarrow$

(5) $a:b$ и $b:a \Rightarrow |a| = |b|$

(6) $\forall a \in Z \setminus \{0\} \Rightarrow 0:a$

(2) $a:b \Rightarrow ak:b (k \in Z)$

(7) $\forall a \in Z \Rightarrow a:1$

(3) $a:b, b:c \Rightarrow a:c$

(8) Если $ab:m$ и $\text{НОД}(a, m) = 1$, то $b:m$

$\uparrow a = bq_1, b = cq_2 \Rightarrow a = c * (q_1 * q_2) \Rightarrow a:c \downarrow$

(9) Если $a:m, a:k$ и $\text{НОД}(m, k) = 1$, то $a:mk$

(4) Если $a \neq 0, a:b \Rightarrow |a| \geq |b|$

$\uparrow a:b \Leftrightarrow a = b * q \Rightarrow |a| = |b| * |q| \Rightarrow$ от противного,
если $|a| < |b|$, то $|q| = \frac{|a|}{|b|} < \frac{|b|}{|b|} = 1 \Rightarrow$ единственная
возможность при целом $q = 0$, но тогда и $a = 0$.
Противоречие. \downarrow

Определение. Натуральное число $p > 1$ называется простым, если оно имеет ровно два натуральных делителя (p и 1).

Все остальные натуральные числа называются составными (кроме 1). Единица не является ни простым, ни составным.

1.1.1 Основная теорема арифметики

Th.1 (Основная теорема арифметики) Всякое натуральное число $n > 1$ может быть представлено в виде $n = p_1 * p_2 * \dots * p_i$, где p_i — простые числа. Это представление единственно с точностью до порядка множителей (т.е. если $n = p_1 * p_2 * \dots * p_r = q_1 * q_2 * \dots * q_s$, то $r = s$ и q_1, q_2, \dots, q_s можно перестановкой получить из чисел p_1, p_2, \dots, p_r)

(1) Докажем существование

Пусть $n \in \mathbb{N}, n > 1$. Среди делителей n есть числа превосходящие 1 (например, само n). Пусть p_1 — наименьший из таких делителей.

p_1 — простое число (если оно само имело бы делитель $1 < a < p_1$, то a было бы меньше p_1 и было бы делителем n (св-ва 4,3), противоречит тому, что выбран наименьший делитель).

Итак, $n = p_1 n_1$, где p_1 — простое, $n_1 \in \mathbb{N}$ и $n_1 < n$ (св-во 4).

Если $n_1 > 1$, то поступим с ним так же, как и числом n , представим его в виде $n_1 = p_2 n_2$, p_2 — простое, $n_2 \in \mathbb{N}, n_2 < n_1 \Rightarrow n = p_1 * p_2 * n_2$ и т.д.

В конце концов, так как $n_i \in \mathbb{N}, i = 1, 2, 3, \dots$ убывают, то $\exists n_r = 1$ и процесс обрывается: $n = p_1 * p_2 * \dots * p_r$

(2) Докажем существование (единственность) От противного. Если \exists хоть одно натуральное число, допускающее два существенно различных разложения, то непременно \exists и наименьшее число с таким свойством:

$$m = p_1 * p_2 * \dots * p_r = q_1 * q_2 * \dots * q_s \quad (1)$$

Можем допустить, что $p_1 \leq p_2 \leq \dots \leq p_r; q_1 \leq q_2 \leq \dots \leq q_s$.

А) Заметим, что $p_1 \neq q_1$.

Если равны, то разделив (1) на $p_1 = q_1$, получили бы два существенно различных разложения на простые множители для числа $< m$ (Противоречие с тем, что m — наименьшее).

На самом деле показали больше: что среди q_j нет чисел равных какому-либо p_i

Б) Из А) $p_1 < q_1$ или $p_1 > q_1$. Пусть $p_1 < q_1$ (для $p_1 > q_1$ доказательство строится аналогично).

