УДК 621.398

© Кукушкин С.С., Белый В.М.
Kukushkin S., Bely V.

ОСНОВЫ КОНСТРУКТИВНОГО ПОДХОДА К ИССЛЕДОВАНИЯМ, ОТНОСЯЩИМСЯ К ТЕОРИИ ЧИСЕЛ И ПРЕДНАЗНАЧЕННЫМ ДЛЯ ПРИКЛАДНОГО ПРИМЕНЕНИЯ В ИНФОРМАТИКЕ

CONSTRUCTIVE APPROACH BASES TO THE RESEARCHES CONCERNING THE THEORY OF NUMBERS AND INTENDED FOR APPLIED APPLICATION IN COMPUTER SCIENCE

Аннотация. *В статье рассматриваются основные положения теории чисел, упрощающие идентификацию структур формирования сложных сигналов и шифров на основе конструктивного подхода, предполагающего упрощение практического применения и реализуемости классических методов математики в информатике. Она имеет двойное назначение: с одной стороны, ее изучение способствует развитию теоретических основ самой древней математической теории – теории чисел, а с другой – подводит к выработке различных рекомендаций по расширенному использованию основных ее положений для повышения эффективности радиотехнических измерений, передачи и обработки информации.*

Annotation. *The substantive provisions of the theory of the numbers which simplify the identification of structures that form difficult signals and code numbers on a basis of the constructive approach which assume a simplification of a practical application and a realizability of mathematical classical methods in computer science are considered in the article. It has a double appointment: on the one hand, its studying promotes a development of theoretical bases of the most ancient mathematical theory - the theory of numbers, and, on the other hand, brings to a development of various recommendations about an expanded use of its basic positions to increase an efficiency of radio technical measurements, transfer and information processing.*

Ключевые слова. *Радиотехнические измерения, помехоустойчивость и защищенность информации, теория чисел, теория конечных полей.*
Key words. *Radio technical measurements, a noise stability and security of the information, the theory of numbers, the theory of final fields.*

Гений есть терпение мысли, сосредоточенное в известном направлении.
И.Ньютон

1. Актуальность решаемой задачи

Самые простые и в то же время наиболее сложные вопросы современной математики связаны с самой древней математической теорией – теорией чисел. Так сложилось, что она многие столетия составляла основу упражнений для тренировки ума (для совершенствования «изящества ума» в определении ученых далекого прошлого). Долгое время она несправедливо считалась бесплодной. Об этом лучше не скажешь, чем Л.Эйлер: «Из всех проблем, рассматриваемых в математике, нет таких, которые считались бы в настоящее время более бесплодными и бесполезными, чем проблемы, касающиеся природы чисел и их делителей. В этом отношении нынешние математики сильно отличаются от древних, придававших гораздо большее значение исследованиям такого рода.... А именно, они не только считали, что отыскание истины похвально само по себе и достойно человеческого познания, но, кроме того, совершенно справедливо полагали, что при этом замечательным образом развивается изобретательность и перед человеческим разумом раскрываются новые возможности решать сложные задачи... Математика, вероятно, никогда не достигла бы такой степени совершенства, если бы древние не приложили столько усилий для изучения вопросов, которыми сегодня многие пренебрегают из-за их мнимой бесплодности». Можно было бы предположить, что приведенная выше цитата, принадлежит кому-то из наших со-

Кукушкин Сергей Сергеевич – доктор технических наук, профессор, ведущий научный сотрудник 4 ЦНИИ Минобороны России, тел.+7(495)502-84-23;
Белый Владимир Макарович – начальник сектора ОАО «НПО Машиностроения», тел. +7(495) 791-95-73.
Kukushkin Sergey – doctor of the technical sciences, professor, the main scientific employee 4 Central Scientific Research Institute Ministry of Defence of Russia, tel. +7(495)502-84-23;
Bely Vladimir - The chief of the sector of Open Joint-stock Company "NPO Mashinostroeniya", tel. +7(495)791-95-73.

временников, а ей на самом деле более 250 лет. Величие проблем, поднятых в теории чисел, сближает прошлое и настоящее, обогащает науку, усиливает потенциальные возможности современных ученых, способствует формированию ядра новой прикладной математики, направленной на решение многочисленных проблем, в том числе и в такой быстропрогрессирующей области знаний, как информатика. Но в современной жизни и науке стало все намного прозаичнее по сравнению с тем, как развитие человечества представляли классики математики. Об этом уже пишет выдающийся математик XX века Г.Штейнгауз: «В математике несравненно явственней, чем в других дисциплинах, ощущается, насколько растянуто шествие всего человечества. Среди наших современников есть люди, чьи познания в математике относятся к эпохе более древней, чем египетские пирамиды, и они составляют значительное большинство. Математические познания незначительной части людей дошли до эпохи средних веков, а уровня математики XVIII века не достигает и один человек на тысячу.... Но расстояние между теми, кто идет в авангарде, и необозримой массой путников все возрастает, процессия все более растягивается и идущие впереди отдаляются все более и более».

