№ 42

P. 1

основная теорема арифметики (формулировка, единственность)

Т-а (основная Т-а арифметики)

$\forall n \in \mathbb{N} : n > 1 \quad \exists !$ набор $p_1 \dots p_s$ — пр-е и $\alpha_1 \dots \alpha_s \geq 1 : \quad n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$

Д-во (д-во единственности)

Л1 $\forall a \in \mathbb{N}, a > 1, \forall p$ — пр-е либо $a \vdots p$, либо $(a, p) = 1$

Д-во

$(a, p) \vdots p$. Т.к. p — пр-е, то его положительные делители это 1 и p. Тогда $(a, p) = \left[\begin{matrix} 1 \\ p \Rightarrow a \vdots p \end{matrix}\right.$ ■

Л2 Если пр-е нескольких чисел > 1 делится на p, то хотя бы один множитель делится на p

Д-во

По Л1 $\forall$ множитель либо делится на p либо взаимно прост с p.

Если все множители взаимно просты с p, то пр-е взаимно просто с p ■

Пусть $n = p_1^{\alpha_1} \dots p_m^{\alpha_m} \quad n = q_1^{\beta_1} \dots q_l^{\beta_l}$.

Тогда $p_1^{\alpha_1} \dots p_m^{\alpha_m} = q_1^{\beta_1} \dots q_l^{\beta_l}$

Запишем как $\underbrace{p_1 \cdot p_1 \dots p_1}_{\alpha_1} \dots = \underbrace{q_1 \dots q_1}_{\beta_1} \dots$

Тогда и левая и пр-я часть делятся на p_1 $\Rightarrow$ какой-то из м-лей делится на p_1. Но все числа пр-е $\Rightarrow$ какой-то $q_i = p_1$. Продолжим расс-е $\Rightarrow$ либо при $m \neq l$ $\left[\begin{matrix} 1 = \prod q_i \; ?! \\ \prod p_i = 1 \end{matrix}\right.$ либо $q_i = p_i$ и $m = l$ ■