Литература

1. Robert C. Martin. Clean Code. A Handbook of Agile Software Craftsmanship. Pearson Education, Inc, 2009. – 462 p.

2. Prykhodko S.B. Developing the software defect prediction models using regression analysis based on normalizing transformations / S. B. Prykhodko // Modern Problems in Testing of the Applied Software : the Research and Practice Seminar (PTTAS-2016), Poltava, Ukraine, May 25–26, 2016 : abstracts. – P. 6–7.

УДК 519.7 **Information Control Systems and Technologies, pp. 217-221**

К.т.н. Востров Г.М., Колесниченко В.Ю.

ТОПОЛОГІЧНІ ТА АЛГЕБРАЇЧНІ ГРУПИ КОНГРУЕНТНИХ НЕЛІНІЙНИХ ДИНАМІЧНИХ СИСТЕМ

Ph.D. Vostrov G., Kolesnichenko V.

TOPOLOGIC AND ALGEBRAIC GROUPS OF CONGRUENT NON-LINEAR DYNAMIC SYSTEMS

Анотація. Роздивимося алгебраїчні динамічні системи на основі теорії лишків за модулем простих чисел та їх узагальнення на скінчеві поля. Досліджена конгруентність нелінійних динамічних систем на інтервалі (0,1). Встановлено, що алгебраїчні динамічні системи однозначно описуються групами $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ за модулем простого числа. Доведено, що деякі класи конгруентних нелінійних динамічних систем характеризуються деякими класами топологічних груп безперервних відображень. Досліджені особливості траекторій нерухомих точок конгруентних нелінійних динамічних систем.

Незважаючи на активні дослідження нелінійних динамічних систем [1] в останні два дисятиліття, кількість невирішених математичних проблем не тільки не зменшується, а навпаки, стабільно зростає. До числа таких задач відноситься дослідження структури траекторій нерухомих точок динамічних систем. З теорії Шарковського [2] про впорядковані нерухомі точки за довжиною траекторій випливає, що якщо динамічна система має хоча б одну нерухому точку з довжиною траекторії три, то це приводить до існування, в заданій динамічній системі, нерухомих точок з будь-якою довжиною траекторії.

Такі траєкторії зазвичай тракують як хаотичний стан динамічної системи. Визначення «хаос» дають як процес розвитку нестійкого стану, що має стохастичну природу. Цей факт використовується в процесі будування генераторів псевдовипадкових чисел [3]. Для вирішення задачі створення подібних генераторів систематично використовуть теорію лишків за модулем величезного звичайного числа, з основою *a*, що є первісним коренем обраного *p*. При цьому, засновуючись на теорії Ферма [4], рівняння $a^{p-1} \equiv 1(\mathrm{mod}\, p)$ є основою ітераційної процедури:

$$x_0 = 1,\ x_{n+1} = a x_n \left(\mathrm{mod}\, p\right)$$

За допомогою визначеного ітераційного процесу отримують послідовність значень у вигляді множини $\left\{x_0, x_1, \ldots, x_n, \ldots, x_{p-1} = 1\right\}$, що інтерпретується як псевдовипадкова послідовність. Засновуючись на статистичному аналізі доводиться, що за великих значеннях *p* надані послідовності для усіх первісних корнів $\left\{a, \ldots, a_{\varphi(p-1)}\right\}$, де $\varphi\left(p-1\right)$– функція Ейлера, уся багатостатність послідовностей має схожу властивість, що інтерпритується як хаос. До наведеного часу відсутнє конструктивне визначення хаосу.

Висновок, щодо хаотичності такого роду, робиться на підставах досліджень їх автокореляційних функцій за різноманітних зміщень послідовностей відносно себе, або між різними послідовностями, що відповідають різним значенням первісних коренів.

Аналіз автокореляційних матриць завжди підтверджує відсутність внутрішньої скорельованості в будь-якій схожій послідовності, а тим паче, між різними послідовностями [4].

Такі ж властивості мають траєкторії нерухомих точок різноманітних відображень. Це вірно навіть для таких простих відображень як $f_1\left(x\right) = \sin \pi x$, $f_2\left(x\right) = 4x\left(1-x\right)$, симетричного та асиметричного «тентів», що задаються виразом

$$f_3\left(x\right), x_0 = 1/\,p\ ,\ x_{n+1} = \begin{cases} 2x_n, x_n < \dfrac{1}{2} \\ 1 - 2x_n, x_n \geq \dfrac{1}{2} \end{cases}$$