«Все законы Природы написаны на языке математики» – это гениальное обобщение (по своему величию, с одной стороны, и по полезности прикладного использования – с другой) принадлежит Г. Галилею. Поэтому, когда кто-то пренебрежительно относится к новым математическим исследованиям, тот, по сути, лишает себя возможности познания и новых законов Природы. Но не все так плохо, как может показаться. В России интерес к математике после сокрушительного развала в 90-е годы уже было отстроенного здания снова возрождается.

Данная статья примечательна еще и тем, что написана в основном сотрудником ОАО «НПО Машиностроения» Белым Владимиром Макаровичем. «Не бездарна та Природа, не погиб еще тот край, что выводит из народа столько славных – то и знай»!» – эти слова великого русского поэта следует рассматривать как оптимистическое заключение, относящееся к приведенной выше краткой характеристике основной проблемы современной математики.

При этом особую значимость в нынешних условиях приобретает развитие прикладной математики. Она находится пока в зачаточном состоянии. Сегодня еще в наших силах направить ее развитие в любую сторону, и мы располагаем в этом отношении неограниченной свободой. Прежде всего, свободой творчества, позволяющей развить и с высоким эффектом применить известный и разработанный математический аппарат для решения практических задач. Необходимо лишь понять, что «математика – не свод готовых ответов на любой вопрос, математика – это школа мышления». При этом естественные и технические науки также нельзя рассматривать лишь как реестр наблюдений и экспериментов. Они никогда не достигли бы такого уровня совершенства, если бы не были ориентированы на прикладную математику.

Однако угроза все более увеличивающегося разрыва между математиками и специалистами-нематематиками, представляющими собой «необозримую массу путников» в образном определении Г.Штейнгауза, становится все более ощутимой.

Эта проблема существенно усугубилась в связи с развалом СССР и последовавшей вслед за этим событием значительной по своим масштабам «утечкой мозгов». Как известно, странами с развитой экономикой, прежде всего, были востребованы математики. К этому необходимо добавить, что хороший математик-прикладник по статистике может появиться не ранее, чем к 50 годам своей жизни. С учетом этого достаточно длительного периода становления (учебы, изучения математики и предметной области, защиты диссертаций, борьбы за выживание и за утверждение своих идей) жизнь человека, к сожалению, оказывается слишком короткой. Далее уже появляется опасность того, что полученные знания можно уже не успеть передать новому поколению.

К этому необходимо еще добавить, что только за редким исключением книги по математике способны научить. Они в том виде, в котором обычно написаны, эту задачу без участия педагога выполнить не могут. Кроме того, «чистый» математик, как правило, недостаточно подготовлен к пониманию существующих технических проблем. Поэтому чаще всего ограничиваются некоей адаптацией языка формул, когда говорят о прикладной математике. Особенно это относится к ее применению в таких областях знаний, как отработка и штатная эксплуатация ракетно-космической техники (РКТ), космическая метрология, управление КА.

К этому необходимо добавить стремительное заполнение всех видов деятельности человека достижениями революции в области вычислительных систем, систем связи, измерительной и управляющей техники.

Веление времени – переход к новым информационным технологиям. Информатизация общества также требует, чтобы больше внимания было уделено развитию прикладных математических методов.

Истоком многих открытий является самая древняя из математических дисциплин – теория чисел [1–5].

Основополагающие закономерности, относящиеся к распределению простых и составных чисел

Многие вопросы новой прикладной математики, призванной решить проблемы в области информатизации, связаны с теорией чисел и установлением различных закономерностей в этой области знаний. При этом наиболее значимая закономерность связана с аналитическим определением распределения простых чисел.

Если рассмотреть множество (1) следующих подряд чисел, образованное элементами рядов $R_1(m)= 6m-1$ и $R_2(m) = 6m + 1$, то несложно определить, что в нем присутствуют все простые числа:

5, 7, 11, 13, 17, 19,..., $(6i-1)$, $(6i+1)$,...,

...,$(6m-1)$, $(6m+1)$,..., (1)

По своей сути представление простых и составных чисел рядами $R_1(m)= 6m-1$ и $R_2(m) = 6m + 1$ представляет собой известное «решето Эратосфена», табличная форма которого приведена на рисунке.

При этом решение проблемы определения, является ли большое число N простым или составным было бы элементарным, если бы в рядах $R_1(m)= 6m-1$ и $R_2(m)= =6m + 1$ не присутствовали бы составные числа.

