О Генераторах Простых Чисел

Дубовая Ольга Александровна

гр. ТКС-14а, ФКИТА, ДонНТУ;

Руководитель: Улитин Геннадий Михайлович,

Профессор, завкафедры,

кафедра высшей математики ДонНТУ

Введение

Еще в Древней Греции было замечено, что некоторые числа имеют много делителей, а другие - меньше. Так, например, число 36 делится на 1, 2, 3, 4, 6, 9, 12, 18, 36, т.е. имеет 9 делителей. Число 5 делится только на 1 и 5, т.е. имеет всего два делителя, а число 1 делиться только само на себя - имеет всего один делитель. Число называется простым, если оно имеет только два делителя.

Простое число делится на единицу и само на себя. Числа, имеющие больше двух делителей, называются составными. Единица, имеющая только один делитель, не относится к простым числам и не является и составным. Это число - как бы исключение из всего множества натуральных чисел. Простыми числами являются: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, … 97, 101, 107, 109, 2503, 2521, 2531, 4297, 4337, 4339, … 4931, 4933, 4937, … 5953, 5981, 5987, … Если присмотреться к этой последовательности, то сразу бросается в глаза «разбросанность» простых чисел. Не видно никакой закономерности в их расположении. В первом и во втором десятках натуральных чисел имеются по 4 простых числа, в третьем и четвертом десятках их по два, в десятом десятке только одно простое число - 97, а в 11-м десятке - 4 простых числа. Среди чисел 431,432 и 433-го десятков нет ни одного простого числа. В 493 десятке имеются 3 простых числа.

Постановка задачи

Ученые на протяжении сотен лет старались раскрыть закономерность распределения простых чисел, но до сих пор им это не удалось сделать. Было выдвинуто множество гипотез, составлено немало формул для нахождения всех простых чисел данного множества натуральных чисел, но при внимательном рассмотрении все они оказались ошибочными. Ошибались не только начинающие математики, ошибались и авторитетнейшие ученые мира. Таким образом, мы рассмотрим некоторые частные случаи возникновения «генераторов простых чисел», т. е. формулы, при помощи которых можно было бы получать простые числа.

Генераторы простых чисел

Очень интересна судьба одной из формул такого рода. Её составил известный французский математик Пьер Ферма. Он обогатил науку важнейшими открытиями. Он является одним из творцов аналитической геометрии и теории вероятностей. Но лучшие его открытия принадлежат теории чисел. Он одним из первых после древнегреческих математиков воскресил этот важнейший раздел математики. Изучая сочинения древнегреческого математика Диофанта, Ферма заинтересовался простыми числами. Он высказал предположения о том, что числа вида  являются простыми при любых целых неотрицательных значениях n, т.е. что эта формула является генератором простых чисел, поскольку формула дает простое число 3 при n = 0, при n = 1 получаем простое число 5, при n = 2 - простое число 17, при n= 3 - простое число 257, при n= 4 - простое число 65 537. Ферма утверждал, что и при любых других значениях n «генератор» будет давать только простые числа. При n = 5 он получил число 4 294 967 297. Ферма был убежден, что и это число, как и все предыдущие, полученные при помощи формулы, простое. Но доказать свое предположение в общем виде он не смог.

Прошло около 90 лет после того, как Ферма высказал свое предположение. И 1 декабря 1729г. 22-летний адъюнкт высшей математики Петербургской академии Леонард Эйлер получил письмо от профессора этой академии Христиана Гольдбаха (1690 - 1764), в котором тот писал ему: «Известно ли тебе замечание Ферма о том, что все числа вида  именно 3,5,17 и т.д. суть простые, причем сам он, по его признанию, не смог этого доказать и, насколько я знаю, после него никто не доказывал».

