МИНОБРНАУКИ РОССИИ

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

Кафедра компьютерной алгебры и теории чисел

Базис Ван дер Пута

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 421 группы

направления 02.03.01 Математика и компьютерные науки

механико-математического факультета

Велиевой Айкун Гасан-Кызы

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 2019

Введение. Изучение динамических систем на p-адических сферах было важно для развития p - адической теории динамических систем. С точки зрения приложений, потребность изучения p-адических динамических систем возникает при решении задачи генерации псевдослучайных чисел: p-адические динамические системы дают широкий класс превосходных генераторов псевдослучайных чисел, которые играют столь важную роль в криптографии, а также в других прикладных областях, таких как численный анализ и компьютерное моделирование.

Теория динамических систем в полях p-адических чисел является важной частью алгебраической и арифметической динамики. Их изучение мотивировано применениями в различных областях математики, физики, генетики, биологии, когнитивной науки, нейрофизиологии, информатики и т.д.

В первом разделе данной работы рассмотрим основные аспекты p-адического анализа. Во втором разделе изучим базисы Ван дер Пута и найдем первообразную функцию. И третий раздел посвятим критерию сохранения меры для p-адических динамических систем в терминах базиса Ван дер Пута.

Основным математическим инструментом, используемым в этой работе, будет представление функции рядом Ван дер Пута, который активно используется в p-адическом анализе. Основным моментом в построении базиса Ван дер Пута будет непрерывность характеристической функции p-адического шара.

Основное содержание работы. Рассмотрим некоторые понятия. При $x = \sum\limits_{j=-\infty}^{\infty} a_j p^j \in \mathbb{Q}_p$ определим его p-адическую целую часть $[x]_p$ по

$$[x]_p := \sum_{j=-\infty}^{\infty} a_j p^j$$

И полагаем, что

$$x_n := p^n [p^{-n} x]_p \sum_{j=-\infty}^{\infty} a_j p^j, (n \in 0, 1, ...)$$

Таким образом, присвоили каждому $x \in \mathbb{Q}_p$ стандартную последовательность $x_0, x_1, ...,$ сходящийся к x. Элемент $x \in \mathbb{Z}_p$ стандартной последовательности состоит из неотрицательных целых чисел; в конечном счете, это постоянная величина, если $x \in 0, 1, ...$ Обозначим $m \lhd x$, $m \in \mathbb{N} \cup 0, x \in \mathbb{Z}_p$, если m один из номеров $x_0, x_1, ...$ Иногда $\lhd$ будем называть соотношением между m и x. 'x начинается с m' или 'm является начальной частью x'.

Если $n \in \mathbb{N}$, то $m : m \lhd n, m \neq n$ финитный (ограничен, конечен) и имеет наибольший элемент (относительно $\lhd$).

Далее, приведем некоторые элементарные факты, относительно этих понятий.

Предложение 5.

1. Пусть $x \in \mathbb{Z}_p, n \in \{0, 1, 2, ...\}$. Тогда $|x - x_n|_p \leq p^{-n}$ и $x_n \in 0, 1, ..., p^n - 1$. Обратно, $y \in 0, 1, ..., p^n - 1, |x - y|_p \leq p^{-n}$, следовательно $y = x_n$

2. Пусть $x, y \in \mathbb{Z}_p, n \in 0, 1, 2, ...$ Тогда

$|x - y|_p \leq p^{-n}$ тогда и только тогда, когда $x_n = y_n$

$|x - y|_p = p^{-n}$ тогда и только тогда, когда $x_n = y_n$ и $x_{n+1} \neq y_{n+1}$.

3. $x \mapsto x_n (x \in \mathbb{Z}_p)$ имеет постоянное значение смежных классов $p^n\mathbb{Z}_p (n \in 0, 1, ...)$.

4. Пусть $x, y \in \mathbb{Z}_p, n \in \{0, 1, 2, ...\}$. Тогда

$$|x - x_n|_p = \begin{cases} 0, & \text{если } |x - y|_p \leq p^{-n}; \\ |x - y|_p, & \text{если } |x - y|_p > p^{-n}. \end{cases}$$

5. $(x_n)_m = x_{min(n,m)} (x \in \mathbb{Z}_p, n, m \in \{0, 1, 2, ...\})$.