Теорема 1. (Теорема о простых числах)

Все простые числа, кроме чисел «2» и «3», принадлежат множеству чисел, образованному объединением элементов рядов

$$R_1(m)= 6m-1; \quad (2)$$

$$R_2(m) = 6m + 1, \quad (3)$$

где $m = 1, 2, 3, \dots, N$ – числа натурального ряда.

Примечания

1. Здесь и далее везде по тексту все переменные принимают только целые ненулевые, положительные значения, если не оговорено ничего дополнительно.

2. Простые числа «2» и «3» не рассматриваются. При подсчете общего количества простых чисел в диапазоне от 1 до N их число увеличивается на два, учитывая простые числа «2» и «3».

Простые и составные числа

Очень часто при решении задач необходимо знать, является ли число простым или составным. Например, в одной из задач международной олимпиады для школьников требуется определить, является ли число N = 2009 простым или нет?

Простым называется число P, которое делится без остатка только на 1 или на себя. Простые числа: 1,2,3,5,7,11,13,17,19,23,… Среди них отличающиеся друг от друга на минимальное значение, равное 2, называются соседними, например, 11 и 13, 17 и 19, 29 и 31, 41 и 43, …
Составным является число M, которое имеет делители d_i, отличные от 1 и M.

Матричная форма «решета» Эратосфена для поиска простых чисел

1	**2**	**3**	4	**5**	6
7	8	9	10	**11**	12
13	14	15	16	**17**	18
19	20	21	22	**23**	24
25	26	27	28	**29**	30
31	32	33	34	35	36
37	38	39	40	**41**	42
43	44	45	46	**47**	48

Вывод. Простые числа при матричном представлении «решета» Эратосфена необходимо искать в 1 и 5 столбцах (простые числа выделены)

Решето Эратосфена позволяет на 2/3 уменьшить множество чисел, которые могут быть «кандидатами» в простые числа. Например, для того, чтобы определить, можно ли считать число **2009** простым, необходимо найти его остаток от деления на 6 (число столбцов ***решета Эратосфена***): **$2009 \equiv 5 \pmod 6$. Остаток 5 свидетельствует о том, что число принадлежит 5-му столбцу. Следовательно, может быть и простым.**

Формула простых чисел Мерсенна: $P = 2^n - 1$: p =1 (n = 1), p = 2 (n = 2), p = 7 (n = 3), p = 31 (n = 5), …
Она может быть разложена следующим образом:

$$(2^n - 1) = (2^{n/2} - 1)(2^{n/2} + 1)$$

Из нее следует, что формула простых чисел Мерсенна, помимо простых чисел, определяет еще и составные M, сомножители которых отличаются друг от друга на 2 (пример, *15 = 3 × 5; 255 = 15×17).*
Формула простых чисел Ферма: $P = 2^k+1$ ($k = 2^n$): p = 5 (n = 1), p = 17 (n = 2), p = 257 (n = 3), p = 65537 (n = 4),…
Формул, которые позволили бы однозначно установить, является ли большое число простым или нет, не существует. Так, число Ферма F_5 является составным. Его разложение нашел Л.Эйлер:

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 641 \cdot 6700417.$$

Табличная форма «решета Эратосфена», позволяющая установить основополагающее аналитическое соотношение, связанное с поиском простых чисел

3. При делении на «6» числа рядов $R_1(m)$ и $R_2(m)$ дают в остатке соответственно «–1» и «+1», что эквивалентно соответственно столбцам «5» и «1» решета Эратосфена (табл. 1).

4. Числа «*m*» в формулах (2) и (3) – "производящие" числа.

5. Каждое производящее число «*m*» может порождать до двух простых чисел.

6. Далее везде по тексту [...] – целая часть числа.

Одно из возможных доказательств *теоремы* 1.

Пусть есть простое число К, которое не входит в множество (1), образованное объединением элементов рядов $R_1(m)$ и $R_2(m)$, тогда остаток от деления К на «6» не равен «+1» или «–1» и может быть лишь «0», «2», «3», «4». Но остаток «0», «2», «4» от деления числа К на «6» может быть лишь для четных, т.е. составных чисел, а остаток «3» – только для чисел, кратных «3», также составных чисел.

Таким образом, предположение о том, что простое число К не принадлежит множеству (1) привело к противоречию, что и доказывает теорему.

Теорема 2. (Теорема о составных числах).

Произведения элементов множества (1), образованного элементами рядов $R_1(m)= 6m–1$ и $R_2(m) = 6m + 1$, также принадлежат этому множеству.

