В.А. Минаев, В.П. Хренов

ОТКРЫТИЕ И ПРИКЛАДНЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ЗАКОНОМЕРНОСТИ ФОРМИРОВАНИЯ РЯДА ПРОСТЫХ ЧИСЕЛ

Доклад посвящен математическому доказательству закона формирования простых (первых) чисел. Описаны соотношения формирования составных чисел. Представлена новая структура натурального ряда чисел, рассмотрены прикладные аспекты полученных результатов, в том числе - в области прикладной математики, ***информационной безопасности***, педагогики.

Об истории вопроса

Со времён древнегреческой цивилизации лучшие умы человечества пытались познать закономерность, согласно которой формируется ряд простых чисел (ПЧ). До наших времён дошли две жемчужины математического мышления древних: "решето просеивания" ПЧ Эратосфена и доказательство Евклида бесконечного числа ПЧ [1].

За прошедшие тысячелетия были успехи на пути познания указанной закономерности, но они не стали кардинальными. В частности, Л. Эйлеру, а также Ю. Матиясевичу удалось составить алгебраические уравнения, с помощью которых в ограниченном интервале натурального ряда получались только простые числа.

Усилиями Гаусса, Чебышева, Адамара, Ле Вале Пуссена и Римана сформирован "Асимптотический закон распределения простых чисел". Но с помощью этого закона, к сожалению, нельзя точно определить ни количество простых чисел в определенном интервале, ни простое число по индексу, ни индекс простого числа.

В настоящее время, в сложившейся парадигме современной математики определяются следующие натуральные числа: чётные {2n} и нечётные {2n - 1}, где n = 1, 2, 3, 4 …, простые {1, 2, 3, 5, 7, …} и составные {4, 6, 9, 10, …}. Такая неоднозначная классификация, когда одно и то же число может быть отнесено к разным классам: 2 – одновременно число и простое, и чётное, 9 – одновременно число нечётное и составное, а 5 – нечётное и простое, вызвана, на наш взгляд, тем обстоятельством, что за всю историю математики поиски элементарных формул, дающих только простые числа (без ограничения диапазона вычислений), оказались тщетными.

Ступени постижения закономерности

На пути постижения закономерностей формирования натурального ряда чисел и его составной части – ряда простых чисел - оказалось четыре

ступени [2-5].

Постижению закономерностей формирования натурального ряда и простых чисел ***на первой ступени*** послужило осмысление способов образования ПЧ, предопределяющих отличия их свойств.

На этой ступени были однозначно определены три качественно отличных подмножества ПЧ: - фундаментальные ПЧ {2, 3}; ***отрицательные ПЧ*** {5, 11, 17, …}, которые образуются от чисел, кратных шести, путём вычитания единицы; ***положительные ПЧ*** {7, 13, 19, …}, образующиеся путём прибавления единицы к числам, кратным шести. Подчеркнем, что 1 (единица) является уникальным числом, не простым и не составным, выступая источником всего натурального ряда.

Однозначное определение трёх качественно отличных подмножеств ПЧ позволило сформулировать правила формирования знаков при образовании всех составных чисел (СЧ) – это произошло ***на второй ступени*** постижения закономерностей.

На третьем уровне выяснилось, что последовательность {2·3·n - 1} содержит все отрицательные ПЧ (кроме фундаментальных) и все ***отрицательные составные числа*** **(*СЧ*),** которые также образуются от чисел, кратных шести, путём вычитания единицы); а {2·3·n + 1} - все положительные ПЧ (кроме фундаментальных) и ***положительные СЧ***, которые образуются от чисел, кратных шести, путём прибавления единицы, при этом n = 1, 2, 3…

Вычитая из этих двух последовательностей, соответственно, все отрицательные СЧ и все положительные СЧ, получаем все ПЧ, кроме фундаментальных ПЧ. Так был преодолен ***четвертый уровень*** познания и открыта закономерность формирования ряда простых чисел.

Пройдем все эти ступени вместе, используя математический аппарат доказательств.

Для начала определим множество всех положительных ПЧ как $\{ {}^{+}P\}$, множество всех отрицательных ПЧ как $\{ {}^{-}P)$, множество всех положительных СЧ как $\{{}^{+}C\}$, а множество всех отрицательных СЧ как $\{ {}^{-}C\}$.

Математическое доказательство закономерности формирования простых чисел

Для начала вспомним знаменитую теорему Евклида [1].

Теорема Евклида – "Простых чисел существует больше их любого указанного числа".

Чтобы понять логику наших дальнейших рассуждений, приведем до-

казательство теоремы Евклида, весьма красивое и элегантное.

***Доказательство*:**

Пусть p_n – максимально известное простое число. Составим произведение всех ПЧ от 2 до p_n (назовем произведение $p_1 \cdot p_2 \cdot \ldots \cdot p_n$ факториалом ПЧ p_n!) и добавим к нему 1:

$$p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 = {}^{+}M. \qquad (1)$$

Это число не может делиться на 2, так как если бы оно делилось на 2, то и разность ${}^{+}M - p_n!$ делилась бы на 2. Но разность этих чисел равна 1 и не делится на 2. Аналогично убеждаемся в том, что ${}^{+}M$ не может делиться на 3, на 5 и вообще ни на какое другое простое число вплоть до p_n.

С другой стороны, ${}^{+}M$ должно делиться на какое-нибудь простое (на само себя и на единицу, если ${}^{+}M$ является ПЧ, или на любой простой делитель, больший p_n, если ${}^{+}M$ является СЧ). Следовательно, существует простое число, отличное от любого из простых 2, 3, 5, ..., p_n и потому большее p_n. Таким образом, ряд простых чисел оборваться не может. ‖

Однако возникает вопрос о полноте представления всех ПЧ соотношением $\{p_n! + 1\}$. Существуют ли ПЧ, не представленные данным соотношением?

Да, существуют. На этот вопрос отвечает следующая теорема.

***Теорема* 1** о бесконечном количестве отрицательных ПЧ: "Простых чисел с недостающей для делимости единицей существует больше любого указанного их числа".