6. Пусть $x \in \mathbb{Z}_p, m \in \mathbb{N}$. Тогда

$m \lhd x$ тогда и только тогда, когда $|x - m|_p < \frac{1}{m}$

7. $|m - m\_| = p^{-s(m)}, (m \in \mathbb{N})$, где $s(m) := [\frac{\log m}{\log p}]$ также определяется $m = a_0 + a_1 p + ... + a_{s(m)} p^{s(m)}, a_{s(m)} \neq 0$.

Теорема 4. Функции $e_0, e_1, ...$ определяемые следующим образом

$$e_n := \begin{cases} 1, & \text{если } n \lhd x \\ 0, & \text{если в противном случае,} \end{cases}$$

где $x \in \mathbb{Z}_p, n \in (\{0,1,,2,...\})$, образуют ортонормированный базис (базис Ван дер Пута) $C(\mathbb{Z}_p \to K)$ раскладывается в ряд

$$f(x) = \sum_{n=0}^{\infty} a_n e_n(x), x \in \mathbb{Z}_p,$$

то $a_0 = f(0)$ и $a_n = f(n) - f(n\_)$ при $n \in \mathbb{N}$.

Теорема 5. (Характеристика липшицевых функций коэффициентов Ван дер Пута). Пусть $f = \sum_{n=0}^{\infty} a_n e_n \in C(\mathbb{Z}_p \to K)$. Тогда, $f \in Lip_1(\mathbb{Z}_p \to K)$ тогда и только тогда, когда $\sup_n \mid a \mid_n n < \infty$. Более точно, для $f = \sum_{n=0}^{\infty} a_n e_n \in C(\mathbb{Z}_p \to K)$ имеем следующее:

(1)$\| \Phi_1 f \|_\infty = \sup\{\mid a_n \mid\mid \gamma_n \mid_p^{-1} : n \in \mathbb{N}\}$

(2) $\| \Phi_1 f \|_\infty \leq \sup\{\mid a_n \mid n : n \in \mathbb{N}\} \leq p \| \Phi_1 f \|_\infty$

(3) Если $f \in Lip_1(\mathbb{Z}_p \to K)$, то $\| f \|_1 = \sup\{\mid a_n \mid\mid \gamma_n \mid_p^{-1} : n \in \{0,1,2,...\}\}$.

Теорема 6. (Характеристика C^1-функций с нулевой производной). Пусть $f = \sum_{m=0}^{\infty} a_n e_n \in C(\mathbb{Z}_p \to K)$. Тогда

$$f \in N^1(\mathbb{Z}_p \to K) \Leftrightarrow \lim_{n\to\infty} \mid a_n \mid n = 0 \Leftrightarrow \lim_{n\to\infty} a_n (n - n\_)^{-1} = 0.$$

Для $f \in C(\mathbb{Z}_p \to K)$, непрерывная функция $g : \mathbb{Z}_p \to K$ однозначно определена, для которого $g(0) = 0$ и $\Phi_1 g(n, n\_) = f(n\_)$ для всех $n \in N$. Действительно, условия на g задаются его коэффициентами Ван дер Пута, поэтому g обязательно имеет вид $g = \sum_{n=1}^{\infty} f(n\_)(n - n\_)_{e_n}$. И наоборот, последняя формула определяет непрерывную функцию g (так как $\lim_{n\to\infty} f(n\_)(n - n\_) = 0$) и $g(n) - g(n\_) = f(n\_)(n - n\_)$ для всех $n \in \mathbb{N}, g(0) = 0$. Таким образом,имеет место следующее определение [1].

Определение 7. Функцию $f \in C(\mathbb{Z}_p \to K)$ обозначим через Pf, единственную непрерывную функцию, удовлетворяющим условиям $Pf(0) = 0$ и $Pf(n) - Pf(n\_) = (n - n\_)f(n\_)$ для любых $n \in N$

[1]Schikhof W.H., Ultrametric calculus. An introduction to p-adic analysis, Cambridge: Cambridge University Press, 1984. 196 c

Теорема 7. (Свойства P). P является линейной изометрией $C(\mathbb{Z}_p \to K)$ в $C^1(\mathbb{Z}_p \to K)$. Для каждого $f \in C(\mathbb{Z}_p \to K)$, Pf является первообразной f вместе со следующим свойством среднего значения.

$$\frac{Pf(x) - Pf(y)}{x - y} \leq \max\{\mid f(z) \mid : z \in [x, y]\} \ (x, y \in \mathbb{Z}_p, x \neq y)$$

(где $[x, y]$ означает наименьший круг, содержащий x и y.)