Рассмотрим все возможные произведения элементов рядов (2) и (3), образующих множество (1)

$$П_1 = R_1(m_i) \times R_2(m_j);$$
$$П_2 = R_1(m_i) \times R_1(m_j);$$
$$П_3 = R_2(m_i) \times R_2(m_j)$$

или

$$П_1 = (6m_i–1) \times (6m_j+1) = 36m_im_j + 6(m_i–m_j)–1;$$
$$П_2 = (6m_i–1) \times (6m_j–1)=36m_im_j – 6(m_i+m_j) + 1;$$
$$П_3 = (6m_i+1) \times (6m_j+1)=36m_im_j+6(m_i+m_j)+1$$

и далее

$$П_1 = 6(6m_im_j + (m_i-m_j))–1;$$
$$П_2 = 6(6m_im_j – (m_i+m_j)) + 1;$$
$$П_3 = 6(6m_im_j + (m_i+m_j)) + 1.$$

Это значит, что

$$П_1 = 6p–1;\ p = 6m_im_j + (m_i-m_j);$$
$$П_2 = 6q+1;\ q = 6m_im_j– (m_i+m_j);$$
$$П_3 = 6r+1;\ r = 6m_im_j + (m_i+m_j),$$

где *p, q, r* – целые положительные числа.

Остатки от деления $П_1$, $П_2$ и $П_3$ на «6» составляют «+1» или «–1», т.е. $П_1$, $П_2$ и $П_3$ также принадлежат множеству (1) и таким образом *теорема* 2 доказана.

Теорема 3. (Теорема о признаках простых чисел).

Для того, чтобы число *N* было простым, необходимо, чтобы остаток от деления числа *N* на 6 равнялся «+1» или «–1», и достаточно, чтобы "производящее" число *m* для числа *N* не являлось значением функций

$$z_1 = 6xy – x + y \qquad (4)$$

или

$$z_2 = 6xy + x – y \qquad (5)$$

в случае принадлежности числа *N* к ряду $R_1(m)= 6m–1$, и значением функций

$$z_3 = 6xy + x + y \qquad (6)$$

или

$$z_4 = 6xy – x – y \qquad (7)$$

в случае принадлежности числа *N* к ряду $R_2(m) = 6m + 1$.

В формулах (4) – (7) *x* и *y* целые положительные числа.

Докажем *теорему* 3.

Необходимость

Если число *N* простое, то по *теореме* 1 оно должно принадлежать множеству чисел, образованному объединением рядов (2) и (3), остаток, от деления элементов которого на число «6», называемое модулем, равен «–1» или «+1».

Достаточность

1. Пусть $N = 6m – 1$.

Тогда, если число *N* составное, то согласно *теореме* 2 *N* может быть представлено в виде

$$N=(6x – 1) \times (6y + 1)$$

или

$$N=(6x + 1) \times (6y – 1),$$

где *x, y* – целые положительные числа.

Далее необходимо заметить, что

$$6m – 1 = 36xy + 6x – 6y – 1$$

с одной стороны, а с другой

$$6m – 1 = 36xy – 6x + 6y – 1.$$

Из этого следует, что

$$m = 6xy + x – y;$$
$$m = 6xy – x + y.$$

Это означает, что *m* является значением функции

$$z_1 = 6xy + x – y$$

или

$$z_2 = 6xy – x + y.$$

2. Пусть $N = 6m + 1$.

Тогда, если число *N* составное, то согласно *теореме* 2 *N* может быть представлено в виде

$$N = (6x+1) \times (6y+1)$$

или

$$N=(6x–1) \times (6y-1),$$

где *x, y* – целые положительные числа.

Следовательно,

$$6m + 1 = 36xy + 6x + 6y + 1;$$
$$6m + 1 = 36xy – 6x – 6y + 1.$$

Это значит, что

$m = 6xy + x + y$;

$m = 6xy - x - y$,

а m является значением функций

$z_3 = 6xy + x + y$

или

$z_4 = 6xy - x - y$.

Теорема 3 доказана.

Для простых чисел N их производящие числа m не принадлежат значениям функций

$z_1 = 6xy + x - y$

$z_2 = 6xy - x + y$.

или

$z_3 = 6xy + x + y$,

$z_4 = 6xy - x - y$.

Теорема 3 – это теорема составных чисел. «Решето» чисел (по типу «решета Эратосфена» для выделения простых чисел) здесь не существует, но заданы формулы для производящих чисел m в случае составного N.

Ее использование позволяет создавать алгоритмы, позволяющие с помощью функций (4) – (7), выделять простые числа (π), простые числа-близнецы (π, $\pi+2$) четверки простых чисел (π, $\pi+2$, $\pi+6$, $\pi+8$) в любом выбранном числовом диапазоне и не хранить таблицы простых чисел.