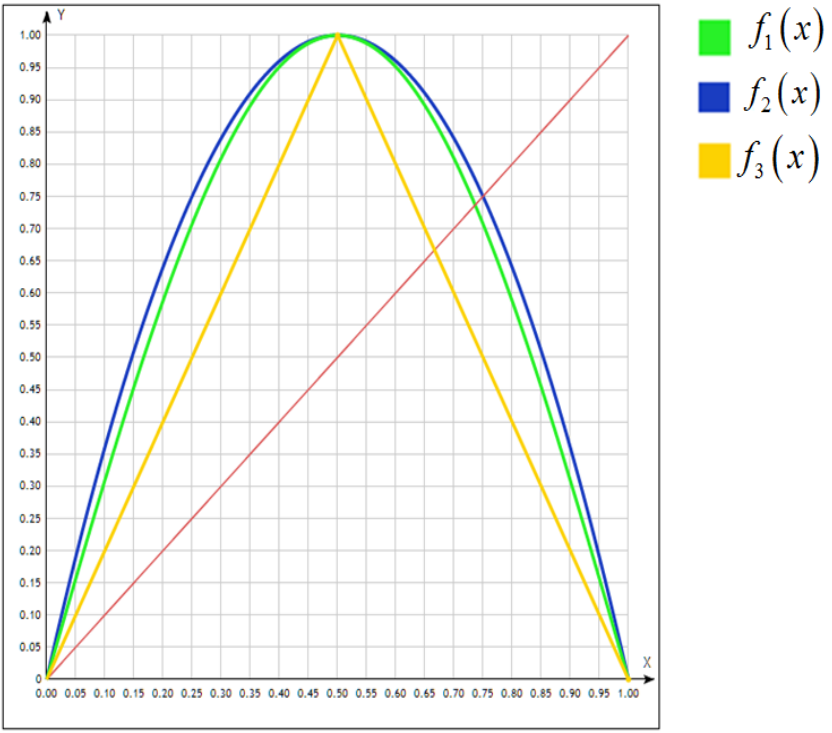

Рис.1. Графіки функцій

Зазвичай, ці відображення досліджуються на інтервалі [0,1], випливаючи зі значної аналогії у їх структурах на рис.1.

В роботі [5] доведена конгруентність $f_1(x)$ та $f_2(x)$. Звісно, що це також вірно для $f_3(x)$. Має сенс обирати числа виду $x_0 = \frac{1}{p}$, де p – просте число, через те, що відображення $f_4(x) = ax_n \pmod p$ за $x = 1$ з урахуванням (1) також породжує ітераційний процес з цим же простим p за різноманітних його первісних коренів a. Виникає питання: що поєднує усі ці відображення, що створюють за великих значень p «хаотичні процеси» у відповідних динамічних системах?

Відображення $f_4(x) \equiv ax^n \pmod p$ наочним способом пов'язується з групою лишків $(Z/pZ)^*$ за модулем p. Якщо a – первісний корень простого числа p, то досить легко довести, що a є породжуючим елементом цієї групи, а ітераційний процес (1) визначає переставлення на множині $\{1,2,3,4,\ldots,p-1\}$, яка утворює циклічну підгрупу переставлень порядку p повної групи переставлень на цієї множині. Цей простий факт є важливою основою для того, щоб стверджувати, що подібна група не може мати хаотичну структуру. Це твердження можна продемонструвати на прикладі, коли $p=19$, та розглядаються усі шість первісних коренів $\{2,3,10,13,14,15\}$. При цьому $\varphi(19-1)=\varphi(2\cdot 3^2)$. Для цієї множини первісних коренів на основі ітераційної процедури (1) отримані наступні переставлення

Таблиця 1

a	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*
2	1	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	1	3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
10	1	10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
13	1	13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	1	14	6	8	11	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	1	15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1

З наведеного прикладу випливає, що для $p=19$ прослідкується чітка структура переставлень. Доведено, що для будь-якого простого числа p, скільки завгодно більшої величини, на множині усіх його первісних коренів реалізується структура, що визначається розкладом на прості співмножники числа $p-1=\prod_{i=1}^{k} p_i^{\alpha_i}$. У наведеному прикладі

$p=19$ та $p-1=2\cdot 3^2$. Вплив співмножників 2 та 3 видно з наведеної таблиці 1. Доведено теорему.

Теорема А. Якщо число p просте, та $p-1=\prod_{i=1}^{k} p_i^{\alpha_i}$, то множина усіх первісних коренів $\{a_1, a_2, a_3, \ldots, a_{\varphi(p-1)}\}$ утворює множину переставлень на множині $\{1,2,3,\ldots,p-1\}$ детермінованої структури, що визначає структуру розкладу $p-1$ на прості співмножники.

Дослідження відображень $f_1(x), f_2(x), f_3(x)$ дозволили довести, що вони попарно конгруентні [5], та в кожній нерухомій точці $\frac{1}{p}\in[0,1]$, де p – просте число, вони утворюють підгрупу переставлень на множині R, у випадку $f_1(x)$, та на множині раціональних чисел Q, у випадках $f_2(x)$ та $f_3(x)$. Звідси випливає, що ітераційні процеси в динамічних системах цього виду не можуть формувати псевдовипадкові послідовності, які могли би бути розглянуті як деякі наближені до випадковості.

Література

1. Каток А., Хассельблат Б., Введение в теорию динамических систем., -М. МЦНМО, 2005. – 464 с.

2. Шарковский А.Н., Аттракторы траекторий и их бассейны. Наукова думка, 2013.

3. Крэнделл Р., Померанс К., Простые числа. Вычислительные и криптографические аспекты, -М.: MRSS, 2011. – 729 с.

4. Манин Ю.М. Введение в современную теорию чисел, -М.: МЦНМО, 2009. – 561 с.

5. Rauch J., Conjugating the Tent and Logistic Maps, Michigan University, 2005.