Доказательство:

Составим произведение, аналогичное применяемому в теореме Евклида, но вычтем из него единицу:

$$p_1 \cdot p_2 \cdot \ldots \cdot p_n - 1 = {}^{-}M. \qquad (2)$$

Допустим, что существует лишь конечное количество ПЧ с недостающей для делимости 1. Тогда всякое иное число является составным, в том числе и новое число ${}^{-}M$ и, соответственно, оно должно делиться без остатка на какое либо ПЧ, входящее в произведение ПЧ. Но при делении на p_1, p_2 и так далее ${}^{-}M$ даёт всякий раз остаток. С другой стороны, ${}^{-}M$ должно делиться на какое-нибудь простое (на само себя и на единицу, если ${}^{-}M$ является ПЧ, или на любой простой делитель, больший p_n, если ${}^{-}M$ является СЧ). Следовательно, существует простое число, отличное от любого из простых 2, 3, 5, ..., p_n и потому большее p_n. Таким образом, ряд простых чисел и в этом случае оборваться не может.

Поэтому сделанное нами допущение, что существует лишь конечное число простых чисел с недостающей для делимости 1 (*отрицательных*),

приводит к противоречию. То есть оно ошибочно, а, следовательно, истинным может быть только противоположное ему. Итак, теорема 1 доказана – существует бесконечное множество *отрицательных* ПЧ (с недостающей для делимости 1). ‖

Отметим, что данные способы образования чисел ($p_n! \pm 1$) дают не только положительные (отрицательные) ПЧ, но и положительные (отрицательные) СЧ. Кроме того, не все положительные (отрицательные) ПЧ и СЧ образуются с помощью соотношения ($p_n! \pm 1$), а только их часть. Как получить все до одного ПЧ и СЧ, мы увидим ниже.

Следует особо подчеркнуть, что вычисляя по соотношениям $\{p_n! + 1\}$ и $\{p_n! - 1\}$ новые ПЧ, мы пропустим множество других ПЧ, находящихся между факториалами простых чисел $p_i!$ и $p_{i+1}!$. Это легко показать на примере ПЧ, образованных от факториалов первых трех простых чисел 1, 2, 3, 5. Очевидно, что добавление 1 к каждому факториалу ПЧ 1·1, 1·2; 1·2·3; 1·2·3·5 даст нам простые числа 7, 31 и фундаментальные ПЧ - 2, 3. А вычитание 1 от каждого факториала 1·2; 1·2·3; 1·2·3·5 даст нам простые числа 5, 29 и единицу. Таким образом, оказались пропущенными простые числа 11, 13, 17, 19, 23.

Очевидно, что число пропущенных отрицательных ПЧ и СЧ между соотношениями $p_{i+1}! -1$ и $p_i! -1$ будет минимальным в том случае, когда разность между ними будет минимальной: $(p_{i+1}! -1) – (p_i! -1) = p_i!(p_{i+1} -1)$.

Таким образом, минимум разности достигается при минимуме каждого из сомножителей. А он достигается при $i = 1$, т.е. при этом $p_i = p_1 = 2$, а $p_{i+1} = p_2 = 3$. Аналогичным образом показывается, что число пропущенных положительных ПЧ и СЧ между соотношениями $p_{i+1}! + 1$ и $p_i! + 1$ будет минимальным также в случае $i = 1$, при этом также $p_i = p_1 = 2$, а $p_{i+1} = p_2 = 3$.

Отсюда возникает очевидное предположение, что для вычисления всех ПЧ и СЧ подряд необходимо взять последовательность, кратную факториалу фундаментальных ПЧ - $p_2! = 2·3 = 6$. Чтобы подтвердить это предположение, докажем следующую теорему.

Теорема 2 о необходимом и достаточном условии существования всех положительных ПЧ $\{^{+}P\}$, СЧ $\{^{+}C\}$ и всех отрицательных ПЧ $\{^{-}P\}$ и СЧ $\{^{-}C\}$: "Последовательность $\{p_2!·n-1\} = \{2·3·n-1\}$ содержит все ***отрицательные ПЧ*** и ***отрицательные СЧ***, а последовательность $\{p_2! ·n + 1\} = \{2·3·n + 1\}$, $n=1,2,3,…$; содержит все ***положительные ПЧ и положительные СЧ*".**

Доказательство:

Допустим, что не $\{p_2!\cdot n - 1\}$, а факториал любого i-го ПЧ ($i > 2$), умноженный на n за вычетом единицы, т.е. $\{p_i!\cdot n - 1\}$, содержит все *отрицательные ПЧ* и *СЧ*.

Очевидно, что количество образуемых *отрицательных ПЧ* и *СЧ* тем меньше, чем больше любое $p_i > p_2$. Это легко показать, взяв любое натуральное число M, заведомо большее $p_i!\cdot n - 1$. На самом деле, интервал (от $p_2!-1$ до M) образования отрицательных ПЧ и СЧ (при $n = 1, 2, 3,\ldots$) для последовательности $p_2!*n - 1$ больше интервала (от $p_i! - 1$ до M) для последовательности $p_i!\cdot n - 1$. А именно, $M - (p_2! - 1) > M - (p_i! - 1)$ или, по определению, $p_i! > p_2!$ при любых $i > 2$.

Пример. Увеличивая количество образуемых отрицательных ПЧ и СЧ путём уменьшения p_n, можно спуститься до $p_n = p_3 = 5$. Но, как мы видели раньше, даже при $p_3! = 2\cdot3\cdot5$ и $n = 1$ пропускаются отрицательные ПЧ 11, 17, 23. При $p_3! = 2\cdot3\cdot5$ и $n = 2$ будут пропущены СЧ 35 и ПЧ 41, 47, 53. Поэтому значение $p_3!\cdot n$ недостаточно для утверждения теоремы "…содержит все отрицательные ПЧ и отрицательные СЧ…".

Нетрудно видеть, что максимальное количество образуемых отрицательных ПЧ и СЧ достигается при $p_n = p_2$.

