Как видно, чем выше уровень, на который воздействует нарушитель, тем больше возможностей по корректировке $Q^{ИС}$ он имеет. Противостоять этому возможно только путем контроля целостности каждого уровня ИС и целостности связей между уровнями (выражения (1), (2) и (3)). Названные выражения *формализуют* базовую закономерность — *целостность информационной системы* и позволяют, применяя готовые математические аппараты, изучать свойства информационной системы.

Таким образом, для обеспечения безопасности информации в информационной системе *необходимо и достаточно обеспечить целостность всех уровней ИС* и реализовать связь между ними как от вышестоящих к нижестоящим, так и, наоборот, от нижестоящих к вышестоящим.

СПИСОК ЛИТЕРАТУРЫ:

1. *Расторгуев С. П.* Информационная война. М., 1998. — 416 с.
2. Теоремы Гёделя о неполноте http://ru.wikipedia.org/wiki.
3. *Бурлов В. Г.* Синтез модели вычислений в условиях разрушаемой программно-аппаратной среды // Сборник алгоритмов и типовых задач. № 20 / Под ред. И. А. Кулешова. СПб., 2002. С. 220–235.
4. *Бурлов В. Г.* Основы моделирования социально-экономических и политических процессов (Методология. Методы.). СПб., 2007. — 267 с.
5. Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации».
6. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
7. Постановление Правительства РФ от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».
8. *Грызунов В. В.* Структурно-функциональный синтез модели системы предотвращения вторжений // Проблемы информационной безопасности. Компьютерные системы. 2006. № 2. С. 31–38.

В. А. Минаев[1] *(д. т. н., профессор)*
Российский новый университет (проректор),
В. П. Хренов[2]
Российский новый университет (заместитель директора Института систем и технологий безопасности)

ФУНДАМЕНТАЛЬНАЯ ЗАКОНОМЕРНОСТЬ ФОРМИРОВАНИЯ ПРОСТЫХ ЧИСЕЛ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

В последовательности простых чисел есть
тайна, непостижимая человеком.
Л. Эйлер

Работа посвящена математическому доказательству фундаментального закона формирования простых (первых) чисел. Описаны соотношения формирования составных чисел. Представлена новая структура натурального ряда чисел, рассмотрены прикладные аспекты открытия, в том числе в области прикладной математики, информационной безопасности, педагогики.

[1] *В. А. Минаев — автор ряда формализаций при математическом обосновании закономерности формирования натурального ряда чисел и описания прикладных аспектов открытия.*
[2] *В. П. Хренов — автор открытия закономерности формирования натурального ряда.*

Введение

Начнем с того, что теория шифрования с использованием открытого ключа была создана в 1976 г. У. Диффи и М. Хеллманом [1] и впервые реализована в 1977 г. в RSA-алгоритме Р. Райвестом, Э. Шамиром и Л. Эдлманом. Она основывалась на так называемых односторонних функциях: по некоторому x легко вычислить его функцию f(x), но, зная f(x), трудно вычислить x.

Понятно, что в RSA-алгоритме была 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) — процедура достаточно трудоемкая, ибо время вычислений экспоненциально возрастает при увеличении количества битов в полученном открытом ключе.

Именно поэтому компания RSA, основанная вышеперечисленными авторами, до сих пор предлагает желающим различные задачи факторизации представленных ею чисел. В частности, задача разложения на множители числа, состоящего из 155 разрядов, требует 35,7 процессорных года на современном компьютере. Хотя для ее решения реально потребовалось 3,7 месяца благодаря распределенным вычислениям в компьютерной сети, алгоритмы компании пользуются успехом, несмотря на увеличивающуюся вычислительную мощность компьютерных систем.

А если знать закономерности формирования простых чисел, как бы изменились алгоритмы шифрования, подобные RSA? А как бы изменились подходы к дешифрованию?

И еще один 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?

Об этом — в следующих статьях. А теперь — о главном.

Из истории проблемы

Со времен древнегреческой цивилизации лучшие умы человечества пытались познать закономерность, согласно которой формируются простые числа (ПЧ)[3]. До нашего времени дошли две жемчужины математического мышления древних: «решето просеивания» ПЧ Эратосфена и доказательство Евклида бесконечного числа ПЧ [2].

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 ПЧ в определенном интервале, ни ПЧ по индексу, ни индекс ПЧ.

В чем же первопричина непостижимости таких непростых и крайне важных для науки и практики «простых» чисел? Давайте попробуем разобраться в этом вопросе, предложив описание закономерностей формирования ПЧ и всего натурального ряда.

В настоящее время, в сложившейся парадигме современной математики, определяются следующие натуральные числа: четные {2n} и нечетные {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 четное, 9 — одновременно число нечетное и составное, а 5 — нечетное и простое), вызвана тем обстоятельством, что за всю историю математики поиски элементарных формул, дающих только ПЧ (без ограничения диапазона вычислений), оказались тщетными.

Ступени постижения закономерностей

На пути постижения авторами закономерностей формирования натурального ряда чисел и его составной части — ПЧ — оказалось четыре ступени, отображенные на рис. 1.

[3] В математическом мире простые числа называют Prime Numbers (первые числа).

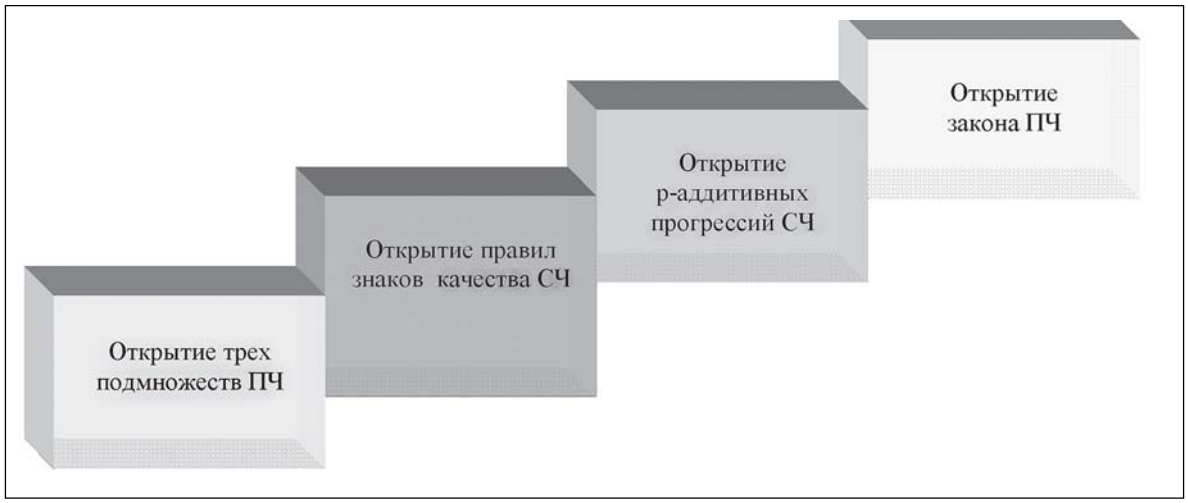

Рис. 1. Ступени постижения закономерностей формирования ПЧ и натурального ряда

Постижению закономерностей формирования натурального ряда и ПЧ **на первой ступени** послужило осмысление способов образования ПЧ. На этой ступени были определены три качественно отличные подмножества ПЧ: ***фундаментальные***[4] ПЧ **{2, 3}**; ***отрицательные*** ПЧ $^{-}P = \{5, 11, 17, \ldots\}$, образующиеся путем вычитания 1 от чисел, кратных 6; ***положительные*** ПЧ $^{+}P = \{7, 13, 19, \ldots\}$, образующиеся путем прибавления 1 к числам, кратным 6.

