ЧЕБЫШЕВСКИЙ СБОРНИК
Том 23. Выпуск 3.

УДК 511.1, 519.1 DOI 10.22405/2226-8383-2022-23-3-77-101

Рекуррентные числовые последовательности: теория и приложения

Е. И. Деза, Л. В. Котова

Деза Елена Ивановна — доктор педагогических наук, кандидат физико-математических наук, доцент, Московский педагогический государственный университет (г. Москва).
e-mail: Elena.Deza@gmail.com
Котова Лидия Владимировна — кандидат педагогических наук, Московский педагогический государственный университет (г. Москва).
e-mail: lv.kotova@mpgu.su

Аннотация

Теория рекуррентных соотношений являются важной составной частью современной математической науки. Множество числовых последовательностей имеют рекуррентную природу. Часто они естественным образом связаны с теорией чисел (числа Фибоначчи, фигурные числа, числа Мерсенна и Ферма, дружественные числа и др.) или имеют комбинаторные "корни" (элементы треугольника Паскаля, числа Стирлинга, числа Белла, числа Каталана и др.). Применяемые для исследования рекуррентных последовательностей производящие функции подробно изучаются в математическом анализе, предоставляя широкий спектр практико-ориентированных примеров использования классических аналитических построений. Рекурсивные функции играют важную роль в теории алгоритмов.

Приложения теории рекуррентных соотношений крайне востребованы в криптографии (генерация псевдослучайных последовательностей над конечными полями), цифровой обработке сигналов (моделирование обратной связи в системе, где выходные данные одновременно становятся входными для будущего времени), экономике (модели различных секторов экономики – финансового, товарного и др., в которых текущие значения ключевых переменных (процентная ставка, реальный ВВП и т.д.) анализируются с точки зрения прошлых и текущих значений других переменных), биологии (например, модели динамики роста той или иной популяции; вспомним числа Фибоначчи) и др.

Мы рассматриваем несколько аспектов указанной тематики, в том числе:

- историю вопроса, место числовых рекуррентных последовательностей в развитии математической науки и математического образования;

- примеры использования рекуррентного подхода при построении различных классов (и подклассов) специальных чисел (фигурных чисел, дружественных чисел и др.);

- теоретические аспекты использования последовательностей больших периодов над конечными полями в радиолокации и методы генерации псевдослучайных последовательностей для обеспечения криптографической защиты информации, передаваемой на большие расстояния.

В частности, в работе представлена рекуррентная схема построения так называемых центрированных k-пирамидальных чисел $CS_k^3(n)$, $n = 1, 2, 3, \ldots$, которые представляют собой конфигурации точек, образующих k-угольную пирамиду, в основании которой лежит центрированное k-угольное число $CS_k(n)$.

Исходя из определения, мы получаем для последовательности $CS_k^3(n)$, $n = 1, 2, 3, \ldots$, рекуррентную формулу $CS_k^3(n+1) = CS_k^3(n) + CS_k(n+1)$, $CS_k^3(1) = 1$. Учитывая, что $CS_k(n+1) = \frac{kn^2+kn+2}{2}$, и пользуясь стандартными подходами, мы доказываем, что производящая функция $f(x)$ последовательности $CS_k^3(n)$, $n = 1, 2, 3, \ldots$, имеет вид

$f(x) = \frac{x(1+(k-2)x+x^2)}{(1-x)^2}$, $|x| < 1$, в то время как явная формула для $CS_k^3(n)$ имеет вид $CS_k^3(n) = \frac{kn^3+n(6-k)}{6}$.

Ключевые слова: Рекуррентное соотношение, рекуррентная числовая последовательность, производящая функция последовательности, треугольник Паскаля, фигурные числа, дружественные числа, рекуррентные последовательности над конечным полем.

Библиография: 11 названий.

Для цитирования:
Е. И. Деза, Л. В. Котова. Рекуррентные числовые последовательности: теория и приложения // Чебышевский сборник, 2022, т. 23, вып. 3, с. 77 – 101.

CHEBYSHEVSKII SBORNIK
Vol. 23. No. 3.

UDC 511.1, 519.1 DOI 10.22405/2226-8383-2022-23-3-77-101

Recurrent numerical sequences: theory and applications

E. I. Deza, L. V. Kotova

Deza Elena Ivanovna — doctor of pedagogical sciences, candidate of physical and mathematical sciences, associate professor, Moscow State Pedagogical University (Moscow).
e-mail: Elena.Deza@gmail.com
Kotova Lidiya Vladomirovna — candidate of pedagogical sciences, Moscow State Pedagogical University (Moscow).
e-mail: lv.kotova@mpgu.su

Abstract

The theory of recurrence relations is an important component of modern mathematical science. Many numerical sequences have a recurrent nature. Often they are naturally related to Number Theory (Fibonacci numbers, figurate numbers, Mersenne and Fermat numbers, amicable numbers, etc.) or have combinatorial "roots"(elements of the Pascal triangle, Stirling numbers, Bell numbers, Catalan numbers, etc.). The generating functions used for the study of recurrent sequences are considered in detail in Mathematical Analysis, providing a wide range of practical-oriented examples of the use of classical analytical constructions. Recursive functions play an important role in the Theory of Algorithms.

Applications of the theory of recurrence relations are extremely in demand in Cryptography (generation of pseudo-random sequences over finite fields), digital signal processing (feedback modeling in a system where the output simultaneously becomes input for future time), Economy (models of various sectors of the economy - financial, commodity, etc., in which the current values of key variables (interest rate, real GDP, etc.) are analyzed in terms of past and current values of other variables), Biology (for example, models of growth dynamics of a particular population; recall Fibonacci numbers), etc.

We consider several aspects of this topic, including:

- history of the issue, place of recurrent numerical sequences in the development of mathematical science and mathematical education;

- examples of using a recurrent approach when constructing various classes (and subclasses) of special numbers (figurate numbers, amicable numbers, etc.);

- theoretical aspects of using of sequences of large periods over finite fields in radar-location and methods for generating pseudo-random sequences to provide cryptographic protection of information transmitted over long distances.

In particular, the paper presents a recurrent scheme for constructing so-called centered k-pyramidal numbers $CS_k^3(n)$, $n = 1, 2, 3, \ldots$, which present configurations of points that form the k-gonal pyramid, at the base of which lies the centered k-gonal number $CS_k(n)$.

Based on the definition, we get for the sequence $CS_k^3(n)$, $n = 1, 2, 3, \ldots$, recurrence formula $CS_k^3(n+1) = CS_k^3(n) + CS_k(n+1)$, $CS_k^3(1) = 1$. Noting that $CS_k(n+1) = \frac{kn^2+kn+2}{2}$, and using standard approaches, we prove that the generating function $f(x)$ of the sequence $CS_k^3(n)$, $n = 1, 2, 3, \ldots$, has the form $f(x) = \frac{x(1+(k-2)x+x^2)}{(1-x)^2}$, $|x| < 1$, while the closed formula for $CS_k^3(n)$ has the form $CS_k^3(n) = \frac{kn^3+n(6-k)}{6}$.

Keywords: Recurrence relation, recurrent numerical sequence, generating function of sequence, Pascal triangle, figurate numbers, amicable numbers, recurrent sequences over finite field.

Bibliography: 11 titles.

For citation:
E. I. Deza, L. V. Kotova, 2022, "Recurrent numerical sequences: theory and applications" , *Chebyshevskii sbornik*, vol. 23, no. 3, pp. 77 – 101.

1. Введение

Часто при решении различных задач, как прикладных, так и теоретических, появляются последовательности [10].

Во многих случаях мы знаем, как определяются элементы последовательности a_n при каждом значении n. Такое описание последовательностей называется *явным*.

Однако при решении ряда задач пользуются методом нахождения n-го элемента последовательности a_n, опираясь на информацию об одном или нескольких предыдущих элементах той же последовательности. Метод сведения задачи к аналогичной задаче для меньшего числа предметов называется *методом рекуррентных соотношений* (от латинского "recurrere" - возвращаться). Другими словами, *рекуррентными соотношениями* называют такие соотношения, которые позволяют получить информацию о n предметах, используя информацию о $n-1$ ($n-2$, $n-3$, ...) предметах. В случае числовых последовательностей – соотношения, которые позволяют найти a_n, используя a_{n-1} (a_{n-2}, a_{n-3}, ...).

Так, из комбинаторики известно, что $P_m = mP_{m-1}$, т.е. число перестановок из m предметов можно вычислить, зная число перестановок из $m-1$ предмета. Таким образом, зная начальное условие $P_1 = 1$, можно найти $P_2, P_3 \ldots, P_n, \ldots$ рекуррентным способом.

Аналогично, формула $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$ дает рекуррентное соотношение для числа сочетаний: число сочетаний из n элементов по k элементов можно найти, используя числа сочетаний из $n-1$ элемента. Таким образом, зная, что $C_0^0 = 1$, $C_n^0 = 1$ и $C_n^n = 1$, можно получить все значения C_n^k последовательными вычислениями:

$$\begin{array}{c} C_0^0 = 1 \\ C_1^0 = 1 \quad C_1^1 = 1 \\ C_2^0 = 1 \quad C_2^1 = C_1^0 + C_1^1 = 1 + 1 = 2 \quad C_2^2 = 1 \\ C_3^0 = 1 \quad C_3^1 = 1 + 2 = 3 \quad C_3^2 = 1 + 2 = 3 \quad C_3^3 = 1 \\ \ldots \quad \ldots \quad \ldots \end{array}$$

Действуя по данной схеме, мы получили арифметический треугольник, внешними элементами которого являются 1, а каждый внутренний элемент получен как сумма двух элементов, расположенных непосредственно над ним. Данный треугольник называется *треугольником Паскаля*.

Одной из наиболее известных задач, связанных с рекуррентными соотношениями, является *задача о кроликах* Фибоначчи (Леонардо Пизанского), появившаяся в 1202 г. в книге "Liber

Abaci". Решение указанной задачи приводит нас к рекуррентному соотношению

$$u_n = u_{n-1} + u_{n-2}$$

с начальными условиями $u_1 = u_2 = 1$, что позволяет последовательно вычислять все элементы последовательности $u_1, u_2, \ldots, u_n, \ldots$, которые называются *числами Фибоначчи*.

Не представляет труда доказать, что существует бесконечно много последовательностей, удовлетворяющих рекуррентному соотношению $u_n = u_{n-1} + u_{n-2}$. Так, если $u_1 = 1, u_2 = 2$, то мы получаем последовательность $1, 2, 3, 5, 8, 13, 21, 34, \ldots$ которая является подпоследовательностью последовательности Фибоначчи. Если $u_1 = 1, u_2 = 3$, то мы получим последовательность *чисел Люка* $1, 3, 4, 7, 11, 18, 29, 47, \ldots$, и т.д. Но при задании начальных условий $u_1 = 1, u_2 = 1$ последовательность Фибоначчи определяется рекуррентным соотношением $u_n = u_{n-1} + u_{n-2}$ однозначно.

Понятие "рекуррентность" (англ. "recurrence" – возвращение, повторение) является универсальным, часто встречаемым в разных областях знания. Оно используется, помимо математики, в биологии (связь с миграцией фауны и флоры) и в геологии (повторение состава продуктов вулканического извержения). В психологии используют словосочетание "рекуррентный образ", что означает образ, возникающий после того, как глаз долго смотрел на освещенный объект. Данное понятие становится частью терминологического аппарата гуманитарных наук — философии, социологии, культурологии, семиотики, лингвистики, педагогики [2].

В статье будут рассмотрены несколько аспектов указанной тематики, в том числе:

- история вопроса, место числовых рекуррентных последовательностей в развитии математической науки и математического образования [1, 5, 7];
- примеры использования рекуррентного подхода при построении различных классов (и подклассов) специальных чисел (фигурных чисел, дружественных чисел и др.) [3, 5];
- теоретические аспекты использования последовательностей больших периодов над конечными полями в радиолокации и методы генерации псевдослучайных последовательностей для обеспечения криптографической защиты информации, передаваемой на большие расстояния [7, 9].

2. Немного истории

2.1. Наиболее известной задачей, связанной с рекуррентными соотношениями, является *задача о кроликах* одного из самых значительных западных математиков средневековья, итальянского купца Фибоначчи (Леонардо Пизанского), появившаяся в 1202 г. в книге "Liber Abaci". Эта книга представляет собой объемный труд, содержащий почти все арифметические и алгебраические сведения того времени и сыгравший значительную роль в развитии математики в Западной Европе в течение нескольких следующих столетий.

