Алгебра 1 семестр ПИ,
Лекция, 10/01/21

Собрано 4 октября 2021 г. в 17:55

Содержание

1.1. Наименьшее общее кратное

Def. 1.1.1. *Общим кратным $a_1, a_2, ..., a_n$ называется число $M > 0 : a_i | M \ \forall i = 1, ..., n$ Наименьшее из общих кратных – НОК.*

Теорема 1.1.2. $\text{lcm}(a, b) = \frac{ab}{\gcd(a,b)}$

Доказательство. $a = a_1 d, b = b_1 d, (a_1, b_1) = 1$

$$M = at = bs \Rightarrow \frac{M}{b} = \frac{at}{b} = \frac{a_1 dt}{b_1 d} = \frac{a_1 t}{b_1} \Rightarrow M = \frac{b \cdot a_1 t}{b_1}$$

t делится на b_1, т.е. $t = b_1 k$

$$M = \frac{b a_1 b_1 k}{b_1} = b a_1 k \text{ - минимально при } k = 1 \Rightarrow M = b a_1 = \frac{b a_1 d}{d} = \frac{ab}{\gcd(a, b)}$$

■

1.2. Математическая индукция

1. Аксоима. $\forall$ подмножество $\mathbb{N}$ имеет наши элементы $\Rightarrow$ ММИ.
2. Аксиома. $A_1, A_n \Rightarrow A_{n+1} \Rightarrow \forall A_n$

Следствие 1.2.1. Пусть $a_1, a_2, ..., a_n$ – попарно взаимно-простые $\Rightarrow \text{lcm}(a_1, a_2, ..., a_n) = a_1 \cdot a_2 \cdot ... \cdot a_n$

Доказательство. $n = 2$. $\text{lcm}(a_1, a_2) = \frac{a_1 a_2}{\gcd(a_1, a_2)} = a_1 \cdot a_2$
Пусть верно для n. Тогда для $n + 1$

$$(a_i, a_n a_{n+1}) = (a_i, a_{n+1}) = 1 \Rightarrow a_1, a_2, ..., a_{n-1}, a_n a_{n+1} \Rightarrow$$

$$\Rightarrow \text{lcm}(a_1, ..., a_{n-1}, a_n \cdot a_{n+1}) = a_1 \cdot a_2 \cdot ... \cdot a_{n-1} \cdot a_n \cdot a_{n+1}$$

■

1.3. Простые числа

Def. 1.3.1. *Число $p > 1$ называется простым, если оно делится только на 1 и на p. Иначе число называется составным.*

Теорема 1.3.2 (о наименьшем делителе)**.** Наименьший делитель $a > 1$ – простое число

Доказательство. $M = \{d | d > 1, d | a\} \neq \varnothing$ Пусть p - наименьший элемент M. Предположим, что p – составное, т.е. $p = bq, q < p, q | p, p | a \Rightarrow q | a$ – противоречие. ■

Теорема 1.3.3. p - наименьший делитель > 1 числа $n \Rightarrow p \leqslant \sqrt{n}$

Доказательство.

$$n = mp, p \leqslant m \Rightarrow np \leqslant nm \Rightarrow mp \cdot p \leqslant nm \Rightarrow p^2 \leqslant n \Rightarrow p \leqslant \sqrt{n}$$

■

Теорема 1.3.4 (Теорема Евклида)**.** Простых чисел бесконечно много

Доказательство. Пусть $p_1, p_2, ..., p_n$ – все простые числа, $a = p_1 \cdot p_2 \cdot ... \cdot p_n + 1$. Если $a \vdots p_i$, то $1 \vdots p_i \Rightarrow a$ – новое простое число. ■

1.4. Основная теорема арифметики

Lm 1.4.1. p – простое $\Rightarrow \forall a > 1 \to p|a \vee (p, a) = 1$

Доказательство.

$$(p, a)|p \Rightarrow (p, a) = 1 \vee (p, a) = p$$

■

Lm 1.4.2. p – простое, $p|a_1 \cdot a_2 \cdot ... \cdot a_n \Rightarrow \exists i = 1, ..., n : p|a_i$

Доказательство. Если $(p, a_i) = 1, i = 1, ..., n \Rightarrow 1 = (p, a_1) = (p, a_1a_2) = (p, a_1a_2a_3) = (p, a_1 \cdot ... \cdot a_n) = 1 \Rightarrow \exists a_i : p|a_i$ ■

Теорема 1.4.3 (Основная теорема арифметики)**.** 1. $\forall a > 1 \to a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}, p_1, p_2, ..., p_k$ – различные простые, $\alpha_1, \alpha_2, ..., \alpha_k \geqslant 1$