Рассмотрим целое число:

$$m' = m - p_1 * q_2 * \dots * q_s \quad (2)$$

Подставляя вместо m два его разложения, получим:

$$m' = p_1 * p_2 * \dots * p_r - p_1 * q_2 * \dots * q_s = p_1(p_2 * \dots * p_r - q_2 * \dots * q_s) \quad (3)$$

$$m' = q_1 * q_2 * \dots * q_s - p_1 * q_2 * \dots * q_s = (q_1 - p_1)q_2 * \dots * q_s \quad (4)$$

Из равенства (4) очевидно $m' > 0$. Из равенства (2) $m' < m$, а значит, для m' разложение на простые множители — единственно (с точностью до порядка сомножителей).

Из (3) $\Rightarrow p_1$ входит множителем в m' , значит, из (4) p_1 входит множителем либо в $q_1 - p_1$, либо в $q_2 * \dots * q_s$. Но последнее невозможно, так как все $q_j > p_1$ ($p_1 < q_1$) и они простые.

Значит, p_1 входит множителем в $q_1 - p_1$, т.е. $(q_1 - p_1) : p_1 \Rightarrow q_1 - p_1 = p_1 h \Rightarrow q_1 = p_1(h + 1)$, т.е. $q_1 : p_1$, чего быть не может. Противоречие. Ч.Т.Д.

1.1.2 Теорема Евклида

Th.2 (Теорема Евклида) Множество простых чисел бесконечно.

↑ Доказательство проведем от противного. Предположим, что множество простых чисел конечно, т.е. $P = \{p_1, p_2, \dots, p_k\}$ — конечная совокупность простых чисел.

Рассмотрим число $p = p_1 * p_2 * \dots * p_k + 1$.

Заметим, что $\forall i, i = 1, 2, \dots, k$ это $p > p_i$, т.е. $p \notin P$, значит, оно составное и по ОТА может быть представлено в виде произведения простых множителей.

Но p не делится ни на какой p_i (при делении дает в остатке 1).

Значит, наше предположение о конечности системы простых чисел неверно. ↓

Утверждение. Существуют сколь угодно длинные участки натурального ряда, вовсе не содержащие простых чисел

↑ Действительно, пусть $n \in \mathbb{N}, n > 1$. Рассмотрим ряд чисел: $n! + 2, n! + 3, \dots, n! + n$.

$n = 2 : 2! + 2$ — одно число в ряду;

$n = 3 : 3! + 2, 3! + 3$ — два числа в ряду; чем больше n , тем больше в ряду

$n = 4 : 4! + 2, 4! + 3, 4! + 4$ — три числа в ряду; чисел $(n - 1)$ число).

и т.д.

В этом ряду нет ни одного простого числа, так как $n! + 2$ делится на 2, $n! + 3$ делится на 3, $n! + n$ делится на n . Таким образом, при больших n такие участки натурального ряда могут быть очень большими. ↓

1.2 Каноническое разложение числа. НОД. НОК

1.2.1 Теорема Эйлера

Th.3 (Теорема Эйлера) Пусть $\tau(n)$ — количество простых чисел $\leq n$. Тогда

$$\frac{\tau(n)}{n} \xrightarrow{n \rightarrow \infty} 0$$

Понятно, что $\tau(n)$ увеличивается (т.е. $\rightarrow \infty$) при $n \rightarrow \infty$ (это означает, что простые числа встречаются все реже и реже).

Мы показали, что любое натуральное число мы можем представить в виде произведения простых множителей (и такое представление единственно с точностью до перестановки множителей): $n = p_1 * p_2 * \dots * p_r$, $p_1 \leq p_2 \leq \dots \leq p_r$. Используя обозначение степени, можем записать так:

$$n = p_1^{a_1} * p_2^{a_2} * \dots * p_k^{a_k}, \text{ (каноническое разложение)}$$

где $p_1 < p_2 < \dots < p_k$ — простые, a_1, a_2, \dots, a_k — натуральные числа.

