МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра компьютерной алгебры и теории чисел

Арифметика M-ичных чисел

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 421 группы
направления 02.03.01 «Математика и компьютерные науки»

механико-математического факультета

Недельскина Олега Вячеславовича

Научный руководитель
зав. каф., к.ф.- м.н., доцент ____________________ А.М. Водолазов
подпись, дата

Зав. кафедрой
зав. каф., к.ф.- м.н., доцент ____________________ А.М. Водолазов
подпись, дата

Саратов 2023

Введение. В алгебре решаются множество различных видов задач для решения которых используются разные числа. Одними из таких являются M-ичные числа.

Изучение данной темы играет большую роль для работы с матрицами и числами двоичной, десятеричной и других систем счисления на отрезках, плоскостях и других пространств. Изучение арифметики M-ичных чисел позволяет активно применять теоретические знания при использовании тайлов и аттракторов, относительно недавно нашедшие себе применение в обработке информации.

Целью данной работы является изучение фундаментальных понятий, таких как М-ичные числа, аттракторы, тайл, основных теорем с целью дальнейшего прикладного применения.

В 1 главе рассмотрены основные понятия для работы с М-числами, множество векторов для данной матрицы, как разложить любой целый вектор по степеням матрицы, доказано существование и единственность разложения целых векторов, приведены примеры их реализации. Во 2 главе указаны свойства многомерного аналога для М-ичных чисел числа (-1), доказано существование разложения для вещественных векторов. В 3 главе дополнены основные понятия из 1 главы для работы с новыми выражениями, показаны объединения подобных копий, образов, аттрактов, подведены теоретические понятия для дальнейшей работы с тайлами.

Основное содержание работы.

Предложение 1.1.1 Пусть M - невырожденная, целочисленная матрица размера $d \times d$. Тогда множество $H(M) = Z^d \cap M[0,1)^d$ состоит из представителей каждого класса смежности.

Следствие 1.1.2. Множество $H(M)$ можно взять в качестве множества M-цифр. В некотором смысле такой выбор наиболее естественен, поскольку в одномерной m-ичной системе счисления набор цифр $\{0, 1, \dots, (m-1)\}$ можно рассматривать как множество $Z \cap m[0,1)$. Иногда бывает удобно в качестве множества M-цифр $D(M)$ взять векторы, лежащие на одной прямой. Если у матрицы M существует вектор $a \in Z^d$ такой, что у вектора

$$M^{-1}a = \left(\frac{a_1}{m}, \frac{a_2}{m}, \dots, \frac{a_d}{m}\right),\ a_1, \dots, a_d \in Z, \tag{1.2}$$

числа $a_1, \ldots, a_d$ взаимно просты, т.е. наибольший общий делитель (НОД) чисел $a_1, \ldots, a_d$ равен 1, то будем говорить, что для такой матрицы выполнено условие $(*)$. Условие $(*)$ выполнено, например, если у матрицы простой определитель (тогда в качестве вектора a можно взять любой не сравнимый с нулем вектор). Также условие $(*)$ выполнено, если из столбцов присоединенной матрицы M существует хотя бы один со взаимно простыми элементами. Не умаляя общности, можно считать, что координаты вектора $(M_{11}, M_{12}, \ldots, M_{1d})^T$ и вектор $a = e_1$ искомый. Условие $(*)$ заведомо не выполнено для целочисленных матриц, у которых НОД всех элементов не равен 1.

Предложение 1.1.3. Пусть M - матрица растяжения, такая что выполнено условие $(*)$. Тогда существует вектор $a \in Z^d$ такой, что множество

$$(a_M) = \{0, a, 2a, \ldots, (m-1)a\}$$

можно взять в качестве множества M-цифр $D(M)$.

Лемма 1.1.4. Пусть M - матрица растяжения, $D(M)$ - набор M-цифр. Тогда для любых $s_k \in D(M)$ и для всех $N \in \mathbb{N}$ имеем

$$\Big|\sum_{k=1}^{N} M^{-k} s_k\Big| \leq C_M,$$

где $C_M = \max\limits_{s \in D(M)} |s| \sum\limits_{k=1}^{+\infty} ||M^{-k}||$.

Определение 1.2.1. Назовем ненулевой вектор $z_0 \in Z^d$ зацикливающим вектором матрицы M длины r (соответствующим набору M-цифр $D(M)$), если

$$z_0 = M^r z_1 + M^{r-1} s_0 + M^{r-2} s_{r-1} + \ldots + s_1. \tag{1.4}$$

где r - это наименьшее число, для которого выполняется равенство.