На второй ступени определение трех качественно отличных подмножеств ПЧ позволило сформулировать правила формирования знаков качества составных чисел (СЧ).

На третьей ступени было определено, что последовательность $6n - 1$ содержит все *отрицательные* ПЧ и СЧ, а $6n + 1$ — все *положительные* ПЧ и СЧ.

Вычитая из этих двух последовательностей соответственно все *отрицательные* СЧ и все *положительные* СЧ, получаем все ПЧ, кроме *фундаментальных*. Так была преодолена **четвертая ступень** познания и открыта закономерность формирования ПЧ.

Пройдем все эти ступени вместе, используя математический аппарат доказательств.

Для начала определим множества всех *отрицательных* ПЧ как ^{-}P, *отрицательных* СЧ как ^{-}C, *положительных* ПЧ как ^{+}P и *положительных* СЧ как ^{+}C.

Доказательство закономерностей формирования ПЧ и натурального ряда

Для начала вспомним знаменитую теорему Евклида [2]: **«Простых чисел существует больше их любого указанного числа».**

Чтобы понять логику наших дальнейших рассуждений, приведем доказательство теоремы Евклида, весьма красивое и элегантное.

Доказательство:

Пусть p_n — максимально известное простое число. Составим произведение всех ПЧ от 2 до 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. ||

[4] Косым шрифтом выделены термины, обозначающие неизвестные ранее свойства и понятия.

Однако возникает вопрос о полноте представления всех ПЧ соотношением $\{\rho_n! + 1\}$. 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:

$$\rho_1 \cdot \rho_2 \cdot \ldots \cdot \rho_n - 1 = {}^{-}M. \qquad (2)$$

Допустим, что существует лишь конечное количество ПЧ с недостающей для делимости 1. Тогда всякое иное число является составным, включая и новое число ^{-}M, и соответственно оно должно делиться без остатка на какое-либо ПЧ, входящее в произведение ПЧ. Но при делении на ρ_1, ρ_2 и т. д. ^{-}M дает всякий раз остаток. С другой стороны, ^{-}M должно делиться на какое—либо ПЧ (на само себя и на единицу, если ^{-}M является ПЧ, или на любой простой делитель, больший ρ_n, если ^{-}M является СЧ). Следовательно, существует ПЧ, отличное от любого из ПЧ 2, 3, 5, ..., ρ_n и потому большее ρ_n. Таким образом, ряд простых чисел и в этом случае оборваться не может.

Сделанное нами допущение, что существует лишь конечное число простых чисел с недостающей для делимости 1 (*отрицательных*), приводит к противоречию, т. е. оно ошибочно, а следовательно, истинным может быть только противоположное ему. Итак, теорема 1 доказана — существует бесконечное множество *отрицательных* ПЧ (с недостающей для делимости 1). || Назовем произведение $\rho_1 \cdot \rho_2 \cdot \ldots \cdot \rho_n$ факториалом ПЧ $\rho_n!$.

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

Следует особо подчеркнуть, что, вычисляя по соотношениям $\rho_n! + 1$ и $\rho_n! - 1$ новые ПЧ, мы пропустим множество других ПЧ, находящихся между факториалами простых чисел $\rho_i!$ и $\rho_{i+1}!$. Это легко показать на примере ПЧ, образованных от факториалов первых ПЧ 2, 3, 5. Очевидно, что прибавление 1 к каждому факториалу ПЧ 1!, 2!, 3!, 5! даст *фундаментальные* ПЧ 2, 3 и *положительные* ПЧ 7, 31. А вычитание 1 от каждого факториала 2!, 3!, 5! дает *отрицательные* ПЧ 5, 29. Таким образом, оказались пропущенными ПЧ 11, 13, 17, 19, 23.

Количество пропущенных *отрицательных* ПЧ и СЧ между соотношениями $\rho_{i+1}! - 1$ и $\rho_i! - 1$ будет минимальным в том случае, когда разность между ними будет минимальной, т. е. $(\rho_{i+1}! - 1) - (\rho_i! - 1) = \rho_i!(\rho_{i+1} - 1) = \min$.

Выполнение этого условия определяется следующей теоремой.

Теорема 2: **«Последовательность $6n - 1$ содержит все *отрицательные* ПЧ и СЧ, а последовательность $6n + 1$, где $n = 1, 2, 3, \ldots$, содержит все *положительные* ПЧ и СЧ».**

Доказательство:

Покажем теперь, что последовательность $\rho_2! \cdot n - 1 = 2 \cdot 3 \cdot n - 1 = 6n - 1$ содержит все *отрицательные* ПЧ и *отрицательные* СЧ.

Величина интервалов между двумя соседними значениями последовательности *отрицательных* ПЧ и СЧ $6n - 1$ и $6(n + 1) - 1$ всегда равна значению 6. Покажем, что на этих интервалах не образуется других (отличных от $6n - 1$) *отрицательных* ПЧ и СЧ. На самом деле, числа $6n - 2$ и $6n - 4$ входят в множество четных чисел, $6n - 3$ — в множество *нечетных* (кратных 3) чисел, а числа $6n - 5 = 6n - (6 - 1) = 6(n - 1) + 1$ входят в множество *положительных* ПЧ и СЧ, не относящихся к рассматриваемому множеству $6n - 1$ *отрицательных* ПЧ и СЧ.

Таким образом, в интервалах между $6n - 1$ и $6(n + 1) - 1$ не существует иных кроме $6n - 1$ *отрицательных* ПЧ и СЧ. Аналогично доказывается и то, что в интервалах между $6n + 1$ и $6(n + 1) + 1$ не существует иных кроме $6n + 1$ *положительных* ПЧ и СЧ.

Отсюда следует, что последовательность $6n - 1$ содержит все *отрицательные* ПЧ и СЧ, а последовательность $6n + 1$ содержит все *положительные* ПЧ и СЧ при $n = 1, 2, 3\ldots$ ||

Объективное существование $^{-}\boldsymbol{\rho}$ и $^{+}\boldsymbol{\rho}$ ставит вопрос о зависимости знака качества «—.» или «+» СЧ от качества и количества ПЧ, образующих СЧ. На этот вопрос отвечает

Теорема 3: **«Произведение нескольких *отрицательных* $^{-}\rho_i$ и *положительных* $^{+}\rho_i$ дает *положительное* СЧ $^{+}c_i$ при четном количестве *отрицательных* $^{-}\rho_i$, и *отрицательное* СЧ $^{-}c_i$ при ином количестве $^{-}\rho_i$».**

Доказательство:

Любые *отрицательные* ПЧ имеют вид $6k - 1$, а *положительные* ПЧ имеют вид $6k + 1$, где $k = 1, 2, 3, \ldots$ — натуральные числа.

a) Произведение двух *отрицательных* ПЧ имеет вид $A = (6k - 1) \cdot (6n - 1) = 36kn - 6k - 6n + 1 = 6(6kn - k - n) + 1 = 6m + 1$, следовательно, $A = (6k - 1) \cdot (6n - 1) = 6m + 1$ — *положительное* СЧ.