Задача состоит в следующем: *пара кроликов приносит раз в месяц приплод из двух крольчат, причем новорожденные крольчата через два месяца после рождения уже приносят приплод. Сколько кроликов получится через год, если в начале года было два кролика?*

Для решения данной задачи проведем простейшие рассуждения, обозначая число пар кроликов в начале i-го месяца через u_i: 1 января мы имели 1 пару новорожденных кроликов ($u_1 = 1$). 1 февраля мы все еще имеем одну пару кроликов ($u_2 = 1$), которые, впрочем, перестали быть новорожденными. 1 марта мы получим первый приплод, то есть 2 пары кроликов ($u_3 = 1 + 1 = 2$), одна из которых новорожденная. 1 апреля одна из наших пар даст приплод, и мы получим 3 пары кроликов ($u_4 = 2 + 1 = 3$), одна из которых новорожденная. 1 апреля одна из наших пар даст приплод, и мы получим 3 пары кроликов ($u_4 = 2 + 1 = 3$), одна из

которых новорожденная. 1 мая две наших пары дадут приплод, и мы получим 5 пар кроликов ($u_5 = 3 + 2 = 5$), 2 из которых новорожденные. 1 июня три наших пары дадут приплод, и мы получим 8 пар кроликов ($u_5 = 5 + 3 = 8$), 3 из которых новорожденные. Рассуждая аналогично, 1 июля мы получим 13 пар ($u_7 = 8 + 5 = 13$), 1 августа - 21 пару ($u_8 = 13 + 8 = 21$), 1 сентября - 34 пары ($u_9 = 21 + 13 = 34$), 1 октября - 55 пар ($u_{10} = 34 + 21 = 55$), 1 ноября - 89 пар ($u_{11} = 55 + 34 = 89$), 1 декабря - 144 пары ($u_{12} = 89 + 55 = 144$), и, наконец, 1 января - 233 пары ($u_{13} = 144 + 89 = 233$).

Из построения следует, что $u_n = u_{n-1} + u_{n-2}$ для $n \geq 3$, в то время как $u_1 = u_2 = 1$.

Таким образом, мы получили рекуррентное соотношение

$$u_n = u_{n-1} + u_{n-2}$$

с начальными условиями $u_1 = u_2 = 1$, что позволяет последовательно вычислять все элементы последовательности $u_1, u_2, \ldots, u_n, \ldots$, которые называются *числами Фибоначчи*.

2.2. *Треугольник Паскаля* стал широко известен благодаря сочинению французского математика Блеза Паскаля "Трактат об арифметическом треугольнике", изданном в 1655 году. Именно, в указанном сочинении была опубликована таблица, в которой каждое число A было равно сумме предшествующего числа в том же, что и A, горизонтальном ряду, и предшествующего числа в том же, что и A, вертикальном ряду:

1	1	1	1	1	1
1	2	3	4	5	6
1	3	6	10	15	21
1	4	10	20	35	56
1	5	15	35	70	126
1	6	21	56	126	252

Таким образом треугольник, представленный во введении, отличается от треугольника, рассматриваемого самим Паскалем, поворотом на 45 градусов.

В действительности треугольник Паскаля был известен задолго до 1655 года. Омар Хайям, бывший не только философом и поэтом, но и математиком, знал о существовании треугольника около 1100 года (в Иране эту схему называют *треугольником Хайяма*), в свою очередь, заимствовав его из более ранних китайских или индийских источников.

Этот треугольник изображен на иллюстрации в книге "Яшмовое зеркало четырех элементов" китайского математика Чжу Шицзе, выпущенной в 1303 году. (Впрочем, в Китае считают, что изобрел треугольник другой китайский математик, Ян Хуэй, поэтому китайцы называют его *треугольником Яна Хуэя*.)

В Италии треугольник Паскаля иногда называют *треугольником Тартальи*, поскольку Никколо Тарталья описал соответствующую таблицу на сто лет раньше Паскаля. Треугольник воспроизведен и на титульном листе учебника арифметики, написанном в начале XVI века Петером Апианом, астрономом из Ингольтштадского университета.

2.3. *Фигурные числа* – числа, которые можно представить с помощью геометрических фигур. Это историческое понятие восходит к пифагорейцам, которые развивали алгебру на геометрической основе и представляли любое положительное целое число в виде набора точек на плоскости. Само построение фигурных чисел носит рекуррентный характер. Так, начиная с 1, каждое *треугольное число* получатся из предыдущего добавлением очередного натурального числа:

$$S_3(n+1) = S_3(n) + (n+1), \;\; S_3(1) = 1.$$

Другими словами, n-е треугольное число $S_3(n)$ есть сумма первых n натуральных чисел, или, что тоже, сумма первых n членов простейшей арифметической прогрессии $1, 2, 3, \ldots, n, \ldots$ с

первым членом 1 и разностью 1. Заменяя разность 1 на $m-2$, $m=4,5,6,\ldots$, мы получим аналогичным образом m-угольные числа (квадратные, пятиугольные, шестиугольные и т.д.).

Указанная связь позволяет успешно использовать многоугольные числа для закрепления понятия "арифметическая прогрессия" у школьников.

Построение пространственных фигурных чисел также подчиняется рекуррентной процедуре. Например, каждое следующее *тетраэдральное число* получается из предыдущего добавлением очередного треугольного числа:

$$S_3^3(n+1)=S_3^3(n)+S_3(n+1),\ S_3(1)=1.$$

На рекуррентной основе строятся и *центрированные k-угольные числа* $CS_k(n)$:

$$CS_k(n+1)=CS_k(n)+nk,\ CS_k(1)=1.$$

2.4. Подчиняются рекуррентным законам (см. [6]) *числа Ферма* $F_n=2^{2^n}+1, n\geq 0$ (Sloane's A000215), и *числа Мерсенна* $M_n=2^n-1$, $n\geq 1$ (Sloane's A000225):

$$F_{n+1}=F_0\cdots F_n+2,\ F_0=3;\ M_{n+1}=2M_n+1,\ M_1=1.$$

2.5. Если для (четных) *совершенных чисел* n, $\sigma(n)=2n$, специальные рекуррентности не требуются, любое четное совершенное число может быть получено по *формуле Евклида-Эйлера* $2^{p-1}(2^p-1)$ из простого числа Мерсенна $M_p=2^p-1$, то для получения новых *дружественных чисел* (m,n), $\sigma(n)=\sigma(n)=m+n$, помимо классических *правила Сабита* (известны ровно 3 пары, получаемые по этому правилу) и *правила Эйлера* (известны ровно 5 пар, получаемых по этому правилу, включая три пары Сабита), с успехом используются рекуррентные схемы, позволяющие получать новые пары, отталкиваясь от уже известных; классическим примером такого алгоритма является *правило Боро* [3].

2.6. Существуют по крайней мере две различные практические задачи, приводящие к необходимости построения периодической последовательности большого периода.

Первая из них связана с радиолокацией. Например, чтобы определить положение движущегося объекта в атмосферере и пространстве, используется радиолокатор, антенна которого излучает электромагнитную энергию узким пучком. Когда пучок достигает объекта, то часть его энергии оражается назад к антенне. Этот сигнал, получаемый антенной, подтверждает наличие объекта в исследуемом направлении. Расстояние до объекта можно определить, если измерить разницу во времени с момента отправления пучка до получения ответного сигнала.Однако объект движется в пространстве, поэтому единичные импульсы или ряд одинаковых импульсов не могут предоставить достоверной информации. Если же отправить серию импульсов, представляющую собой периодическую последовательность с достаточно большим периодом, то ответный импульс будет давать точную информацию о времени, прошедшем с момента отправки. Например, период порядка 10^6 достаточен для локации Луны, а порядка 10^9 – для локации Венеры.

В данном случае нам необходима последовательность большого приода, которая фиксирована и хорошо известна исследователям.

2.7. Второе применение последовательностей большого периода носит закрытый характер, именно, используется в шифровании,имеющим очень древние корни. *Шифр Цезаря* (Gaius Iulius Caesar, 100 – 44 до н.э.), представляет собой подстановку символов открытого символом, находящимся на 3 позиции правее него в том же алфавите (сдвиг). Для затруднения частотного анализа вместо шифров подстановки (простой замены) (называемых также моноалфавитными, поскольку каждый символ открытого текста переходит в некоторый, фиксированный при данном ключе, символ того же алфавита) с XV в. стали использовать более сложные подстановочные шифры, в том числе полиалфавитные, состоящие в повторяющемся применении нескольких сдвигов алфавита к определенному числу букв шифруемого текста.

Примером построения полиалфавитного шифра является *шифр Тритемиуса* – система шифрования, разработанная Иоганном Тритемием (Iohannes Trithemius, 1462 – 1516), которая подразумевает для каждого символа сообщения свой сдвиг, определяемый некоторым ключом.

Говоря математическим языком, символ, стоящий на i-ой позиции открытого сообщения, заменяется при осуществлении данного алгоритма по закону $l_i \equiv m_i + k_i (mod\ N)$, где m_i - числовой эквивалент i-го символа открытого сообщения, k_i - числовой эквивалент i-го символа ключа, получающегося последовательным повторением заданного ключевого слова, и l_i - числовой эквивалент i-го символа шифротекста. Для дешифрования достаточно провести обратную операцию: $m_i \equiv l_i - k_i (mod\ N)$, то есть для расшифровки шифротекста из номера очередной буквы зашифрованного сообщения вычитают номер соответствующей буквы ключа, осуществляя эту операцию по модулю N.

Однако по настоящему стойким такой шифр будет, если использовать ключевое слово бесконечной длины.

Реализацией данной идеи является *шифр Вернама* (одноразовый шифровальный блокнот) - единственная система шифрования, для которой доказана абсолютная криптографическая стойкость (Claude Elwood Shannon, 1945).

Существенной проблемой для данного способа шифрования является хранение и передача последовательности-ключа. Кроме того, для работы шифра Вернама необходима истинно случайная последовательность, а используемые на практике последовательности, генерируемые с помощью различных, как правило, арифметических алгоритмов, являются лишь псевдослучайными [9].

Таким образом, классическая идея шифровального блокнота привела к использованию в шифровании *псевдослучайных последовательностей* – последовательностей такого большого периода, чтобы их трудно было восстановить непосвященному и достаточно легко сгенерировать для простейшего шифрования с помощью суммирования исходного сообщения и ключа (и дешифрования аналогичным способом). При этом абоненты, находясь на расстоянии друг от друга, используют открытые каналы связи. Для одновременной работы им требуется открытый экспоненциальный ключ (но это другая задача).

3. Рекуррентные соотношения и фигурные числа

3.1. Определим n-ое *m-угольное пирамидальное число* $S_m^3(n)$ как сумму первых n m-угольных чисел [4]:

$$S_m^3(n) = S_m(1) + S_m(2) + \ldots + S_m(n).$$

Таким образом, имеет место следующая рекуррентная формула:

$$S_m^3(n) = S_m^3(n-1) + S_m(n),\ S_m^3(1) = 1.$$

Отсюда следует, что n-ое m-угольное пирамидальное число имеет вид

$$S_m^3(n) = \frac{n(n+1)((m-2)n - m + 5)}{6}.$$

□. Докажем данное утверждение по индукции.

Для $n = 1$ имеем $S_m^3(1) = S_m(1) = 1 = \frac{1 \cdot 2((m-2)\cdot 1 - m + 5)}{6}$. Переходя от n к $n+1$, получим

$$S_m^3(n+1) = S_m^3(n) + S_m(n+1) =$$

$$= \frac{n(n+1)((m-2)n - m + 5)}{6} + \frac{(n+1)((m-2)(n+1) - m + 4)}{2} =$$

$$= \frac{(n+1)}{6} \cdot (n^2(m-2) + n(5-m) + 3(n+1)(m-2) + 3(4-m)) =$$

$$= \frac{(n+1)}{6} \cdot ((n^2+3n+3)(m-2)+n(5-m)+3(4-m)) =$$

$$= \frac{(n+1)}{6} \cdot ((n^2+3n+2)(m-2)+(n+2)(5-m)+(m-2)-2(5-m)+3(4-m)) =$$

$$= \frac{(n+1)}{6} \cdot ((n+2)(n+1)(m-2)+(n+2)(5-m)+(m-2-10+2m+12-3m)) =$$

$$= \frac{(n+1)}{6} \cdot (n+2)((n+1)(m-2)+(5-m)) = \frac{(n+1)(n+2)((m-2)(n+1)-m+5)}{6}. \square$$

Эта формула была известна уже Архимеду (287 – 212 до н.э.) и использовалась им для вычисления объемов.