Да, рассуждал Эйлер, формула Ферма дает простые числа для n. При n =5 получается число 4 294 967 297. А простое ли это число? Ученый перебирал все возможные делители этого числа, отвергая их один за другим. Вот отвергнуты все делители, меньше ста, меньше двухсот. Так он дошел до числа 641, оно является делителем искомого. Предположение гениального Ферма оказалось неверным. Но, может быть, формула Ферма дает «осечку» только при n = 5. Нет, это число не является единственным исключением. До недавнего времени, кроме этого числа, были известны еще 14 чисел, для которых формула Ферма дает составные числа. Вот они: 6, 7, 8, 9, 10, 11, 12, 13, 16, 18, 23, 26, 38, 73. В 1957г польский математик Д.Л. Селфридж с помощью электронной счетной машины нашел еще 14 новых составных чисел Ферма. Эти числа получаются при n = 39, 55, 63, 117, 125, 144, 150, 207, 226, 228, 268, 284, 316 и 452. Таким образом, наибольшее из известных сейчас составных чисел Ферма равно  и состоит оно не меньше, чем из 10135 цифр. Один из его делителей равен 27\*2455 + 1 и состоит из 139 цифр.

Попыток создания формул для нахождения простых чисел было множество. Имеется немало формул для нахождения простых чисел. Но все эти «генераторы простых чисел» дают лишь ограниченное число простых чисел. Тем не менее, многие из этих формул довольно любопытны.

Ферма была сформулирована и доказана важнейшая теорема сравнений. Сущность ее заключается в следующем. Нетрудно проверить, что 23-2 делится на 3, 25-2 делится на 5, 27-2 делится на 7 и т.д. Может быть, основание 2 такое «счастливое» число? Нет. Возьмем другое основание. Пусть это будет число 5. Легко убедиться, что число 53-5 делится на 3, что 57 -5 делится на 7, что 1013-10 делится на 13 и т.д. Очевидно число an -a делится всегда на n при любом натуральном основании a, если показатель степени простое число. Эта теорема вошла в историю под названием «Малой теоремы Ферма».

Доказательство «Малой теоремы Ферма» не сохранилось, Леонард Эйлер не только доказал «Малую теорему Ферма», но и обобщил ее. Для этого он в 1759г применил впервые в математике новый метод доказательства. Математики назвали его впоследствии теоретико-групповым.

Приведем еще один пример, где Эйлер дополнил Ферма. Все простые числа, кроме 2, нечетны. Любое нечетное число можно представить в виде 4n+1 или 4n-1, где n= 0,1,2,3,4, …Возьмем простые числа вида 4n+1. Например, 5, 13, 17, 29, 37. Оказывается, каждое из этих чисел равно сумме квадратов двух натуральных чисел. На самом деле: 5=22 +12, 13=32+22, 17=42+12, 29=52+22 и т.д. Ферма доказал эту теорему в общем виде. Эйлер дал строгое ее доказательство и поставил проблему определения вида простых чисел, могущих быть делителями формы x2±ny2. Этот общий подход позволил Эйлеру сформулировать в 1772 г фундаментальную теорему всей теории делимости чисел - так называемую «золотую теорему» о квадратичном законе взаимности. Первое доказательство этой теоремы дал Гаусс.

Из этой теоремы получилось много «генераторов простых чисел». Такими формулами являются: х2+х+17, 2х2+29, х2+х+41, х2-79х+1601, х2+х+72 491 и др. Если в этих формулах подставить последовательно 0, 1, 2, 3, 4, 5…, то первая формула даст 16 простых чисел, вторая - 29, третья - 40, четвертая - 80, пятая - 4923 и т. д.

Прошло 190 лет, и об этих формулах Эйлера заговорили в ученом мире.

В 1964 г известный американский математик С. Улам случайно оказался на лекции, тема которой его совсем не интересовала. От скуки он решил заняться шахматной композицией. Достав блокнот, он разлиновал листок на 64 клетки. Затем Улам отвлекся, а рука его автоматически вычерчивала спираль. Посмотрел на нее и стал нумеровать точки пересечения спирали с линиями сетки. Затем, тоже автоматически, стал обводить кружочками простые числа. Всмотревшись в свой рисунок, Улама удивили простые числа. Вернее не сами числа, а их расположение на рисунке в блокноте. Казалось бы, что простые числа должны быть разбросаны в таблице как попало, без всякого порядка, и чем дальше от центра таблицы, тем эти числа должны быть все более изолированы, как отдельные островки в океане. А на своем рисунке ученый увидел, что простые числа обнаружили склонность выстраиваться в шеренги. И как бы далеко число ни находилось от центра, оно в большинстве случаев не находится в одиночестве, а рядом с ним на одном отрезке гладкой кривой находятся еще несколько простых чисел. Но, может быть, все это случайно для немногих первых последовательных чисел! А если взять сотни, тысячи, миллионы последовательных чисел? Чтобы проверить это положение вручную, необходимо было бы затратить несколько лет кропотливой работы. Да к тому же никто в таком трудном деле не гарантирован от ошибок. Улан обратился в вычислительный центр. Электронно-вычислительная машина (Маниак) быстро расположила числа по спирали. На магнитной ленте была построена спираль и вдоль ее было расположено 65 тысяч простых чисел. При этом была использована магнитная лента Вычислительного центра Лос-Аламоса, на которой записано 90 миллионов простых чисел. И тогда ученый еще раз убедился, что как бы далеко простые числа не находились от центра, они по-прежнему сохраняли в основном тенденцию выстраиваться вдоль плавных кривых.