Теорема 1.2.2. (О «девятках»). Пусть M- матрица растяжения, $D(M)$ - набор M-цифр, вектор z_0 - зацикливающий вида (1.4). Тогда

$$-z_0 = \sum_{l=0}^{\infty} M^{-lr} \sum_{k=1}^{r} M^k s_{r-k} = \sum_{l=1}^{\infty} M^{-l} y_l, \tag{1.5}$$

где $y_l = y_{rk+n} = s_{r-n} \in D(M)$, $n = 0, \ldots, r-1, k \in Z^d$.

Следствие 1.2.3. Пусть M - матрица растяжения. Тогда

$$|z_0| \leq C_M$$

для всех зацикливающих векторов z_0 матрицы M, где C_M - константа из леммы 1.1.4 .

Теорема 1.2.4. (О разложении целочисленных векторов). Пусть M - матрица растяжения, $D(M)$ - набор M-цифр. Тогда для любого $x \in Z^d$ существует представление

$$x = M^{N+1} z_0 + \sum_{k=0}^{N} M^k y_k, \tag{1.7}$$

где $N \in \mathbb{N}$, $y_0, \ldots, y_N \in D(M)$, а вектор $z_0 \in Z^d$ либо зацикливающий, либо нулевой. Кроме того, представление (1.7) единственно, если в случае $z_0 = 0$ исключить возможность $y_N = 0$(т.е. считать, что ищем разложение порядка $N-1$), а в случае, когда z_0 - зацикливающий вектор, считать, что M-цифра y_N не является соответствующей M-девяткой (т.е. в этом случае вектор Mz_0+s_0 надо заменить на z_1, где z_1 либо равен z_0 либо является другим вектором из цепочки зацикливающих векторов длины $r > 1$).

Предложение 1.2.5. Пусть $n \in Z$, $|n| > 1$ - основание системы счисления. Тогда если $n \neq 2$, то можно выбрать множество цифр $D(n)$ так, чтобы зацикливающие числа отсутствовали, и любое число $x \in Z$ можно было представить (единственным образом) в виде

$$x = \sum_{k=0}^{N} n^k d_k,$$

где $d_k \in D(n), k = 1, \ldots, N$.

Если $n = 2$, то при любом выборе множества цифр будет существовать зацикливающее число, а значит и «отрицательные» числа.

Лемма 1.2.6. Пусть n - основа одномерной системы счисления. Тогда можно выбрать «цифры» так, чтобы существовало $(n-1)$ зацикливающих векторов длины 1.

Следствие 1.2.7. Для любого $k,\ 1 \le k \le n-1$, можно выбрать множество цифр так, чтобы количество зацикливающих векторов равнялось k. Если $n \ne$ $\ne 2$, то k может быть равен нулю.

Следствие 1.2.8. Для любого $k,\ 1 \le k \le n-1$, можно выбрать множество цифр так, чтобы количество этих зацикливающих векторов равнялось k. Если $n \ne 2$, то k может быть равно нулю (предложение 1.2.5.). Возьмем в качестве множества цифр множество

$$D(n) = \{0, 1, \ldots, n-k-1, (n-1), 2(n-1), \ldots, k(n-1)\}.$$

При $n = 10$ выбор множества цифр $\{0, 9, 18, 27, 36, 45, 54, 63, 72, 81\}$ влечет 9 зацикливающих чисел

$$-1 = 10 \cdot (-1) + 9; \quad -2 = 10 \cdot (-2) + 18; \quad -3 = 10 \cdot (-3) + 27; \ldots;$$

выбор множества цифр $\{0, 1, 9, 18, 27, 36, 45, 54, 63\}$ влечет 7 зацикливающих чисел и т.д.

Теорема 2.0.1. (Обратная). Пусть M - матрица растяжения, $D(M)$ - набор M-цифр. Пусть целочисленный вектор z представим в виде $z =$ $= \sum_{l=1}^{\infty} M^{-1} y_l, y \in D(M)$. Тогда либо z - нулевой вектор и все M-цифры y_l равны нулю, либо вектор $-z$ - зацикливающий и M-цифры y_l расположены в заданном порядке и повторяются периодично (теорема 1.2.2).

Следствие 2.0.4. (О разложении нулевого вектора). Если

$$0 = \sum_{l=-\infty}^{N} M^l y_l, \quad y_l \in D(M),$$

то $y_l = 0$ для любого $l = N, N-1, \ldots$.

Следствие 2.0.5. (О единственности разложения целочисленных векторов). Если исключить случай бесконечного повторения M-девяток, то разложение целочисленных векторов по любым (положительным и/или отрицательным) степеням матриц M единственно.