Теорема 3 – это еще и «теорема-генератор» простых чисел для выбранного диапазона чисел в обычном компьютере, на столе любого математика или любителя математики.

Время создания необходимых таблиц простых чисел определяется лишь алгоритмом вычисления значений функций (4) – (7), заданным диапазоном чисел и техническими характеристиками компьютера (форматы данных, размер оперативного запоминающего устройства (ОЗУ), разрядность процессора, скорость вычислений и пр.).

Теорема 3 позволяет дать интерпретацию составных чисел, содержащихся в рядах (2) и (3).

Если производящее число m при целых положительных значениях x и y является значением целочисленной функции двух переменных $z_1(x,y) = 6xy - x - y$ или $z_2(x,y) = 6xy + x + y$, то оно не порождает простого числа вида $6m + 1$, но может порождать простое число вида $N = 6m - 1$.

Если производящее число m при целых положительных значениях x и y является значением целочисленной функции двух переменных $z_3(x,y) = 6xy + x - y$ или $z_4(x, y) = 6xy + x - y$, то оно не порождает простого числа вида $6m - 1$, но может порождать простое число $N = 6m + 1$.

Примечание

1. Вышеперечисленные функции $z_i=f(x,y)$ $i=1...4$ при целых положительных значениях x, y образуют в пространстве гиперболические поверхности целочисленных значений.

2. Множество значений функций $z_i=f(x,y)$ из формул (4) – (7) эквивалентны значениям целочисленной трехмерной функции

$$z = |6xy+x+y| = \begin{cases} 6xy-x+y & \text{при } x>0, y<0; \\ 6xy+x-y & \text{при } x<0, y>0; \\ 6xy+x+y & \text{при } x>0, y>0; \\ 6xy-x-y & \text{при } x<0, y<0, \end{cases}$$

образующей в пространстве множество значений производящих чисел m, порождающих составные числа в ряду (1).

Образованная при этом поверхность представляет собой гиперболоид составных чисел

$z = |6xy+x+y|$.

Целочисленные значения z, которые не принадлежат поверхности гиперболоида, порождают только простые числа.

Из доказанных теорем можно сформулировать следствия.

Следствие 1.

Если "производящее" число m может быть представлено в виде (4) или (5) при целых положительных значениях x и y, то оно не порождает простого числа N вида $6m-1$.

Пример 1.

Пусть производящее число m=11.

По формуле $m=6xy-x+y$ при x=2 и y=1 получим $m=6\times2\times1-2+1$. Число m – простое 11≡11.

Далее $N=6m-1$; $N=6\times11-1=65$. Число N=5×13 – составное, а это означает, что производящее число m=11 не порождает простого числа вида $6m-1$, но порождает для данного m простое число вида $6m+1$, равное 67.

Следствие 2.

Если "производящее" число m может быть представлено в виде (6) или (7) при целых положительных значениях x и y, то оно не порождает простого числа N вида $6m+1$.

Пример 2.

Пусть m=15; по формуле $m=6xy+x+y$ при x=2 и y=1

$m=6\times2\times1+2+1$; т.е. 15≡15.

Далее $N=6m+1$; $N=6\times15+1=91$. Число N=7×13 – составное и, следовательно, производящее число m=15 не порождает простого числа вида $6m+1$, но порождает для данного m простое число вида $6m-1$, равное 89.

Следствие 3.

Если "производящее" число m может быть представлено в виде (4) или (5) и в виде (6) или (7) при целых положительных значениях x и y, то оно вообще не порождает простых чисел.

Пример 3.

Пусть m=20; по формуле $m=6\times x\times y+x-y$

при x=3 и y=1; $m=6\times3\times1+3-1$; 20≡ 20.

Далее $N=6m-1$; N=6×20−1=119; $N=7\times17$ – составное число.

По формуле $m=6\times x\times y-x-y$ при x=2 и y=2;

$m=6\times2\times2-2-2$; 20 ≡ 20.

Далее $N=6m+1$; $N=6\times20+1=121$; $N=11\times11$– составное число, а это означает, что производящее число m=20 вообще не порождает простых чисел.

Следствие 4. (Определение чисел-близнецов).

Если "производящее" число m при целых положительных значениях x и y не может быть представлено ни в виде (4)−(5), ни в виде (6)−(7), то оно порождает два простых числа $N_1= 6m-1$ и $N_2= 6m+1$, отличающиеся друг от друга на 2 единицы. Это так называемые простые числа-близнецы – числа, происходящие от одного производящего числа m (m – «родитель»).

Пример 4.

Пусть m=17. Тогда

$17\neq 6xy-x+y$;

$17\neq6xy+x-y$;

ни при каких x и y,

$17\neq6xy-x-y$; $17\neq6xy+x+y$;

ни при каких x и y.