В частности, n-ое *тетраэдральное число* $S_3^3(n)$ имеет вид $S_3^3(n) = \frac{n(n+1)(n+2)}{6}$. Таким образом, последовательность тетраэдральных чисел представляет собой последовательность частичных сумм ряда $1, 3, 6, 10, 15, 21, 28, 36, 45, 55, \ldots$ (Sloane's A000217) треугольных чисел и начинается с элементов 1, 4, 10, 20, 35, 56, 84, 120, 165, 220, ... (Sloane's A000292).

Аналогично, n-ое *квадратное пирамидальное число* $S_4^3(n)$ имеет вид $S_4^3(n) = \frac{n(n+1)(2n+1)}{6}$. Последовательность квадратных пирамидальных чисел представляет собой последовательность частичных сумм ряда $1, 4, 9, 16, 25, 36, 49, 64, 81, 100, \ldots$ (Sloane's A000290) квадратных чисел и начинается с элементов 1, 5, 14, 30, 55, 91, 140, 204, 285, 385, ... (Sloane's A000330). Производящая функция последовательности $S_m^3(1)$, $S_m^3(2)$, ..., $S_m^3(n)$, ... m-угольных пирамидальных чисел имеет вид $f(x) = \frac{x(1+(m-3)x)}{(1-x)^4}$, то есть имеет место разложение

$$\frac{x(1+(m-3)x)}{(1-x)^4} = S_m^3(1)x + S_m^3(2)x^2 + S_m^3(3)x^3 + \ldots + S_m^3(n)x^n + \ldots, \ |x| < 1.$$

В частности, $\frac{x}{(1-x)^4} = x + 4x^2 + 10x^3 + \ldots + S_3^3(n)x^n + \ldots, \ |x| < 1$, для тетраэдральных чисел, и $\frac{x(x+1)}{(x-1)^4} = x + 5x^2 + 14x^3 + \ldots + S_4^3(n)x^n + \ldots, \ |x| < 1$, для квадратных пирамидальных чисел. $\square$ Этот результат может быть получен с помощью стандартной процедуры [8]. Рассмотрим линейное рекуррентное соотношение

$$S_m^3(n+1) = S_m^3(n) + S_m(n+1).$$

Переходя от n к $n+1$, получим соотношение

$$S_m^3(n+2) = S_m^3(n+1) + S_m(n+1).$$

Вычитая первое равенство из второго, получим

$$S_m^3(n+2) - S_m^3(n+1) = S_m^3(n+1) - S_m^3(n) + S_m(n+1) - S_m(n),$$

или, что то же,

$$S_m^3(n+2) = 2S_m^3(n+1) - S_m^3(n) + (1+(m-2)(n+1)).$$

Аналогично,

$$S_m^3(n+3) = 2S_m^3(n+2) - S_m^3(n+1) + (1+(m-2)(n+2)),$$

и

$$S_m^3(n+3) - S_m^3(n+2) = 2S_m^3(n+2) - 2S_m^3(n+1) - S_m^3(n+1) + S_m^3(n) + (m-2),$$

то есть

$$S_m^3(n+3) = 3S_m^3(n+2) - 3S_m^3(n+1) + S_m^3(n) + (m-2).$$

Переходя от $n+2$ к $n+3$, получаем

$$S_m^3(n+4) = 3S_m^3(n+3) - 3S_m^3(n+2) + S_m^3(n+1) + (m-2).$$

Следовательно,

$$S_m^3(n+4) - S_m^3(n+3) =$$
$$= 3S_m^3(n+3) - 3S_m^3(n+2) - 3S_m^3(n+2) + 3S_m^3(n+1) + S_m(n+1) - S_m(n),$$

откуда следует, что

$$S_m^3(n+4) = 4S_m^3(n+3) - 6S_m^3(n+2) + 4S_m^3(n+1) - S_m^3(n). \ \square$$

Таким образом, мы получили для последовательности m-угольных пирамидальных чисел линейное рекуррентное соотношение $S_m^3(n+4) - 4S_m^3(n+3) + 6S_m^3(n+2) - 4S_m^3(n) + S_m^3(n) = 0$ 4-го порядка с постоянными коэффициентами. Учитывая начальные условия $S_m^3(1) = 1$, $S_m^3(2) = 1+m$, $S_m^3(3) = 4m-2$, $S_m^3(4) = 10m-10$, перепишем соотношение в виде

$$c_{n+4} - 4c_{n+3} + 6c_{n+2} - 4c_{n+1} + c_n = 0,\ c_0 = 1,\ c_1 = m+1,\ c_2 = 4m-2,\ c_3 = 10m-10,$$

где $S_m^3(n+1)$ заменено на c_n. В этом случае (см. [8]) производящая функция имеет вид

$$\frac{f(x)}{g(x)} = \frac{a_0 + a_1x + a_2x^2 + a_3x^3}{b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4},$$

где $b_0 = 1, b_1 = -4, b_2 = 6, b_3 = -4, b_4 = 1$, и $a_0 = b_0c_0 = 1, a_1 = b_0c_1 + b_1c_0 = 1\cdot(m+1) + (-4)\cdot 1 = m-3$, $a_2 = b_0c_2 + b_1c_1 + b_2c_0 = 1\cdot(4m-2) + (-4)(m+1) + 6\cdot 1 = 0$, $a_3 = b_0c_3 + b_1c_2 + b_2c_1 + b_3c_0 = 1\cdot(10m-10) + (-4)(4m-2) + 6(1+m) + (-4)\cdot 1 = 0$. Так как многочлен $g(x) = 1 - 4x + 6x^2 - 4x^3 + x^4 = (1-x)^4$ имеет 4 совпавших корня $x_1 = \ldots = x_4 = 1$, то производящая функция последовательности m-угольных пирамидальных чисел имеет вид

$$\frac{1+(m-3)x}{(1-x)^4} = S_m^3(1) + S_m^3(2)x + S_m^3(3)x^2 + \ldots + S_m^3(n)x^{n-1} + \ldots,\ |x| < 1.$$

Этот результат может быть получен также с помощью производящей функции

$$\frac{1+(m-3)x}{(1-x)^3} = S_m(1) + S_m(2)x + S_m(3)x^2 + \ldots + S_m(n)x^{n-1} + \ldots$$

последовательности m-угольных чисел и разложения $\frac{1}{1-x} = 1 + x + x^2 + \ldots + x^n + \ldots$. Именно,

$$\frac{1+(m-3)x}{(1-x)^4} = \frac{1+(m-3)x}{(1-x)^3}\cdot\frac{1}{1-x} =$$
$$= (S_m(1) + S_m(2)x + S_m(3)x^2 + \ldots + S_m(n)x^{n-1} + \ldots)(1 + x + x^2 + \ldots + x^n + \ldots) =$$
$$= S_m(1) + (S_m(1) + S_m(2))x + (S_m(1) + S_m(2) + S_m(3))x^2 + \ldots + (S_m(1) + \ldots +$$
$$+ S_m(n))x^{n-1} + \ldots = S_m^3(1) + S_m^3(2)x + S_m^3(3)x^2 + \ldots + S_m^3(n)x^{n-1} + \ldots,\ |x| < 1. \ \square$$

3.2. Рассмотрим пространственные фигурные числа, образованные центральной точкой, окруженной последовательными слоями-многогранниками, прежде всего – центрированные числа, соответствующие правильным многогранникам (тетраэдру, кубу, октаэдру, икосаэдру, додекаэдру), и центрированные m-пирамидные числа.

Так, *центрированные кубические числа* – это числа, представляющее "центрированный куб". Любой центрированный куб образован центральной точкой, окруженной последовательными кубическими слоями. На n-ом шаге предыдущая конструкция окружается слоем новых

точек, образующих куб, каждая грань которого содержит ровно n^2 точек. Другими словами, n-ый слой представлят собой n-ое кубическое число n^3 без внутренности, то есть без $(n-2)$-го кубического числа $(n-2)^3$.

Таким образом, начиная с 1, мы получим на втором шаге куб, сформированный из 8 точек, что соответствует $C(2) = 2^3$ без пустой внутренности. На третьем шаге добавим куб, сформированный из 28 точек, что соответствует $C(3) = 3^3$ без одноточечной внутренности: $28 = C(3) - C(1)$, и т.д.

Другими словами, центрированные кубические числа могут быть получены как частичные суммы последовательности $1^3, 2^3 - 0^3, 3^3 - 1^3, 4^3 - 2^3, \ldots, n^3 - (n-2)^3, \ldots$. Следовательно, n-ое центрированное кубическое число $\overline{C}(n)$ имет вид

$$\overline{C}(n) = 1^3 + (2^3 - 0^3) + (3^3 - 1^3) + (4^3 - 2^3) + \ldots + (n^3 - (n-2)^3).$$

Отсюда следует рекуррентная формула

$$\overline{C}(n+1) = \overline{C}(n) + ((n+1)^3 - (n-1)^3),\ \overline{C}(1) = 1.$$

Так как $(n+1)^3 - (n-1)^3 = 6n^2 + 2$, мы получаем, что

$$\overline{C}(n+1) = \overline{C}(n) + (6n^2 + 2),\ \overline{C}(1) = 1.$$

Легко видеть, что

$$1^3 + (2^3 - 0^3) + (3^3 - 1^3) + (4^3 - 2^3) + \ldots + (n^3 - (n-2)^3) = n^3 + (n-1)^3,$$

то есть что любое центрированное кубическое число является суммой двух последовательных кубических чисел:

$$\overline{C}(n) = C(n) + C(n-1).$$

Следовательно, поскольку $n^3 + (n-1)^3 = n^3 + (n^3 - 3n^2 + 3n - 1) = (2n^3 - n^2) - (2n^2 + n) + (2n-1) = (2n-1)n^2 - (2n-1)n + (2n-1) = (2n-1)(n^2 - n + 1)$, имеет место формула

$$\overline{C}(n) = (2n-1)(n^2 - n + 1).$$

Первыми центрированными кубическими числами являются числа 1, 9, 35, 91, 189, 341, 559, 855, 1241, 1729, ... (Sloane's A005898).

3.3. Центрированные пирамидные числа соответствуют конструкциям, образованным центральной точкой, окруженной пирамидальными слоями. Каждый слой может рассматриваться как соответствующее пирамидальное число без внутренности.

Так, *центрированные тетраэдральные числа* соответствуют центрированным тетраэдрам. Начиная с одной точки, получаем на 2-ом уровне тетраэдр, образованный из 4 точек. Он соответствует 2-му тетраэдральному числу $S_3^3(2) = 4$ без пустой внутренности. 3-ий уровень – тетраэдр, образованный из 10 точек. Он соответствует 3-му тетраэдральному числу $S_3^3(3) = 10$ без пустой внутренности. Аналогично, 4-ый уровень соответствует $S_3^3(4) = 20$ без пустой внутренности, 5-й уровень образован из 34 точек и соответствует $S_3^3(5) = 35$ без 1-точечной внутренности: $34 = S_3^3(5) - S_3^3(1)$. 52 точки 6-го уровня соответствуют $S_3^3(6) = 56$ без 4-точечной внутренности: $52 = S_3^3(6) - S_3^3(2)$, и т.д. В общем случае, центрированные тетраэдральные числа являются частичными суммами элементов последовательности

$$S_3^3(1), S_3^3(2), S_3^3(3), S_3^3(4), S_3^3(5) - S_3^3(1), S_3^3(6) - S_3^3(2), \ldots, S_3^3(n+4) - S_3^3(n), \ldots .$$

Начиная с $n = 4$, n-ое центрированное тетраэдральное число $\overline{S}_3^3(n)$ может быть получено как

$$\overline{S}_3^3(n) = S_3^3(1) + S_3^3(2) + S_3^3(3) + S_3^3(4) + (S_3^3(5) - S_3^3(1)) + (S_3^3(6) - S_3^3(2)) + \ldots + (S_3^3(n+4) - S_3^3(n)).$$

Поскольку телескопическая сумма равна $S_3^3(n)+S_3^3(n-1)+S_3^3(n-2)+S_3^3(n-3)$, то

$$\overline{S}_3^3(1)=S_3^3(1)=1,\ \overline{S}_3^3(2)=S_3^3(2)+S_3^3(1)=5,\ \overline{S}_3^3(3)=S_3^3(3)+S_3^3(2)+S_3^3(1)=15,$$

$$\overline{S}_3^3(n)=S_3^3(n)+S_3^3(n-1)+S_3^3(n-2)+S_3^3(n-3),\ n\geq 4.$$

Итак, первые элементы последовательности центрированных тетраэдральных чисел равны 1, 5, 15, 35, 69, 121, 195, 295, 425, 589, ... (Sloane's A005894).