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

b) Произведение двух *положительных* ПЧ имеет вид $B = (6k + 1) \cdot (6n + 1) = 36kn + 6k + 6n + 1 = 6(6kn + k + n) + 1 = 6m + 1$, следовательно, B — *положительное* СЧ.

Аналогичным образом легко показать, что произведение любого числа *положительных* ПЧ является *положительным* СЧ.

c) Произведение отрицательного и положительного ПЧ имеет вид $C = (6k - 1) \cdot (6n + 1) = 36kn + 6k - 6n - 1 = 6(6kn + k - n) - 1 = 6m - 1$, где m — натуральное число.

Группируя любое количество *отрицательных* и *положительных* ПЧ и руководствуясь выводами a, b, c теоремы 3, мы придем к заключению: произведение любого сочетания отрицательных и положительных ПЧ в произведении, образующем СЧ, сводится к виду $6m + 1$ при четном количестве $^{-}\rho$ либо к виду $6m - 1$ при нечетном количестве $^{-}\rho$. ||

На основании теоремы 3 сформулируем **«правило знаков СЧ»:**

$$^{-}\rho_i \cdot {}^{-}\rho_j = {}^{+}c_k;\ {}^{-}\rho_i \cdot {}^{+}\rho_j = {}^{-}c_k;\ {}^{+}\rho_i \cdot {}^{+}\rho_j = {}^{+}c_k. \qquad (5)$$

«Произведение нескольких *отрицательных* и *положительных* ПЧ дает *положительное* СЧ при четном количестве *отрицательных* ПЧ и *отрицательное* СЧ при их ином количестве».

Обоснование понятия ρ-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 $\{a_n\}$, определенная 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, а d — разностью арифметической прогрессии.

Известно, что арифметическая прогрессия позволяет путем неограниченного **сложения** выявленную закономерность устремить в бесконечность, а НОД позволяет устанавливать свойства целых чисел относительно деления (**умножения**).

Синтез этих двух понятий позволяет получать **аддитивные** прогрессии. Если, базируясь на Основной теореме арифметики, в качестве НОД принимать только одно ПЧ ρ_i, то можно получать аддитивные относительно ρ_i прогрессии, которые будем называть ***ρ-аддитивные*** прогрессии. При

этом НОД обретает смысл нового математического понятия — ***наименьшего общего делителя или множителя***, который будем обозначать ***НОМ***.

Последовательное присоединение к ρ_i кратного количества этого же ρ_i образует арифметическую прогрессию с *НОМ*, равным этому ПЧ:

$$\{\rho_i, (\rho_i + k \cdot \rho_i), (\rho_i + 2 \cdot k \cdot \rho_i), (\rho_i + 3 \cdot k \cdot \rho_i), \dots\} = \{\rho_i + \rho_i kn\} = \rho_i\{1 + kn\}, \quad (6)$$

где ρ_i — какое-либо ПЧ, k — коэффициент кратности, а n = 0, 1, 2, 3, …

Соотношение (6) отражает сущность простых (первых) чисел быть первыми в образуемых ими *ρ-аддитивных* прогрессиях с *НОМ*, равным ρ_i.

Для $\rho_1 = 2$ имеем $_2\mathbf{C} = \{2, 2 + 2 \cdot 1, 2 + 2 \cdot 2, 2 + 2 \cdot 3, \dots\} = \mathbf{\{2 + 2 \cdot n\}}$. (7)

При n = 0 это *фундаментальное* ПЧ = 2, а при n ≥1, k = 1 это все четные числа {4, 6, …}.

Применяя соотношение (6) к *фундаментальному* ПЧ = 3 и приняв k = 2, имеем:

$$_3\mathbf{C} = \{3, 3 + 3 \cdot 2 \cdot 1, 3 + 3 \cdot 2 \cdot 2, 3 + 3 \cdot 2 \cdot 3, \dots\} = \mathbf{\{3 + 3 \cdot 2n\}}. \quad (8)$$

При n = 0 это ПЧ = 3, а при n≥1 имеем (по аналогии) все *нечетные* числа {9, 15, …}.

Применяя соотношение (6) ко всем остальным ПЧ {5, 7, 11, …}, необходимо учитывать закон правила знаков качества, которому подчиняются образуемые ими СЧ. Каждое из этих СЧ, в зависимости от знаков качества сомножителей, входит либо в 6n — 1, либо в 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 ПЧ, так как в ином случае будут пропущены наименьшие значения СЧ и утверждение «**…все …**» станет некорректным;

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

3) четыре возможных сочетания качественно отличных ПЧ «—»•«—», «—»•«+», «+»•«—» и «+»•«+» должны быть последовательно (по мере увеличения модуля СЧ) размещены в двух качественно отличных («—» или «+») областях существования СЧ 6n — 1 и 6n + 1.

1. Сначала рассмотрим принципы образования прогрессий *отрицательных* СЧ.

1.1. Начнем с наименьшего *отрицательного* ПЧ $^{-}\rho_1$[5] = 5. Два качественно различных подмножества $^{-}\rho$ и $^{+}\rho$ требуют своей независимой индексации. При этом одинаковый индекс будут иметь и *положительные* и *отрицательные* ПЧ.

Первый, наименьший член арифметической прогрессии подмножества *отрицательных* СЧ по сочетанию «—»•«+» образуется произведением наименьшего *отрицательного* ПЧ $^{-}\rho_1 = 5$ и наименьшего *положительного* ПЧ $^{+}\rho_1 = 7$, т. е. $_5{}^{-}c_1 = {}^{-}\rho_1 \cdot {}^{+}\rho_1$. Для того чтобы получить арифметическую прогрессию с *НОМ* = $^{-}\rho_1$ = 5, необходимо к $^{-}\rho_1 \cdot {}_*{}^{+}\rho_1$ прибавлять кратные k количества $^{-}\rho_1$, т. е. $_5{}^{-}C = \{{}^{-}\rho_1 \cdot {}^{+}\rho_1 + {}^{-}\rho_1 \cdot k \cdot {}_*m\} = \{{}^{-}\rho_1 \cdot ({}^{+}\rho_1 + k \cdot m)\}$; m = 0, 1, 2, …

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 четных 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 *нечетных* чисел (кратных 3).

Не может k принимать и значения {4, 10, 16, …}, так как в этом случае {7 + 4, 7 + 10, 7 + 16, …}= —1mod, элементы прогрессии $_5{}^{-}C$ по закону качества знаков $^{-}\rho_1 \cdot$ —1mod будут принадлежать множеству *положительных* ПЧ и СЧ.