Покажем теперь, что последовательность $\{p_2!\cdot n - 1\} = \{2\cdot3\cdot n - 1\}$ содержит все отрицательные ПЧ и отрицательные СЧ.

Представив n в канонической форме $p_1^{\alpha1}\cdot p_2^{\alpha2}\cdot p_3^{\alpha3}\cdot \ldots \cdot p_n^{\alpha n}$ в $\{2\cdot3\cdot n - 1\}$, мы будем получать ПЧ и СЧ вида $p_1^{1+\alpha1}\cdot p_2^{1+\alpha2}\cdot p_3^{\alpha3}\cdot p_4^{\alpha4}\ldots \cdot p_n^{\alpha n} - 1$. Очевидно, что наличие в данном факториале, модифицированном по сравнению с теоремой 1, фундаментальных ПЧ в любой, отличной от 1, степени, не меняет вышеуказанное свойство неделимости из-за недостающей 1, а лишь увеличивает интервал появления новых *отрицательных ПЧ и СЧ*.

Очевидно, что величина интервалов между двумя соседними значениями последовательности $\{6n + 1\}$ всегда равна значению 6. Покажем, что на этих интервалах не образуется ни простых, ни составных чисел. На самом деле, число $6n + 2$ – образует подмножество множества четных чисел, $6n + 3$ – множество нечетных чисел, $6n + 4$ – также подмножество чисел четных. Следующее значение $6n + 5=6(n + 1) - 1$ образует отрицательные ПЧ или СЧ. Аналогичным образом осуществляется и проверка для последовательности $\{6n - 1\}$.

Таким образом, в интервалах между $6n + 1$ и $6(n + 1)-1$, или анало-

гично между 6n - 1 и 6(n - 1) + 1не образуется ни ПЧ, ни СЧ.

Отсюда следует, что последовательность {6n - 1} содержит все *отрицательные* ПЧ и СЧ, а последовательность {6n + 1} содержит все *положительные* ПЧ и СЧ при n = 1, 2, 3… ‖

На основании теоремы 2 мы можем сформулировать:

***Утверждение первое*:**

Множество 6n - 1 содержит всё подмножество *отрицательных* ПЧ $\{^{-}P\}$ и всё подмножество *отрицательных* СЧ $\{^{-}C\}$:

$$\{^{-}P\} \cup \{^{-}C\} = \{6n-1\} = \{5, 11, 17, 23, 29, 35, 41, \ldots\}. \quad (3)$$

Множество 6n + 1 содержит всё подмножество *положительных* ПЧ $\{^{+}P\}$ и всё подмножество *положительных* СЧ $\{^{+}C\}$:

$$\{^{+}P\} \cup \{^{+}C\} = \{6n+1\} = \{7, 13, 19, 25, 31, 37, 43, 49, \ldots\}. \quad (4)$$

Исходя из теоремы 2, сформулируем:

Лемму 1 о правиле знаков при образовании составных чисел: "Произведение нескольких отрицательных и положительных ПЧ p_i дает положительное составное число $^{+}c_i$ при четном количестве отрицательных ПЧ $^{-}p_i$, и отрицательное составное число $^{-}c_i$ при нечетном количестве $^{-}p_i$".

***Доказательство*:**

Любое отрицательное ПЧ имеет вид 6k - 1, а любое положительное ПЧ имеет вид 6k + 1, где k = 1, 2, 3,… – натуральные числа.

a) Произведение двух отрицательных ПЧ имеет вид A = (6k - 1)·(6n - 1), где n = 1, 2, 3…. - натуральные числа;

A = (6k - 1)·(6n - 1) = 36kn - 6k – 6n + 1 = 6(6kn – k - n) + 1 = 6m + 1, где m = 6kn – k - n – также натуральное число; 6kn – k - n = 3kn – k + 3kn - n = k(3n - 1) + n(3k - 1) > 0.

Следовательно, A = (6k - 1)·(6n - 1) = 6m + 1 – положительное число.

Используя полученное доказательство для произведения двух отрицательных ПЧ, нетрудно показать, что произведение любого четного количества отрицательных ПЧ также будет числом положительным, сводясь к числу вида 6q + 1, где q натуральное число.

b) Произведение двух положительных ПЧ

B = (6k + 1)·(6n + 1) = 36kn + 6k + 6n + 1 = 6(6kn + k + n) + 1 = 6m + 1, m = 6kn + k + n, где m – натуральное число. Следовательно, B – положительное число.

Аналогичным образом легко показать, что произведение любого числа положительных ПЧ – положительно.

c) Произведение отрицательного и положительного ПЧ – отрица-

тельно:

$C = (6k - 1)\cdot(6n + 1) = 36kn + 6k - 6n - 1 = 6(6kn + k - n) - 1 = 6m - 1$, где натуральное число $m = 6kn + k - n = k(3n + 1) + n(3k - 1) > 0$.

Нетрудно показать, что группируя любое количество отрицательных и положительных ПЧ и руководствуясь выводами a, b, c теоремы 4, мы придём к заключению: произведение любого сочетания отрицательных и положительных" ПЧ в произведении, образующем СЧ, сводится к виду $6m + 1$ при чётном количестве ^{-}p, либо к виду $6m - 1$ при нечётном количестве ^{-}p. ‖

На основании леммы 1 сформулируем:

Утверждение второе:

$$^{-}p_i \cdot {}^{-}p_j = {}^{+}c_k; \quad {}^{-}p_i \cdot {}^{+}p_j = {}^{-}c_k; \quad {}^{+}p_i \cdot {}^{+}p_j = {}^{+}c_k \qquad (5)$$

"Произведение нескольких *отрицательных* и *положительных* ПЧ дает *положительное* СЧ при четном количестве *отрицательных* ПЧ и *отрицательное* СЧ при их нечетном количестве".