Замечание. Бывает полезно записать в разложение все простые числа $\leq p_k$ и использовать показатель равный 0.

Если число m является делителем n , то несложно понять, что $m = p_1^{\beta_1} * p_2^{\beta_2} * \dots * p_k^{\beta_k}$, где $0 \leq \beta_i \leq a_i$.

Можно посчитать число всех натуральных делителей числа n . Любой делитель n имеет следующую структуру: $m = p_1^{0,1,2,\dots,a_1} * p_2^{0,1,\dots,a_2} * \dots * p_k^{0,1,\dots,a_k}$

Для первого множителя $(a_1 + 1)$ возможность для второго $(a_2 + 1)$ возможностей и т.д. Таким образом, число всех делителей $(a_1 + 1) * (a_2 + 1) * \dots * (a_k + 1)$.

Пример. Сколько делителей у числа 120 (включая 1 и само число)?

120		2
60		2
30		2
15		3
5		5
1		

$120 = 2^3 * 3^1 * 5^1$. Значит, число всех делителей $= (3 + 1) * (1 + 1) * (1 + 1) = 4 * 2 * 2 = 16$.

Определение. d — общий делитель a и $b \Leftrightarrow a:d$ и $b:d$.

Определение. Наибольший общий делитель чисел a и b обозначается $\text{НОД}(a, b)$.

Определение. Наименьшее общее кратное $\text{НОК}(a, b) = k$ — наименьшее натуральное число такое, что $k:a$ и $k:b$.

Пусть $a = p_1^{a_1} * p_2^{a_2} * \dots * p_k^{a_k}$, $b = p_1^{\beta_1} * p_2^{\beta_2} * \dots * p_k^{\beta_k}$

Здесь использовали показатель 0 для тех простых множителей, которые входят только в одно из разложений.

Тогда

$$\text{НОД}(a, b) = p_1^{\min(a_1, \beta_1)} * p_2^{\min(a_2, \beta_2)} * \dots * p_k^{\min(a_k, \beta_k)}$$

$$\text{НОК}(a, b) = p_1^{\max(a_1, \beta_1)} * p_2^{\max(a_2, \beta_2)} * \dots * p_k^{\max(a_k, \beta_k)}$$

$$\text{НОД}(a, b) * \text{НОК}(a, b) = a * b$$

Пример. $a = 2 * 3^3 * 5^2 * 7$, $b = 2^2 * 3 * 7^2 * 11 \Rightarrow a = 2^1 * 3^3 * 5^2 * 7^1 * 11^0$, $b = 2^2 * 3^1 * 5^0 * 7^2 * 11^1 \Rightarrow \text{НОД}(a, b) = 2^1 * 3^1 * 5^0 * 7^1 * 11^0$, $\text{НОК}(a, b) = 2^2 * 3^3 * 5^2 * 7^2 * 11^1$.

Чтобы получить каноническое разложение полезно помнить признаки делимости.

1) на 2 и 5. Легко.

2) на 4. $n = \overline{a_k a_{k-1} \dots a_1 a_0} = 100 * \overline{a_k a_{k-1} \dots a_2} + \overline{a_1 a_0}$. $100:4 \Rightarrow n:4 \Leftrightarrow \overline{a_1 a_0}:4$.

3) на 8. $n:8 \Leftrightarrow \overline{a_2 a_1 a_0}:8$.

4) на 3. $n = \overline{a_k a_{k-1} \dots a_1 a_0} = a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10 + a_0 = a_k (\underbrace{999 \dots 9}_k + 1) + a_{k-1} (\underbrace{999 \dots 9}_{k-1} + 1) + \dots + a_1 (9 + 1) + a_0 = (a_k \underbrace{999 \dots 9}_k + a_{k-1} \underbrace{999 \dots 9}_{k-1} + \dots + a_1 9) + (a_k + a_{k-1} + \dots + a_1 + a_0)$

Аналогично для 9.