Остаются только значения k, равные числам, кратным 6, т. е. k = 6m (m = 1, 2, 3, …), которые обеспечивают прогрессии $^{-}\rho_1\{7 + k \cdot n\} = {}^{-}\rho_1\{7 + 6mn\} = {}^{-}\rho_1[6\{1 + mn\} + 1] = {}^{-}\rho\{6q + 1\}$ по закону качества знаков «—»•«+» = «—» принадлежность к множеству *отрицательных* СЧ 6n — 1, так как {6q + 1} — *положительные* по определению числа.

[5] Обратим внимание читателя, что далее индексация простых чисел осуществляется следующим образом: *отрицательные* ПЧ начинаются с $^{-}\rho_1 = 5$, далее $^{-}\rho_2 = 11$ и т. д.; *положительные* — с $^{+}\rho_1 = 7$, далее $^{+}\rho_2 = 13$ и т. д.

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

$${}_{\rho 1}{}^{-}C = \{{}^{-}\rho_1 \cdot {}^{+}\rho_1 + {}^{-}\rho_1 \cdot 6 \cdot n\};\ n = 0, 1, 2, \ldots \quad (9)$$

1.2. Следующим по модулю является первое *положительное* ПЧ ${}^{+}\rho_1 = 7$.

Первый, наименьший член арифметической прогрессии подмножества *отрицательных* СЧ по сочетанию «+»•«—» образуется произведением наименьшего *положительного* ПЧ ${}^{+}\rho_1 = 7$ и следующего *отрицательного* ПЧ ${}^{-}\rho_2 = 11$, т. е. ${}_7{}^{-}c_1 = {}^{+}\rho_1 \cdot {}^{-}\rho_2$. Для того чтобы получить арифметическую прогрессию с *НОМ* ${}^{+}\rho_1 = 7$, необходимо к ${}^{+}\rho_1 \cdot {}^{-}\rho_2$ прибавлять кратные k количества ${}^{+}\rho_1$, т. е. ${}^{-}C = {}^{+}\rho_1 \cdot {}^{-}\rho_2 + {}^{+}\rho_1 \cdot k \cdot n = {}^{+}\rho_1\{11 + k \cdot n\};\ n = 0, 1, 2, 3, \ldots$

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

Также k не может принимать значения {2, 8, 14, …}, так как в этом случае {11 + 2, 11 + 8, …} = {(2 • 6 + 1), (3 • 6 + 1), …} положительные числа и по закону качества знаков (+ • + = +) элементы прогрессии ${}_7{}^{-}C$ будут принадлежать множеству *положительных* ПЧ и СЧ.

Также k не может принимать значения {4, 10, 16, …}, так как в этом случае {11 + 4, 11 + 10, …}, элементы прогрессии ${}_7{}^{-}C$ будут принадлежать множеству *нечетных* чисел (кратных 3).

Только значения k, равные числам кратным 6, т. е. k = 6m (m = 1, 2, 3, …), обеспечивают прогрессии ${}^{-}\rho_1(11 + k \cdot n)$ по закону качества знаков (+ • — = —) принадлежность к множеству *отрицательных* СЧ, так как 11 + kn = (2 • 6 — 1) + 6mn = 6(2 + mn) — 1 = 6q — 1 — *отрицательное* по определению число. Таким образом, для ${}_7{}^{-}C$ окончательно получаем:

$${}_{+\rho 1}{}^{-}C = \{{}^{+}\rho_1 \cdot {}^{-}\rho_2 + {}^{+}\rho_1 \cdot 6 \cdot n\};\ n = 0, 1, 2, \ldots \quad (10)$$

По методу математической индукции получаем:

$${}_{-\rho 2}{}^{-}C = \{{}^{-}\rho_2 \cdot {}^{+}\rho_2 + {}^{-}\rho_2 \cdot 6 \cdot n\}, \quad (11)$$

$${}_{+\rho 2}{}^{-}C = \{{}^{+}\rho_2 \cdot {}^{-}\rho_3 + {}^{+}\rho_2 \cdot 6 \cdot n\}, \quad (12)$$

$${}_{-\rho i}{}^{-}C = \{{}^{-}\rho_i \cdot {}^{+}\rho_i + {}^{-}\rho_i \cdot 6 \cdot n\}, \quad (13)$$

$${}_{+\rho i}{}^{-}C = \{{}^{+}\rho_i \cdot {}^{-}\rho_{i+1} + {}^{+}\rho_i \cdot 6 \cdot n\}. \quad (14)$$

2. Теперь рассмотрим принципы образования прогрессий *положительных* СЧ.

2.1. Начнем с наименьшего *отрицательного* ПЧ ${}^{-}\rho_1 = 5$. Первый член арифметической прогрессии подмножества *положительных* СЧ по сочетанию «—»•«—» образуется произведением наименьших *отрицательных* ПЧ ${}^{-}\rho_1 = 5$, т. е. ${}_5{}^{+}c_1 = {}^{-}\rho_1 \cdot {}^{-}\rho_1$. Для того чтобы получить арифметическую прогрессию *положительных СЧ* с НОД ${}^{-}\rho_1 = 5$, необходимо к ${}^{-}\rho_1 \cdot {}^{-}\rho_1$ прибавлять кратные k количества ${}^{-}\rho_1$, т. е. ${}_5{}^{+}C = \{{}^{-}\rho_1 \cdot {}^{-}\rho_1 + {}^{-}\rho_1 \cdot k \cdot n\} = {}^{-}\rho_1\{5 + k \cdot n\};\ n = 0, 1, 2, \ldots$

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 *четных* чисел.

Не может k принимать и значения {2, 8, 14, …}, так как в этом случае {5 + 2, 5 + 8, 5 + 14, …} = {6 + 1, 2 • 6 + 1, …} — *положительные* числа, и поэтому элементы прогрессии ${}_5{}^{+}C$ будут по закону качества знаков (— • + = —) 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 *нечетных* чисел (кратных 3).

Как и в предыдущих случаях, значения k могут быть кратны только 6, т. е. k = 6m; m = 0, 1, 2, … Это обеспечивает прогрессии ${}^{-}\rho_1\{5 + k \cdot n\}$ по закону качества знаков (— • — = +) принадлежность к множеству *положительных* СЧ, так как {5 + 6m • n} = {6(1 + m • n) — 1} = {6q — 1} — *отрицательные* по определению числа, где q = 1 + m • n — натуральное число. Таким образом, для ${}_5{}^{+}C$ окончательно получаем:

$${}_{-\rho 1}{}^{+}C = \{{}^{-}\rho_1 \cdot {}^{-}\rho_1 + {}^{-}\rho_1 \cdot 6 \cdot n\}. \quad (15)$$

2.2. Следующим по модулю ПЧ является ${}^{+}\rho_1 = 7$. Первый член арифметической прогрессии подмножества *положительных* СЧ по сочетанию «+»•«+» образуется произведением наименьших

