УДК 511

Мамараимов М.Т.,
канд. пед. наук,
Южно-Казахстанский
педагогический
университет,
Казахстан
Уштенов Е.Р.,
инженер-механик
ТОО «Талапкер-ЮК»,
Казахстан

Участники конференции,
Национального первенства
по научной аналитике,
Открытого Европейско-
Азиатского первенства по
научной аналитике

ПРОБЛЕМЫ ПРОСТЫХ ЧИСЕЛ И ТЕОРЕМА О КРИТЕРИИ ПРОСТОГО ЧИСЛА

Мировая научная общественность считает решение проблемы простых чисел и гипотезы Римана о нулях дзета-функции, тесно связанной с простыми числами, наиболее приотитеными задачами современной науки. Так, Давид Гильберт, выступавший на Международном Парижском математическом конгрессе в 1900 году с подведением итогов развития науки и рассмотрением планов на будущее, включил проблему простых чисел в список 23 проблем, подлежащих решению в новом столетии и способных продвинуть науку далеко вперед. Однако ни проблема простых чисел, ни гипотеза Римана за прошедшие 100 лет не была решена. Мировая научная общественность считает решение проблемы простых чисел и гипотезы Римана о нулях дзета-функции, тесно связанной с простыми числами, наиболее приотитеными задачами современной науки. Так, Давид Гильберт, выступавший на Международном Парижском математическом конгрессе в 1900 году с подведением итогов развития науки и рассмотрением планов на будущее, включил проблему простых чисел в список 23 проблем, подлежащих решению в новом столетии и способных продвинуть науку далеко вперед. Однако ни проблема простых чисел, ни гипотеза Римана за прошедшие 100 лет не была решена.

Введение.

На рубеже веков, подводя итоги, американский институт “The Mathematics Institute” им. Клея включил гипотезу Римана в одну из 7 приоритетных задач современности.

Гипотеза Римана связана с проблемой распределения простых чисел в натуральном ряде. До сих пор не установлена простая закономерность распределения простых чисел, нет эффективного метода определения простоты числа, нет удовлетворительной формулы количества простых чисел, и вообще, сумма знаний о свойствах, признаках, характере поведения простых чисел является очень скудной и поэтому нет полной картины этого явления. Это связано в первую очередь с их исключительной сложностью.

Теорема о критерии простого числа.

Представляем Вам нашу теорему о критерии простого числа, авторы – Уштенов Еесенбек Рискулович и Мамараимов Мухидин Ташбулатович. Авторское свидетельство зарегистрированно в Комитете по правам интелектуальной собственности Министерства юстиции Республики Казахстан за № 067 от 19.01.2012 год.

Вначале приведем наиболее важные из признаков и свойств простых чисел:

1. Всякое простое число, большее 3, представимо в виде $6k+1$ или $6k–1$, обратное утверждение неверное.

2. Если p число простое, то $p^2 – 1$ кратно 24; обратное утверждение неверное.

3. Если p-число простое, то верно сравнение: $a^{\varphi(m)} \equiv 1$ $(mod\ p)$, $(a,m) = 1$, что означает, остаток от деление $a^{\varphi(m)} \equiv 1$ на p равен 1. (Теорема Эйлера). Обратное утверждение неверное.

4. Если p число простое, то верно сравнение: $a^{p-1} \equiv 1$ $(mod\ p)$, $(a,p) = 1$, и $a^p \equiv a (mod\ p)$, $(a,p) = 1$, что означает, остаток от деления a^{p-1} на p равен 1, и соответственно остаток от деления a^p на p равен a. (Малая теорема Ферма), Обратное утверждение неверное.

Есть и другие критерии (признаки) простоты числа и они является необходимыми условиями, но не достаточными.

Необходимым и достаточным условием простоты числа являются в основном два критерия: теорема Вильсона и метод определения числа, основанный на решете Эротосфена.

1. Теорема Вильсона: Если p простое число, то имеет место сравнение

$$(p – 1)! + 1 \equiv 0\ (mod\ p). \qquad (1)$$

Так же справедлива обратная теорема: Если для целого положительного p имеет место соотношение (1), то p число простое, т.е. если сумма $(p – 1)! + 1$ делится на p без остатка, то число p является простым числом.

Однако!... дело в том, что даже небольших чисел n, число $(n–1)! + 1$ очень большое число!

Если бы мы при помощи указанного критерия захотели бы узнать, например, является ли число 997 простым, то надо было бы проверить делимость числа 996! + 1 (число, содержащее 2556 десятичных знаков) на 997. А проверить многозначные числа на простоту даже на современном компьютере не представляется возможным.

2. Также верным способом определение числа на простату является деление определяемого числа x на все простые числа $p_1; p_2; p_3 \ldots p_n \le \sqrt{x}$. Если в результате этих операций не будет получено ни одного числа без остатка, то это определяемое число x-является простым. Этот метод тоже является точным, но не имеет практического применения. В самом деле, если определяемое число x является 32-х десятизначным, то его необходимо делить на все простые числа, меньшие $\sqrt{x}$. Это количество операций будет примерно равно

$$\frac{\sqrt{x}}{\ln\sqrt{x}},$$

что значит большое количество делителей с числами до 16-ти десятичных цифр.