Обоснование понятия "спектрально аддитивная прогрессия"

Напомним, что всякое наибольшее целое число, которое нацело делит целые числа a, b, c, … называется их ***наибольшим*** общим делителем (НОД), а также то, что всякая последовательность $\{a_n\}$, определённая следующим рекуррентным способом: a_1 задано, и для всех $n \geq 1$ справедливо равенство $a_{n+1} = a_1 + d$, где d также некоторое заданное число, называется *арифметической прогрессией,* a d – *разностью арифметической прогрессии.*

Известно, что арифметическая прогрессия позволяет путём неограниченного сложения выявленную закономерность устремить в бесконечность, а НОД позволяет устанавливать свойства целых чисел относительно умножения.

Синтезируя эти два понятия, можно получить п-аддитивные прогрессии, то есть арифметические прогрессии, где ***наименьшим*** общим делителем (нОД) выступают простые числа. Подчеркнем, что нОД отличается от НОД – это новое понятие.

Очевидно, что последовательное присоединение к простому числу кратного количества этого же простого числа образует арифметическую прогрессию с нОД, равным этому простому числу:

$$\{p_i,\ (p_i + k\cdot p_i),\ (p_i + 2\cdot k\cdot p_i),\ (p_i + 3\cdot k\cdot p_i),\ \ldots\} = \{p_i + p_i kn\}, \qquad (6)$$

где p_i – какое-либо ПЧ, k - коэффициент кратности, a $n = 0, 1, 2, 3\ldots$

Итак, мы получили арифметическую прогрессию, где p_i является

нОД.

Соотношение (6) отражает сущность простых чисел быть первыми в образуемых ими арифметических прогрессиях с нОД, равным ПЧ.

Например, $\{2, 2 + 2\cdot1, 2 + 2\cdot2, 2 + 2\cdot3, \ldots\} = \{2 + 2\cdot n\}$.

При $n = 0$, это фундаментальное ПЧ = 2, а при $n \geq 1$, $k = 1$ это прогрессия чётных чисел {4, 6, 8,…}.

Применяя соотношение (6) к фундаментальному ПЧ = 3 и приняв $k = 1$, имеем:

$\{3, 3 + 3\cdot1, 3 + 3\cdot2, 3 + 3\cdot3, \ldots\} = \{3 + 3n\} = \{3\ (1 + n)\}$.

При $n = 0$, это ПЧ = 3, а при $n \geq 1$ имеем прогрессию {6, 9, 12, 15, …}.

Для получения однозначности принадлежности чисел кратных 6, в прогрессии с $p_3 = 3$ необходимо принять $k = 2$:

$\{3, 3 + 3\cdot2\cdot1, 3 + 3\cdot2\cdot2, 3 + 3\cdot2\cdot3,\ldots\} = \{3 + 3\cdot2n\}$.

Тогда мы получаем прогрессию чисел, которые по аналогии назовём *нечётными* числами: при $n = 0$, это *фундаментальное* ПЧ = 3, а при $n \geq 1$ это прогрессия *нечётных* чисел {9, 15, 21, …}.

Применяя соотношение (6) ко всем (кроме фундаментальных) ПЧ {5, 7, 11,…}, мы должны учитывать закон правила знаков, которому подчиняются образуемые ими СЧ. Каждое из этих СЧ, в зависимости от знаков сомножителей, входит в последовательность либо $\{6n - 1\}$, либо $\{6n + 1\}$.

Для того чтобы правомерно утверждать, что последующие множества *отрицательных* СЧ содержат все СЧ, образованные произведением всех *отрицательных* и *положительных* ПЧ, необходимо:

1) начинать последовательности СЧ с наименьших значений качественно отличных ПЧ, так как в ином случае будут пропущены наименьшие значения СЧ, что сделает некорректным утверждение теоремы "… все …";

2) не пропускать ни одного ПЧ, следующего друг за другом по индексу во всех сочетаниях знаков качества ПЧ;

3) 4-е возможные сочетания качественно отличных ПЧ "-"·"-", "-"·"+", "+"·"-" и "+"·"+" должны быть последовательно (по мере увеличения модуля СЧ) размещены в 2-х качественно отличных ("-" или "+") областях существования СЧ $\{6n - 1\}$ и $\{6n + 1\}$.

1. Сначала рассмотрим принципы образования *отрицательных* прогрессий СЧ, входящих во множество $\{6n - 1\}$.

Обратим внимание читателя, что далее для удобства восприятии материала индексация простых чисел осуществляется следующим образом:

отрицательные ПЧ начинаются с $^{-}p_1 = 5$, далее $^{-}p_2 = 11$ и т.д.; *положительные с* $^{+}p_1 = 7$, далее $^{+}p_2 = 13$ и т.д.

1.1. Начнём с наименьшего *отрицательного* ПЧ $^{-}p_1 = 5$. Два фундаментальных ПЧ для удобства расчета индексов пока не будем учитывать. При этом одинаковый индекс у нас будут иметь и положительные, и отрицательные ПЧ.

От числа $^{-}p_1 = 5$ должно образоваться два подмножества - *отрицательных и положительных* СЧ, входящие в множества {6n-1} и {6n+1} соответственно.

Первый член арифметической прогрессии подмножества *отрицательных* СЧ по сочетанию "-"·"+" образуется произведением ***наименьшего отрицательного*** ПЧ $^{-}p_1 = 5$ и ***наименьшего положительного*** ПЧ $^{+}p_1 = 7$, то есть $_5{}^{-}c_1 = {}^{-}p_1 \cdot {}^{+}p_1$. Для того, чтобы получить арифметическую прогрессию с нОД $^{-}p_1 = 5$, необходимо к $^{-}p_1 \cdot {}^{+}p_1$ прибавлять кратные k количества $^{-}p_1$, то есть:

$$_5{}^{-}C = \{{}^{-}p_1 \cdot {}^{+}p_1 + {}^{-}p_1 \cdot k \cdot m\} = \{{}^{-}p_1 \cdot ({}^{+}p_1 + k \cdot m)\};\ m = 0, 1, 2,\ldots$$

При этом k не может принимать значения {1, 3, 5, 7, …}, так как в этом случае {7 + 1, 7 + 3, 7 + 5,…} элементы прогрессии $_5{}^{-}C$ будут принадлежать множеству *чётных* чисел.