Теорема 8. (Формула для Pf). Пусть x_n в предложении 1. Тогда имеем для $f \in C(\mathbb{Z}_p \to K)$

$$Pf(x) = \sum_{n=0}^{\infty} f(x_n)(x_{n+1} - x_n) \ (x \in \mathbb{Z}_p).$$

Более конкретно, если $x = \sum_{n=0}^{\infty} b_n p^n \in \mathbb{Z}_p$, то

$$Pf(x) = f(0)b_0 + \sum_{n=1}^{\infty} f\left(\sum_{j=0}^{n-1} b_j p^j\right) b_n p^n.$$

Если $f = \sum_{n=0}^{\infty} a_n e^n$, то

$$Pf(x) = \sum_{n=0}^{\infty} a_n (x - n) e_n(x) \ (x \in \mathbb{Z}_p).$$

В итоге, имеем

$$Pf(x) = \sum_{n=0}^{\infty} f(n\_)(n - n\_)e_n.$$

Теорема 9. Пусть $A \in C(\mathbb{Z}_p \to K) \to C(\mathbb{Z}_p \to K)$ удовлетворяет условию Липшица $\parallel Af - Ag \parallel_\infty \leq \parallel f - g \parallel_\infty, (f, g \in C(\mathbb{Z}_p \to K))$. Тогда существует изометрическое отображение (относительно $\|\|_\infty$) в $N^1(\mathbb{Z}_p \to K)$ на множестве решений дифференциального уравнения $f' = Af, (f \in C^1(\mathbb{Z}_p \to K))$.

Из теории p-адических дифференциальных уравнений с аналитическими решениями выделим одну конкретную проблему для которых C^1-теория может помочь. Пусть $\lambda \in \mathbb{Z}_p$. Рассмотрим дифференциальное уравнение

$$xf'(x) - \lambda f(x) = (1 - x)^{-1} \ (x \in D). \tag{1}$$

Определение 8. Для каждого $\lambda \in \mathbb{Z}_p$ положим $\nu(\lambda) := \lim\_{n\to\infty} \sqrt[n]{\mid n-\lambda \mid_p}$.

λ является p-адическим числом Лиувилля, если $\nu(\lambda) = 0$.

Теорема 10. Пусть $g : \mathbb{Z}_p \to K$ непрерывная функция, значит дифференцируема в точке 0 и пусть $\lambda \in \mathbb{Z}_p$. Если $\lambda = 0$, то предположим, что $g(0) = 0$ и $g'(0) = 0$. Тогда существует C^1-функция $f : \mathbb{Z}_p \to K$ такой, что $xf'(x) - \lambda f(x) = g(x)$ для всех $x \in \mathbb{Z}_p$

Произошло знакомство с p-адическими числами Лиувилля, то есть числа $\lambda \in \mathbb{Z}_p$ для которых $\lim\_{n\to\infty} \sqrt[n]{\mid n-\lambda \mid_p} = 0$. Свойства этих чисел покажет поразительную аналогию с вещественными числами Лиувилля.

Разрыв в p-адическом разложении $x = \sum_{j=0}^{\infty} a_j p^j$ элемента $x \in \mathbb{Z}_p$ является пара чисел $s < t$, такой что $a_s \neq 0, a_{s+1} = a_{s+2} = ... = a_{t-1} = 0, a_t \neq 0$. Длина такого разрыва является число $[t/p^s]$. Условие (β) из следующей теоремы делает его более видимым. P-адические целые числа являются числами Лиувилля, а также дают метод для их создания.

Теорема 11. Пусть $\lambda \in \mathbb{Z}_p$. Следующие условия эквивалентны.

(α). λ является числом Лиувилля.

(β). У разрыва λ есть произвольные промежутки.

Теорема 12. p-адическое число Лиувилля не является алгебраическим относительно $\mathbb{Q}$.