На основании вышеизложенного считаем востребованной нашу теорему о критерии простого числа.

Теорема о критерии простого числа.

Пусть n – нечетное натуральное число. Необходимым и достаточным условием простоты числа n является условие выполнения сравнения:

$$(-1)\frac{n-1}{2}\cdot\left(\left(\frac{n-1}{2}\right)!\right)^2+1\equiv 0 \pmod{n},$$

Доказательство.

На основании теоремы Вильсона: если имеет место сравнение:

$$(n-1)!+1\equiv 0 \pmod{n}, \qquad (1)$$

то верно утверждение, что число n – простое.

Преобразуем член $(n-1)!$ в следующий вид:

$$\begin{aligned}&(n-1)!=1\cdot 2\cdot 3\cdot 4\cdot\ldots\cdot(n-1)=\\&=1\cdot 2\cdot 3\cdot 4\cdot\ldots\cdot\left(\frac{n-1}{2}\right)\left(n-\frac{n-1}{2}\right)\times\\&\times\ldots\times(n-4)(n-3)(n-2)(n-1)=\\&=1(n-1)(n-2)(n-3)(n-4)\times\\&\times\ldots\times\left(\frac{n-1}{2}\right)\left(n-\frac{n-1}{2}\right)=\\&=(n-1)(2n-2^2)(3n-3^2)(4n-4^2)\times\\&\times\ldots\times\left(\frac{n-1}{2}n-\left(\frac{n-1}{2}\right)^2\right). \qquad (2)\end{aligned}$$

Так как, члены, содержащие n, равны нулю по модулю n , то выражение (1) можно записать в виде:

$$\begin{aligned}&(-1)\cdot(-2^2)\cdot(-3^2)\cdot(-4^2)\times\\&\times\ldots\times\left(-\frac{n-1}{2}\right)^2+1\equiv 0 \pmod{n}. \qquad (3)\end{aligned}$$

Преобразуем последнее выражение (3):

$$\begin{aligned}&(-1)\cdot(-1)2^2\cdot(-1)3^3\cdot(-1)(-4^2)\times\\&\times\ldots\times(-1)\left(\frac{n-1}{2}\right)^2+1\equiv 0 \pmod{n}. \qquad (4)\end{aligned}$$

И окончательно сравнение выглядит так:

$$(-1)\frac{n-1}{2}\cdot\left(\left(\frac{n-1}{2}\right)!\right)^2+1\equiv 0 \pmod{n}. \qquad (5)$$

Последнее выражение (5) также можно представить в виде:

$$\left(\left(\frac{n-1}{2}\right)!\right)^2\equiv(-1)^{\frac{n+1}{2}} \pmod{n}. \qquad (6)$$

Теорема доказана.

Следствия из теоремы.

Из нашей теоремы можем получить два результата:

1.

$$\left[\left(\frac{p-1}{2}\right)!\right]^2+1\equiv 0 \pmod{p}.$$

если $p = 4k + 1$,

Этот результат известен как теорема В. Серпинского.

2.

$$\left[\left(\frac{p-1}{2}\right)!\right]^2-1\equiv 0 \pmod{p}.$$

если $p = 4k + 3$.

Второй результат раньше в технической литературе не встречался.

Последнее сравнение значит, что $(y-1)(y+1)\equiv 0 \pmod{p}$, где

$$y=\left(\frac{p-1}{2}\right)!.$$

Отсюда вытекает утверждение:

3.

$$\left[\left(\frac{p-1}{2}\right)!\right]\equiv\varepsilon_p \pmod{p};\ \ \varepsilon_p=\pm 1,$$

для простых чисел вида $p = 4k + 3$, где положительный и отрицательный ε_p одновременно при одном и том же простом числе место не имеет. Примеры показывают, что для одних простых чисел выполняется $\varepsilon_p = +1$ и для других $\varepsilon_p = -1$. Критерий при каких простых числах $\varepsilon_p = +1$ и при каких $\varepsilon_p = -1$ пока нами не установлен, вероятно, что оба случая будут встречаться бесчисленное множество раз.

Заключение.

Метод основанный на решете Эротосфена предполагает деление данного числа x на все простые числа $\le\sqrt{x}$ и потому он не практичен.

Теорема Лейбница фактически выводится из теоремы Вильсона и повторяет ее.

Теорема В. Серпинского имеет недостаток что она действительна только на числа вида $4k + 1$, на числа вида $4k + 3$ она не применима.

В отличие от этих теорем наша теорема критерия простого числа является более прогрессивной, чем все предыдущие и она отличается от теоремы Вильсона, что в ней в 2 раза меньше сомножителей, и соответственно в 2 раза меньше операций по определению простого числа.

Литература:

1. Виноградов И.М. Основы теории чисел. Издательство «Лань», 2009 г.

2. Титмарш Е.К. Теория дзета-функции Римана. Изд. иностранной литературы. Москва, 1953 г.

3. Серпинский В. Что мы знаем и что мы не знаем о простых числах. Гос. издат.физ-мат. литературы. Москва, Ленинград. 1963 г.

4. Трост Э. Простые числа. Гос. издат. физ-мат. литературы. Москва 1959 г.