Не может k принимать и значения {2, 8, 14,…}, так как в этом случае {7+2, 7 + 8, 7 +14 ,…}, элементы прогрессии $_5{}^{-}C$ будут принадлежать множеству *нечётных* чисел (кратных 3).

Не может k принимать и значения {4, 10,16,…}, так как в этом случае {7 + 4, 7 + 10, 7 + 16,…}, элементы прогрессии $_5{}^{-}C$ будут принадлежать множеству *положительных* ПЧ и СЧ.

Остаются только значения k, равные числам кратным 6, то есть k = 6m (m = 1, 2, 3…), которые обеспечивают прогрессии $^{-}p_1\{7 + k \cdot n\}$ принадлежность к множеству *отрицательных* СЧ {6n - 1}, т.к. 7 + kn = 7 + 6mn = 6(1 + mn) + 1 = 6q + 1 – *положительное* по определению число, где q = 1 + mn –натуральное число.

Таким образом, для $_5{}^{-}C$ окончательно получаем:

$$_{p1}{}^{-}C = \{{}^{-}p_1 \cdot {}^{+}p_1 + {}^{-}p_1 \cdot 6 \cdot n\};\ n = 0, 1, 2,\ldots \qquad (7)$$

1.2. Следующим по модулю является первое *положительное* ПЧ $^{+}p_1 = 7$.

От этого числа также должно образоваться два подмножества *отрицательных и положительных* СЧ, входящих в множества {6n - 1} и {6n + 1} соответственно. Первый член арифметической прогрессии под-

множества *отрицательных* СЧ по сочетанию "+"·"-" образуется произведением наименьшего *положительного* ПЧ $^{+}p_1 = 7$ и следующего *отрицательного* ПЧ $^{-}p_2 = 11$, то есть $_7\bar{c}_1 = {}^{+}p_1 \cdot \bar{p}_2$. Для того, чтобы получить арифметическую прогрессию с нОД $^{+}p_1 = 7$, необходимо к $^{+}p_1 \cdot \bar{p}_2$ прибавлять кратные k количества $^{+}p_1$, то есть:

$$_7\bar{C} = \{{}^{+}p_1 \cdot \bar{p}_2 + {}^{+}p_1 \cdot k \cdot n\} = {}^{+}p_1\{11 + k \cdot n\};\ n = 0, 1, 2, 3\ldots.$$

При этом k не может принимать значения {1, 3, 5, 7, …}, так как в этом случае {11+1, 11+3, …} элементы прогрессии $_7\bar{C}$ будут принадлежать множеству *чётных* чисел.

Также k не может принимать значения {2, 8, 14,…}, так как в этом случае {11 + 2, 11 + 8, …}, элементы прогрессии $_7\bar{C}$ будут принадлежать множеству *положительных* ПЧ и СЧ.

Кроме того, k не может принимать значения {4, 10, 16,…}, так как в этом случае {11 + 4, 11 + 10, …}, элементы прогрессии $_7\bar{C}$ будут принадлежать множеству *нечётных* чисел (кратных 3).

Остаются только значения k, равные числам кратным 6, то есть k = 6m (m = 1, 2, 3…), которые обеспечивают прогрессии $\bar{p}_1\{7 + k \cdot n\}$ принадлежность к множеству *отрицательных* СЧ {6n - 1}, т.к. 7 + kn = = 7 + 6mn = 6(1 + mn) + 1 = 6q + 1 – *положительное* по определению число, где q = 1 + mn –натуральное число.

Только значения k, равные числам, кратным 6, то есть k = 6m; m = 0, 1, 2,…обеспечивают прогрессии $^{+}p_1\{11 + k \cdot n\}$ принадлежность к множеству *отрицательных* ПЧ и СЧ, т. к. {11 + k·n} = {6(2 + mn) - 1} = {6q - 1} – отрицательное по определению число, где q = 2 + mn – натуральное число. Таким образом, для $_7\bar{C}$ окончательно получаем:

$$_{+p1}\bar{C} = \{{}^{+}p_1 \cdot \bar{p}_2 + {}^{+}p_1 \cdot 6 \cdot n\};\ n = 0, 1, 2,\ldots \quad (8)$$

По методу математической индукции получаем:

$$_{-p2}\bar{C} = \{\bar{p}_2 \cdot {}^{+}p_2 + \bar{p}_2 \cdot 6 \cdot n\} \quad (9)$$

$$_{+p2}\bar{C} = \{{}^{+}p_2 \cdot \bar{p}_3 + {}^{+}p_2 \cdot 6 \cdot n\} \quad (10)$$

…….

$$_{-pi}\bar{C} = \{\bar{p}_i \cdot {}^{+}p_i + \bar{p}_i \cdot 6 \cdot n\} \quad (11)$$

$$_{+pi}\bar{C} = \{{}^{+}p_i \cdot \bar{p}_{i+1} + {}^{+}p_i \cdot 6 \cdot n\} \quad (12)$$

2. Теперь рассмотрим принципы образования *положительных* прогрессий СЧ, входящих в множество {6n + 1}.

2.1. Начнём с наименьшего *отрицательного* ПЧ $\bar{p}_1 = 5$. От этого числа должно образоваться два подмножества *отрицательных и положительных* СЧ, входящих в множества {6n - 1} и {6n + 1} соответственно.

Первый член арифметической прогрессии подмножества *положительных* СЧ по сочетанию "-"·"-" образуется произведением наименьших *отрицательных* ПЧ $^{-}p_1 = 5$, то есть ${}_5^{+}c_1 = {}^{-}p_1 \cdot {}^{-}p_1$. Для того, чтобы получить арифметическую прогрессию *положительных СЧ* с НОД $^{-}p_1 = 5$, необходимо к $^{-}p_1 \cdot {}^{-}p_1$ прибавлять кратные k количества $^{-}p_1$, то есть:

${}_5^{+}C = \{{}^{-}p_1 \cdot {}^{-}p_1 + {}^{-}p_1 \cdot k \cdot n\} = {}^{-}p_1\{5 + k \cdot n\}$; n = 0, 1, 2,….