$N_1=17\times6-1=101$;

$N_2=17\times6+1=103$,

где N_1 и N_2 – простые числа-близнецы.

Следствие 4 предоставляет возможность компактного хранения чисел-близнецов – вместо хранения двух чисел-близнецов достаточно хранить одно "производящее" число. Например, вместо хранения чисел близнецов 41 и 43 достаточно хранить производящее число m=7, что уменьшает объем файлов и таблиц не менее, чем в два раза.

Следствие 5. (Определение четверок подряд следующих простых чисел).

Если два "производящих" числа m_1 и m_2 отличаются друг от друга на 1 и оба порождают по два простых числа, согласно следствию 4, то эти простые числа образуют последовательность четырех простых чисел вида π, π +2, π +6 и π +8, исследованием которых занимались многие математики [1,2,4]. Условимся называть их числами Фрютля.

Пример 5.

1. Предположим, что m_1=17. При этом

$17\neq 6xy-x+y$; $17\neq 6xy+x-y$;

$17\neq6xy-x-y$; $17\neq 6xy+x+y$;

ни при каких x и y.

Значит, $N_1=17\times6-1=101$ и $N_2=17\times6+1=103$ простые числа-близнецы.

2. Далее примем производящее число на единицу больше m_1=17: m_2=18. Также будем считать, что при различных x и y выполняются следующие неравенства:

$18\neq6xy-x+y$; $18\neq6xy+x-y$;

$18\neq6xy-x-y$; $18\neq6xy+x+y$.

Значит, $N_3=18\times6-1=107$; $N_4=18\times6+1=109$ также простые числа-близнецы. Это значит, что N_1, N_2, N_3 и N_4 (101; 103; 107; 109) – четверка простых чисел Фрютля.

Следствие 5 дает возможность компактного хранения четверок чисел-близнецов – вместо хранения четырех чисел Фрютля достаточно хранить одно (первое или второе) "производящее" число. Например, вместо хранения чисел-близнецов 101, 103, 107 и 109 достаточно хранить производящее число m=17 (или m=18), что уменьшает объем файлов и таблиц не менее, чем в четыре раза.

Учитывая свойства производящих чисел, исходя из элементарных соображений, можно дать приближенные (грубые) оценки максимального количества простых чисел, чисел-близнецов, четверок чисел Фрютля на числовом интервале от 1 до N

Теорема 4. (О количестве простых чисел).

Количество простых чисел на числовом интервале от 1 до N не превышает числа $\pi(x) \le \frac{8}{5} \times [\frac{N}{6}] \approx \frac{4\times N}{15}$.

Общее максимально возможное количество простых чисел на интервале от 1 до N составляет $K_1= [N/6]\times2$, т.е. равно удвоенному количеству производящих чисел для заданного интервала чисел с учетом того, что каждое производящее число может порождать до двух простых чисел. При этом необходимо учесть, что производящие числа, оканчивающиеся на 1, 4 , 6 и 9 (или, что то же самое, числа натурального ряда, дающие остатки 1 и 4 по модулю «5»), могут порождать не более одного простого числа. Таким образом, максимально возможное количество простых чисел составит лишь составит 4/5 от K_1, т.е.

$$\pi(x) \le \frac{8}{5} \times [\frac{N}{6}] \approx \frac{4\times N}{15}. \qquad (8)$$

Теорема 5. (О количестве чисел-близнецов)

Количество простых чисел-близнецов на числовом интервале от 1 до N не превышает

$\pi_2(x)=3/5\times[N/6] \approx N/10$.

Производящие числа, дающие при делении на

число-модуль «5» в остатке «1» и «4», могут порождать не более одного простого числа, поэтому максимально возможное количество пар простых чисел-близнецов составит не более 3/5 от общего количества производящих чисел на интервале 1 до N, равного $[N/6]$, или

$$\pi_2(x)=3/5\times[N/6]\approx N/10. \quad (9)$$

Теорема 6. (О количестве четверок подряд следующих простых чисел).

Количество четверок подряд следующих простых чисел типа π, $\pi+2$, $\pi+6$ и $\pi+8$ (числа Фрютля) на числовом интервале от 1 до N не превышает числа

$$\pi_4(x)=1/5\times[N/6]\approx N/30. \quad (10)$$

Из анализа закономерностей формирования остатков от деления на 5 чисел натурального ряда (0, 1, 2, 3, 4, 0, 1, ...) следует, что следующие подряд пары чисел натурального ряда, остатки от деления которых на 5 равны 0 и 1, 1 и 2, 3 и 4, 4 и 0, не могут порождать четверок простых чисел типа m, $m+2$, $m+6$, и $m+8$, так как в каждой паре имеется, как минимум, одно составное число кратное 5. Только одна пара чисел, из каждой пятерки подряд следующих чисел, остатки от деления в которой на 5 оканчиваются на 2 и 3, может порождать четверку чисел Фрютля. Таким образом, максимальное количество чисел Фрютля на интервале от 1 до N составит не более 1/5 от количества производящих чисел равного $[N/6]$ или

$$\pi_4(x)=1/5\times[N/6]\approx N/30. \quad (10^*)$$

Теорема 6 позволяет сделать важный вывод, что все четверки подряд следующих простых чисел принадлежат комбинированному ряду чисел

