8ВМ, спецкурс, занятие 9
14 октября 2022
Основная теорема арифметики

Определение. Натуральное число $p > 1$ называется *простым*, если его нельзя представить в виде произведения двух натуральных чисел, ни одно из которых не равно единице.

0 Вспомните, как доказывается, что простых чисел бесконечно много.

Теорема (Основная теорема арифметики, ОТА)**.** Любое натуральное число $n \neq 1$ можно представить в виде произведения простых множителей. Это представление единственно с точностью до порядка множителей.

Существование такого представления легко доказывается по индукции/при помощи принципа наименьшего элемента. (Вспомните, как это делается.) А вот единственность совсем не очевидна. Чтобы в этом убедиться, приведем пример, в котором ОТА не работает.

1 Злой волшебник уничтожил все нечетные натуральные числа, остались только четные. Их по-прежнему можно складывать, вычитать и умножать. Понятие «делиться» тоже сохранилось: говорим, что $a \vdots b$, если существует такое число c (конечно, четное), что $a = bc$.

a Делится ли теперь число 6 на число 2?

b Какие числа теперь являются простыми?

c Приведите пример числа, которое раскладывается в произведение простых двумя разными способами.

Доказательство ОТА.

Лемма (Обратный алгоритм Евклида)**.** Если числа a и b взаимно просты, то существуют такие целые числа x и y, что $ax + by = 1$.

Лемма (Евклида)**.** Пусть p — простое число. Если $ab \vdots p$, то $a \vdots p$ или $b \vdots p$.

Доказательство. Допустим, $a \not\vdots p$. Тогда a и p взаимно просты. По обратному алгоритму Евклида, существуют такие целые x и y, что $ax + py = 1$. Умножим это равенство на b, получим $abx + pby = b$. Первое слагаемое делится на p, поскольку $ab \vdots p$. Второе слагаемое делится на p. Но тогда и их сумма b делится на p, что и требовалось доказать.

2 Докажите обобщения леммы Евклида.

a Пусть p — простое число. Если произведение $a_1 a_2 \ldots a_k$ делится на p, то какой-то из множителей a_i делится на p.

b Пусть $(a, c) = 1$ и $ab \vdots c$. Тогда $b \vdots c$.

3 a Воспользуйтесь принципом наименьшего элемента и докажите ОТА.

b Какая именно часть этого доказательства не работает в арифметике четных чисел?

Следствие. Любое натуральное число n можно единственным образом представить в виде $n = 2^a \cdot 3^b \cdot 5^c \cdot 7^d \cdot \ldots$, где a, b, c, d, ... — целые неотрицательные числа.

Например, $500 = 2^2 \cdot 3^0 \cdot 5^3 \cdot 7^0 \cdot 11^0 \cdot \ldots$.

Часто разложение числа n на простые множители записывают в еще чуть более общем виде. Пусть $p_1, p_2, p_3, \ldots$ — последовательность простых чисел в порядке возрастания ($p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$). Тогда $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, где $\alpha_1, \alpha_2, \ldots$ — целые неотрицательные числа.

$\boxed{\mathbf{4}}$ Пусть p — простое число. Докажите, что если $n^k \vdots p$, то $n^k \vdots p^k$.

$\boxed{\mathbf{5}}$ $\boxed{\text{a}}$ Пусть числа a и b разложены на простые множители: $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ и $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$. Найдите разложения НОД$(a, b) = (a, b)$ и НОК$(a, b) = [a, b]$.

$\boxed{\text{b}}$ Докажите, что $a \cdot b = (a, b) \cdot [a, b]$.

Замечание: *вообще говоря, разложения у чисел a и b могут быть разной длины. Например, $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$ и $605 = 5 \cdot 11^2$. В этом случае можно дополнить эти разложения нулевыми степенями, сделав их длины равными:*

$$420 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^0$$
$$605 = 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot 11^2$$

$\boxed{\mathbf{6}}$ Найдите наименьшее такое число, которое при делении на 2 дает остаток 1, при делении на 3 — остаток 2, при делении на 4 — остаток 3,..., при делении на 10 — остаток 9.

$\boxed{\mathbf{7}}$ Пусть $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Найдите $\boxed{\text{a}}$ количество; $\boxed{\text{b*}}$ сумму всех делителей числа n.

$\boxed{\mathbf{8}}$ Число делится $\boxed{\text{a}}$ на 100; $\boxed{\text{b}}$ на 1000. Может ли у него быть ровно 15 делителей?

$\boxed{\mathbf{9}}$ Существует ли натуральное число, которое при умножении на 2 станет квадратом, при умножении на 3 — кубом, а при умножении на 5 — пятой степенью?

$\boxed{\mathbf{10}}$ Число n не является точным квадратом. Докажите, что не существует таких натуральных чисел x и y, что $x^2 = ny^2$.