Министерство образования и науки Российской Федерации

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

название темы выпускной квалификационной работы

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студента 2 курса 227 группы

направления 02.04.01 «Математика и компьютерные науки»
код и наименование направления

механико-математического факультета
наименование факультета

Лугового Никиты Владимировича
фамилия, имя, отчество

Научный руководитель

Зав.каф., к.ф.-м.н		А.М. Водолазов
должность, уч. степень, уч. звание	подпись, дата	инициалы, фамилия

Зав. кафедрой:

Зав. каф., к.ф.-м.н.		А.М. Водолазов
должность, уч. степень, уч. звание	подпись, дата	инициалы, фамилия

Саратов 2017 г.

Введение. В этой работе подробно исследуется эргодическое поведение p-адических мономиальных динамических систем. Поведение p-адических динамических систем существенно зависит от простого параметра p.

Изучение эргодичности мономиальных динамических систем на p-адических сферах было важно для развития p - адической теории динамических систем. С точки зрения приложений, потребность изучения эргодичности p-адических динамических систем возникает при решении задачи генерации псевдослучайных чисел: p-адические эргодические 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. Изучение p-адических динамических систем мотивировано их применениями в различных областях математики, физики, генетики, биологии, когнитивной науки, нейрофизиологии, информатики, криптологии и т.д. В частности, p-адические динамические системы нашли применение в криптографии, что стимулировало интерес к негладким динамическим отображениям. Важный класс (в общем случае) негладких отображений задается липшицевыми функциями класса 1. В настоящей работе приводится краткий обзор результатов о липшицевых функциях класса 1 и описывается сохранение меры (для меры Хаара на кольце целых p-адических чисел) и эргодических функций. Основным математическим инструментом, используемым в этой работе, является представление функции рядом Ван дер Пута, который активно используется в p-адическом анализе. Основным моментом в построении базиса Ван дер Пута является непрерывность характеристической функции p-адического шара. Также мы используем алгебраическую структуру (перестановки), индуцированную координатными функциями с частично замороженными переменными.

Основное содержание работы. Локально-компактная группа — это топологическая группа G, которая является локально-компактной как топологической пространство.

Пусть G — локально-компактная группа. Обозначим через R и L правое

и левое действие группы G на себя:

$$R_t(x) = xt^{-1}, \quad L_t(x) = tx, \quad t, x \in G.$$

Левая (правая) мера Хаара на топологической группе G есть мера Радона (мера на сигма-алгебре борелевских множеств на хаусдорфовом топологическом пространстве X, которая является локально конечной и внутреннее регулярной), которая инвариантна относительно левого (правого) действия. На всякой локально-компактной группе G существует ненулевая левая (правая) мера Хаара и эта мера Хаара единственна с точностью до положительного скалярного множителя. Поскольку $\mathbb{Q}_p$ – локально-компактная группа, то на $\mathbb{Q}_p$ можно определить меру Хаара.

Так как $\mathbb{Q}_p$ является локально-компактной коммутативной группой по сложению, то на нем можно определить аддитивную меру Хаара, которая будет положительной мерой dx, инвариантной относительно сдвигов,
$d(x + a) = dx$, $a \in \mathbb{Q}_p$. Если меру dx нормировать с помощью равенства

$$\int_{\mathbb{Z}_p} dx = 1,$$

то dx будет единственной.

Мономиальной динамической системой в $\mathbb{Q}_p$ мы называем дискретную динамическую систему, которая описывается итерационными уравнениями

$$f(x) = x^n, n \in \mathbb{N}, n \geqslant 2. \tag{1}$$

В этом разделе подробно исследуем эргодическое поведение p-адических мономиальных динамических систем. Поведение p-адических динамических систем существенно зависит от простого параметра p.

Изучение эргодичности мономиальных динамических систем на p-адических сферах было важно для развития p-адической теории динамических систем. С точки зрения приложений, потребность изучения эргодичности p-адических динамических систем возникает при решении задачи генерации псевдослучайных чисел: p-адические эргодические динамические системы дают широкий класс превосходных генераторов псевдослучайных чисел, которые играют столь важную роль в криптографии, а также в других при-

кладных областях, таких как численный анализ и компьютерное моделирование.