Замечание 2.0.6. Об M-рациональных дробях. В одномерном случае при разложении рациональной дроби в десятичное разложение, дробь будет периодичной, начиная с некоторого места, например, $4/7 = 0,(571428)$; $7/65 = = 0,1(076923)$. По аналогии, называем M-рациональной дробью вектор, в M-разложении которого, начиная с некоторого места, M-цифры повторяются периодически:

$$M^{-1}d_1 + \ldots + M^{-n}d_n + M^{-n-1}d_1 + \ldots + M^{-2n}d_n + M^{-2n-1}d_1 + \\ + \ldots = (M^n - I_d)^{-1}g = \sum_{k=1}^{\infty} M^{-kn}g,$$

где $g = M^{n-1}d_1 + \ldots + Md_{n-1} + d_n$.

Теорема 2.1.1. (Существование). Пусть M - матрица растяжения, $D(M)$ - набор M-цифр. Тогда любой вектор $x \in R^d$ можно представить в виде

$$x = M^{N+1}z_0 + \sum_{l=-N}^{\infty} M^{-l}s_l, \ s_l \in D(M) \tag{2.5}$$

где $N \in \mathbb{N}$, а вектор z_0 либо зацикливающий, либо нулевой.

Свойства отрезка $\{0, 1\}$:

1) Самоподобие, то есть отрезок разбивается на две части, каждая из которых подобна исходной. Если обозначить отрезок $\{0, 1\}$ как G, тогда

$$G = \frac{1}{2}G \cup \frac{1}{2}(1 + G)$$

Сделали два аффинных преобразования - это сжатие относительно нуля и сжатие относительно единицы, оба в два, так как система счисления равна двойке.

2) Тайлинг $\bigcup\limits_{k \in Z}(G + k)$ сумма параллельных сдвигов отрезка есть вся прямая.

Определение 3.0.1. Единичный отрезок в M-ичной системе счисления, так же как в двоичной, есть множество всех M-ичных дробей со старшей цифрой 0. $G = \{0, s_1, \ldots, s_k, \ldots, |$, где любое $s_j \in D\}$.Иначе говоря $0, s_1, \ldots, s_k = \sum\limits_{k=1}^{\infty} M^{-k} s_k$, получилась бесконечная сумма, в которой любой коэффициент принадлежит множеству цифр, в частности, если определить матрицу +-2, то получится двухциферная система, то есть либо 0, либо одна какая-то цифра, которая не сравнима с 0. Иногда очевидная система цифр таковой не оказывается, например если рассмотреть матрицу $M = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$ $D = \{d_0, d_1\}, d_0 = (0, 0)$, а в качестве d_1 возьмем вектор e_1, то есть $d_1 = (1, 0)$, так делать нельзя, $(1, 0)$ принадлежит той же самой подрешетке, которой принадлежит $(0, 0)$, потому что $d_1 - d_0$ есть $(1, 0) = M \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, получается что этот базисный вектор принадлежит MZ^2, поэтому это не цифра, в данном случае цифрой будет e_2 $d - 2 = (0, 1)$, сразу этот выбор бывает интуитивно не понятен, надо проверять, может заданная точка быть цифрой или нет.

Предложение 3.0.2. Ряд сходится => $||M^{-k}|| \to 0, \quad k \to \infty$. Если А - линейный оператор, то его нормой называется максимальная длина образа, максимальное растяжение, которое эта матрица A делает с вектором $||A|| = \max\limits_{|x|=1} |Ax|$, при том что x находится на единичной окружности. Наиболее удаленная точка эллипса, в данном случае, будет нормой матрицы(длина полуоси). Норма обладает свойством $||A|| \cdot ||B|| \geq ||AB||$. Отсюда получается что $||A^k|| \leq ||A||^k$. A - сжимающее => $||A||^k \to 0$, сжимающее означает что $||A|| < 1$, поэтому очевидным и достаточным условием следует что $||M^{-1}||$ - сжимающее, тогда все хорошо, сжимающая - это значит что она единичный круг переводит в себя строго внутрь. Неприятность здесь состоит в том, что сжимающей она никогда не будет.

Теорема 3.1.1. Вектор называется собственным, если он переходит в коллинеарный вектор. Пусть v_1 и v_2 - собственные вектора $Mv_1 = \lambda v_2$. Собственное значение может быть отрицательным, тогда вектор перевернется. Если матрица имеет два собственных вектора, тогда она может быть записана в этих самых векторах.

$$v_1 = \lambda_1 v_2$$

$$Mv_2 = \lambda_2 v_2$$

В этом случае, можно любой вектор разложить в новом базисе и записать как $x = \alpha_1 v_1 + \alpha_2 v_2$, где α_1 и α_2 - это коэффициенты по которым разложили точку x. Если теперь применять k-ую степень к вектору x, получится $M^{-k}x = \alpha_1 \lambda_1^k v_1 + \alpha_2 \lambda_2^k v_2$. Теперь сразу можно понять когда k-ая степень стремится к нулю, стремиться ровно в тех случаях, когда степени λ_1^{-k} и λ_2^{-k} будут стремиться к нулю. Значит модули собственных значений должны быть строго меньше единицы $|\lambda_1| < 1, |\lambda_2| < 1$.