При этом k не может принимать значения {1, 3, 5, 7, …}, так как в этом случае {5+1, 5+3, 5+5,…} элементы прогрессии ${}_5^{+}C$ будут принадлежать множеству *чётных* чисел.

Не может k принимать и значения {2, 8, 14,…}, так как в этом случае {5+2, 5+8, 5+14 ,…}, элементы прогрессии ${}_5^{+}C$ будут принадлежать множеству *отрицательных* ПЧ и СЧ.

Кроме того, k не может принимать значения {4, 10, 16,…}, так как в этом случае {5+4, 5+10, 5+16 ,…}, элементы прогрессии ${}_5^{+}C$ будут принадлежать множеству *нечётных* чисел (кратных 3).

Как и в предыдущих случаях, значения k могут быть только кратны 6, то есть k = 6m; m = 0, 1, 2,…Это обеспечивает прогрессии $^{-}p_1\{5+k \cdot n\}$ принадлежность к множеству *положительных* ПЧ и СЧ {6n+1}, т.к. $\{5 + 6m \cdot n\} = \{6(1 + m \cdot n) - 1\} = \{6q - 1\}$ – отрицательные по определению числа, где $q = 1 + m \cdot n$ –натуральное число, Таким образом, для ${}_5^{+}C$ окончательно получаем:

$$ {}_{-p1}^{+}C = \{{}^{-}p_1 \cdot {}^{-}p_1 + {}^{-}p_1 \cdot 6 \cdot n\}. \qquad (13) $$

2.2. Следующим по модулю ПЧ является $^{+}p_1 = 7$. Первый член арифметической прогрессии подмножества *положительных* СЧ по сочетанию "+"·"+" образуется произведением наименьших *положительных* ПЧ $^{+}p_1 = 7$, то есть ${}_7^{+}c_1 = {}^{+}p_1 \cdot {}^{+}p_1$. Для того, чтобы получить арифметическую прогрессию *положительных СЧ* с НОД $^{+}p_1 = 7$, необходимо к $^{+}p_1 \cdot {}^{+}p_1$ прибавлять кратные k количества $^{+}p_1$, то есть:

$$ {}_{+p1}^{+}C = \{{}^{+}p_1 \cdot {}^{+}p_1 + {}^{-}p_1 \cdot 6 \cdot n\} \qquad (14) $$

По методу математической индукции получаем:

$$ {}_{-p2}^{+}C = \{{}^{-}p_2 \cdot {}^{-}p_2 + {}^{-}p_2 \cdot 6 \cdot n\} \qquad (15) $$

$$ {}_{+p2}^{+}C = \{{}^{+}p_2 \cdot {}^{+}p_2 + {}^{+}p_2 \cdot 6 \cdot n\} \qquad (16) $$

…….

$$ {}_{-pi}^{+}C = \{{}^{-}p_i \cdot {}^{-}p_i + {}^{-}p_i \cdot 6 \cdot n\} \qquad (17) $$

$$ {}_{+p1}^{+}C = \{{}^{+}p_i \cdot {}^{+}p_1 + {}^{+}p_i \cdot 6 \cdot n\} \qquad (18) $$

Из полученных соотношений (7)-(12) формулируем:

Следствие 1 – об образовании *отрицательных* составных чисел:

Каждое первое (простое) число p_i образует *спектрально аддитивные* арифметические прогрессии *отрицательных* СЧ $^{-}_{pi}C$, спектр которых определяется ПЧ p_i = нОД при к = 6 по формуле:

$$^{-}C = \{\Sigma_{Pi}\,^{-}C\} = \{^{-}p_1 \cdot {}^{+}p_1 + {}^{-}p_1 \cdot 6m\} U \{^{+}p_1 \cdot {}^{-}p_2 + {}^{+}p_1 \cdot 6m\} U \{^{-}p_2 \cdot {}^{+}p_2 + {}^{-}p_2 \cdot 6m\} U \ldots$$
$$U \{^{-}p_i \cdot {}^{+}p_i + {}^{-}p_i \cdot 6m\} U \{^{+}p_i \cdot {}^{-}p_{i+1} + {}^{+}p_i \cdot 6m\} U \{^{-}p_{i+1} \cdot {}^{+}p_{i+1} + {}^{-}p_{i+1} \cdot 6m\} U \ldots, \quad (19)$$

где i - индексы ПЧ = {1, 2, 3…}, т. е. $^{-}p_1 = 5$, $^{+}p_1 = 7$, $^{-}p_2 = 11$, $^{+}p_2 = 13$, …, а m = {0, 1, 2, 3…}; U – символ объединения множеств.

Пример: ^{-}C={5·7 + 5·6 m} U {7·11 + 7·6m} U {11·13 + 11·6m} U {13·17 + 13·6m} U … =

{35, 65, 95,…} U {77, 119, 161,…} U {143, 209, 275,…} U {221, 299, 377,…} U …;

Из полученных соотношений (13)-(18) формулируем:

Следствие 2 – об образовании *положительных* составных чисел:

Каждое первое (простое) число p_i образует *спектрально аддитивные* арифметические прогрессии *положительных* СЧ $\{_{pi}{}^{+}C\}$, спектр которых определяется ПЧ p_i = нОД при к = 6 по формуле:

$$^{+}C = \{\Sigma_{Pi}\,^{+}C\} = \{^{-}p_1{}^2 + {}^{-}p_1 \cdot 6m\} U \{^{+}p_1{}^2 + {}^{+}p_1 \cdot 6m\} U \{^{-}p_2{}^2 + {}^{-}p_2 \cdot 6m\} U \ldots$$
$$\ldots U \{^{-}p_i{}^2 + {}^{-}p_i \cdot 6m\} U \{^{+}p_i{}^2 + {}^{+}p_i \cdot 6m\} U \{^{-}p_{i+1}{}^2 + {}^{-}p_{i+1} \cdot 6m\} U \{^{+}p_{i+1}{}^2 + {}^{+}p_{i+1} \cdot 6m\} U \ldots \quad (20)$$

где i - индексы ПЧ ={1, 2, 3…}, т. е. $^{-}p_1 = 5$, $^{+}p_1 = 7$, $^{-}p_2 = 11$, $^{+}p_2 = 13$…, а m = {0, 1, 2, 3….}.