положительных ПЧ $^{+}\rho_1 = 7$, т. е. $_7{}^{+}c_1 = {}^{+}\rho_1 \cdot {}^{+}\rho_1$. Для того чтобы получить арифметическую прогрессию *положительных* СЧ с $HOM\ {}^{+}\rho_1 = 7$, необходимо к ${}^{+}\rho_1 \cdot {}^{+}\rho_1$ прибавлять кратные k количества ${}^{+}\rho_1$, т. е. $_{+\rho 1}{}^{+}C = \{{}^{+}\rho_1 \cdot {}^{+}\rho_1 + {}^{-}\rho_1 \cdot k \cdot n\} = {}^{+}\rho_1\{11 + k \cdot n\}$; $n = 0, 1, 2, 3, \ldots$

Как и во всех предыдущих случаях условию образования ${}^{+}C$ при $HOM = {}^{+}\rho_1 k$ должно быть равно 6: $_{+\rho 1}{}^{+}C = \{{}^{+}\rho_1 \cdot {}^{+}\rho_1 + {}^{-}\rho_1 \cdot 6 \cdot n\}$. (16)

По методу математической индукции получаем:

$_{-\rho 2}{}^{+}C = \{{}^{-}\rho_2 \cdot {}^{-}\rho_2 + {}^{-}\rho_2 \cdot 6 \cdot n\}$, (17)

$_{+\rho 2}{}^{+}C = \{{}^{+}\rho_2 \cdot {}^{+}\rho_2 + {}^{+}\rho_2 \cdot 6 \cdot n\}$, (18)

$_{-\rho i}{}^{+}C = \{{}^{-}\rho_i \cdot {}^{-}\rho_i + {}^{-}\rho_i \cdot 6 \cdot n\}$, (19)

$_{+\rho 1}{}^{+}C = \{{}^{+}\rho_i \cdot {}^{+}\rho_1 + {}^{+}\rho_i \cdot 6 \cdot n\}$. (20)

Из полученных соотношений (9)—(14) формулируем:

Следствие 1 — об образовании *отрицательных* составных чисел:

Каждое простое (первое) число ρ_i образует *ρ-аддитивные* прогрессии *отрицательных* СЧ $_{\rho i}{}^{-}C$ с $HOM = \rho_i$ при к = 6 по формуле:

$$^{-}C = \Sigma_{\rho_i}{}^{-}C = \{{}^{-}\rho_1 \cdot {}^{+}\rho_1 + {}^{-}\rho_1 \cdot 6m\} \cup \{{}^{+}\rho_1 \cdot {}^{-}\rho_2 + {}^{+}\rho_1 \cdot 6m\} \cup \{{}^{-}\rho_2 \cdot {}^{+}\rho_2 + {}^{-}\rho_2 \cdot 6m\} \cup \ldots$$
$$\ldots \cup \{{}^{-}\rho_i \cdot {}^{+}\rho_i + {}^{-}\rho_i \cdot 6m\} \cup \{{}^{+}\rho_i \cdot {}^{-}\rho_{i+1} + {}^{+}\rho_i \cdot 6m\} \cup \{{}^{-}\rho_{i+1} \cdot {}^{+}\rho_{i+1} + {}^{-}\rho_{i+1} \cdot 6m\} \cup \ldots \quad (21)$$

где i — индексы ПЧ = {1, 2, 3…}, т. е. ${}^{-}\rho_1 = 5$, ${}^{+}\rho_1 = 7$, ${}^{-}\rho_2 = 11$, ${}^{+}\rho_2 = 13$, …, а m = {0, 1, 2, 3…}; U — символ объединения множеств.

Пример: ${}^{-}C = \{5 \cdot 7 + 5 \cdot 6m\} \cup \{7 \cdot 11 + 7 \cdot 6m\} \cup \{11 \cdot 13 + 11 \cdot 6m\} \cup \{13 \cdot 17 + 13 \cdot 6m\} \cup \ldots =$

$\{35, 65, 95, \ldots\} \cup \{77, 119, 161, \ldots\} \cup \{143, 209, 275, \ldots\} \cup \{221, 299, 377, \ldots\} \cup \ldots$

Из полученных соотношений (15)—(20) формулируем:

Следствие 2 — об образовании *положительных* составных чисел:

Каждое простое (первое) число ρ_i образует *ρ-аддитивные* прогрессии *положительных* СЧ $_{\rho i}{}^{+}C$, с $HOM = \rho_i$ при к = 6 по формуле:

$$^{+}C = \Sigma_{\rho_i}{}^{+}C = \{{}^{-}\rho_1{}^2 + {}^{-}\rho_1 \cdot 6m\} \cup \{{}^{+}\rho_1{}^2 + {}^{+}\rho_1 \cdot 6m\} \cup \{{}^{-}\rho_2{}^2 + {}^{-}\rho_2 \cdot 6m\} \cup \ldots$$
$$\ldots \cup \{{}^{-}\rho_i{}^2 + {}^{-}\rho_i \cdot 6m\} \cup \{{}^{+}\rho_i{}^2 + {}^{+}\rho_i \cdot 6m\} \cup \{{}^{-}\rho_{i+1}{}^2 + {}^{-}\rho_{i+1} \cdot 6m\} \cup \{{}^{+}\rho_{i+1}{}^2 + {}^{+}\rho_{i+1} \cdot 6m\} \cup \ldots \quad (22)$$

где i — индексы ПЧ = {1, 2, 3…}, т. е. ${}^{-}\rho_1 = 5$, ${}^{+}\rho_1 = 7$, ${}^{-}\rho_2 = 11$, ${}^{+}\rho_2 = 13\ldots$, а m = {0, 1, 2, 3, …}.

Пример: ${}^{+}C = \{5 \cdot 5 + 5 \cdot 6m\} \cup \{7 \cdot 7 + 7 \cdot 6m\} \cup \{11 \cdot 11 + 11 \cdot 6m\} \cup \{13 \cdot 13 + 13 \cdot 6m\} \cup \ldots =$

$\{25, 55, 85, \ldots\} \cup \{49, 91, 133, \ldots\} \cup \{121, 187, 253, \ldots\} \cup \{169, 247, 325, \ldots\} \cup \ldots$

На основании (7), (8), (21) и (22) формулируется

«Закон формирования составных чисел», по которому образуются все числа натурального ряда (кроме ${}^{-}\rho$ и ${}^{+}\rho$):

«**Множество всех простых (первых) чисел образуют *ρ-аддитивные* прогрессии по формуле**

$$_{\rho i}C = \rho_i \cdot к_i + \rho_i \cdot к_j \cdot n, \quad (6)$$

где $n = 0, 1, 2, 3, \ldots$; $к_i$ и $к_j$ — константы, принимающие следующие значения:

1) **у фундаментальных ПЧ $_1\rho = 1 + 1n$ при $\rho_0 = 1$, $k_i = 1$; $k_j = 1$ и $n \le 2$;**

2) **у четных (двухкратных) чисел $_2C = 2 + 2n$ при $\rho_1 = 2$, $k_i = 1$ и $k_j = 1$;**

3) **у *нечетных* (трехкратных) чисел $_3C = 3 + 3_*2n$ при $\rho_2 = 3$, $k_i = 1$ и $k_j = 2$;**