Но самое поразительное заключается в том, что каждый из этих отрезков можно описать уравнением параболы, т.е. квадратным уравнением. Поясним это положение на примере. Справа от главной диагонали находиться отрезок простых чисел 53, 73, 101, 137, 181, 233, 293. Этот отрезок можно описать параболой y=4x2+16x+53. На самом деле, если вместо x подставить последовательно числа 0, 1, 2, 3, 4, 5, 6, то получим все простые числа данного отрезка. Действительно, при x=0 y=53. При x=1 y=73, при x=2 y=101, при x=3 y=137, при x=4 y=181, при x=5 y=233, при x=6 y=293. На этой же таблице находится «отрезок простых чисел» 47, 59, 79. Нетрудно убедиться, что его можно описать параболой y=4x2+8x+47. «Отрезок» 103, 137, 179, 229 описывается параболой y=4x2+30x+103.

Оказывается, все простые числа, которые производят генераторы простых чисел Эйлера: х2+х+17, х2+х+41 и др., можно получить при помощи спирали Улама.

Если за начало спирали взять не единицу, а 17, то на главной диагонали квадрата выстроятся все 16 простых чисел, соответствующих Эйлеровской формуле х2+х+17. Если спираль началась с числа 41, то 40 простых чисел, соответствующих формуле х2+х+41 выстроятся по главной диагонали квадрата 40\*40. Конечно, Уламовские спирали не дают нам всеобщего способа для объяснения расположения всех простых чисел. К тому же в расположении чисел (речь идет о простых числах) на спирали много неясного. Можно ли при помощи спирали получить гладкую кривую, составленную из бесконечного множества простых чисел, есть ли разница в средней плотности простых чисел вверху и внизу, в правой и в левой частях спирали, как часто на спирали попадаются изолированные простые числа и какими особыми свойствами обладают эти числа. Если «каждый отрезок чисел» на спирали можно описать той или иной квадратной функцией, то нельзя ли привести все эти функции в систему и существует ли такая система? Все эти и множество других вопросов возникают при рассмотрении спиралей Улама.

Имеется множество и других «генераторов» простых чисел. Вот еще один из них: А=(2р+1)/3. Правда, этот «генератор» работает совсем по другому принципу. Если р принимает значение последовательных простых чисел 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, то «генератор» тоже дает простые числа. Но при р =37 «генератор» не срабатывает. В этом случае получается число А = 45 812 984 491, которое разлагается на два множителя 1 777 \* 25 781 083.

Вывод

генератор простой число ферма

Есть ли «всеобщий генератор» всех простых чисел? Пока за 2 500 лет от возникновения понятия «простое число» до наших дней ни одному математику не удалось ответить на этот вопрос. Во всяком случае этот «генератор» не может быть многочленом. Еще Леонард Эйлер доказал, что ни один многочлен относительно х с целыми коэффициентами А0хn + А1хn-1 + А2хn-3+…+ Аn не может для всех целых значений х принимать значения, равные простым числам.

Таким образом, проблема универсального «генератора простых чисел» до настоящего времени остается открытой.

Литература

1. Фаермарк, Д. С. Задача пришла с картины / Д. С. Фаермарк. - М.: Наука, 1974. - 159 с.

. Серпинский, В. Что мы знаем и чего не знаем о простых числах/ В. Серпинский. - М.: Государственное издательство физико-математической литературы, 1963. - 90 с.

. Трост, Э. Простые числа / Э. Трост. - М.: Государственное издательство физико-математической литературы, 1959. - 135 с.