Пример: ^{+}C = {5·5 + 5·6 m} U {7·7 + 7·6m} U {11·11 + 11·6m} U {13·13 + 13·6m} U …=

{25, 55, 85,…} U {49, 91, 133,…} U {121, 187, 253,…} U {169, 247, 325,…}U … .

Из вышесказанного следует:

Утверждение 3 о множестве всех ПЧ: "Последовательность всех первых (простых) *отрицательных* ПЧ $\{^{-}P\}$ равна разности между множеством, образуемым последовательностью {6n - 1} и суммой всех "спектрально аддитивных" арифметических прогрессий *отрицательных* СЧ $\{\Sigma_{Pi}\,^{-}C\}$, а последовательность всех первых (простых) *положительных* ПЧ $\{^{+}P\}$ равна разности между множеством, образуемым последовательностью {6n + 1} и суммой всех *спектрально аддитивных* арифметических прогрессий *положительных* СЧ $\{\Sigma_{Pi}\,^{+}C\}$".

Исходя из совокупности вышеизложенных теорем, леммы, утверждений и следствий, сформулируем:

Закон формирования первых (простых) чисел

Множество всех первых (простых) чисел (кроме фундаментальных) $\{P\} = \{^{-}P\} U \{^{+}P\}$ образуется как две разности множеств $\{6n - 1\} \backslash \{_{Pi}{}^{-}C\}$ и $\{6n + 1\} \backslash \{_{Pi}{}^{+}C\}$ и описывается следующим соотношением:

$$P=[\{6n - 1\} \backslash [[\{^{-}p_1 \cdot {}^{+}p_1 + {}^{-}p_1 \cdot 6m\} U \{^{+}p_1 \cdot {}^{-}p_2 + {}^{+}p_1 \cdot 6m\} U \ldots U \{^{-}p_i \cdot {}^{+}p_i + {}^{-}p_i \cdot 6m\} U \{^{+}p_i \cdot {}^{-}p_{i+1} + {}^{+}p_i \cdot 6m\} U \ldots] U [\{6n + 1\} \backslash \{^{-}p_1{}^2 + {}^{-}p_1 \cdot 6m\} U \{^{+}p_1{}^2 + {}^{+}p_1 \cdot 6m\} U \ldots U \{^{-}p_i{}^2 + {}^{-}p_i \cdot 6m\} U \{^{+}p_i{}^2 + {}^{+}p_i \cdot 6m\} U \{^{-}p_{i+1}{}^2 + {}^{-}p_{i+1} \cdot 6m\} U \ldots]], \quad (21)$$

где \ - знак вычитания множеств.

Очевидно, что множества арифметических прогрессий позволяют только операциями сложения получать все СЧ (произведения) в заданном диапазоне вычислений и, таким образом, соотношение (21) позволяет создать линейный генератор ПЧ подряд. И он был создан одним из авторов настоящего доклада [8].

Таким образом, учитывая совокупность вышеизложенного, мы можем сформулировать:

Закон формирования структуры натурального ряда:

$$N = 1 U \{P_ф\} U \{^{-}P\} U \{^{+}P\} U \{_2C \supset _6C\} U \{_3C\} U [\{\Sigma_{Pi}{}^{-}C\} U \{\Sigma_{Pi}{}^{+}C\}], \quad (22)$$

где $\supset$ - знак включения множества.

Числовая система природы (натуральный ряд N) состоит из эталона счётного множества натурального ряда 1; последовательности *фундаментальных* ПЧ $P_ф = \{2, 3\}$; *отрицательных* ПЧ $\{^{-}P\}$ и *положительных* ПЧ $\{^{+}P\}$; чётных СЧ $\{_2C\}$, куда входят *циклические* числа $\{_6C\}$; *нечетных* СЧ $\{_3C\}$; бесконечного множества *спектрально аддитивных* арифметических прогрессий *отрицательных* СЧ $\{\Sigma_{Pi}{}^{-}C\}$ и *положительных* СЧ $\{\Sigma_{Pi}{}^{+}C\}$, образуемых от бесконечного множества *отрицательных* и *положительных* ПЧ".

Этот закон однозначно расщепляет натуральный ряд на 7 качественно различных множеств подобно призме Френеля, расщепляющей белый свет на 7 цветов радуги.

В отличие от "Асимптотического закона распределения простых чисел", представленные в настоящем докладе закономерности натурального ряда позволяют абсолютно точно вычислить как количество простых чисел в произвольно задаваемых диапазонах, так и простое число по задаваемому индексу.

Для большей наглядности приведём новую структурную схему натурального ряда с числовыми примерами (рис. 1).