Определение 3.2.1. Множество G является объединением своих подобных копий, причем эти копии устроены так, что $M^{-1} \cdot (x + d_j)$, множества будут отличаться лишь сдвигами на различные вектора.

Определение 3.2.2. Покрытие - это одинаковое множество, отличающееся только параллельным переносом и каждое из них подобно исходному множеству G. Точка $x = M^{-1}s_1 + M^{-2}s_2 + M^{-3}s_3 + \ldots$, s может быть любая цифра, они независимо принимают каждое M значений, в частности начало координат будет если все положить равное нулю, то есть начало координат всегда входит во множество G, преобразуем.

$$x = M^{-1}s_1 + M^{-2}s_2 + M^{-3}s_3 + \ldots \equiv M^{-1}(s_1 + z) = A_j z \qquad (3.1)$$

$M^{-2}s_2 + M^{-3}s_3 \equiv M^{-1}z, \quad z \in G$, $s_1 = d_j$, s_1 равно какому-то d_j, зависит от цифры s_1 какой оператор будет A_j. Каждую точку множества (3.1) можно представить в виде $A_j z$. Это означает что все такие множества $A_j z$ покрывают все множество G, то есть $G \subset \bigcup\limits_{j=0}^{m-1} A_j G$. Условно отбрасываем левую часть выражения (3.1). Возьмем произвольную точку z в которой есть M-ичное разложение и подставляем в формулу $M^{-1}(s_1 + z)$ получится $A_j z$, но раскрыть скобки, то получим разложение той же точки с другими цифрами, то есть ту же самую строку прочли в обратном направлении и получилось что какую бы точку из G не взять, образ ее под действием преобразования

$A_j z$ тоже будет лежать G, так что это отображение сюрьективно, то есть оно покрывает все множество $G => G = \bigcup\limits_{j=0}^{m-1} A_j G$.

Теорема 3.3.1.Аттрактор - это компактное множество. Можно написать разложение в другом виде, теперь определение аттракторов можно дать с помощью операторов $A_j G$. Есть разбиение задаваемое преобразованием $A_j G$, раз каждый элемент подобен исходному, значит у него тоже есть разбиение. Берем все разбиение, отображение аффинное, которое переводит весь аттрактор допустим в нижнюю часть множества, соответственно со всем отображением точно так же, дробит ее на отдельные кусочки, потом их взять и проделать с ними те же действия и так далее. Если взять любую точку внутри этого аттрактора, то она оказывается в одной из частей, после этого берем эту часть и дальше дробим ее, точка оказывается в одной из частей и получается что в пределе получается эта точка. Части могут не совпадать, они могут быть выбрано неоднозначно, потому что можно оказаться на границе, на границе может сходиться их много, как минимум могут быть три такие точки, так что у точек лежащих на границе этих множеств три разложения, можно взять любое, это не имеет значения. Если сейчас выписать конечную сумму $0, s_1, \ldots, s_n = \sum\limits_{k=1}^{n} M^{-k} s_k$ - эта сумма конечная, если $k \to \infty$, то получаем точку аттрактора. Эту конечную сумму можно представить в виде композиции преобразований A:

$$0, s_1, \ldots, s_n = \sum_{k=1}^{n} M^{-k} s_k = A_{s_1}, \ldots A_{s_n} d_0 \tag{3.2}$$

s_1 не ясно что это за цифра, однако все это может быть применено к нулю, ноль тоже цифра d_0. В умножении на нуль, нуль выступает как начало координат, а преобразование аффинное так что эту точку куда-то переводит.

Определение 3.3.3. Если $n = 1 <=> \{G + k | k \in Z^2\}$ - разбиение R^2. Для того чтобы покрытие было в один слой они образовывали обычное покрытие, разбиение, замощение, они все параллельны друг другу, так что это именно замощение, тайлинг параллельными друг другу множествами. Тогда G -

тайл, а вся совокупность его целых сдвигов - это тайлинг всей плоскости. Получается что чтобы отличить тайл от не тайла нужно оценить его площадь.
Заключение. В этой работе рассмотрены основные понятия М-чисел, множества векторов для работы с матрицами, собственных векторов, их разложения, методы подсчета, арифметика этих чисел и их реализация. Были определены и посчитаны факторгруппы, объединения, тайлы.

Арифметика М-ичных чисел является одним из перспективных направлений для изучения, множество открытых проблем и нерешенных задач показывают что есть куда стремиться в этом направлении.

Посчитанные и доказанные понятия позволяют начать применять теоретический багаж знаний в практическом применении различных задач, например в задачах инженерии, передачи источников информации, сжатия изображений, построения компьютерной графики.