Пусть ψ_n – (мономиальное) отображение на $\mathbb{Z}_p$, которое переводит x в x^n. Тогда все сферы $S_{p^{-l}}(1)$ являются ψ_n-инвариантными тогда и только тогда, когда n – единица относительно умножения, т.е. $(n,p)=1$.

В частности, ψ_n является изометрией на $S_{p^{-l}}(1)$ тогда и только тогда, когда $(n,p)=1$. В дальнейшем будем считать, что n является единицей. Заметим также, что, как следствие, $S_{p^{-l}}(1)$ не является группой по умножению. Таким образом, мы рассматриваем динамические системы не на компактной (абелевой) группе. А значит обширная теория эргодических систем, развитая для локально компактных групп, неприменима к нашей проблеме.

Начнем с нескольких понятий. При $x=\sum_{j=-\infty}^{\infty} a_j p^j \in \mathbb{Q}_p$ 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, мы 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 1.

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

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

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

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

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

$$m \triangleleft x \text{ тогда и только тогда, когда } |x - m|_p < \tfrac{1}{m}$$

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

Доказательство. Докажем только 6 и 7. Если $m \triangleleft x$, то $m = a_0 + a_1 p + ... + a_s p^s$ для некоторого $s, x = \sum_{j=0}^{\infty} a_j p^j$. Стало бы $|x - m|_p \leq p^{-(s+1)} < 1/m$. Обратно, если $|x - m|_p < \frac{1}{m}$ и $m = a_0 + a_1 p + ... + a_s p^s, (a_s \neq 0)$, то $1/m \leq p^{-s}$ так что $|x - m|_p < p^{-s}$. А это означает, что первые $s + 1$ коэффициенты в p-адическом разложении ряда x должны быть равны m. Значит $m \triangleleft x$. Чтобы доказать пункт 7, предположим $m = a_0 + a_1 p + ... + a_s p^s, (a_s \neq 0)$. Поэтому $p^s \leq m < p^{s+1}$, следовательно, $s = \left[\frac{\log m}{\log p}\right]$ и $|m - m\_|_p = p^{-s}$. □

Теорема 1. *Функции $e_0, e_1, ...$ определяемые следующим образом*

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

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

Доказательство. Пусть $f \in C(\mathbb{Z}_p \to K)$ и предположим, что $a_0, a_1, ... \in K$, так что $f(x) = \sum_{n=0}^{\infty} a_n e_n(x), x \in \mathbb{Z}_p$.

Поэтому $f(0) = 0$ и при $m \in \mathbb{N}, f(m) = \sum_{n \lhd m} a_n, f(m\_) = \sum_{n \lhd m\_} a_n$, так что $f(m) - f(m\_) = a_m$.

Пусть теперь $f \in C(\mathbb{Z}_p \to K)$ произвольная функция. Рассмотрим ряд

$$g(x) := f(0)e_0 + \sum_{n=1}^{\infty}(f(n) - f(n\_))e_n(x), x \in \mathbb{Z}_p$$

Поскольку f равномерно непрерывен, $\lim_{n\to\infty}(f(n) - f(n\_)) = 0$ и ряд равномерно сходится, следовательно, g является вполне определенным элементом $C(\mathbb{Z}_p \to K)$. Из рассмотренного выше имеем $f(0) = g(0)$ для всех $n \in \mathbb{N} \cup \{0\}$. По условию непрерывности, $f = g$. На этом этапе известно, что для каждого $f \in C(\mathbb{Z}_p \to K), x \in \mathbb{Z}_p$

$$f(x) := f(0)e_0 + \sum_{n-1}^{\infty}(f(n) - f(n\_))e_n(x) = \sum_{n=0}^{\infty} a_n e_n(x)$$

Очевидно, что $\|f\|_\infty \leq \sup|a_n|$. С другой стороны, $|f(0)| \leq \|f\|_\infty$; $|f(n) - f(n\_)| \leq \|f\|_\infty$, стало быть $\|f\|_\infty = \sup|a_n| = \max_n|a_n|$.