2. с точностью до перестановки множителей это представление единственно

Доказательство. 1. из всех делителей a выбираем наименьший – p_1 - простое $\Rightarrow a = p_1 \cdot a_1$. Рассмотрим a_1 – наименьший делитель - $p_2 \Rightarrow a_1 = p_1 \cdot p_2 \cdot a_2$ и т.д.

$$a_1 > a_2 > a_3 > ... \Rightarrow \exists a_n = 1 \Rightarrow a = \text{ разложение на простые}$$

2. Предположим, что представление не одно, то есть

$$a = p_1 \cdot p_2 \cdot ... \cdot p_s = q_1 \cdot q_2 \cdot ... \cdot q_n$$

Не умаляя общности, пусть $n \geqslant s \Rightarrow p_1|q_1...q_n$. Тогда, по лемме 2 $p_1|q_i \Rightarrow p_1 = q_i$. Перенумеруем $i = 1 \Rightarrow p_2p_3...p_s = q_2q_3...q_n \Rightarrow$ все p_s сократятся, т.е. $1 = q_{s+1}...q_n \Rightarrow s = n$

■

Def. 1.4.4. $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_k^{\alpha_k}$ — *каноническое разложение числа* a

Следствие 1.4.5. Любой делитель $a = p_a^{\alpha_1}...p_k^{\alpha_k}$ имеет вид $b = p_1^{\beta_1} \cdot ... \cdot p_k^{\beta_k}, 0 \leqslant \beta_i \leqslant \alpha_i$

Доказательство. $b|a \Rightarrow b$ содержит в разложении p_i ■

Следствие 1.4.6. $\gcd(a_1, ..., a_n)$ имеет вид $p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, где
$a_i = \min$ {показатель степени p_i, с которым p_i входит в разложение $a_1, a_2, ..., a_n$}

Следствие 1.4.7. $\operatorname{lcm}(a_1, ..., a_n)$ имеет вид $p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, где
$a_i = \max$ {показатель степени p_i, с которым p_i входит в разложение $a_1, a_2, ..., a_n$}

1.5. Непрерывные дроби (Цепные дроби)

Def. 1.5.1. *Выражение вида*

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + ...}}}$$

называется непрерывной дробью. Обозначение: $[a_0, a_1, a_2, ...]$

Теорема 1.5.2. Любое вещественное число может быть представлено в виде непрерывной дроби.
Если число иррационально – в виде бесконечной дроби, если рациональное – в виде конечной.

Доказательство. $a > b$

$$\frac{a}{b} = a_0 + \frac{r_1}{b} = a_0 + \frac{1}{\frac{b}{r_1}} = a_0 + \frac{1}{a_1 + \frac{r_2}{r_1}} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{r_3}{r_2}}} \text{ и т.д.}$$

где

$$a = b \cdot a_0 + r_1$$
$$b = r_1 \cdot a_1 + r_2$$
$$r_1 = r_2 \cdot a_2 + r_3$$

■

Def. 1.5.3. *Для* $\frac{a}{b}$ $\delta_0 = \frac{a_0}{1}, \delta_1 = a_0 + \frac{1}{a_1}, \delta_2 = a_0 + \frac{1}{a_1 + \frac{1}{a_2}}$ *и т.д. называются подходящими дробями.*

Теорема 1.5.4 (Формулы подходящих дробей)**.** $\delta_k = \frac{p_k}{q_k}, p_{-1} = 1, q_{-1} = 0, p_0 = a_0, q = 1$

$$\Rightarrow \begin{cases} p_k = a_k \cdot p_{k-1} + p_{k-2} \\ q_k = a_k \cdot q_{k-1} + q_{k-2} \end{cases}$$

Доказательство. $\delta_1 = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1 \cdot 1 + 0} = \frac{a_1 \cdot p_0 + p_{-1}}{a_1 \cdot q_0 + q_{-1}}$
Предположим, что для k верно. Тогда для $k+1$

$$\delta_{k+1} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + ... \frac{1}{a_k + \frac{1}{a_{k+1}}}}} = \frac{(a_k + \frac{1}{a_{k+1}}) \cdot p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}}) \cdot q_{k-1} + q_{k-2}} =$$

$$= \frac{(a_{k+1} \cdot a_k + 1) \cdot p_{k-1} + p_{k-2} \cdot a_{k+1}}{(a_{k+1} \cdot a_k + 1) \cdot q_{k-1} + q_{k-2} \cdot a_{k+1}} = \frac{a_{k+1}(a_k \cdot p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} = \frac{a_{k+1} \cdot p_k + p_{k-1}}{a_{k+1} \cdot q_k + q_{k-1}}$$

■