4) **у *отрицательных* СЧ $\Sigma_{\rho i}{}^{-}C$ при $к_i = {}^{+}\rho_i$ (при $HOM = {}^{-}\rho_i$) или $к_i = {}^{-}\rho_{i+1}$ (при $HOM = {}^{+}\rho_i$) и $k_j = 6$;**

5) **у *положительных* СЧ $\Sigma_{\rho i}{}^{-}C$ при $к_i = {}^{+}\rho_i$ (при $HOM = {}^{+}\rho_i$) или $к_i = {}^{-}\rho_i$ (при $HOM = {}^{-}\rho_i$) и $k_j = 6$.**

Учитывая «Закон формирования простых чисел» и выводы теоремы 2, сформулируем:

Закон простых (первых) чисел: «**Множество всех первых (простых) чисел состоит из подмножества *фундаментальных* ПЧ $_1$Р, подмножества *отрицательных* ПЧ $^-$Р, равного разности между множеством 6n – 1 и суммой всех *ρ-аддитивных* прогрессий *отрицательных* СЧ $\Sigma_{\rho_i}{}^-$С, и подмножества всех *положительных* ПЧ $^+$Р, равного разности между множеством 6n + 1 и суммой всех *ρ-аддитивных* прогрессий *положительных* СЧ $\Sigma_{\rho_i}{}^+$С».**

$$\mathbf{P = {}_1PU[\{6n-1\}\backslash[[\{^-\rho_1\cdot{}^+\rho_1+{}^-\rho_1\cdot 6m\}\ U\ \{^+\rho_1\cdot{}^-\rho_2+{}^+\rho_1\cdot 6m\}\ U\ \dots\ U\ \{^-\rho_i\cdot{}^+\rho_i+{}^-\rho_i\cdot 6m\}\ U\ \{^+\rho_i\cdot{}^-\rho_{i+1}+{}^+\rho_i\cdot 6m\}\ U\ \dots]U\ [\{6n+1\}\backslash\{^-\rho_1{}^2+{}^-\rho_1\cdot 6m\}U\{^+\rho_1{}^2+{}^+\rho_1\cdot 6m\}\ U\ \dots\ U\ \{^-\rho_i{}^2+{}^-\rho_i\cdot 6m\}\ U\ \{^+\rho_i{}^2+{}^+\rho_i\cdot 6m\}\ U\ \{^-\rho_{i+1}{}^2+{}^-\rho_{i+1}\cdot 6m\}\ U\ \dots],} \quad (23)$$

где U — знак объединения множеств, а \ — знак вычитания множеств.

Соотношение (23) состоит только из арифметических прогрессий, что позволяет только операциями сложения получать все ПЧ и СЧ в заданном диапазоне вычислений и, таким образом, создать линейный генератор ПЧ подряд. И он был создан одним из авторов настоящей статьи [8].

Учитывая совокупность вышеизложенного, можно сформулировать:

Закон формирования структуры натурального ряда:

$$\mathbf{N = 1\ U\ {}_1P\ U\ {}^-P\ U\ {}^+P\ U\ {}_2C \supset {}_6C\ U\ {}_3C\ U\ \Sigma_{\rho_i}{}^-C\ U\ \Sigma_{\rho_i}{}^+C,} \quad (24)$$

где ⊃ — знак включения множества.

Натуральный ряд N состоит из 1; двух *фундаментальных* ПЧ $_1$Р = 2 и 3; *отрицательных* ПЧ $^-$Р и *положительных* ПЧ $^+$Р; четных СЧ $_2$С, куда входят *циклические* числа $_6$С; *нечетных* СЧ $_3$С и бесконечных множеств *ρ-аддитивных* прогрессий *отрицательных* $\Sigma_{\rho_i}{}^-$С и *положительных* $\Sigma_{\rho_i}{}^+$С СЧ».

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

Для большей наглядности выделим ПЧ прямым, СЧ — косым шрифтом, а также оттенками серого:

Теперь приведем новую однозначную классификацию натурального ряда с числовыми примерами (Рис. 2), которая со всей очевидностью демонстрирует философский закон взаимовлияния количественных и качественных изменений. Последовательное присоединение 1 к любому числу каждый раз приводит к изменению его качества! Пришло время вернуться к единству качественно—количественного математического отображения проявлений природы. Пора понять, что количество атомов в объекте определяет его форму (качество) так же, как количество 1 в числе определяет его качество.

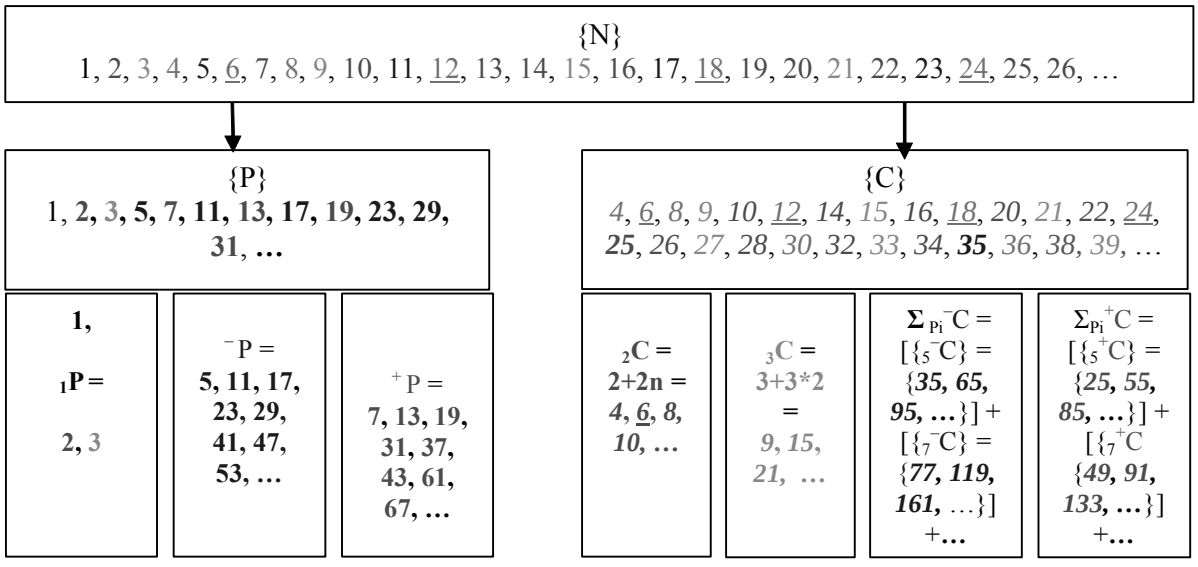

Рис. 2. Однозначная классификация натурального ряда

Закономерности натурального ряда позволили иллюстративно представить весь натуральный числовой ряд в виде изображенного на рис. 3 «Древа чисел».

Здесь *четные* и *нечетные* числа образуют «почву», *циклические* (кратные 6) являются «корнями дерева», которые, соединившись с 1 или –1, образуют «ствол» — все ПЧ. А от каждого ПЧ отходят по две «ветки» *ρ-аддитивных прогрессий* СЧ с «листиками» — *положительных СЧ* и *отрицательных СЧ*.

