Элементы теории чисел. Теория сравнений.

Ученик 10-4 класса Оконешников Д.Д. по лекции Протопоповой Т.В.

от 12 января 2021 г.

1 Лекция №12

Определение. $a \in Z$ и $b \in Z \backslash \{0\}$ 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 ($a \vdots b$). Число b при этом называется делителем числа a.

Пример. -7 на 5 $\qquad -7 = 5 * (-2) + 3$

1.1 Свойства делимости (нацело). ОТА

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

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

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

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

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

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

$\uparrow a \vdots b \Leftrightarrow a = b * q \Rightarrow |a| = |b| * |q| \Rightarrow$ 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. $\downarrow$

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

(6) $\forall\ a \in Z \backslash \{0\} \Rightarrow 0 \vdots a$

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

(8) Если $ab \vdots m$ и НОД$(a,\ m) = 1,$ то $b \vdots m$

(9) Если $a \vdots m,\ a \vdots k$ и НОД$(m,\ k) = 1,$ то $a \vdots mk$

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 $n = p_1 * p_2 * ... * p_i$, где p_i — простые числа. Это представление единственно с точностью до порядка множителей (т.е. если $n = p_1 * p_2 * ... * p_r = q_1 * q_2 * ... * q_s$, то $r = s$ и $q_1,\ q_2, ...,\ q_s$ можно перестановкой получить из чисел $p_1,\ p_2, ...,\ p_r$)

(1) Докажем существование

Пусть $n \in N,\ n > 1$. 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, $n_1 \in N$ 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, $n_2 \in N, n_2 < n_1 \Rightarrow n = p_1 * p_2 * n_2$ и т.д.

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

(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:

$$m = p_1 * p_2 * ... * p_r = q_1 * q_2 * ... * q_s \qquad (1)$$

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

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:

$$m' = m - p_1 * q_2 * ... * q_s \qquad (2)$$

Подставляя вместо m два его разложения, получим:

$$m' = p_1 * p_2 * ... * p_r - p_1 * q_2 * ... * q_s = p_1(p_2 * ... * p_r - q_2 * ... * q_s) \qquad (3)$$

$$m' = q_1 * q_2 * ... * q_s - p_1 * q_2 * ... * q_s = (q_1 - p_1)q_2 * ... * q_s \qquad (4)$$

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 $q_2 * ... * q_s$. 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. $(\mathbf{q_1} - \mathbf{p_1}) \vdots \mathbf{p_1} \Rightarrow q_1 - p_1 = p_1 h \Rightarrow q_1 = p_1(h + 1)$, т.е. $\mathbf{q_1} \vdots \mathbf{p_1}$, чего быть не может. Противоречие. Ч.Т.Д.

1.1.2 Теорема Евклида

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

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

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

Заметим, что $\forall\ i, i = 1, 2, ..., k$ 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. $\downarrow$

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

$\uparrow$ Действительно, пусть $n \in N, n > 1$. Рассмотрим ряд чисел: $n! + 2, n! + 3, ..., n! + n$.

$n = 2 : 2! + 2$ — 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. $\downarrow$

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

$$\frac{\tau(n)}{n} \xrightarrow[n\to\infty]{} 0$$

Понятно, что $\tau(n)$ увеличивается (т.е. $\to \infty$) при $n \to \infty$ (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): $n = p_1 * p_2 * ... * p_r,\ p_1 \leq p_2 \leq ... \leq p_r$. Используя обозначение степени, можем записать так:

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

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

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

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

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

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

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

$$\begin{array}{r|l} 120 & 2 \\ 60 & 2 \\ 30 & 2 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}$$

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

Определение. d — общий делитель a и $b \Leftrightarrow \mathbf{a \vdots d}$ и $\mathbf{b \vdots d}$.

Определение. Наибольший общий делитель чисел a и b обозначается НОД(a, b).

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

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

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

Тогда

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

Пример. $a = 2 * 3^3 * 5^2 * 7,\ b = 2^2 * 3 * 7^2 * 11 \Rightarrow a = 2^1 * 3^3 * 5^2 * 7^1 * 11^0,\ b = 2^2 * 3^1 * 5^0 * 7^2 * 11^1 \Rightarrow$ НОД$(a, b) = 2^1 * 3^1 * 5^0 * 7^1 * 11^0$, 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. $n = \overline{a_k a_{k-1} ... a_1 a_0} = 100 * \overline{a_k a_{k-1} ... a_2} + \overline{a_1 a_0}$. $\quad 100 \vdots 4$. $\Rightarrow n \vdots 4 \Leftrightarrow \overline{a_1 a_0} \vdots 4$.

3) на 8. $n\vdots 8 \Leftrightarrow \overline{a_2a_1a_0}\vdots 8$.
4) на 3. $n = \overline{a_ka_{k-1}...a_1a_0} = a_k10^k + a_{k-1}10^{k-1} + ... + a_110 + a_0 = a_k(\underbrace{999...9}_{k}+1) + a_{k-1}(\underbrace{999...9}_{k-1}+1) + ... + a_1(9+1) + a_0 = (a_k\underbrace{999...9}_{k}+a_{k-1}\underbrace{999...9}_{k-1}+ ... + a_19) + (a_k + a_{k-1} + ... + a_1 + a_0)$

Аналогично для 9.

5) на 6. $n\vdots 2$ и $n\vdots 3 \Rightarrow$ (так как 2 и 3 взаимно просты) $n\vdots 6$
6) на 11.

$$n = \overline{a_ka_{k-1}...a_1a_0} = a_0 + a_110 + a_2100 + a_3 + 1000 + ... + a_k10^k =$$
$$= a_0 + a_1(11-1) + a_2(99+1) + a_3(1001-1) + a_4(9999+1) + a_5(100001-1) + ... + a_k10^k =$$
$$= (a_0 - a_1 + a_2 - a_3 + a_4 - ...) + (a_111 + a_31001 + a_5100001 + ... + a_{2l+1}1\underbrace{00...0}\,1_{2l} + ...)+$$
$$+(a_299 + a_49999 + ... + a_{2m}\underbrace{99...99}_{2m}+...)$$

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

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

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:

$$a = q_1b + r_1,\ 0 \le r_1 < |b| \quad (1)$$

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:

$$b = q_2r_1 + r_2,\ 0 \le r_2 < r_1 \quad (2)$$

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

3) Разделим r_1 на r_2 с остатком:

$$r_1 = q_3r_2 + r_3,\ 0 \le r_3 < r_2 \quad (3)$$

При этом НОД$(r_1,r_2) =$ НОД(r_2,r_3).
И т.д.

Посмотрим на остатки. $|b| > r_1 > r_2 > r_3 > ... \ge 0$. 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.