НАМ ПИШУТ

ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ В ШКОЛЕ

Как известно, основная теорема арифметики утверждает, что всякое натуральное число можно разложить на простые множители, причем это разложение единственно с точностью до перестановки множителей. Благодаря этой теореме существует каноническая форма записи натурального числа, которая дает описание всех его делителей.

Естественно, что основная теорема арифметики используется в школе. Однако в большинстве учебников ее нет, и это порождает странную ситуацию. Например, школьники используют разложение на простые множители при сокращении дробей, причем единственность разложения лишь подразумевается, но не доказывается.

Причина такого положения в том, что наиболее известное доказательство этой теоремы — довольно длинное и сложное. Точнее говоря, существование разложения на простые множители доказывается легко, а вот его единственность выводится из другой теоремы: если произведение двух натуральных чисел делится на некоторое простое число, то на него делится хотя бы один из сомножителей. В свою очередь, при доказательстве этой теоремы используется тот факт, что наибольший общий делитель двух чисел является их целочисленной линейной комбинацией; есть варианты, использующие индукцию.

В действительности основная теорема арифметики может быть доказана непосредственно, причем это доказательство вполне подходит для факультативных занятий в школе. Оно приведено,например, в книге Р.Куранта и Г.Роббинса «Что такое математика?» (М.: Просвещение, 1967. — с. 47–48). Придумать такое рассуждение непросто, зато оно короткое и прозрачное. Поскольку это доказательство недостаточно известно, то приведем его здесь (с небольшими изменениями).

Будем доказывать теорему «от противного»: допустим, что некоторые натуральные числа можно разложить на простые множители двумя или более способами. Тогда среди таких чисел существует наименьшее. Однако мы построим еще меньшее число, которое также имеет не менее двух разложений. Полученное противоречие докажет теорему.

Пусть N — наименьшее число с неоднозначным разложением на простые множители. Рассмотрим два его различных разложения:

$$P_1 \cdot P_2 \cdot \ldots \cdot P_k = Q_1 \cdot Q_2 \cdot \ldots \cdot Q_l .$$

Все множители в левой части отличаются от всех множителей в правой (иначе можно сократить на одинаковые множители и получить меньшее число с неоднозначным разложением). Можно считать, что $P_1 < Q_1$. Положим

$$M = \left(Q_1 - P_1\right) \cdot Q_2 \cdot \ldots \cdot Q_l .$$

Тогда M — натуральное число, меньшее N. Докажем, что M также имеет хотя бы два разложения на простые множители, вопреки выбору числа N.

С одной стороны, M делится на P_1, поскольку

$$M = Q_1 \cdot Q_2 \cdot \ldots \cdot Q_l - P_1 \cdot Q_2 \cdot \ldots \cdot Q_l =$$

$$= P_1 \cdot P_2 \cdot \ldots \cdot P_k - P_1 \cdot Q_2 \cdot \ldots \cdot Q_l =$$

$$= P_1 \cdot \left(P_2 \cdot \ldots \cdot P_k - Q_2 \cdot \ldots \cdot Q_l\right).$$

Поэтому M имеет разложение, содержащее P_1.

С другой стороны, $Q_1 - P_1$ не делится на P_1, а простые числа Q_2, …, Q_l не равны P_1. Поэтому, разложив $Q_1 - P_1$ на простые множители, мы придем к разложению для M, не содержащему P_1. Искомое противоречие получено.

Примененный метод доказательства называют методом бесконечного спуска (по натуральному числу с данным свойством строим меньшее число с тем же свойством). Он знаком школьникам: например, так устанавливается иррациональность квадратного корня из двух. По существу это одна из форм метода математической индукции.

В заключение напомним, почему единицу не относят к простым числам. Многие считают это произвольным соглашением. На самом деле причина состоит в том, что иначе не будет выполняться основная теорема арифметики.

А.Ковальджи, Б.Френкин