Теорема 13. p-адические числа Лиувилля образуют компактное $G_\delta-$-подмножество $\mathbb{Z}_p$.

Теорема 14. p-адические числа Лиувилля образуют нулевое множество в $\mathbb{Z}_p$.

Теорема 15. Пусть $\gamma_0, \gamma_1, ...p$-адические целые числа, определяемые как: $\gamma_0 := 1, \gamma_n := n - n\_(\forall n \in \mathbb{N})$. Пусть P-первообразная функция, удовлетворяющая условиям $Pf(0) = 0$ и $Pf(n) - Pf(n\_) = (n - n\_)f(n\_)$ для любых $n \in N$. Тогда функции $\gamma_0 e_0, \gamma_1 e_1, ..., Pe_0, Pe_1, ...$ образуют ортонормированный базис $C^1(\mathbb{Z}_p \to K)$; $\gamma_0 e_0, \gamma_1 e_1, ...$ являются ортонормированным базисом $N^1(\mathbb{Z}_p \to K)$.

Следствие 2. Коэффициенты относительно$e_0, e_1, ..., Pe_0, Pe_1, ...$

Пусть $f \in C^1(\mathbb{Z}_p \to K)$, имеет разложение

$$f = \sum_{n=0}^{\infty} a_n e_n + \sum_{n=0}^{\infty} b_n P e_n$$

Тогда

$$a_n = \begin{cases} f(0), & \text{если } n = 0 \\ f(n) - f(n\_) - (n - n\_)f'(n), & \text{если } n \in N \end{cases}$$

$$b_n = \begin{cases} f'(0), & \text{если } n = 0 \\ f'(n) - f'(n\_), & \text{если } n \in N. \end{cases}$$

Следствие 3. Локально постоянные функции образуют компактное подмножество $N^1(\mathbb{Z}_p \to K)$. Локально линейные функции образуют компактное подмножество $C^1(\mathbb{Z}_p \to K)$.

Теория динамических систем в полях p-адических чисел и их алгебраические расширения являются важной частью алгебраической и арифметической динамики. Как и в общей теории динамических систем, вопросы эргодичности и сохранения меры играют фундаментальные роли в теории p-адических динамических систем. Обычно исследования в этих областях p-адической динамики ограничивались аналитическими или, по крайней мери, гладкими отображениями $f : \mathbb{Q}_p \to \mathbb{Q}_p$, где $\mathbb{Q}_p$- поле p-адических чисел. Однако, внутренняя математическая разработка теории p-адических динамических систем, а также приложений к криптографии стимулировали интерес к негладким динамическим картам. Важный класс негладких отображений дается липшицевыми функциями. В криптографических приложениях такие функции называются совместимыми.

Пусть $p > 1$-произвольное простое число. Кольцо целых p-адических чисел обозначается символом $\mathbb{Z}_p$. p-адическое нормирование обозначается $|\ |_p$. Эта оценка удовлетворяет сильному неравенству треугольника:

$$|\ x + y\ |_p \leq [|\ x\ |_p, |\ y\ |_p].$$

Это основное отличительное свойство p-адической оценки, вызывающее существенное отклонение от реального или комплексного анализа.

Ряды Ван дер Пута определяется следующим образом. Пусть $f : \mathbb{Z}_p \to \mathbb{Z}_p$-непрерывная функция. Тогда существует единственная последовательность p-адических коэффициентов $B_0, B_1, ...$, такая, что

$$f(x) = \sum_{m=0}^{\infty} B_m \chi(m, x)$$

Для всех $x \in \mathbb{Z}_p$. Здесь характеристическая функция $\chi(m, x)$ задается формулой

$$\chi(m, x) = \begin{cases} 1, & \text{если } \mid x - m \mid_p \leq p^{-n}, \\ 0, & \text{в противном случае,} \end{cases}$$

где $n = 1$, если $m = 0$, и n однозначно определяется неравенством $p^{n-1} \leq m \leq p^n - 1$ в противном случае.