Так как $S_3^3(n)=S_3^3(n-1)+S_3(n)$, получаем, для $n\geq 4$, рекуррентную формулу

$$\overline{S}_3^3(n)=\overline{S}_3^3(n-1)+(S_3(n)+S_3(n-1)+S_3(n-2)+S_3(n-3)).$$

Другими словами, для $n\geq 4$ имеет место соотношение $\overline{S}_3^3(n)=\overline{S}_3^3(n-1)+(2n^2-4n+4)$. Более того, нетрудно проверить, что эта формула работает и для $n=2,3$. Таким образом, замечая, что $2(n+1)^2-4(n+1)+4=2n^2+2$, получаем рекуррентную формулу

$$\overline{S}_3^3(n+1)=\overline{S}_3^3(n)+(2n^2+2),\ \overline{S}_3^3(1)=1.$$

Кроме того, для $\overline{S}_3^3(n)$ легко получить и явную формулу

$$\overline{S}_3^3(n)=\frac{(2n-1)(n^2-n+3)}{3}=\frac{2n^3-3n^2+7n-3}{3}.$$

□ Действительно, для $n\geq 4$ имеем: $S_3^3(n)+S_3^3(n-1)+S_3^3(n-2)+S_3^3(n-3)=\frac{n(n+1)(n+2)}{6}+$ $+\frac{(n-1)n(n+1)}{6}+\frac{(n-2)(n-1)n}{6}+\frac{(n-3)(n-2)(n-1)}{6}=\frac{n(n+1)(2n+1)}{6}+\frac{(n-2)(n-1)(2n-3)}{6}=\frac{(n^2+n)(2n+1)}{6}+$ $+\frac{(n^2-3n+2)(2n-3)}{6}=\frac{(2n^3+2n^2+n^2+n)+(2n^3-6n^2+4n-3n^2+9n-6)}{6}=\frac{4n^3-6n^2+14n-6}{6}=\frac{2n^3-3n^2+7n-3}{3}=$ $=\frac{(2^3-n^2)-(2n^2-n)+(6n-3)}{3}=\frac{(2n-1)(n^2-n+3)}{3}$. Для $n=1,2,3$ достаточно использовать прямой подсчет: $\frac{(2\cdot 1-1)(1^2-1+3)}{3}=1=\overline{S}_3^3(1)$, $\frac{(2\cdot 2-1)(2^2-2+3)}{3}=5=\overline{S}_3^3(2)$, $\frac{(2\cdot 3-1)(3^2-3+3)}{3}=35=\overline{S}_3^3(3)$ □.

Мы можем получить последовательность центрированных тетраэдральных чисел путем подсчета частичных сумм последовательности 1, 4, 10, 20, 34, 52, 74, 100, 130, 164, ... (Sloane's A005893), дающей количества точек на поверхности тетраэдра. Первый элемент этой последовательности равен 1, в то время как n-ый элемент, $n\geq 2$, имеет вид $2(n-1)^2+2=2n^2-4n+4$.

Этот результат можно получить по формуле $v+s(n-2)+f\cdot int(S_3(n))$, где $v=4$, $s=6$ и $f=4$ – числа вершин, сторон и граней тетраэдра, в то время как $int(S_3(n))$ – число точек внутри n-го треугольного числа. Для $n\geq 2$ получаем: $v+s(n-2)+f\cdot int(S_3(n))=4+6(n-2)+$ $+4(\frac{n(n+1)}{2}-3(n-1))=6n-8+2(n^2-5n+6)=2n^2-4n+4=2(n-1)^2+2$.

При таком подходе вышеуказанная рекуррентная формула для центрированных тетраэдральных чисел становится очевидной, в то время как явная формула для $\overline{S}_3^3(n)$ может быть получена в результате следующего суммирования: $\overline{S}_3^3(n)=1+\sum_{i=1}^{n-1}(2i^2+2)=1+2\sum_{i=1}^{n-1}i^2+$ $+2(n-1)=2\cdot\frac{(n-1)n(2n-1)}{6}+(2n-1)=\frac{(2n-1)(n^2-n+1)}{3}$.

3.4. С помощью той же процедуры можно построить *центрированные m-пирамидные числа* для любого $m\geq 3$.

Именно, последовательность $\overline{S}_m^3(1),\overline{S}_m^3(2),\ldots,\overline{S}_m^3(n),\ldots$ центрированных m-пирамидных чисел можно получить как последовательность частичных сумм ряда $1, m+1, 4m-2, 9m-7, 16m-14, \ldots$, задающего количества точек на поверхности m-угольной пирамиды. Первый элемент этой последовательности равен 1, в то время как n-ый элемент, $n\geq 2$, имеет вид $(m-1)(n-1)^2+2=(m-1)n^2-2(m-1)n+(m+1)$.

Этот результат можно получить по формуле $v+s(n-2)+f_\triangle\cdot int(S_3(n))+int(S_m(n))$, где $v=m+1$, $s=2m$ и $f_\triangle=m$ – числа вершин, сторон и граней m-угольной пирамиды, в то время как $int(S_m(n))$ – число точек внутри n-го m-угольного числа. Для $n\geq 2$ имеем:

$v+s(n-2)+f_{\triangle}\cdot int(S_3(n))+int(S_m(n)) = (m+1)+2m(n-2)+m(\frac{n(n+1)}{2}-3(n-1))+(\frac{m-2}{2}(n^2-n)+$
$+ n - m(n-1)) = (m-1)n^2 - 2(m-1)n + (m+1) = (m-1)(n-1)^2 + 2.$

Таким образом, рекуррентная формула для последовательности центрированных m-пирамидных чисел имеет вид

$$\overline{S}^3_m(n+1) = \overline{S}^3_m(n) + (m-1)n^2 + 2,\ \overline{S}^3_m(1) = 1.$$

Явная формула для $\overline{S}^3_m(n)$ имеет вид

$$\overline{S}^3_m(n) = \frac{(2n-1)((m-1)n^2 - (m-1)n + 6}{6}.$$

□ Ее можно получить в результате суммирования $\overline{S}^3_m(n) = 1 + \sum_{i=1}^{n-1}((m-1)i^2 + 2) = 1 +$
$+ (m-1)\sum_{i=1}^{n-1} i^2 + 2(n-1) = (m-1)\cdot\frac{(n-1)n(2n-1)}{6} + (2n-1) = \frac{(2n-1)((m-1)n^2-(m=1)n+6)}{6}$. □

Производящая функция последовательности $\overline{S}^3_m(1)$, $\overline{S}^3_m(2)$, ..., $\overline{S}^3_m(n)$, ... имеет вид

$$f(x) = \frac{x(1+(m-2)x+(m-2)x^2+x^3)}{(1-x)^4} = \frac{x(1+x)(1+(m-3)x+x^2)}{(1-x)^4}.$$

Другими словами,

$$\frac{x(1+x)(1+(m-3)x+x^2)}{(x-1)^4} = \overline{S}^3_m(1)x + \overline{S}^3_m(2)x^2 + \overline{S}^3_m(3)x^3 + \ldots + \overline{S}^3_m(n)x^n + \ldots,\ |x| < 1.$$

□ Этот результат может быть получен стандартной процедурой, приводящей к линейному рекуррентному уравнению $\overline{S}^3_m(n+4) - 4\overline{S}^3_m(n+3) + 6\overline{S}^3_m(n+2) - 4\overline{S}^3_m(n+1) + \overline{S}^3_m(n) = 0$ с начальными значениями $\overline{S}^3_m(1) = 1$, $\overline{S}^3_m(2) = m+1$, $\overline{S}^3_m(3) = 4m-2$, $\overline{S}^3_m(4) = 9m-7$. □

3.5. В этом разделе мы построим два класса пространственных фигурных чисел, которые используют как строительные блоки центрированные многоугольные числа. Они представляют собой центрированные m-пирамидальные числа и центрированные m-гранные призматические числа, $m \geq 3$.

Центрированные 6-пирамидальные числа являются наиболее известными объектами такого рода. Они соответствуют конфигурации точек, которые образуют шестиугольную пирамиду, основанием которой служит центрированное шестиугольное число.

По определению, центрированные 6-пирамидальные числа представляют собой частичные суммы элементов последовательности 1, 7, 19, 37, 61, 91, 127, 169, 217, 271, ... (Sloane's A003215) центрированных шестиугольных чисел:

$$CS_3(n) = CS_6(1) + CS_6(2) + \ldots + CS_6(n).$$

Так как $CS_6(n) = 3n^2 + 3n + 1 = n^3 - (n-1)^3$ (см. [4]), мы получаем, что n-ое центрированное шестиугольное пирамидальное число равно n^3. Это означает, что центрированные 6-пирамидальные числа эквивалентны кубическим числам, но по-разному расположены в пространстве. Первыми элементами последовательности являются числа 1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, ... (Sloane's A000578).

Конечно, можно построить подобные объекты для любого типа центрированных многоугольных чисел.

Центрированное m-пирамидальное число соответствует конфигурации точек, образующих m-угольную пирамиду, в основании которой лежит центрированное m-угольное число.

По определению, такие числа являются последовательными суммами ряда $CS_m(1) = 1$, $CS_m(2) = 1+m, CS_m(3) = 1+3m, CS_m(4) = 1+6m, \ldots, CS_m(n) = 1 + \frac{n(n+1)}{2}, \ldots$ центрированных m-угольных чисел. Другими словами,

$$CS^3_m(n) = CS_m(1) + CS_m(2) + \ldots + CS_m(n).$$

В частности, *центрированные 3-пирамидальные числа* являются частичными суммами ряда 1, 4, 10, 19, 31, 46, 64, 85, 109, 136, ... (Sloane's A005448) центрированных треугольных чисел. Первыми элементами последовательности являются числа 1, 5, 15, 34, 65, 111, 175, 260, 369, 505, ...

Центрированные 4-пирамидальные числа являются частичными суммами ряда 1, 5, 13, 25, 41, 61, 85, 113, 145, 181, ... (Sloane's A001844) центрированных квадратых чисел. Первыми элементами последовательности являются числа 1, 6, 19, 44, 85, 111, 146, 231, 344, 489, ...

Центрированные 5-пирамидальные числа являются частичными суммами ряда 1, 6, 16, 31, 51, 76, 106, 141, 181, 226, ... (Sloane's A005891) центрированных пятиугольных чисел. Первыми элементами последовательности являются числа 1, 7, 23, 54, 105, 181, 287, 428, 609, 835, ... Они совпадают с Sloane's A004068, давая число точек в додекаэдре с n оболочками.

Как было показано ранее, центрированные 6-пирамидальные числа являются частичными суммами ряда 1, 7, 19, 37, 61, 91, 127, 169, 217, 271, ... (Sloane's A003215). Последовательность начинается с элементов 1, 8, 27, 64, 125, 216, , 512, 729, 1000, ... (Sloane's A000578).

Следуя этой процедуре, можно построить центрированные 7-пирамидальные числа 1, 9, 31, 74, 145, 251, 399, 596, 849, 1165, ...; центрированные 8-пирамидальные числа 1, 10, 35, 84, 165, 286, 455, 680, 969, 1330, ...; центрированные 9-пирамидальные числа 1, 11, 39, 94, 185, 321, 511, 764, 1089, 1495, ...; центрированные 10-пирамидальные числа 1, 12, 43, 104, 205, 356, 567, 848, 1209, 1660, ...; центрированные 11-пирамидальные числа 1, 13, 47, 114, 225, 391, 623, 932, 1329, 1825, ...; центрированные 12-пирамидальные числа 1, 14, 51, 124, 245, 426, 679, 1016, 1449, 1990, ... и т.д.