Этот факт, вместе с замечанием, что $\lim_{n\to\infty} a_n = 0$, означает, что $e_0, e_1, ...$ образует ортонормированный базис $C(\mathbb{Z}_p \to K)$. Теорема доказана. □

Вернемся к базису Ван дер Пута $e_0, e_1, ...$ в $C(\mathbb{Z}_p \to K)$. Является ли последний базисом $C^1(\mathbb{Z}_p \to K)$? Нетрудно заметить, что ответ отрицательный. На самом деле, элементы $e_0, e_1, ...$ являются локально постоянными, поэтому их K-линейная оболочка $N^1(\mathbb{Z}_p \to K)$ и последняя являются замыканием соответствующего подпространства $C^1(\mathbb{Z}_p \to K)$.

Теорема 2. *Пусть $\gamma_0, \gamma_1, ...$ p-адические целые числа, определяемы следующим образом. $\gamma_0 := 1$ и $\gamma_n := n - n\_$ для всех $n \in \mathbb{N}$. Пусть P первообразная функция из определения* **??**. *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 $N^1(\mathbb{Z}_p \to K)$.*

Доказательство. Функции $e_0, e_1, ...$ образуют ортонормированное множество

в $C(\mathbb{Z}_p \to K)$. Поскольку $P : C(\mathbb{Z}_p \to K) \to C^1(\mathbb{Z}_p \to K)$ является отображением (теорема **??**), мы имеем, что $Pe_0, Pe_1, ...$ является ортонормированным в $C^1(\mathbb{Z}_p \to K)$. Из теоремы **??** (3) применяется для конечной линейной комбинации $e_0, e_1, ...$, что приводит к выводу, что $\gamma_0 e_0, \gamma_1 e_1, ...$ ортонормированный. Для $f \in N^1(\mathbb{Z}_p \to K)$ и $g \in C(\mathbb{Z}_p \to K)$ имеем

$$\|f + Pg\|_1 \geq \|(f + Pg)'\|_\infty = \|(Pg)'\|_\infty = \|g\|_\infty = \|Pg\|_1.$$

Пусть E нормированное пространство над полем K. Пусть $x, y \in E$. Запишем одну лемму.

Предположим, что $c \in (0, 1]$ такое, что

$$\|x + y\| \geq c\|x\|$$

Тогда также

$$\|x + y\| \geq c\|y\|$$

По этой лемме мы также имеем $\|f + Pg\|_1 \geq \|f\|_1$, также $N^1(\mathbb{Z}_p \to K) \perp \mathrm{Im}\ P$, в частности $[e_0, e_1, ...] \perp [Pe_0, Pe_1, ...]$. Мы видим, что $\{\gamma_0 e_0, \gamma_1 e_1, ..., Pe_0, Pe_1, ...\}$ является ортонормированным множеством в $C^1(\mathbb{Z}_p \to K)$. Чтобы доказать, что он на самом деле является базисом, предположим, что $f \in C^1(\mathbb{Z}_p \to K)$. Имеем

$$f = f - Pf' + Pf'$$

и

$$f' = f'(0)e_0 + \sum_{n=1}^{\infty}(f'(n) - f'(n\_))e_n$$

в том смысле, что $\|\ \ \|_\infty$. P является линейным отображением, поэтому мы имеем

$$Pf' = f'(0)Pe_0 + \sum_{n=1}^{\infty}(f'(n) - f'(n\_))Pe_n$$

В том смысле, что $\|\ \ \|_1; g := f - Pf'$ в $N^1(\mathbb{Z}_p \to K)$, пусть

$$g = g(0)e_0 + \sum_{n=1}^{\infty}(g(n) - g(n\_))e_n \tag{2}$$

будет его разложением в $C(\mathbb{Z}_p \to K)$. Согласно теореме **??** $\lim_{n\to\infty} \Phi_1 g(n, n\_) = 0$, так что

$$\|(g(n) - g(n\_))e_n\|_1 = \|\Phi_1 g(n, n\_), \gamma_n e_n\|_1 = |\Phi_1 g(n, n\_)|$$

стремится к нулю при $n \to \infty$.