(11, 13, 17, 19); (41, 43, 47, 49);

(71, 73, 77, 79); (101, 103, 107, 109), ...,

, ..., (11+30n, 13+30n, 17+30n, 19+30n), ...

где n =0, 1, 2, ... , k.

Приведенные теоремы дают оценки максимально возможного количества простых чисел, чисел-близнецов и четверок чисел-близнецов на выбранном интервале числовой оси.

Для больших числовых интервалов оценки будут всегда давать завышенные значения, так как они не учитывают составные числа ряда простых чисел некратные «5», а их количество возрастает по мере увеличения N.

Рассмотрим пример на применение приведенных теорем и алгоритмов.

Пример 6.

Пусть N=157. Определить, является ли N простым или составным числом?

1. Находим остаток от деления числа N на 6. Остаток R= +1. Необходимое условие для простых чисел (теорема 3) выполняется – число N=157 принадлежит к ряду $R_2(m)=6m+1$. Находим "производящее" число m=[157/6]=26. Так как R= +1, то проверяем выполнение условий (6)–(7):

$m=6xy+x+y$;

$m=6xy-x-y$.

a) $26=6xy+x+y$;

$x=(26-y)/(6y+1)$. Задавая y, находим x, а полученные данные сводим в табл. 1.

Таблица 1

x	y
–	1
–	2
–	3

при $y\geq4$ $x<1$. Число m=26 не является значением функции $m=6xy+x+y$.

b) $26=6xy-x-y$; проводим вычисления $x=(26+y)/(6y-1)$, аналогичные предыдущему пункту.

Задавая y, находим x, данные сводим в табл. 2.

Таблица 2

x	y
–	1
–	2
–	3
–	4
–	5

при $y>5$ и $x<1$.

Вычисления окончены. Число m=26 не является значением функции $m=6xy-x-y$. Производящее число m=26 нельзя представить ни в виде (6), ни в виде (7), значит, N=157 – простое число.

Примечание. Прочерк в графе x табл. 1 и 2 означает, что x –дробное число.

Полученные результаты позволяют поставить и наметить пути решения задачи по определению количества простых чисел в диапазоне от 1 ... N.

Теорема 7.

Количество простых чисел $\pi(x)$ на интервале 1... N равно

$$\pi(x) = 2 + [N/6]\times2 - K_{f1f2} - K_{f3}, \quad (11)$$

где $[N/6]\times2$ – максимально возможное количество простых чисел (количество элементов множества, образованного рядами (2), (3)) в диапазоне 1 ... N;

K_{f1f2} – количество различных целочисленных положительных значений функций $f_1(x,y)=6xy+x+y$ и $f_2(x,y)=6xy-x-y$ в диапазоне от 1 до $[N/6]$;

K_{f3} – количество различных целочисленных положительных значений функции $f_3(x,y)=6xy+x-y$ или

$f_4(x,y)=6xy-x+y$ в диапазоне от 1 до $[N/6]$.

Примечания.

1. Слагаемое «2» в формуле (11) учитывает простые числа 2 и 3, не входящие в множество, образованное рядами (2), (3).

2. Для определения коэффициентов K_{f1f2} и K_{f3} в формуле (11) необходимо произвести подсчет соответствующих положительных целочисленных значений указанных функций.

3. Алгоритмы и методы подсчета необходимо выбирать, сообразуясь с конкретными задачами и имеющимися в распоряжении вычислительными средствами. Вычисление количества простых чисел по формуле (11) приводит к решению неопределенных уравнений Диофанта в целых числах.

С помощью приведенных теорем разработан алгоритм и реализован один из возможных вариантов программы для определения простых чисел, чисел-близнецов и чисел Фрютля. Найдено количество чисел Фрютля до миллиона – 166, до двух миллионов – 295 (подтверждается имеющимися материалами в литературе), до миллиарда – 28388 и до 100 миллиардов – 1209318.

Впервые приведены формулы для рядов, содержащих все простые числа и четверки простых, подряд следующих чисел.

Из табл. 1 и 2 видно, что наиболее близко отражает количество простых чисел формула интегрального логарифма.

Заключение

В качестве заключения следовало бы, прежде всего, ответить на основной вопрос: «Для чего нужна теория чисел?». Ранее говорили, что для упражнения ума. Участникам математических олимпиад знание теории чисел было необходимо для того, чтобы решить задачи. Кажущаяся простота подобных задач чаще всего оказывается обманчивой. Классическим примером этому может служить великая теорема П. Ферма: на первый взгляд ее решение такое простое, что в его плену был и сам ее создатель. Об этом свидетельствовала его пометка: «Я знаю ее решение, но края бумаги настолько малы, что оно не поместится». Однако ее доказательство Л. Эйлером для показателя $n = 3$ свидетельствовало о том, насколько оно сложно. Более того, Л. Эйлер применил много изобретательства для того, чтобы его найти. Он вынужден был впервые использовать новые (алгебраические) числа вида: $a+b\sqrt{-3}$. Таким образом, было положено начало новому математическому разделу – теории алгебраических чисел. Впоследствии Э.Куммер для расширенного доказательства великой теоремы Ферма вынужден был ввести понятие «идеальных чисел (дивизоров)». Появился очередной новый раздел – теория дивизоров.

В современной школе этому не учат и в этом одна из причин того, что математические олимпиады, в состав которых все больше включают задач из теории чисел, становятся все более сложными для подавляющего большинства школьников. При этом высказывание Г. Штейнгауза, приведенное в начале статьи, все более обретает черты научного прогноза.

В последнее время много делается для того, чтобы такая прекрасная наука, как теория чисел, составила бы основу разработки новых интеллектуальных технологий радиотехнических измерений, передачи информации и ее защиты от помех и несанкционированного доступа (НСД). В результате проведенных исследований появилась новая прикладная математическая наука – конструктивная теория конечных полей [9–11]. Она составила основу конструктивной теории измерений, передачи информации и ее защиты от НСД [9–11].

Известны традиционные области прикладного применения теории чисел и теории конечных полей в информатике – это синтез сложных сигналов с заданными свойствами (к числу наиболее часто упоминаемых среди них относят широкополосные сигналы (ШПС)) и помехоустойчивое кодирование информации. Также известными являются и основные противоречия при их применении. Так, например, прием ШПС с малой базой В наиболее просто реализуем, но обладает недостаточной скрытностью и помехустойчивостью. ШПС с большой базой требует значительного усложнения процессов его приема и выделения на фоне помех. Но существует направление кардинального разрешения этого противоречия: оно связано с тем, что для передачи используют несколько $ШПС_i$ с малой и определенным образом различающейся между базой B_i ($i = 1,2,..,n$), а при приеме $ШПС_i$ разворачивают на основе операция свертки в ШПС с большой базой B. При этом распараллеливается и сама процедура выделения на фоне помех переданной информации. Этому способствовало использование следующих новых знаний, полученных на основе прикладной конструктивной теории конечных полей: возможность значительного упрощения процедуры обработки сигналов-образов (в приведенном примере B_i ($i = 1,2,..,n$) и их свертки с получением ШПС с большой базой B. При этом, чем меньше различие между модулями сравнения (в нашем случае B_i ($i = 1,2,..,n$), тем более простой становится новая операция свертки.

Этому условию оптимальным образом соответствуют числа Фрютля, которые рассмотрены в статье, по-

этому проведенные исследования приобретают не только чисто познавательное значение, но и большую прикладную научную и практическую значимость.

Литература
1. Бухштаб АА., «Теория чисел», 1960.
2. Михелович Ш.Х., «Теория чисел», 1967.
3. Прахар К., «Распределение простых чисел», 1967.
4. Виноградов И.М., «Основы теории чисел», 1972.
5. Математическая энциклопедия в V-томах, 1977.
6. Поляков Д.Б. , Круглов И.Ю. «Программирование в среде ТУРБО ПАСКАЛЬ», 1992 .
7. Фаронов В.В. , «Delphi 4. Учебный курс», 1998г.
8. Епаншенков А.М., Епаншенков В.А., «DELPHI 4. Среда разработки», 1999.
9. Кукушкин С.С. «Теория конечных полей и информатика»/том 1 – «Методы и алгоритмы, классические и нетрадиционные, основанные на использовании конструктивной теоремы об остатках» – М.: Минобороны России, 2003 – 281с.
10. Кукушкин С.С, Гладков И.А., Чаплинский В.С. «Методы и информационные технологии контроля состояния динамических систем» – М.: Минобороны России, 2008 – 327с.
11. Кукушкин С.С. «Математические методы преобразования и обработки измерительной информации при испытаниях и штатной эксплуатации ракетно-космической техники» – М.: Минобороны России, 2009 – 276с.

Материал поступил в редакцию 20. 12. 2010 г.