По определению, мы получаем следующую рекуррентную формулу для последовательности $CS_m^3(1)$, $CS_m^3(2)$, ..., $CS_m^3(n)$, ... центрированных m-пирамидальных чисел:

$$CS_m^3(n+1) = CS_m^3(n) + CS_m(n+1),\ CS_m^3(1) = 1.$$

Так как $CS_m(n+1) = \frac{mn^2+mn+2}{2}$ (см. [4]), то

$$CS_m^3(n+1) = CS_m^3(n) + \frac{mn^2+mn+2}{2},\ CS_m^3(1) = 1.$$

Явная формула для n-го центрированного m-пирамидального числа $CS_m^3(n)$ имеет вид

$$CS_m^3(n) = \frac{mn^3 + n(6-m)}{6}.$$

□ Поскольку $CS_m(n) = 1 + mS_3(n-1)$, то $CS_m^3(n)$ имеет вид

$$CS_m^3(n) = n + m(S_3(n-1) + S_3(n-2) + \ldots + S_3(2) + S_3(1)).$$

Сумма первых $(n-1)$ треугольных чисел дает $(n-1)$-ое тетраэдральное число $S_3^3(n-1)$. Следовательно, $CS_m^3(n) = n + mS_3^3(n-1)$. Поскольку $S_3^3(n-1) = \frac{(n-1)\cdot n\cdot (n+1)}{6}$, то $CS_m^3(n) = \frac{mn^3+n(6-m)}{6}$. □

Производящая функция последовательности $CS_m^3(1)$, $CS_m^3(2)$, ..., $CS_m^3(n)$, ... имеет вид $f(x) = \frac{x(1+(m-2)x+x^2)}{(1-x)^4}$, то есть

$$\frac{x(1+(m-3)x)}{(1-x)^4} = CS_m^3(1) + CS_m^3(2)x + CS_m^3(3)x^2 + \ldots, |x| < 1.$$

□ Этот факт может быть получен стандартной процедурой, приводящей к линейному рекуррентному соотношнию с постоянными коэффициентами. Именно, рассмотрим рекуррентное соотношние

$$CS_m^3(n+1) = CS_m^3(n) + CS_m(n+1).$$

Переходя от n к $n+1$, получим:

$$CS_m^3(n+2) = CS_m^3(n+1) + CS_m(n+1).$$

Вычитая первое равенство из второго, получим, что

$$CS_m^3(n+2) - CS_m^3(n+1) = CS_m^3(n+1) - CS_m^3(n) + CS_m(n+1) - CS_m(n),$$

то есть

$$CS_m^3(n+2) = 2CS_m^3(n+1) - CS_m^3(n) + m(n+1).$$

Аналогично,

$$CS_m^3(n+3) = 2CS_m^3(n+2) - CS_m^3(n+1) + m(n+2),$$

и

$$CS_m^3(n+3) - CS_m^3(n+2) = 2CS_m^3(n+2) - 2CS_m^3(n+1) - CS_m^3(n+1) + CS_m^3(n) + m,$$

то есть

$$CS_m^3(n+3) = 3CS_m^3(n+2) - 3CS_m^3(n+1) + CS_m^3(n) + m.$$

Переходя от $n+3$ к $n+4$, получим

$$CS_m^3(n+4) = 3CS_m^3(n+3) - 3CS_m^3(n+2) + CS_m^3(n+1) + m.$$

Следовательно,

$$CS_m^3(n+4) - CS_m^3(n+3) =$$
$$= 3CS_m^3(n+3) - 3CS_m^3(n+2) - 3CS_m^3(n+2) + 3CS_m^3(n+1) + CS_m(n+1) - CS_m(n),$$

то есть

$$CS_m^3(n+4) = 4CS_m^3(n+3) - CS_m^3(n+2) + 4CS_m^3(n+1) - CS_m^3(n).$$

Таким образом, мы получаем для последовательности центрированных m-пирамидальных чисел линейное рекуррентное уравнение

$$CS_m^3(n+4) - 4CS_m^3(n+3) + 6CS_m^3(n+2) - 4CS_m^3(n) + CS_m^3(n) = 0$$

4-го порядка с постоянными коэффициентами. Начальные значения задаются соотношениями $CS_m^3(1) = 1$, $CS_m^3(2) = 2+m$, $CS_m^3(3) = 3+4m$, и $CS_m^3(4) = 4+10m$. Обозначая $CS_m^3(n+1)$ через c_n, перепишем соотношение в виде

$$c_{n+4} - 4c_{n+3} + 6c_{n+2} - 4c_{n+1} + c_n = 0 \ \text{ с } c_0 = 1,\ c_1 = m+2,\ c_2 = 4m+3,\ c_3 = 10m+4.$$

Таким образом, производящая функция последовательности центрированных m-пирамидальных чисел имеет следующий вид (см. [8]):

$$\frac{f(x)}{g(x)} = \frac{a_0 + a_1x + a_2x^2 + a_3x^3}{b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4},$$

где $b_0 = 1, b_1 = -4, b_2 = 6, b_3 = -4, b_4 = 1$, и $a_0 = b_0c_0 = 1$, $a_1 = b_0c_1 + b_1c_0 = 1\cdot(m+2) + (-4)\cdot 1 = m-2$, $a_2 = b_0c_2 + b_1c_1 + b_2c_0 = 1\cdot(4m+3) + (-4)(m+2) + 6\cdot 1 = 1$, $a_3 = b_0c_3 + b_1c_2 + b_2c_1 + b_3c_0 = 1\cdot(10m+4) + (-4)(4m+3) + 6(m+2) + (-4)\cdot 1 = 0$. Так как $g(x) = 1 - 4x + 6x^2 - 4x^3 + x^4 = (1-x)^4$ имеет 4 совпавших корня $x_1 = \ldots = x_4 = 1$, производящая функция имеет вид

$$\frac{1 + (m-2)x + x^2}{(1-x)^4} = CS_m^3(1) + CS_m^3(2)x + CS_m^3(3)x^2 + \ldots + CS_m^3(n)x^{n-1} + \ldots,\ |x| < 1.$$

Этот результат может быть получен также с помощью производящей функции $\frac{1+(m-2)x+x^2}{(1-x)^3}$ для центрированных m-угольных чисел и разложения $\frac{1}{1-x} = 1+x+x^2+\ldots+x^n+\ldots$. Именно, $\frac{1+(m-2)x+x^2}{(1-x)^4} = \frac{1+(m-3)x}{(1-x)^3}\cdot\frac{1}{1-x} = (CS_m(1)+CS_m(2)x+CS_m(3)x^2+\ldots+CS_m(n)x^{n-1}+\ldots)(1+x+$ $+x^2+\ldots+x^n+\ldots) = CS_m(1)+(CS_m(1)+CS_m(2))x+(CS_m(1)+CS_m(2)+CS_m(3))x^2+\ldots+$ $+(CS_m(1)+\ldots+CS_m(n))x^{n-1}+\ldots = CS^3_m(1)+CS^3_m(2)x+CS^3_m(3)x^2+\ldots+CS^3_m(n)x^{n-1}+\ldots$, $|x|<1$. □

3.6. Построение центрированных m-пирамидальных чисел аналогично построению обычных m-угольных пирамидальных чисел. Однако любое центрированное m-пирамидальное число может рассматриваться как конфигурация точек, образованных центральной точкой, окруженных пирамидальными слоями. В этом смысле они образуют класс центрированных фигурных чисел. Естественный "центр" n-ого центрированного m-пирамидального числа – центральная точка n-го центрированного m-угольного числа, образующего основание соответствующей пирамиды. Эта центральная точка окружена пирамидальными слоями. Каждый слой представляет собой k-ое m-угольное пирамидальное число (с $k = 1,3,\ldots,n$) без внутренности; более того, его основание также не имеет внутренности.

Например, первый уровень центрированного 3-пирамидального числа является просто центральной точкой его основания. 2-ой уровень образован из 4 точек; он соответствует 2-му тетраэдральному числу $S^3_3(2) = 4$ без пустой внутренности; его основание – 2-ое треугольное число без пустой внутренности. Аналогично, 3-ий уровень состоит из 10 точек. Он соответствует 3-му тетраэдральному числу $S^3_3(3) = 10$ без пустой внутренности; его основание – 3-е треугольное число 6 без пустой внутренности. 4-ый уровень формируется из 19 точек. Он соответствует 4-ому тетраэдральному числу $S^3_3(4) = 20$ без пустой внутренности; его основание – 4-ое треугольное число 10 без 1-точечной внутренности. 5-ый уровень формируется из 31 точки. Он соответствует 5-му тетраэдральному числу $S^3_3(5) = 35$ без 1-точечной внутренности; его основание – 5-ое треугольное число 15 без 3-точечной внутренности, и т.д.

Таким образом, число точек в k-ом уровне равно $S^3_3(k) - S^3_3(k-3)$, $k \geq 4$.

Это означает, что центрированные 3-пирамидальные числа являются частичными суммами ряда

$$S^3_3(1), S^3_3(2), S^3_3(3), S^3_3(4)-S^3_3(1), S^3_3(5)-S^3_3(2), \ldots, S^3_3(n+3)-S^3_3(n), \ldots .$$

Следовательно,

$$CS^3_3(1) = CS^3_3(1) = 1,\ CS^3_3(2) = S^3_3(2)+S^3_3(1) = 5,\ CS^3_3(n) = S^3_3(n)+S^3_3(n-1)+S^3_3(n-2), n \geq 3.$$

Таким образом,

$$\overline{S}^3_3(1) = CS^3_3(1),\ \overline{S}^3_3(2) = CS^3_3(2),\ \overline{S}^3_3(3) = CS^3_3(3),\ \overline{S}^3_3(n) = CS^3_3(n) + S^3_3(n-3),\ n \geq 4.$$

Аналогично, центрированные 4-пирамидальные числа являются частичными суммами ряда

$$S^3_4(1), S^3_4(2), S^3_4(3)-S^3_4(1), S^3_4(4)-S^3_4(2), S^3_4(5)-S^3_4(3), \ldots, S^3_4(n+2)-S^3_4(n), \ldots .$$

Таким образом,

$$CS^3_4(1) = CS^3_4(1) = 1,\ CS^3_4(n) = S^3_4(n) + S^3_4(n-1),\ n \geq 2.$$

Следовательно, имеет место соотношение

$$\overline{S}^3_4(1) = CS^3_4(1),\ \overline{S}^3_4(2) = CS^3_4(2),\ \overline{S}^3_4(n) = CS^3_4(n) + S^3_4(n-2),\ n \geq 3.$$

3.7. *Призматические числа* (точнее, *m-гранные призматические числа*) соответствуют правильной прямой m-призме: многограннику, образованному двумя конгруэнтными правильными m-угольниками (основания) и m прямоугольниками (боковые грани). Они получаются путем сложения нескольких конгруэнтных копий центрированного m-угольного числа.

Так, n-ое *шестигранное призматичское число* может быть получено как сумма n копий n-го центрированного шестиугольного числа $CS_6(n)$; оно имеет вид

$$PCS_6(n) = nCS_6(n) = n(3n^2 - 3n + 1).$$

Данная последовательность начинается с чисел 1, 14, 57, 148, 305, 546, 889, 1352, 1953, ...(Sloane's A005915). Шестигранные призматичские числа можно рассматривать в форме $\frac{1}{6}(18n^3 - 18n^2 + 6n)$, что совпадает со структурированными ромбододекаэдральными числами.

Рекуррентная формула последовательности имеет вид

$$PCS_6(n+1) = PCS_6(n) + (9n^2 + 3n + 1),\ PCS_6(1) = 1.$$

□ Это следует, например, из рекуррентной формулы $CS_6(n+1) = PCS_6(n)+6n$ для центрированных шестиугольных чисел. Именно, $PCS_6(n+1) = (n+1)CS_6(n+1) = (n+1)(CS_6(n)+ +6n) = nCS_6(n)+CS_6(n)+6n(n+1) = nCS_6(n)+(3n^2-3n+1)+6n(n+1) = PCS_6(n)+(9n^2+3n+ +1)$. □

Производящая функция последовательности $PCS_6(1)$, $PCS_6(2)$, ..., $PCS_6(n)$, ... имеет вид $f(x) = \frac{x(1+10x+7x^2)}{(1-x)^4}$, то есть, имеет место разложение

$$\frac{x(1+10x+7x^2)}{(1-x)^4} = PCS_6(1)x + PCS_6(2)x^2 + PCS_6(3)x^3 + \ldots + PCS_6(n)x^n + \ldots,\ |x| < 1.$$

□ Этот факт может быть получен стандартной процедурой (см. [4]), приводящей к линейному рекуррентному уравнению $PCS_6(n+4) - 4PCS_6(n+3) + 6PCS_6(n+2) - 4PCS_6(n+1) + + PCS_6(n) = 0$ с начальными значениями $PCS_6(1) = 1$, $PCS_6(2) = 14$, $PCS_6(3) = 57$ и $PCS_6(1) = 148$. □

4. Рекуррентные процедуры для дружественных чисел

4.1. Простой конструктивный способ получения новых *дружественных пар* из данной пары можно получить, используя известное *правило Боро* (см. [3]):

• *если известна дружественная пара ($X = a \cdot u$, $Y = a \cdot s$), где s – простое, $(a, us) = 1$, $p = u + s + 1$ – простое, и a не делится на p, то пара $(M = X \cdot p^n \cdot q_1, N = a \cdot p^n \cdot q_2)$ является дружественной для всех $n = 1, 2, 3, \ldots$, таких что $q_1 = (u+1) \cdot p^n - 1$ и $q_2 = (u+1) \cdot (s+1) \cdot p^n - 1$ – простые.*

Соответствующий рекуррентный алгоритм поиска новых дружественных пар на отрезке $[A, B]$ представлен ниже:

- выберем дружественную пару $(X = a \cdot u, Y = a \cdot s)$ с простым s и $(a, us) = 1$;
- найдем $p = u + s + 1$;
- если p простое и $(p, a) = 1$, то рассмотрим все n от A до B;
- для данного n от A до B найдем

$$q_1 = (u+1) \cdot p^n - 1,\ q_2 = (u+1) \cdot (s+1) \cdot p^n - 1;$$

- если q_1, q_2 простые, то найдем $M = Xp^n q_1, N = ap^n q_2$ и объявим пару (M, N) дружественной.

