ПРОСТЫЕ ЧИСЛА

Андрей Иванович Касьян, к.т.н., МФПУ "Синергия"

Рассматриваются свойства простых чисел, теорема Евклида.
Euclidean theorem and properties of prime numbers are considered.
Ключевые слова: *простые числа, теорема Евклида.*
Keywords: *prime numbers, Euclidean theorem.*

В данной статье мы не выходим за границы множества натуральных чисел. Простые числа являются аналогом иррациональных чисел, т.к. они "соизмеримы" только с собой (единицу не рассматриваем). Простые числа представляют собой кирпичики, из которых сложены натуральные числа. Но в последовательности доказательств ряда теорем о простых числах необычен порядок и имеются некоторые тонкие места. Попытаемся в какой-то мере кратко разобраться в этих вопросах.

Для краткости введем Постулат (эквивалентный аксиоме о составном числе): каждое натуральное число, большее единицы имеет не меньше двух делителей. Этот постулат нам поможет, но определение делителя опустим. Надо дать следующее определение: если натуральное число p имеет ровно два делителя (т.е. 1 и само p), то это число называется простым.

Сформулируем предложение 1. Для любого натурального числа n>1 наименьший отличный от 1 делитель представляет собой простое число. В доказательстве используется, в том числе, теорема о том, что всякое непустое подмножество натуральных чисел содержит наименьшее число.

Далее, установим размер множества P простых чисел, представив теорему Евклида [1]: простых чисел больше, чем любое число их. При доказательстве часто используется следующее рассуждение: возьмем любую конечную группу простых чисел: $p_1, p_2,..., p_k$. Тогда существует простое p, не входящее в эту группу. Рассмотрим натуральное число, которое равно произведению k рассматриваемых простых чисел, плюс единица, т.е. $p_1 p_2 ... p_k+1$. Полученное число имеет не менее двух делителей. Если оно имеет два делителя (простое), то это и есть искомое p. Если полученное число имеет больше делителей, то в качестве p возьмем наименьший делитель, отличный от 1. Очевидно, p есть искомое простое число, которое не может совпадать ни с одним из чисел $p_1, p_2,..., p_k$. Число p есть делитель $p_1 p_2 ... p_k+1$, которое при делении на любое из чисел $p_1, p_2,..., p_k$ дает в остатке 1 и, следовательно, не делится нацело. Таким образом, p отлично от любого $p_1, p_2,..., p_k$. В этом доказательстве есть тонкости, но мы вернемся к ним позже.

Рассмотрим, для иллюстрации, основную теорему арифметики. Предложение 2. Каждое натуральное число, отличное от 1, можно представить в виде произведения простых чисел. Доказательство хорошо известно. Оно базируется на аксиоме индукции. Возьмем базу индукции - число 2, для которого утверждение верно. Предположим, что утверждение верно для всех натуральных k<n. По Предложению 1 находим наименьший делитель p числа n. Тогда n= p n1. Если n1=1, то для n=p утверждение верно. Если n1>1, то n1<n и согласно сделанному предположению для натурального n1, меньшего n, выполняется условие о произведении. Следовательно, как n1, так и число n представимо в виде произведения простых чисел.

Основная теорема арифметики базируется на Предложении 3. Для каждого натурального числа n>1, существует единственное разложение на простые множители. Кратко можно наметить схему доказательства. Сначала предположим, что множество M натуральных чисел, для которого единственность разложения на простые множители нарушена, не пусто [2]. Далее используем теорему о том, что всякое непустое подмножество натуральных чисел содержит наименьшее число n. Это число представимо в виде двух разложений $n = p_1 p_2...p_k = q_1 q_2 ... q_k$. Для нас это главное. Далее, среди множества $p_1p_2...p_k$, $q_1 q_2...q_k$ выберем наименьшее число, например p_1. Число p_1 отличается от всех q_i. Если бы $p_1 = q_i$, то сокращая равенство $n = p_1p...p_k = q_1 q_2 ... q_k$ на p_1, получили бы два различных разложения на простые множители для числа, меньшего n. Доказательство прерываем. Здесь обратим внимание на то, что простые числа берем из вышерассмотренного множества P.

Возвращаемся к множеству P и доказательству его бесконечности. Здесь фактически использовано доказательство по индукции, т.к. требуется доказать бесконечность множества P. Только на основе аксиомы индукции в классическом случае можно вывести утверждение о бесконечности того или иного множества. Для k=1, т.е. для случая p_1 возьмем любое другое простое число p. Это база индукции в доказательстве. Предположим, что для группы из k-1 простых существует отличное k-ое простое p_k. Тогда, как было доказано выше, и для этой группы существует отличное от них простое p. В чем заключается тонкость. Что бы понять, приведем "доказательство" гипотезы Гольдбаха. Исходя из известной формулы для количества простых чисел, не превосходящих N, т.е. $\pi(N)$, имеем для n=kN/lnN (k-коэффициент, доказательство проводится также на основе индукции, но для краткости его опускаем) верное неравенство $p_n<N$. Отсюда получаем для любого натурального n и для четного 2N сумму меньшую2N ($p_n+p_n=2p_n <2N$), т.е. всегда можно найти четное число, которое больше суммы двух простых (вместо $2p_n$ можно брать $p_{n-m} + p_n$). В чем "тонкость" доказательства? В том, что мы рассматриваем простые числа вида $p_n = p(n)$, но это отображение множества простых чисел P в множество натуральных чисел нам не дано. Можно утверждать, что высказывание "возьмем для натурального n простое p_n" в настоящий момент не имеет конструктивного смысла.

Возвращаемся к основной теореме арифметики. Здесь встречается подобная тонкость. Опять, как и выше, рассматривается отображение в множество натуральных $p_n = p(n)$. Имеются и другие тонкости, о которых будет сказано в продолжении.

Литература

1. Евклид. Начала. М.: ГИТЛ, 1950.
2. А. Бухштаб. Теория чисел. М.: Просвещение, 1966.

Связь с автором: a.kasyan1@yandex.ru

Самое большое из известных сейчас простых чисел: число Марсенна равно 2 в степени 77232917 минус единица.

31
331
3331
33331
333331
3333331
33333331

Удивительно, но следующее число 33333331 не является простым! Оно делится на 17: