ПРОСТЫЕ И СОСТАВНЫЕ ЧИСЛА

Определение. Натуральное число называется простым, если оно имеет ровно два натуральных делителя – единицу и само это число.

Определение. Натуральное число, имеющее натуральные делители, отличные от единицы и самого числа, называется составным.

Ясно, что каждое натуральное число, большее единицы, является простым или составным.

Лемма. Любое натуральное число, большее 1, является либо простым, либо имеет простой делитель.

Доказательство. Если натуральное число n не является простым числом, то у него имеется наименьший делитель, больший 1. Этот делитель и будет простым, так как если бы он был составным, то n имело бы еще меньший делитель.

Следующая теорема была доказана Евклидом в его "Началах", книга IX.

Теорема. Множество простых чисел бесконечно.

Доказательство. Предположим противное. Пусть множество простых чисел конечно и состоит из чисел $p_1, \ldots, p_n$. Рассмотрим число $p = p_1 \ldots p_n + 1$. Оно не делится ни на одно простое число $p_1, \ldots, p_n$ (дает в остатке 1) и, следовательно, само должно являться простым. С другой стороны, оно больше всех простых чисел $p_1, \ldots, p_n$. Противоречие.

Среди первых ста натуральных чисел простыми являются: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Одним из наиболее простых способов составления таблицы простых чисел основан на использовании решета Эратосфена. Он был предложен около 2000 лет назад астрономом и математиком из Александрии Эратосфеном и состоит в том, что в ряду натуральных чисел последовательно вычеркиваются числа кратные двум, трем и т.д. Оставшиеся числа, большие единицы, и будут простыми.

По-видимому, не существует формулы для нахождения всех простых чисел, однако некоторые из них можно получить как значения довольно простых выражений. Так, например, квадратный трехчлен Эйлера $x^2 + x + 41$ позволяет получить 40 последовательных простых чисел, начиная с 41. Перебрав все значения этого квадратного трехчлена, не превышающие 10 000 000, математики обнаружили, что доля простых чисел среди них составляет 0,475…

Несмотря на то, что множество простых чисел бесконечно и, значит, простые числа встречаются сколь угодно далеко, существуют сколь угодно большие участки натурального ряда, не содержащие простых чисел.

Действительно, для $n > 1$ в ряду чисел $n! + 2, n! + 3, \ldots, n! + n$ длины $n - 1$ нет ни одного простого числа, так как $n! + 2$ делится на 2, $n! + 3$ делится на 3, … $n! + n$ делится на n. Причем во всех случаях делитель меньше делимого.

С другой стороны, для любого натурального $n > 1$ среди чисел $n + 1, n + 2, \ldots, n! - 1$ есть простое число.

Действительно, если числа $n + 1, n + 2, \ldots, n! - 2$ составные, то все их делители меньше или равны n. Число $n! - 1$ не делится на 2, 3, …, n. Если бы

оно делилось на одно из чисел $n + 1$, $n + 2$, …, $n! – 2$, то оно делилось бы и на число меньшее или равное n. Следовательно, $n! – 1$ не делится ни на одно меньшее число, большее 1. Значит, $n! – 1$ – простое.

Важнейшими результатами в области распределения простых чисел являются результаты Л. Эйлера, П.Л. Чебышева и Ж. Адамара.

Теорема Эйлера утверждает, что отношение числа простых чисел, не превосходящих n, к самому числу n стремится к нулю при n стремящемся к бесконечности.

Теоремы Чебышева и Адамара уточняют теорему Эйлера. В частности, теорема Адамара (1894 г.) утверждает, что число простых чисел, не превосходящих n, стремится к бесконечности так же, как и отношение $\frac{n}{\ln n}$.

В течение веков велись поиски формул для нахождения простых чисел. Многие стремились к открытию новых простых чисел. Одним из них был французский математик М. Мерсенн (1588-1648), который искал простые числа вида $2^p – 1$, и в честь которого эти числа называются простыми числами Мерсенна.

Заметим, что числа вида $a^n – 1$, где a – натуральное число, большее 2, не является простым. Это следует из формулы

$$a^n – 1 = (a – 1)(a^{n-1} + a^{n-2} + \ldots + 1),$$

которая доказывается перемножением выражений, стоящих в скобках.

Аналогично, если n – составное число, то $2^n – 1$ также будет составным. Действительно, пусть $n = mk$. Тогда $2^{mk} – 1 = (2^m)^k – 1$и, следовательно, является составным.

Таким образом, единственными простыми числами вида $a^n – 1$ могут быть только числа $2^p – 1$.

Прямые вычисления показывают, что не все числа вида $2^p – 1$ оказываются простыми. Например,

$M_2 = 2^2 – 1 = 3$ (простое);
$M_3 = 2^3 – 1 = 7$ (простое);
$M_5 = 2^5 – 1 = 31$ (простое);
$M_7 = 2^7 – 1 = 127$ (простое);
$M_{11} = 2^{11} – 1 = 2047 = 23 \cdot 89$ (составное).
$M_{13} = 2^{13} – 1$ (простое);
$M_{17} = 2^{17} – 1$ (простое);
$M_{19} = 2^{19} – 1$ (простое);

В 1750 году Л. Эйлер установил, что число $M_{31} = 2\,147\,483\,647$ является простым. Более ста лет оно оставалось самым большим известным простым числом.

В 1876 г. французский математики Лукас нашел простое число Мерсенна с 39 цифрами

$M_{127} = 170\,141\,183\,460\,469\,231\,731\,687\,303\,715\,884\,105\,727$.

43-е простое число Мерсенна $M_{30402457}$ было получено с использованием компьютера 15.12.2005.

Для того, чтобы оценить количество цифр в этом числе воспользуемся

логарифмами, и заметим, что $2^p - 1$ и 2^p имеют одинаковое число цифр. Действительно, если бы они имели разное число цифр, то 2^p должно было бы оканчиваться цифрой 0, чего не происходит ни при какой степени двойки. С помощью таблиц, калькулятора или компьютера находим, что lg 2 равняется 0,30102999… . Умножая на него число 30402457, получим, что целая часть lg $2^{30402457}$ равняется 9152052. Это число и есть искомое число цифр в данном простом числе Мерсенна.

44-е число Мерсенна $M_{32582657}$ было получено 04.09.2006. В нем 9808358 цифр.

В настоящее время известно 47 простых чисел Мерсенна. Последнее, 47-е число $M_{42643801}$ имеет 12837064 цифр.

Числа Мерсенна непосредственно связаны с совершенными числами – такими, которые равны сумме всех своих делителей (включая 1, но исключая само число). Совершенные числа были известны еще в Древней Греции. Они пользовались большим уважением, считались эталоном гармонии и красоты. Им приписывались мистические свойства.

Наименьшим совершенным числом является число 6 = 1 + 2 + 3. За ним следует число 28 = 1 + 2 + 4 + 7 + 14, далее число 496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248.

Связь между совершенными числами и числами Мерсенна установил Евклид.

Теорема. Если $M_p = 2^p - 1$ – простое число Мерсенна, то число $2^{p-1}(2^p - 1)$ является совершенным.

Доказательство. Выпишем делители числа $2^{p-1}M_p$, меньшие самого числа: $1, 2, 2^2, \dots 2^{p-1}, M_p, 2M_p, 2^2M_p, \dots 2^{p-2}M_p$. Посчитаем их сумму. Имеем
$1 + 2 + 2^2 + \dots + 2^{p-1} = 2^p - 1 = M_p$;
$M_p + 2M_p + 2^2M_p + \dots + 2^{p-2}M_p = (1 + 2 + 2^2 + \dots + 2^{p-2})M_p = (2^{p-1} - 1)M_p$.
Следовательно, $1 + 2 + 2^2 + \dots + 2^{p-1} + M_p + 2M_p + 2^2M_p + \dots + 2^{p-2}M_p = M_p + (2^{p-1} - 1)M_p = 2^{p-1}(2^p - 1)$.

Л. Эйлер доказал, что числами вида $2^{p-1}(2^p - 1)$, где $2^p - 1$ – простое число Мерсенна, исчерпываются все четные совершенные числа. В настоящее время известно 47 четных совершенных числа. Неизвестно, бесконечно много таких чисел или нет. Вопрос о существовании нечетных совершенных чисел также остается открытым.

Рассмотрим еще один тип чисел, введенных французским математиком П. Ферма (1601 – 1665). Это числа вида $2^{2^n} + 1$. Показатель 2^n здесь взят не случайно. Докажем, что числа вида $2^m + 1$ могут быть простыми только в случае, когда $m = 2^n$. Для этого воспользуемся формулой

$$a^{2k+1} + b^{2k+1} = (a + b)(a^{2k} - a^{2k-1}b + a^{2k-2}b^2 - \dots + b^{2k}),$$

которая доказывается непосредственным перемножением скобок. Из нее следует, что числа вида $a^{2k+1} + 1$ при натуральных k и $a > 1$ являются составными. Если m имеет нечетный делитель, т.е. $m = l(2k + 1)$, то $2^m + 1 = 2^{l(2k+1)} + 1 = (2^l)^{2k+1} + 1$ – составное число.

Ферма предполагал, что все числа вида $2^{2^n}+1$ являются простыми. Действительно, первые пять чисел Ферма $F_0 = 2^{2^0}+1 = 3$; $F_1 = 2^{2^1}+1 = 5$; $F_2 = 2^{2^2}+1 = 17$; $F_3 = 2^{2^3}+1 = 257$; $F_4 = 2^{2^4}+1 = 65537$ являются простыми. Однако Л. Эйлер доказал, что следующее число Ферма является составным $F_5 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$.

До сих пор неизвестно, существуют ли другие простые числа Ферма. Неизвестно также бесконечно или нет множество составных чисел Ферма.

Числа Ферма связаны с задачей построения правильных многоугольников с помощью циркуля и линейки.

Еще древние греки занимались построением правильных многоугольников. Они умели строить 2^n-угольники, $3\cdot 2^n$-угольники, $5\cdot 2^n$-угольники, $15\cdot 2^n$-угольники.

Окончательное решение вопроса о том, какие правильные многоугольники можно построить с помощью циркуля и линейки, было получено лишь в 1796 г. немецким математиком К.Ф. Гауссом (1777 – 1855). Он доказал, что правильный n-угольник может быть построен с помощью циркуля и линейки тогда и только тогда, когда $n = 2^m p_1 \ldots p_k$, где числа $p_1, \ldots, p_k$ – различные простые числа Ферма. В частности, из этой теоремы следует, что правильные 7-угольник, 9-угольник, 11-угольник, 13-угольник не могут быть построены циркулем и линейкой.

Задачи.

1. Докажите, что число 1001 – составное.
2. Докажите, что число 9991 – составное.
3. Докажите, что числа вида $8^n + 1$ – составные.
4. Докажите, что число $2^9 + 5^{12}$ – составное.
5. Докажите, что число $222^{555} + 555^{222}$ – составное.
6. Докажите, что числа вида $n^4 + 4$ – составные при $n > 1$.
7. Найдите все простые числа p, для которых $p + 10$ и $p + 14$ – простые.
8. Найдите все простые числа p, для которых $2p + 1$ и $4p + 1$ – простые.
9. Найдите все простые числа p, для которых $8p^2 + 1$ – простое.
10. Найдите все простые числа p, для которых $4p^2 + 1$ и $6p^2 + 1$ – простые.
11. Числа p и $p^2 + 2$ – простые. Докажите, что число $p^3 + 2$ – простое.
12. Найдите все натуральные n, при которых $2^n - 1$ и $2^n + 1$ – простые.

Литература

1. Гарднер М. Математические досуги. – М.: Мир, 1972.
2. Гарднер М. Математические новеллы. – М.: Мир, 1974.
3. Генкин С.А., Итенберг И.В., Фомин Д.В. Ленинградские математические кружки. – Киров, 1994.
4. Горбачев Н.Н. Сборник олимпиадных задач по математике. – М.: МЦНМО, 2004.
5. Оре О. Приглашение в теорию чисел. – М.: Наука, 1980.
6. Г. Радемахер, О.Теплиц. Числа и фигуры. – М.: Наука, 1966.

7. Энциклопедия элементарной математики, книга I. – М.: Физматгиз, Москва, 1961 - 1966.
8. http://www.mersenne.org
9. http://www.vasmirnov.ru