5) на 6. $n:2$ и $n:3 \Rightarrow$ (так как 2 и 3 взаимно просты) $n:6$

6) на 11.

$$n = \overline{a_k a_{k-1} \dots a_1 a_0} = a_0 + a_1 10 + a_2 100 + a_3 1000 + \dots + a_k 10^k =$$

$$\begin{aligned}
&= a_0 + a_1(11 - 1) + a_2(99 + 1) + a_3(1001 - 1) + a_4(9999 + 1) + a_5(100001 - 1) + \dots + a_k 10^k = \\
&= (a_0 - a_1 + a_2 - a_3 + a_4 - \dots) + (a_1 11 + a_3 1001 + a_5 100001 + \dots + a_{2l+1} \underbrace{100\dots 0}_{2l} 1_{2l} + \dots) + \\
&\quad + (a_2 99 + a_4 9999 + \dots + a_{2m} \underbrace{99\dots 99}_{2m} + \dots)
\end{aligned}$$

А) числа, состоящие из четного числа 9-ок, делятся на 11, т.е. последняя скобка :11;

Б) заметим, что $1001 = (1100 - 99) : 11$, $100001 = (110000 - 9999) : 11$, $1 \underbrace{00\dots 00}_{2l} 1 = (11 \underbrace{00\dots 00}_{2l} - \underbrace{99\dots 99}_{2l} : 11)$.

1.2.2 Алгоритм Евклида нахождения НОД(a,b)

Пусть требуется найти НОД(a, b). Будем считать, что $|a| > |b|$.

1) Разделим a на b с остатком:

$$a = q_1 b + r_1, \quad 0 \leq r_1 < |b| \quad (1)$$

Заметим, что любой делитель пары a и b будет делителем r_1 , а значит пары b и r_1 . С другой стороны, любой делитель пары (b, r_1) будет делителем a , а значит пары (a, b) . Таким образом (равенство множеств), множество делителей пары (a, b) совпадает с множеством делителей пары (b, r_1) , а значит и НОД(a, b) = НОД(b, r_1).

2) Разделим b на r_1 с остатком:

$$b = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1 \quad (2)$$

При этом получаем, что НОД(b, r_1) = НОД(r_1, r_2)

3) Разделим r_1 на r_2 с остатком:

$$r_1 = q_3 r_2 + r_3, \quad 0 \leq r_3 < r_2 \quad (3)$$

При этом НОД(r_1, r_2) = НОД(r_2, r_3).

И т.д.

Посмотрим на остатки. $|b| > r_1 > r_2 > r_3 > \dots \geq 0$. Получили строго убывающую последовательность неотрицательных целых чисел. Эта последовательность конечна. Существует $r_{k+1} = 0$, т.е.

k+1)

$$r_{k-1} = q_{k+1} r_k + 0 \quad (k+1)$$

При этом НОД(a, b) = НОД(b, r_1) = НОД(r_1, r_2) = НОД(r_2, r_3) = ... = НОД(r_{k-1}, r_k) = r_k . Таким образом, НОД(a, b) равен последнему ненулевому остатку в алгоритме Евклида.

Весь алгоритм:

1) $a = q_1 b + r_1, \quad 0 \leq r_1 < |b|$

2) $b = q_2 r_1 + r_2, \quad 0 \leq r_2 < |r_1|$

3) $r_1 = q_3 r_2 + r_3, \quad 0 \leq r_3 < |r_2|$

...

k) $r_{k-2} = q_k r_{k-1} + r_k$

k+1) $r_{k-1} = q_{k+1} r_k + 0$

НОД(a, b) = r_k

Пример. НОД(5083, 3553)-?

$$5083 = 1 * 3553 + 1530$$

$$3553 = 2 * 1530 + 493$$

$$493 = 9 * 51 + 34$$

$$51 = 1 * 34 + 17$$

$$34 = 2 * 17 + 0 \Rightarrow \text{НОД}(5083, 3553) = 17$$