4.2. В 1984 году Те Риле предложил новый алгебраический конструктивный метод поиска новых дружественных пар. *Правило Риле* (см. [11]) утверждает, что:

• *если* $(M', N') = (a \cdot u, a \cdot p)$ *– дружественная пара с* $(a, p) = 1$, *где* p *– простое; если существует пара* (r, s) *простых чисел с* $p < r < s$ *и* $(a, rs) = 1$, *удовлетворяющая билинейному диофантову уравнению*

$$(r - p)(s - p) = (p + 1)(p + u),$$

и если существует третье простое число q *с* $(au, q) = 1$, *такое что* $q = r + s + u$, *то пара* $(M = a \cdot u \cdot q, N = a \cdot r \cdot s)$ *является дружественной.*

Так, выбрав пару $(3^2 \cdot 5^3 \cdot 13 \cdot 59, 3^2 \cdot 5^3 \cdot 13 \cdot 18719)$, мы имеем $a = 3^2 \cdot 5 \cdot 13$, $u = 5^2 \cdot 11 \cdot 59 = 16225$, $p = 18719$, и после факторизации получаем $(p + 1)(p + u) = 2^{12}3^3 \cdot 5 \cdot 7 \cdot 13^2$. Записав $(p + 1)(p + u)$ как $2688 \cdot 243360$, мы получим три простых $r = 18719 + 2688 = 21407$, $s = 18719 + 243360 = 262079$, $q = 21407 + 262079 + 16225 = 299711$, и, следовательно, дружественную пару

$$(3^2 \cdot 5^3 \cdot 13 \cdot 11 \cdot 59 \cdot 299711, 3^2 \cdot 5^3 \cdot 13 \cdot 21407 \cdot 262079).$$

Вторую дружественную пару получим, записав $(p + 1)(p + u)$ как $3120 \cdot 20964$.

4.3. В 1968 году Ли предложил общий алгебраический метод построения дружественных пар. Он основывается на очевидном факте, состоящем в том, что любая дружественная пара может быть записана в форме $(M = a_1 \cdot p \cdot q, N = a_2 \cdot r)$, где $(a_1, p) = (a_1, q) = (a_2, r) = 1$.

Для заданных a_1 и a_2 метод Ли (см. [11]) позволят найти все возможные значения p, q, r, используя все возможные разложения $X \cdot Y$ величины $\sigma(a_2)(a_1 a_2 \sigma(a_2) + \sigma(a_1)(a_1 - a_2)(a_1 - \sigma(a_2)))$.

4.4. Янь (см. [11]) в 1996 году предложил другой общий метод построения дружественных пар. Его алгоритм, начиная с пары $(M', N') = (a_1 p, a_2 q)$, использует заданные числа a_1, a_2 для вычисления константы $W = W(a_1, a_2)$. После полной факторизации W следует рассмотреть все возможные разложения $W = UV, U < V$. Для каждой комбинации $W = UV, U < V$, вычислим $q_1 = q_1(U, a_1, a_2)$, $q_2 = q_2(V, a_1, a_2)$, $p_1 = p_1(q_1, q_2, a_1, a_2)$. Если все три полученных числа q_1, q_2, p_1 простые, то, при условии выполнения дополнительных ограничений $q_1 \neq q_2$, $(a_2, q_1 q_2) = 1$, $(a_1, p_1) = 1$, мы получим новую дружественную пару $(M = a_1 \cdot p_1, N = a_2 \cdot q_1 \cdot q_2)$.

Подробное рассмотрение этих и других методов можно найти в [11]. Для получения дополнительной информации см., например, [3].

5. Псевдослучайные последовательности

5.1. Последовательности, генерируемые с помощью различных, как правило, арифметических алгоритмов, называются *псевдослучайными* [9]. Мы рассматриваем задачу построения псевдослучайных последовательностей, прежде всего, в связи с задачей получения последовательности, по свойствам близкой к случайной, имеющей очень большой период, для использования ее в качестве ключа шифрования, заменяющего одноразовый шифровальный блокнот.

Поскольку для кодирования любого множества сообщений достаточно алфавита из двух символов, можно использовать конечное поле $\mathbb{F}_2$, в котором суммирование принимает простейший вид: $0 + 0 = 1 + 1 = 0$, $1 + 0 = 0 + 1 = 1$.

Например, простейшим случаем рекуррентной последовательности, которую можно получить с помощью арифметическойх функции, является последовательность $\alpha_0 = 0$, $\alpha_1 = 1$, и $\alpha_{n+1} = \mathrm{rest}(\alpha_n + \alpha_{n-1}, 2)$ при любом натуральном n. заметим, что значения очень быстро начинают повторяться: $\alpha_n = 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, \ldots$.

5.2. Для генерации псевдослучайных последовательностей можно использовать многочлены над конечными полями. Рассмотрим основы теории таких построений [7], [9].

Пусть $S(\mathbb{F}_p) = \{\alpha = \{\alpha_n\}_n | n = 0, 1, 2, \ldots, \alpha_n \in F_p\}$ - множество всех последовательностей $\alpha = \{\alpha_n\}_n$ элементов поля $\mathbb{F}_p$.

Определим на множестве $S(\mathbb{F}_p)$ бинарную операцию $+$ и две унарные операции – *умножение на элемент с поля* $\mathbb{F}_p$ и *сдвиг* T:

$$\alpha + \beta = \{\alpha_n\}_n + \{\beta_n\}_n = \{\alpha_n + \beta_n\}_n;\ c\alpha = c\{\alpha_n\}_n = \{c\alpha_n\}_n,\ T \bullet \alpha = T \bullet \{\alpha_n\}_n = \{\alpha_{n+1}\}_n.$$

Нетрудно убедиться, что теперь множество $S(\mathbb{F}_p)$ образует векторное пространство над полем $\mathbb{F}_p$, замкнутое относительно сдвига.

С каждым многочленом $g(\lambda) = b_0 + b_1\lambda + b_2\lambda^2 + \ldots + b_k\lambda_k \in F_p[\lambda]$ сопоставим *полиномиальный оператор* g^T, определяемый по следующему закону:

$$g^T \bullet \alpha = g^T \bullet \{\alpha_n\}_n = \{\beta_n\}_n = \beta,$$

где, для любого целого неотрицательного n, $\beta_n = b_0 \cdot \alpha_n + b_1\alpha_{n+1} + b_2\alpha_{n+2} + \ldots + b_k\alpha_{n+k}$.

Полиномиальные операторы удовлетворяют свойствам:

1. $g^T \bullet (\alpha + \beta) = g^T \bullet \alpha + g^T \bullet \beta$.
2. $(g + f)^T \bullet \alpha = g^T \bullet \alpha + f^T \bullet \alpha$.
3. $g^T \bullet (h^T \bullet \alpha) = (gh)^T \bullet \alpha$.
4. $g(\lambda) \equiv h(\lambda) \Leftrightarrow \forall \alpha \in S\ g^T \bullet \alpha = h^T \bullet \alpha$.
5. Если $g(\lambda) = \lambda + 1$, то $g^T \bullet \alpha = T \bullet \alpha$.
6. Если $g(\lambda) \equiv c$, $c \in F_p$, то $g^T \bullet \alpha = c\alpha$.

Так если $g(\lambda) = \lambda^2 + \lambda + 1 \in F_2[\lambda]$, $\alpha = \{\alpha_n\}_n \in S(\mathbb{F}_2)$, то $g^T \bullet \alpha = g^T \bullet \{\alpha_n\}_n = \{\alpha_n + \alpha_{n+1} + \alpha_{n+2}\}_n$. Последовательность $\varepsilon = \{1\}_n$, состоящая из одних единиц (как и последовательность $\theta = \{0\}_n$, состоящая из одних нулей), перейдет при этом отображении в себя, а, например, последовательность $000100010001\ldots$ – в последовательность $101110111011\ldots$.

Многочлен $g(\lambda) = 1 + \lambda$ соответствует сдвигу T, переводя последовательность ε (как и последовательность θ) в себя, а последовательность $000100010001\ldots$ - в последовательность $001000100010\ldots$.

Многочлен $g(\lambda) \equiv c$ соответствует оператору умножения на элемент $c \in F_p$. Над полем $\mathbb{F}_2$ мы имеем ровно две возможности: при $c = 1$ оператор $g(\lambda) \equiv c$ переводит каждую последовательность в себя, в то время как при $c = 0$ оператор $g(\lambda) \equiv c$ переводит каждую последовательность в нулевую последовательность $\theta = \{0\}_n$.

Назовем уравнение вида

$$\delta_{x+n} = a_{n-1} \cdot \delta_{x+n-1} + a_{n-2} \cdot \delta_{x+n-2} + \ldots + a_0 \cdot \delta_x, \quad \text{где } a_i \in F_p,$$

линейным рекуррентным уравнением порядка n над полем F_p, а многочлен $f(\lambda) = \lambda^n - a_{n-1} \cdot \cdot \lambda^{n-1} - \ldots - a_0 \in F_p[x]$ - *характеристическим многочленом* этого уравнения.

Уравнение определяет линейную рекуррентную последовательность $\{\delta_x\}_x$ над полем F_p, которая называется *решением* данного линейного уравнения и однозначно определяется своими начальными членами $\delta_0, \delta_1, \ldots, \delta_{n-1}$.

Так, линейное рекуррентное уравнение второго порядка $\delta_{x+2} = \delta_{x+1} + \delta_x$ над полем F_2 отвечает характеристическому многочлену $f(\lambda) = \lambda^2 - \lambda - 1$. Решениями уравнения являются четыре последовательности, три из которых ненулевые. Все три ненулевые последовательности имеют период 3 и являются сдвигами друг друга.

x	0	1	2	3	4	5	6	...	
δ_x	0	0	0	0	0	0	0	...	$per\,\delta = 1$
δ_x	0	1	1	0	1	1	0	...	$per\,\delta = 3$
δ_x	1	0	1	1	0	1	1	...	$per\,\delta = 3$
δ_x	1	1	0	1	1	0	1	...	$per\,\delta = 3$

Линейное рекуррентное уравнение $\delta_{x+2} = \delta_x$ второго порядка над полем F_2 отвечает характеристическому многочлену $g(\lambda) = \lambda^2 - 1$. Как и в предыдущем случае, решениями уравнения являются четыре последовательности, три из которых ненулевые. Среди ненулевых последовательностей две имеют период 2, и одна - период 1. При этом последовательности, имеющие период 2, являются сдвигами друг друга.

x	0	1	2	3	4	5	6	...	
δ_x	0	0	0	0	0	0	0	...	$per\,\delta = 1$
δ_x	0	1	0	1	0	1	0	...	$per\,\delta = 2$
δ_x	1	0	1	0	1	0	1	...	$per\,\delta = 2$
δ_x	1	1	1	1	1	1	1	...	$per\,\delta = 1$

Рассматривая эти примеры, мы видим, что число решений линейного рекуррентного уравнения конечно, и каждое решение - периодично. Оба этих факта тривиальны. Поскольку решение линейного рекуррентного уравнения однозначно определяется начальным набором $\delta_0, \delta_1, \ldots, \delta_{n-1}$, и над полем $\mathbb{F}_p$ существует ровно p^n таких наборов, то *число* $|S(f)|$ *решений уравнения* $\delta_{x+n} = a_{n-1} \cdot \delta_{x+n-1} + a_{n-2} \cdot \delta_{x+n-2} + \ldots + a_0 \cdot \delta_x$, отвечающего характеристическому многочлену $f(\lambda) = \lambda^n - a_{n-1}\lambda^{n-1} - \ldots - a_0$, равно p^n.