Используя иллюстрацию на рис. 3, раскроем суть математического открытия.

Начинается древо с 1, несущей в себе «геном» всей числовой системы природы. Присоединение к 1 другой 1 дает первое *фундаментальное* ПЧ = 2, являющееся основанием прогрессии *четных* чисел $C_2 = 2 + 2n$, (n = 1, 2, 3, …), образующей самое мощное (50 %) подмножество натуральных чисел. Они расположены под линией, соединяющей 1 и 2.

Присоединение к 2 еще одной 1 дает второе фундаментальное ПЧ = 3, являющееся основанием прогрессии *нечетных* чисел $C_3 = 3 + 3 \cdot 2n$, n = 1, 2, 3, … Оно образует подмножество натуральных чисел, по мощности равное 16,666…%, и на рисунке 3 занимают сектор между линией, соединяющей 1 с 3, и линией, за которой начинается область *циклических* (кратных 6) чисел $C_6 = 6 + 6n$, (n = 0, 1, 2, 3, …).

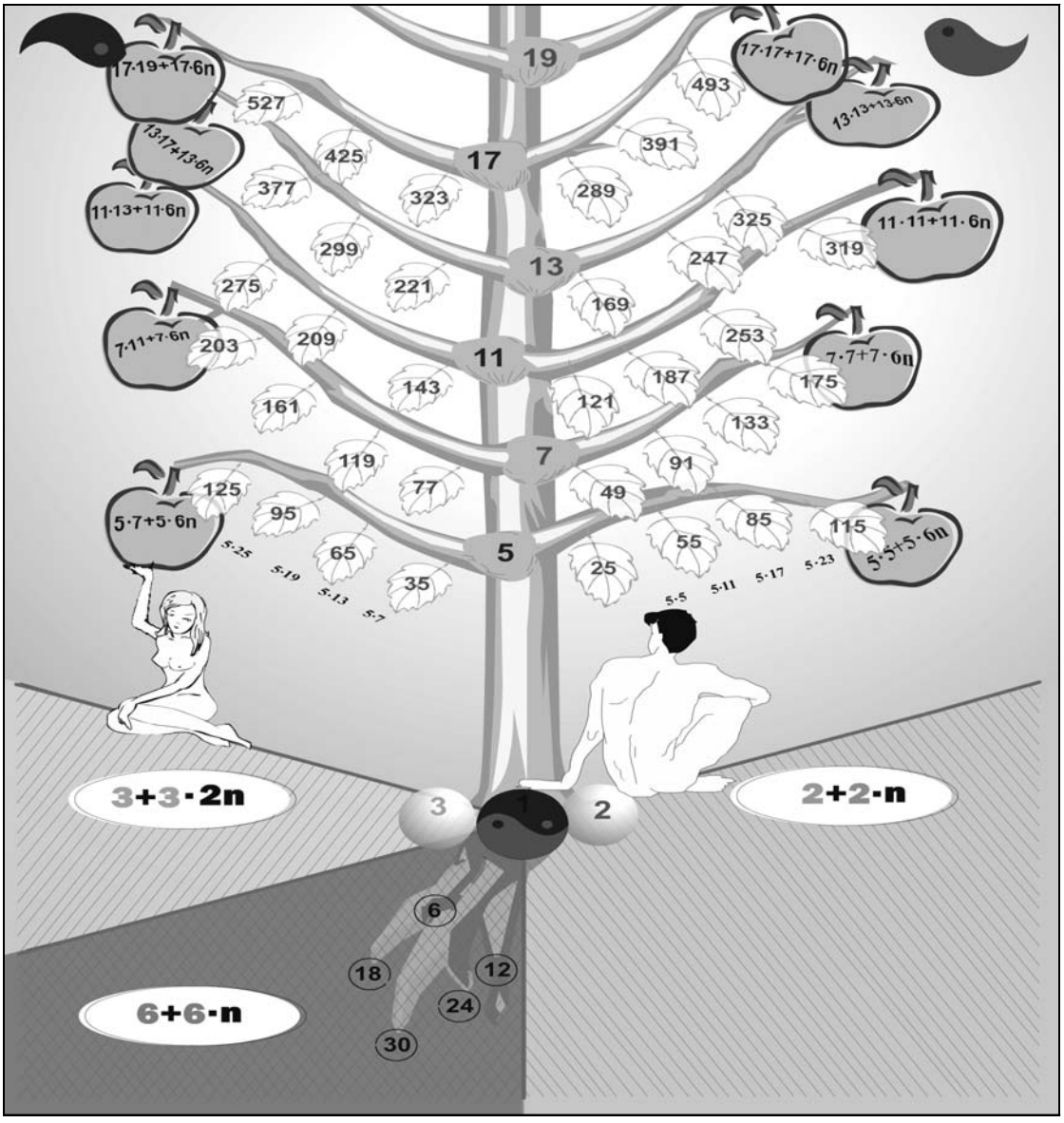

Рис. 3. «Древо чисел»

Циклические числа образуют «корневую систему» древа, благодаря которой может расти «ствол» древа из ПЧ.

Так, первое циклическое число 6, как бы «прорастая» через 1, образует первое *отрицательное* ПЧ = 5 путем вычитания 1 из 6 и первое *положительное* ПЧ = 7 путем присоединения 1 к 6.

От каждого образованного таким образом ПЧ отходят по две «ветки» *ρ-аддитивных* прогрессий *отрицательных* и *положительных* СЧ.

Так, от 5 по формуле (9) образуется ветка «листиков» *отрицательных* СЧ с $НОМ = \mathbf{5}_{5}{}^{-}C = \mathbf{5} \cdot 7 + \mathbf{5} \cdot 6m = \{35(\mathbf{5} \cdot 7), 65(\mathbf{5} \cdot 13), 95(\mathbf{5} \cdot 19), 125(\mathbf{5} \cdot 25), \ldots\}$ и по формуле (15) образуется ветка «листиков» *положительных* СЧ с $НОД = 5\ \{{}_{5}{}^{+}C\} = \mathbf{5} \cdot 5 + \mathbf{5} \cdot 6m = \{25(\mathbf{5} \cdot 5), 55(\mathbf{5} \cdot 11), \ldots\}$.

Аналогично от **7** по формуле (16) ${}_{7}{}^{+}C = \mathbf{7} \cdot 7 + 7 \cdot 6m = \{49(\mathbf{7} \cdot 7), 91(\mathbf{7} \cdot 13), 133(\mathbf{7} \cdot 19), 175(\mathbf{7} \cdot 25), \ldots\}$ образуется ветка «листиков» *положительных* СЧ с $НОМ = 7$ и по формуле (10) ${}_{7}{}^{-}C = \mathbf{7} \cdot 11 + 7 \cdot 6m = \{77(\mathbf{7} \cdot 11), 119(\mathbf{7} \cdot 17), 161(\mathbf{7} \cdot 23), 203(\mathbf{7} \cdot 29)\ldots\}$ образуется ветка «листиков» *отрицательных* СЧ с $НОМ = 7$; при $m = 0, 1, 2, 3\ldots$

Точно так же до бесконечности от других «стволовых» ПЧ соответственно образуются по две «ветки» *ρ-аддитивных* прогрессий СЧ — *отрицательных* и *положительных*.