Поэтому ряд в (2) сходится в том смысле, что $\| \ \|_1$ и (2) является верным тождеством в $C^1(\mathbb{Z}_p \to K)$. Имеем, что $f = f - Pf' + Pf'$ может быть записана в виде сходящейся линейной комбинации $e_0, e_1, ..., Pe_0, Pe_1, ...$ и что если $f \in N^1(\mathbb{Z}_p \to K)$, тогда $f = f - Pf'$ является комбинацией $e_0, e_1, ...$ Следовательно, теорема доказана. □

Следствие 1 (Коэффициента 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

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

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

Доказательство. В соответствии с доказательством теоремы 2 следует, что

$$g = f - Pf')f = g(0)e_0 + \sum_{n=1}^{\infty}(g(n) - g(n\_))e_n + f'(0)Pe_0 + \sum_{n-1}^{\infty}(f'(n) - f'(n\_))Pe_n.$$

В заключении следует отметить, что $a_0 = g(0) = f(0) - Pf'(0) = f(0)$ и

$$g(n) - g(n\_) = f(n) - f(n\_) - Pf'(n) + Pf'(n\_) = f(n) - f(n\_) - (n - n\_)f'(n\_)$$

по определению **??**. □

Следствие 2. *Локально постоянные функции образуют компактное подмножество* $N^1(\mathbb{Z}_p \to K)$*. Локально линейные функции образуют компактное подмножество* $C^1(\mathbb{Z}_p \to K)$*.*

Доказательство. Конечные линейные комбинации $e_0, e_1, ...$ являются локально постоянными. Конечные линейные комбинации $Pe_0, Pe_1, ...$ являются локально линейными. Теперь применим теорему 2. □

Теория динамических систем изучает траектории (орбиты), т.е. последовательности итераций

$$x_0, x_1 = f(x_0), ..., x_{i+1} = f(x_i) = f^{(i+1)}(x_0), ...,$$

где $f^{(s)}(x) = \underbrace{f(f(...f(x))...)}_{s}$.

Рассмотрим -адическую автономную динамическую систему $\langle \mathbb{Z}_p, \mu_p, f \rangle$. Пространство $\mathbb{Z}_p$ снабжено естественной вероятностной мерой, а именно мерой Хаара μ_p, нормированной так, что $\mu_p(\mathbb{Z}_p) = 1$. Шары $B_{p^{-r}}(a)$ отличных от нуля радиусов составляют базу соответствующей σ-алгебры измеримых подмножеств, $\mu_p(B_{p^{-r}}(a)) = p^{-r}$.

Как обычно, измеримое отображение $f : \mathbb{Z}_p \to \mathbb{Z}_p$ называется сохраняющим меру, если $\mu_p(f^{-1}(U)) = \mu_p(U)$ для каждого измеримого подмножества $U \subset \mathbb{Z}_p$.

Сохраняющее меру отображение $f : \mathbb{Z}_p \to \mathbb{Z}_p$ называется эргодическим, если $f^{-1}(U) = U$ подразумевает либо $\mu_p(U) = 0$, либо $\mu_p(U) = 1$.

Пусть функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$ представлена в координатной форме $f(x) = \delta_0(f(x)) + p\delta_1(f(x)) + ... + p^k\delta_k(f(x)) + ...$ f — функция класса Липшица 1 тогда и только тогда, когда для каждого $k \geq 1$ k-ая координатная функция $\delta_f(f(x))$ не зависит от $\delta_{k+s}(x)$ для всех $s \geq 1$, т.е.

$$\delta_k(f(x + p^{k+1}\mathbb{Z}_p)) = \delta_k(f(x))$$

для всех $x \in \{0, 1, ..., p^{k+1} - 1\}$. Принимая во внимание, что

$$[x]_k = (x_0, x_1, ..., x_{k-1}, ...)$$

для $k \geq 0$, рассмотрим функцию p-значной логики

$$\varphi_k : \underbrace{\{0, ..., p-1\} \times \cdots \times \{0, ..., p-1\}}_{k+1} \to \{0, ..., p-1\}$$

и $\varphi_k : [x]_{k+1} \mapsto \delta_k(f(x))$.