Из конечности числа возможных наборов $(\delta_x, \delta_{x+1}, \ldots, \delta_{x+n-1})$ длины n над конечным полем $\mathbb{F}_p$ следует и периодичность линейных рекуррентных последовательностей: для любого решения $\delta = \{\delta_x\}_x \in S(f)$ линейного рекуррентного уравнения над полем $\mathbb{F}_p$, отвечающего характеристическому многочлену степени n, существует натуральное τ, такое что $\delta_x = \delta_{x+\tau}$ для любого целого неотрицательного x.

5.3. Наименьший натуральный период τ решения δ называется *примитивным периодом* решения δ и обозначается символом $per\ \delta$. Поскольку число ненулевых наборов $(\delta_x, \delta_{x+1}, \ldots, \delta_{x+n-1})$ длины n над конечным полем $\mathbb{F}_p$ равно $p^n - 1$, то наименьший натуральный период τ решения δ не превосходит $p^n - 1$.

Эти и другие свойства линейных рекуррентных последовательностей делают их необычайно полезными при решении практических криптографических задач [7], [9].

Поскольку множество $S(f)$ решений линейного рекуррентного уравнения, отвечающего характеристическому многочлену $f(\lambda) \in F_p[\lambda]$, замкнуто относительно сложения и умножения на элементы поля $\mathbb{F}_p$, то оно формирует векторное пространство над полем $\mathbb{F}_p$. Сопоставив каждой линейной рекуррентной последовательности $\delta = \{\delta_x\}_x$ вектор $(\delta_0, \delta_1, \ldots, \delta_n)$ ее начальных значений (полностью эту последовательность задающий), мы убедимся, что векторное пространство решений линейного рекуррентного уравнения над полем $\mathbb{F}_p$, отвечающего характеристическому многочлену степени n, изоморфно классическому n-мерному векторному пространству над полем $\mathbb{F}_p$.

5.4. Назовем решение $\delta = \{\delta_x\}_x$ линейного рекуррентного уравнения *главным*, если вместе со своими сдвигами оно образует базис пространства $S(f)$ всех решений данного линейного рекуррентного уравнения.

Максимальной линейной рекуррентной последовательностью порядка n назовем любое главное решение линейного рекуррентного уравнения порядка n.

Для рассмотренного выше линейного уравнения $\delta_{x+2} = \delta_{x+1} + \delta_x$ над полем $\mathbb{F}_2$, отвечающего характеристическому многочлену $f(\lambda) = \lambda^2 - \lambda - 1$, главным решением является любое ненулевое решение, так как все остальные ненулевые решения являются его сдвигами, а нулевое есть сумма всех этих сдвигов. Следовательно, каждое из указанных трех ненулевых решений является максимальной линейной рекуррентной последовательностью порядка 2.

Для уравнения $\delta_{x+2} = \delta_x$ над полем $\mathbb{F}_2$, отвечающего характеристическому многочлену $g(\lambda) = \lambda^2 - 1$, в качестве главных решений могут выступать только второе и третье решения. Четвертое (ненулевое) решение вместе со своими сдвигами не может породить все пространство решений, в то время как сумма второго и третьего (сдвига второго) дают нам четвертое

решение, а нулевое решение может быть получено путем сложения четвертого решения с его копией.

Многочлен $g(\lambda) \in F_2[\lambda]$ называют *аннулирующим последовательность* $\delta = \{\delta_n\}_n \in S(\mathbb{F}_p)$, если $g^T \bullet \delta = \theta$. Нормированный и наименьшей степени многочлен, аннулирующий $\delta = \{\delta_n\}_n \in \in S(\mathbb{F}_p)$, называют *минимальным многочленом последовательности* δ и обозначают символом $m_\delta(\lambda)$.

Нетрудно убедиться в том, что для нулевой последовательности $\theta = \{0\}_n$ любой многочлен будет аннулирующим, и, следовательно, $m_\theta(\lambda) \equiv 1$.

Для единичной последовательности $\varepsilon = \{1\}_n$ любой многочлен $\lambda^k - 1$, $k \in \mathbb{N}$, будет аннулирующим, и, следовательно, $m_\varepsilon(\lambda) = \lambda - 1$. Аналогичный результат можно получить для любой ненулевой последовательности-константы $\delta = \{\delta\}_n$.

Для последовательности $010101010101\ldots$ аннулирующим будет любой многочлен $\lambda^{2k} - 1$, $k \in \mathbb{N}$. Непосредственная проверка показывает, что минимальным многочленом данной последовательности будет многочлен $\lambda^2 - 1$. Вспомнив, что последовательность $010101010101\ldots$ является одним из решений линейного рекуррентного уравнения $\delta_{x+2} = \delta_x$, отвечающего характеристическому многочлену $f(\lambda) = \lambda^2 - 1$, мы замечаем, что минимальный многочлен одного из решений линейного рекуррентного уравнения $\delta_{x+2} = \delta_x$ совпадает с характеристическим многочленом данного линейного рекуррентного уравнения. Случайность ли это?

Для того, чтобы ответить на этот вопрос, рассмотрим поведение многочленов, аннулирующих линейные рекуррентные последовательности ([7], [9]).

Выделим ряд свойств аннулирующих многочленов.

1. Минимальный многочлен любого ненулевого решения $\delta \in S(f)$ является многочленом ненулевой степени: $\delta \neq \theta \Leftrightarrow deg\ m_\delta(\lambda) \geq 1$.

2. Если τ - примитивный период решения $\delta \in S(f)$, то многочлен $\lambda^\tau - 1$ является аннулирующим для решения $\delta \in S(f)$.

3. Характеристический многочлен линейного рекуррентного уравнения аннулирует любое решение этого уравнения.

4. Пусть $\delta \in S(\mathbb{F}_p)$, и $f(\lambda) = \lambda^n - a_1\lambda^{n-1} - \ldots - a_{n-1}\lambda - a_n$ - нормированный многочлен степени n над полем $\mathbb{F}_p$ с не равным нулю свободным членом. Оператор f^T аннулирует последовательность δ тогда и только тогда, когда δ - решение линейного рекуррентного уравнения с характеристическим многочленом f.

5. Многочлен g над полем $\mathbb{F}_p$ аннулирует последовательность $\delta \in S(\mathbb{F}_p)$ тогда и только тогда, когда g делится на минимальный многочлен последовательности δ (*основное свойство минимального многочлена*): $g^T \bullet \delta = \theta \Leftrightarrow m_\delta(\lambda) | g(\lambda)$.

6. Минимальный многочлен главного решения уравнения есть характеристический многочлен этого уравнения.

Изучая свойства аннулирующих многочленов, мы убеждаемся в том, что длина периода того или иного решения δ линейного рекуррентного уравнения над полем $\mathbb{F}_p$ с характеристическим многочленом $f(\lambda)$ степени n зависит как от свойств самой последовательности δ – для практических целей целесообразно использовать главные решения линейного рекуррентного уравнения, – так и от свойств характеристического многочлена $f(\lambda)$.

Поэтому необходимо внимательнее отнестись к многочленам, порождающим последовательности, и исследовать их свойства.

5.5. Многочлен $f(x) \in F[x]$ называется *неприводимым* над полем $\mathbb{F}$ (или в кольце $\mathbb{F}[x]$), если $deg\, f(x) > 0$, и из разложения $f(x) = g(x) \cdot h(x)$, где $g(x), h(x) \in F[x]$, следует, что либо $g(x)$, либо $h(x)$ - многочлен нулевой степени.

В остальных случаях многочлен положительной степени $f(x) \in F[x]$ называется *приводимым* над $\mathbb{F}$ (или в $\mathbb{F}[x]$): для приводимого многочлена существует хотя бы одно разложение $f(x) = g(x) \cdot h(x)$, где $g(x), h(x) \in F[x]$, $deg\ g(x) > 0$, и $deg\ h(x) > 0$.

Ясно, что многочлен первой степени всегда неприводим.

Рассмотрим многочлены второй степени над полем $\mathbb{F}_2$. Их всего четыре: $x^2 + x + 1$, $x^2 + x$ $x^2 + 1$, x^2. Многочлены $x^2 + x = x(x + 1)$, $x^2 + 1 = (x + 1)^2$ и $x^2 = x \cdot x$ приводимы. Многочлен $f(x) = x^2 + x + 1$ неприводим: если бы он раскладывался на нетривиальные множители, то каждый из этих множителей имел бы степень 1, а, следовательно, многочлен $f(x) = x^2 + x + 1$ имел бы корень в $\mathbb{F}_2$, однако $f(0) = f(1) = 1 \neq 0$.

Обратим внимание, что в рассмотренных выше примерах решения уравнений имели разные периоды; максимально возможный период имели решения рекуррентного уравнения, заданного именно неприводимым характеристическим многочленом

Найдем все неприводимые многочлены степени 3 над $\mathbb{F}_2$. Многочлены третьей степени имеют вид $a_3x^3 + a_2x^2 + a_1x + a_0$, где $a_1 \in \{1, 0\}$. Очевидно, $a_3 = 1$, и мы получаем ровно 8 многочленов, однако, если исключить очевидно приводимые многочлены с $a_0 = 0$, то останется всего 4 многочлена: $x^3 + x^2 + x + 1$, $x^3 + x + 1$, $x^3 + x^2 + 1$, $x^3 + 1$.

Для многочлена третьей степени нетривиальное разложение обязательно будет содержать множители первой и второй степени, следовательно, у приводимых многочленов должны быть корни, в частности, для многочленов из нашего списка - корень, равный единице. Непосредственная проверка показывает, что неприводимыми будут лишь многочлены $x^3 + x + 1$ и $x^3 + x^2 + 1$.

Продолжая исследование, мы получим что, неприводимыми многочленами четвертой степени над $\mathbb{F}_2$ являются многочлены $x^4 + x^3 + 1$, $x^4 + x + 1$, $x^4 + x^3 + x^2 + x + 1$, и только они.

Для поиска всех неприводимых многочленов заданной степени полезно знать, что число $a_p(n)$ неприводимых над полем $\mathbb{F}_p$ многочленов степени n вычисляется (см. [9]) по формуле

$$a_p(n) = \frac{1}{n} \sum_{m|n} p^{\frac{n}{m}} \mu(m), \text{ где } \mu(n) - \textit{функция Мебиуса}.$$

Таким образом, для всякого простого p и для всякого натурального n существуют неприводимые многочлены над полем $\mathbb{F}_p$ степени n.

Напоминим (см. [1]), что *функция Мебиуса* $\mu(n)$ определена для всех натуральных n и принимает значения из множества $\{-1, 0, 1\}$ в зависимости от разложения n на простые множители: $\mu(n) = 1$, если n - бесквадратное число с четным числом простых делителей; $\mu(n) = -1$, если n - бесквадратное число с нечетным числом простых делителей; $\mu(n) = 0$, если n не является бесквадратным ([1]).

Поскольку $\mu(1) = 1$, $\mu(3) = -1$, то

$$a_2(3) = \frac{1}{3} \sum_{m|n} p^{\frac{n}{m}} \mu(m) = \frac{1}{3} \left(2^{\frac{3}{1}} \mu(1) + 2^{\frac{3}{3}} \mu(3) \right) = \frac{1}{3} \left(2^3 \cdot 1 + 2^1 \cdot (-1) \right) = \frac{1}{3}(8 - 2) = 2.$$

Таким образом, над $\mathbb{F}_2$ имеется ровно два нормированных и неприводимых многочлена степени 3, и мы их нашли: это многочлены $x^3 + x^2 + 1$ и $x^3 + x + 1$.

5.6. Не ограничивая общности, будем считать, что $f \in F_p[x]$ - нормированный многочлен над полем F_p ненулевой степени n, и $f(0) \neq 0$ [9].

В этом случае среди p^n многочленов $1, x, x^2, x^{p^n-1}$, заведомо не делящихся на f (и, следовательно, имеющих ненулевые остатки при делении на f), найдутся два сравнимых по модулю $f(x)$. Таким образом, $f|(x^i - x^j)$, то есть $f|x^j(x^{i-j} - 1)$. Следовательно, в наших условиях $f|(x^{i-j} - 1)$, причем $1 \leq i - j \leq p^n - 1$.

Другими словами, любой нормированный многочлен $f \in F_p[x]$ ненулевой степени n, такой что $f(0) \neq 0$, делит многочлен $x^\delta - 1$ при некотором натуральном δ, $1 \leq \delta \leq p^n - 1$.