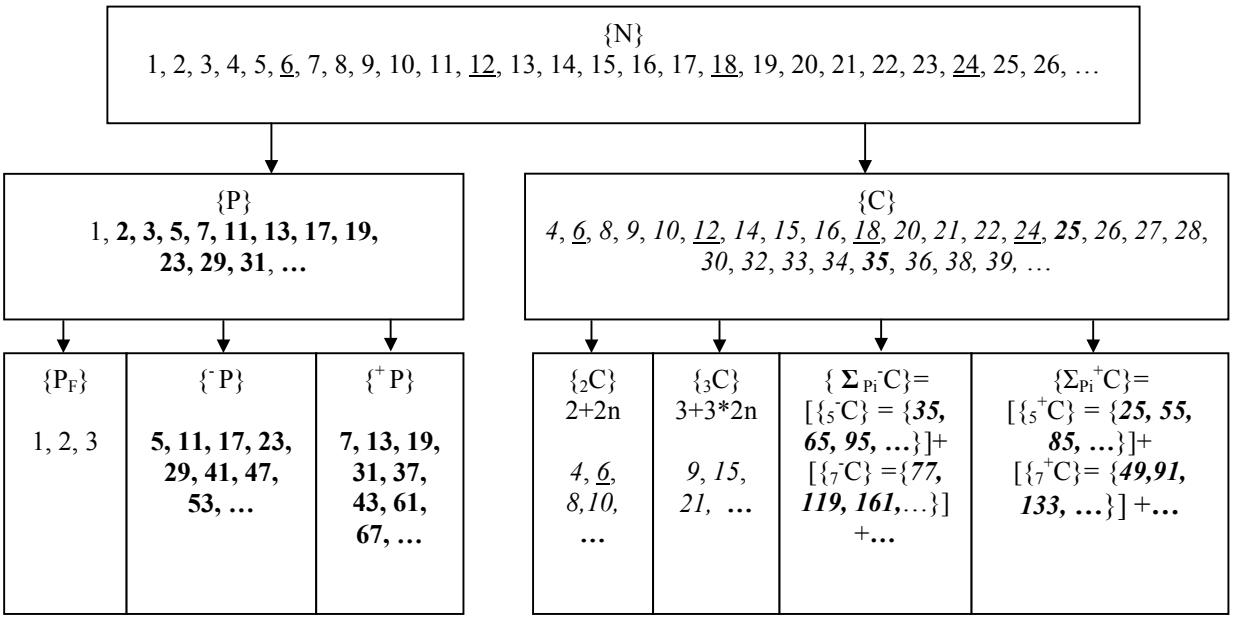

Рис. 1. Новая структура натурального ряда

Мировоззренческие и прикладные аспекты открытых закономерностей

С открытием закономерностей формирования натурального ряда и ряда ПЧ, однозначно идентифицирующих каждое число и его качественные свойства, понимание числовой системы Природы приобрело законченный вид. Это, на наш взгляд, послужит переосмыслению ряда ранее открытых законов математики и решению части её проблемных вопросов. Вероятно, ускорится решение некоторых проблем целочисленной математики, формирования мировых констант, создания компьютеров нового поколения на более эффективных системах счисления.

Чтобы говорить с Природой на одном языке, потребуется изучить и развить изложенную в данной работе "азбуку" этого языка. Настоящая работа - только первый шаг к серьёзному переосмыслению окружающего нас мира и присущих ему математических и физических закономерностей.

Кроме общенаучного значения, открытые законы формирования ряда ПЧ имеет особое значение в области создания ***систем защиты информации*** (СЗИ). Именно здесь сугубо математическая проблема факторизации (определение делителей составного числа) была положена в основу асимметричных систем защиты информации, пригодной для широкого пользования [6].

Теория шифрования с использованием открытого ключа, созданная в 1976 г. У. Диффи и М. Хеллманом и впервые реализованная в 1977 г. в RSA-алгоритме Р. Райвестом, Э. Шамиром и Л. Эдлманом, основывалась на так называемых односторонних функциях: по некоторому x легко вычислить его функцию $f(x)$, но, зная $f(x)$, трудно вычислить x.

В RSA-алгоритме использована достаточно простая идея - вычислить произведение двух простых чисел легко (прямая задача), а разложение полученного в результате этой операции числа на простые множители (обратная задача), достаточно трудоемка. Ибо время вычислений экспоненциально возрастает при увеличении количества битов в полученном сомножителе. В частности, задача на разложение числа, состоящего из 155 цифр, требует 35,7 процессорных года на современном компьютере, при распределенной обработке информации в компьютерной сети - 3,7 месяца.

А если знать закономерности формирования простых чисел, как бы изменилось время факторизации? И второй вопрос. В каком направлении пошла бы разработка новых современных алгоритмов шифрования со знанием законов формирования натурального ряда? Квантовая криптография – как соединение физики и математики, или иная – невероятная еще вчера идея?..

Можно сказать одно - открытые математические закономерности позволяют создать СЗИ нового поколения на одноразовых ключах и одноразовых непериодических гаммах псевдослучайных чисел, что до настоящего времени считалось невозможным [7]. Такие СЗИ будут обладать теоретически максимальной надёжностью и быстродействием режима on line.

Реализация открытых законов началась и в практическом плане – В.П. Хреновым получено свидетельство № 2005613012 от 22.09.2005 г. о регистрации программы "Линейный генератор простых чисел подряд" [8], которое получило высокую оценку коммерческой значимости. Члены Государственной комиссии в своём заключении от 26.04.2005 г. подтвердили, что зависимость времени вычислений последовательностей простых чисел подряд от разрядности задаваемого диапазона вычислений носит линейный характер, что было бы невозможно без знания закона их формирования.

Получены два положительных решения на выдачу патентов, защищающих новые способы защиты информации [9, 10].

Литература

1. Евклид. Начала математики.

2. Хренов В.П. "Новая парадигма мировосприятия", журнал Российской Народной Академии Наук "Академические записки", № 4 и 5, 2005 г.

3. Хренов В.П. Проблемы и перспектива создания систем защиты информации нового поколения, журнал "Глобальная безопасность", № 3, 2005 г.

4. Хренов В.П. Новый этап развития систем защиты информации (СЗИ), журнал "Наука и технологии в промышленности", №3, 2005 г.

5. Хренов В.П. Prime Numbers Technology (PNT)™ – основа создания систем защиты информации (СЗИ) нового поколения и перспективы её применения в различных сегментах информационных технологий // Журнал "Бизнес и Безопасность в России" №46, январь 2007 г., стр. 86-96.

6. Diffie W., Hellman M. "New Directions in Cryptography", IEEE Transactions on

Information Theory, v. IT-22, n. 6, Nov 1977, pp. 74-84.

7. Schneier B. Applied Cryptography, John Wiley & Sons, Inc., 1996.

8. Свидетельство № 2005613012 от 22.09.2005 г. о регистрации программы "Линейный генератор простых чисел подряд".

9. Решение о выдаче патента по заявке № 200128954/09(032494) от 19.09.2005.

10. Решение о выдаче патента по заявке № 200128777/09(032303) от 16.09.2005.