Коэффициенты Ван дер Пута B_m связаны со значениями f следующим образом. Пусть $m = m_0 + ... + m_{n-2}p^{n-2} + m_{n-1}p^{n-1}$ представление m в p-арной системе счисления, т.е. $m_j \in \{0, ..., p-1\}, j = 0, ..., n-1$ и $m_{n-1} \neq 0$. Тогда

$$B_m = \begin{cases} f(m) - f(m - m_{n-1}p^{n-1}), & \text{если } m \geq p, \\ f(m), & \text{в противном случае,} \end{cases}$$

Пусть $f : \mathbb{Z}_p \to \mathbb{Z}_p$-функция и f удовлетворяет условию Липшица с константой 1 (относительно p-адического нормирования $\mid \mid_p$):

$$\mid f(x) - f(y) \mid_p \leq \mid x - y \mid_p \ \ (\forall x, y \in \mathbb{Z}_p).$$

Снова утверждаем, что отображение алгебраической системы A на себя называется совместимым, если оно сохраняет все конгруэнции A. Легко проверить, что отображение $f : \mathbb{Z}_p \to \mathbb{Z}_p$ является липшицевым тогда и только тогда, когда оно согласовано, относительно $\mod p^k, k = 1, 2, ...$ конгруэнции.

Пространство $\mathbb{Z}_p$ оснащено естественной вероятностной мерой, а именно мерой Хаара μ_p, нормированной так, что $\mu_p(\mathbb{Z}_p) = 1$. Отображение $f : \mathbb{S} \to \mathbb{S}$

измеримого пространства $\mathbb{S}$ с вероятностной мерой μ называется сохраняющим меру, если $\mu(f^{-1}(S)) = \mu(S)$ для любого измеримого подмножества $S \subset \mathbb{S}$.

Скажем, что совместимая функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$ является биективным модулем p^k, если индуцированное отображение $x \mapsto f(x) \mod p^k$ является перестановкой на $\mathbb{Z}/p^k\mathbb{Z}$. Совместимая функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$ сохраняет меру тогда и только тогда, когда она биективна по модулю p^k для всех $k = 1, 2, ...$

Теорема 16. Пусть $f : \mathbb{Z}_p \to \mathbb{Z}_p$ совместимая функция и

$$f(x) = \sum_{m=0}^{\infty} p^{\log_p m} b_m \chi(m, x)$$

представление Ван дер Пута этой функции, где $b_m \in \mathbb{Z}_p, m = 0, 1, 2, ...$ Тогда $f(x)$ сохраняет меру Хаара тогда и только тогда, когда

1) $b_0, b_1, ..., b_{p-1}$ устанавливает полный набор модулей вычетов p, т.е. функция $f(x)$ биективна по модулю p;

2) $b_{m+p^k}, ..., b_{m+(p-1)p^k}$ для любого $m = 0, ..., p^k - 1$ все ненулевые вычеты по модулю p при $k = 2, 3, ...$

Следствие 4. Пусть $f : \mathbb{Z}_p \to \mathbb{Z}_p$-локально совместимая функция и

$$f(x) = \sum_{m=0}^{\infty} p^{[\log_p m]} b_m \chi(m, x)$$

представление Ван дер Пута этой функции, где $b_m \in \mathbb{Z}_p, m \geq N$. Тогда $f(x)$ сохраняет меру Хаара тогда и только тогда, когда

1. Функция $f(x)$ биективна по модулю p^N;

2. $b_{m+p^k}, ..., b_{m+(p-1)p^k}$ для любого $m = 0, ..., p^k - 1$ все ненулевые вычеты по модулю p при $k > N$.

Заключение. В представленной работе были рассмотрены некоторые аспекты p-адического анализа, базис Ван дер Пута, критерий сохранения меры для p-адических динамических систем в терминах базиса Ван дер Пута. Даны их определения, условия выполнения, а также доказаны некоторые теоремы. Основным математическим инструментом, используемым в этой работе, было представление функции рядом Ван дер Пута, который активно используется

в p-адическом анализе. И основным моментом в построении базиса Ван дер Пута была непрерывность характеристической функции p-адического шара. Данная тема является достаточно актуальной, так как с точки зрения приложений, потребность изучения p-адических динамических систем возникает при решении задачи генерации псевдослучайных чисел: p-адические динамические системы дают широкий класс превосходных генераторов псевдослучайных чисел, которые играют столь важную роль в криптографии, а также в других прикладных областях, таких как численный анализ и компьютерное моделирование.