На примере «падения» на «почву» одного «листика» — минимального СЧ = 25 — можно проиллюстрировать кругооборот вещества в природе и закон «Отрицания отрицания». «Падая» на «почву» из *четных* и *нечетных* чисел и проникая к корням, оно образует кратное 6 циклическое число 150 = (25 · 6), которое, «прорастая» через 1, дает жизнь новым «стволовым» ПЧ *отрицательному* 149 и *положительному* 151. Для определения ПЧ по индексам необходимо воспользоваться следующей таблицей (фрагмент):

										0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
ρ_i		**1**	**7**	**3**	**9**	**1**	**7**	**3**	**9**	**1**	**3**	**9**	**01**	**07**	**13**	**31**	**37**	**49**	**67**
ρ_i		3	9	1	7	3	1	7	3	9	7	03	09	27	39	51	57	63	81

По открытым законам натурального ряда от каждого вновь образованного ${}^{-}\rho_{18} = 149$ и ${}^{+}\rho_{18} = 163$ отходят по две «ветки» *ρ-аддитивных* прогрессий:

с $НОМ = 149$ по формуле (13) ${}_{149}{}^{-}C = \mathbf{149} \cdot 163 + \mathbf{149} \cdot 6m = \{24287(149 \cdot 163), 25181(149 \cdot 169), 26075(149 \cdot 175\}$ образуется ветка «листиков» *отрицательных* СЧ и по формуле (19) ${}_{149}{}^{+}C = \mathbf{149} \cdot 149 + \mathbf{149} \cdot 6m = \{22201(149 \cdot 149), 23095(149 \cdot 155), 23989(149 \cdot 161), \ldots\}$ образуется ветка «листиков» *положительных* СЧ;

с $НОМ = 151$ по формуле (14) $\{{}_{151}{}^{-}C\} = \mathbf{151} \cdot 137 + \mathbf{151} \cdot 6m = \{20687(151 \cdot 137), 21593(151 \cdot 143), 22499(151 \cdot 149), \ldots\}$ прогрессия отрицательных СЧ составных чисел — «листиков» при ${}^{+}\rho_{16} = 151$ и ${}^{-}\rho_{17} = 137$; по формуле (20) $\{{}_{151}{}^{+}C\} = \mathbf{151} \cdot 151 + 6m = \{22801(151 \cdot 151), 23707(151 \cdot 157), 24613(151 \cdot 163), \ldots\}$ прогрессия последовательность положительных СЧ составных чисел — «листиков»; $m = 0, 1, 2, 3\ldots$

Мировоззренческие вопросы открытых закономерностей

С открытием закономерностей формирования натурального ряда и ряда ПЧ числовая система Природы обрела кристальную ясность и может положить начало универсальному языку познания — математике Природы — Натуральной математике, основанной на парадигме дискретно-непрерывного пространства и закономерностях натурального ряда.

Чтобы говорить с Природой на одном языке, потребуется изучить и развить изложенную в данной работе «азбуку» этого языка. Настоящая работа — только первый шаг к серьезному переосмыслению

окружающего нас мира и присущих ему математических и физических закономерностей, а также основам преподавания математики.

А теперь самое интересное, почему даже Всемогущий Бог не мог сотворить мир за 1–5 дней, лет, столетий?.. Даже Ему, чтобы сотворить мир, потребовалось на завершение **цикла** творения не менее 6 дней, а весь седьмой день Он этот мир «одухотворял», т. е. наполнял духом — светом — материей.

Почему в книге «Дзиан», написанной на тысячелетия раньше священных книг всех религий, записано магическое слово «Оеаоhоо», имеющее три перевода: «Отец-Матерь (единородное начало) всех богов (законов природы)», «Вечная первопричина» и «Семеричный корень», или один в шести? (Буквальное значение этого слова — «спиральный ветер». Этот термин используется для определения беспрестанного и вечного космического движения.)

Потому, что **1 атом — это эталон пространства**, числом которых можно определить длину, площадь и объем, а **6 положений**, которые должен пройти наименьший циклический процесс, — **эталон времени.** Двух эталонов — времени и пространства — Материи достаточно, чтобы в процессах самоорганизации и самодеструкции вечно циклически «творить» все многообразие природы! Число 7 потому «вечная первопричина» и «отец-матерь всех богов», что реализует совокупность двух эталонов — пространства и времени.

В этом суждении можно было бы сомневаться до открытия закона ПЧ, по которому все простые и составные числа образуются из двух констант 1 и 6.

Некоторые аспекты научного и практического применения открытых закономерностей изложены в публикациях [3–6].

Кроме общенаучного значения, открытый Закон формирования 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.

Открытые математические закономерности позволяют создать СЗИ нового поколения на одноразовых ключах и одноразовых непериодических гаммах псевдослучайных чисел на конечных автоматах, что до настоящего времени считалось невозможным [7]. Такие СЗИ будут обладать теоретически максимальной надежностью и быстродействием режима on line.

Началась реализация открытых законов в практическом плане — В. П. Хреновым получено свидетельство № 2005613012 от 22 сентября 2005 г. о регистрации программы «Линейный генератор простых чисел подряд» [8], которое получило высокую оценку коммерческой значимости. Члены Государственной комиссии в своем заключении от 26 апреля 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].

Последнее публичное изложение открытых закономерностей проходило 25 апреля 2008 г. в Российском новом университете на Международной научной конференции «Цивилизация знаний: инновационный переход к обществу высоких технологий».

СПИСОК ЛИТЕРАТУРЫ:

1. *Diffie W., Hellman M.* New Directions in Cryptography. IEEE Transactions on Information Theory. V. IT-22. N. 6. Nov. 1977. P. 74–84.
2. *Евклид*. Начала. М.; Л., 1949–1951.

3. *Хренов В. П.* Новая парадигма мировосприятия // Журнал Российской Народной Академии Наук «Академические записки». 2005. № 4, 5.
4. *Хренов В. П.* Проблемы и перспектива создания систем защиты информации нового поколения // Глобальная безопасность. 2005. № 3.
5. *Хренов В. П.* Новый этап развития систем защиты информации // Наука и технологии в промышленности. 2005. № 3.
6. *Хренов В. П.* Prime Numbers Technology (PNT)™ — основа создания систем защиты информации (СЗИ) нового поколения и перспективы ее применения в различных сегментах информационных технологий // Бизнес и Безопасность в России. Январь 2007. № 6.
7. *Schneier B.* Applied Cryptography. John Wiley & Sons, Inc. 1996.
8. Свидетельство № 2005613012 от 22 сентября 2005 г. о регистрации программы «Линейный генератор простых чисел подряд».
9. *Хренов В. П.* «Способ защиты информации», решение о выдаче патента по заявке № 200128954/09(032494) от 19 сентября 2005 г.
10. *Хренов В. П.* Способ защиты информации», решение о выдаче патента по заявке № 200128777/09(032303) от 16 сентября 2005 г.