Наименьшее натуральное число δ, такое что $f|(x^\delta-1)$, будем называть *порядком многочлена* f, и обозначать символом $ord\ f(x)$. (Если $f(0)=0$, то представим его в виде $f(x)=x^\alpha g(x)$, $g(0)\neq 0$, и назовем порядком $f(x)$ порядок многочлена $g(x)$.)

Для определения порядка многочлена укажем ряд его важных практических свойств.

1. $1 \leq ord\ f(x) \leq p^n-1$.
2. $f(x)|(x^m-1)$ тогда и только тогда, когда $ord\, f(x)|m$.
3. Порядок многочлена f над полем $\mathbb{F}_p$ равен порядку этого многочлена над любым расширением поля $\mathbb{F}_p$.
4. $ord\, f(x)|(p^n-1)$, если $f(x)\in F_p[x]$ - неприводимый многочлен.
5. $ord\,(f(x))^n = p^t ord\, f(x)$, где t - наименьшее целое число, такое что $p^t \geq n$, и $f(x)\in F_p[x]$ - неприводимый многочлен.
6. Если $(g_i(x), g_j(x))=1$ для $i\neq j$, то $ord\,(g_1(x)\cdot g_2(x)\cdot\ldots\cdot g_k(x)) = [ord\, g_1(x),\ldots, ord\, g_k(x)]$.
7. Если $f(x) = f_1^{m_1}(x)\cdot\ldots\cdot f_k^{m_k}(x)$, где $f_i\in F_p[x]$ - неприводимые многочлены, то $ord\, f(x) = p^t[ord\, f_1(x),\ldots, ord\, f_k(x)]$, где t - наименьшее целое число, такое что $p^t \geq \max\{m_1,\ldots,m_k\}$.

Например, найдем порядок многочлена $f(x)=(x^2+x+1)^3(x^4+x+1)(x^3+1)$ над полем $\mathbb{F}_2$.

Как было доказано ранее, многочлены x^2+x+1 и x^4+x+1 неприводимы. С другой стороны, многочлен x^3+1 приводим: $x^3+1=(x+1)(x^2+x+1)$. Таким образом, $f(x)=(x^2+x+1)^4(x^4+x+1)(x+1)$.

По свойствам порядка многочлена, $ord\, f(x) = 2^t[ord\,(x^2+x+1), ord\,(x^4+x+1), ord\,(x+1)]$.

1. $ord\,(x^2+x+1)|(2^2-1)$, $ord\,(x^2+x+1)\neq 1$, следовательно, $ord\,(x^2+x+1)=3$.

2. $ord\,(x^4+x+1)|(2^4-1)=15$, то есть принадлежит множеству $\{1,3,5,15\}$. Непосредственная проверка показывает, что $x^4+x+1 \nmid (x^1-1)$, $x^4+x+1\nmid (x^3-1)$, $x^4+x+1\nmid (x^5-1)$ (при делении многочлена на многочлен мы получаем, что $x^5-1=(x^4+x+1)\cdot x+(x^2+x+1)$). Таким образом, $ord\,(x^4+x+1)=15$.

3. $ord\,(x+1)|(2^1-1)=1$, то есть $ord\,(x+1)=1$.

Наибольшая из степеней вхождения многочленов в произведение $f(x)=(x^2+x+1)^4(x^4+x+1)(x+1)$ равна 4, то есть для нахождения t нужно рассмотреть соотношение $2^t\geq 4$, из которого следует, что $t=2$.

Таким образом, $ord\, f(x) = 2^2\cdot[3,15,1]=60$.

Заметим, что "суммарная" степень многочлена $f(x)$ равна 13, но $60\nmid 2^{13}-1$, то есть для приводимого многочлена $f(x)$ аналог свойства $ord\ f|(x^{p^{deg\ f}}-1)$, имеющего место для неприводимых многочленов, нарушен.

Отметим, что неприводимый над полем $\mathbb{F}_p$ многочлен степени n делит многочлен $x^{p^n}-x$. Из этого следует, что неприводимый над полем $\mathbb{F}_p$ многочлен степени n делит многочлен $x^{p^n-1}-1$.

5.7. Многочлен $f\in F_p[x]$ степени n над полем $\mathbb{F}_p$ называется *примитивным*, если $ord\,(f(x))=p^n-1$. Другими словами, примитивным мы называем многочлен, имеющий максимальный возможный порядок [9].

Ранее мы получили, что, над полем $\mathbb{F}_2$, $ord\,(x^2+x+1)=3=2^2-1$, $ord\,(x^4+x+1)=15=2^4-1$, $ord\,(x+1)=1=2^1-1$, и $f(x)=(x^2+x+1)^3(x^4+x+1)(x^3+1)=60\neq 2^{13}-1$. Отсюда следует, что первые три многочлена являются примитивными, а последний - нет.

Очевидно любой примитивный многочлен f над полем $\mathbb{F}_p$ неприводим над полем $\mathbb{F}_p$.

Число $b_p(n)$ примитивных многочленов степени n над полем $\mathbb{F}_p$ можно вычислить (см. [9]) по формуле

$$b_p(n) = \frac{\varphi(p^n-1)}{n} .$$

Следовательно, для любого простого числа p и любого натурального числа n существует примитивный над полем $\mathbb{F}_p$ многочлен степени n.

Найдем число примитивных многочленов 3 степени над $\mathbb{F}_2$: $b_2(3) = \frac{\varphi(2^3-1)}{3} = 2$. Таким образом, оба найденные ранее неприводимых многочлена x^3+x^2+1 и x^3+x+1 степени 3 над $\mathbb{F}_2$ являются примитивными и имеют порядок $2^3-1=7$.

Свяжем полученные результаты с о свойствами аннулирующих последовательностей.

1. Пусть $\delta \in S(f)$. Тогда $per\ \delta = ord\ m_\delta(\lambda)$.

2. Для главного решения δ линейного рекуррентного уравнения, отвечающего характеристическому многочлену $f(\lambda)$, $per\ \delta = ord\ f(\lambda)$.

3. Если характеристический многочлен $f(\lambda)$ линейного рекуррентного уравнения неприводим, то $f(\lambda) = m_\delta(\lambda)$ для любого ненулевого решения δ этого уравнения.

4. Если δ – ненулевое решение линейного рекуррентного уравнения с неприводимым характеристическим многочленом $f(\lambda)$, то $per\ \delta | (p^n-1)$, в частности, $per\ \delta = p^n-1$, если $f(\lambda)$ – примитивный многочлен.

Таким образом, если характеристический многочлен $f(\lambda)$, порождающий линейное рекуррентное уравнение, неприводим, то все ненулевые решения линейного рекуррентного уравнения становятся в некотором смысле “равноправными”, то есть нас может не заботить их оптимальный выбор. Если же, кроме того, многочлен примитивен, то генерируемые соответствующим линейным рекуррентным уравнением последовательности будут иметь максимально возможный период.

5.8. Рассмотрим уравнение $\delta_{x+5} = \delta_x + \delta_{x+3}$. Его характеристический многочлен имеет вид $f(\lambda) = \lambda^5 + \lambda^3 + 1$. Следовательно, период любого ненулевого решения заданного линейного рекуррентного уравнения должен быть равен 31.

Выбирая первоначальное заполнение $\delta_0 = 1$, $\delta_1 = 0$, $\delta_2 = 0$, $\delta_3 = 0$, $\delta_4 = 0$, получим периодическую последовательность 10000101011101100011111100110100100000 . . . . Непосредственная проверка показывает, что примитивный период этой последовательности равен 31. Это означает, что, шаг за шагом рассматривая 5-символьные наборы $(\delta_x, \delta_{x+1}, \delta_{x+2}, \delta_{x+3}, \delta_{x+4})$ элементов нашей последовательности для $x = 0$ (набор 10000), $x = 1$ (набор 00001), . . . , $x = 30$ (набор 01000), мы получим каждый ненулевой набор из пяти знаков 0 и 1 ровно один раз. Если с набором $(\delta_x, \delta_{x+1}, \delta_{x+2}, \delta_{x+3}, \delta_{x+4})$ сопоставить число $a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + a_3 \cdot 2^3 + a_4 \cdot 2^4$, то нашу линейную рекуррентную последовательность можно рассматривать и как последовательность чисел 1 16 8 20 10 21 26 29 14 23 27 13 6 3 17 24 28 30 31 15 7 19 25 12 22 11 5 18 9 4 2 . . . .

Нетрудно убедиться, что период этой последовательности равен 31, и каждое из чисел от 1 до 31 встречается на начальном отрезке последовательности ровно один раз.

Всего у уравнения $2^5 = 32$ решения, из них 31 ненулевое. При этом остальные ненулевые решения – это 30 различных сдвигов решения, полученного выше.

Так, работая над полем F_2 и имея в запасе примитивный многочлен степени 100 над F_2, мы имеем возможность, задавая вектор начальных условий относительно небольшой длины 100, получать на выходе последовательность, период которой $2^{100}-1$ необычайно велик. Это определяет высокую меру близости заданной псевдослучайной последовательности к случайной. При этом, учитывая, что имеется $b_2(100) = \frac{\varphi(2^{100}-1)}{100}$ различных примитивных многочленов

степени 100 над полем F_2, и каждый из них дает нам $2^{100}-1$ различных последовательностей, мы получаем серьезный арсенал ключей.

Еще одним техническим, но существенным преимуществом генерирования псевдослучайных последовательностей является необычайная простота технической реализации этого процесса, выражающаяся в использовании специальной электронной схемы: *регистра сдвига*, получающегося комбинацией ячеек памяти и сумматора, в котором происходит побитовое сложение приходящей на два имеющихся у него входа информации ([9]).

6. Заключение

Наш короткий обзор истории, теоретических основ и практических приложений рекуррентных числовых последовательностей позволяет утверждать, что данный раздел математической науки обладает высоким исследовательским потенциалом, позволяющим привлекать к самостоятельной творческой работе в этой области не только ученых и профессионалов-прикладников, но и относительно широкий контингент людей, интересующихся математикой, в том числе, безусловно, студентов-математиков, будущих педагогов.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Бухштаб А.А. Теория чисел. – М.: РиполКлассик, 2013.
2. Григорян Н.Е., Лопатухина Т.А. Феномен рекуррентности как системообразующий прецедентный признак образовательного дискурса // Актуальные исследования. 2019. № 3 (3).
3. Деза Е.И. Специальные числа натурального ряда. – М.: URSS, 2010.
4. Deza E.I., Deza M.M. Figurate numbers. – World Scientific Publishing Company, 2012.
5. Деза Е.И., Деза М.М. Фигурные числа. – М.: МЦНМО, 2016.
6. Deza E.I. Mersenne and Fermat Numbers. – World Scientific Publishing Company, 2021.
7. Деза Е.И., Котова Л.В. Введение в криптографию. – М.: URSS, 2018.
8. Деза Е.И., Модель Д.Л. Основы дискретной математики. – М.: URSS, 2010.
9. Нечаев В.И. Основы защиты информации. – М.: МГУ, 1999.
10. Sloane N.J.A., Plouffe S. The Encyclopedia of Integer Sequences. – San Diego: Academic Press, 1995.
11. Yan S.Y. Perfect, Amicable and Sociable Numbers. A Computational Approach. – World Scientific, 1996.

REFERENCES

1. Buchstab, A.A. 2013, “Number Theory”, *RipolKlassik*. (Russian)
2. Grigoryan, N.E., Lopatukhina, T.A. 2019, “The phenomenon of recurrence as a system-forming precedent sign of educational discourse”, *Actual research*, № 3 (3). (Russian)
3. Deza, E.I. 2010, “Special numbers of the natural series”, *URSS*. (Russian) ,

4. Deza, E.I., Deza, M.M. 2012, "Figurate numbers", *World Scientific Publishing Company.*

5. Deza, E.I. 2016, "Figurate numbers", *MCCME.* (Russian)

6. Deza, E.I. 2021, "Mersenne and Fermat Numbers", *World Scientific Publishing Company.*

7. Deza, E.I., Kotova, L.V. 2018, "Introduction to Cryptography", *URSS.* (Russian)

8. Deza, E.I., Model, D.L. 2010, "Basics of discrete mathematics", *URSS.* (Russian)

9. Nechaev, V.I. 1999, "Fundamentals of information security", *MGU.* (Russian)

10. Sloane N.J.A., Plouffe S. 1995, "The Encyclopedia of Integer Sequences", *San Diego: Academic Press.*

11. Yan, S.Y. 1996, "Perfect, Amicable and Sociable Numbers. A Computational Approach", *World Scientific Publishing Company.*

Получено 18.07.2022
Принято в печать 14.09.2022