Используя эти функции p-значной логики, любая функция класса Липшица 1 $f : \mathbb{Z}_p \to \mathbb{Z}_p$ может быть представлена в виде:

$$f(x) = f(x_0 + \cdots + p^k x_k + \cdots) = \sum_{k=0}^{\infty} p^k \varphi_k(x_0, \ldots, x_k) = \sum_{k=0}^{\infty} p^k \varphi_k([x]_{k+1})$$

Например, функции $f_k, k \geq 0$ могут быть представлены как $f_k(x) = \sum_{i=0}^{k} p^i \varphi_i([x]_{i+1})$. Функция $\varphi_k(x_0, \ldots, x_k)$ может быть определена ее подфункциями, полученными путем фиксации первых k переменных $(x_0, \ldots, x_{k-1})$. Принимая во внимание подфункцию функции $\varphi_k(x_0, \ldots, x_k)$, полученной фиксацией переменных $x_0 = a_0, \ldots, x_{k-1} = a_{k-1}, a_i \in \{0, \ldots, p-1\}$, обозначенной как $\varphi_{k,[a]_k}$, где $a = a_0 + pa_1 + \ldots + p^{k-1}a_{k-1}$. В этих обозначениях функцию $\varphi_k(x_0, \ldots, x_k)$ можно представить в виде

$$\varphi_k(x_0, \ldots, x_k) = \sum_{a=0}^{p^k-1} I_{[a]_k}(x_0, \ldots, x_{k-1}) \varphi_{k,[a]_k}(x_k), \tag{3}$$

где $I_{[a]_k}$ характеристическая функция, такая что

$$I_{[a]_k}(x_0, \ldots, x_{k-1}) = \begin{cases} 1, & \text{если } (x_0, \ldots, x_{k-1}) = [a]_k; \\ 0, & \text{в противоположном случае.} \end{cases}$$

В этих обозначениях функция Липшица класса 1 $f : \mathbb{Z}_p \to \mathbb{Z}_p$ становится

$$f(x) = \sum_{k=0}^{\infty} p^k \varphi_k(x_0, \ldots, x_k) = \varphi_0 + \sum_{k=1}^{\infty} p^k \sum_{a=0}^{p^k-1} I_{[a]_k}([x]_{k-1}) \varphi_{k,[a]_k}(x_k) \tag{4}$$

Соотношение вида (4) назовем координатным представлением функции Липшица f класса 1.

Теорема 3. *Пусть $f : \mathbb{Z}_p \to \mathbb{Z}_p$ функция Липшица класса 1 в координатном представлении (4). Функция f сохраняет меру тогда и только тогда, когда все функции φ_0 и $\varphi_{k,[a]_k}$, $a \in \{0, 1, \ldots, p^k - 1\}$ и $k \geq 1$ являются биективными на множестве $\{0, \ldots, p-1\}$.*

Доказательство. Пусть $f(x) = \sum_{m=0}^{\infty} B_m \chi(m,x) = \sum_{m=0}^{\infty} p^{\lfloor \log_p m \rfloor} b_m \chi(m,x)$ является представлением Ван дер Пута функции f и $a \in \{0,1,\ldots,p^k-1\}$. Найдем значения коэффициентов b_m.

Тогда $b_m(f) = B_m(f) = f(m)$ для $m \in \{0,\ldots,p-1\}$ и для $m = a+p^k x_k$, $a \in \{0,1,\ldots,p^k-1\}$, $x_k \neq 0$, $k \geq 1$

$$b_{a+p^k x_k}(f) = \frac{1}{p^k} B_{a+p^k x_k}(f) = \frac{f(a+p^k x_k) - f(a)}{p^k} =$$

$$= \varphi_k([a]_k, x_k) - \varphi_k([a]_k, 0) + p(\varphi_{k+1}([a]_k, x_k, 0) - \varphi_{k+1}([a]_k, 0, 0) + \ldots)$$

Таким образом $b_m(f) \equiv \varphi_0(m) (\mathrm{mod}\ p)$, $m \in \{0,\ldots,p-1\}$

$$b_m(f) = b_{a+p^k x_k}(f) \equiv \varphi_k([a]_k, x_k) - \varphi_k([a]_k, 0) \equiv$$

$$\equiv \varphi_{k,[a]_k}(x_k) - \varphi_{k,[a]_k}(0) (mod p), m = a + p^k x_k, x_k \neq 0$$

Функция f сохраняет меру тогда и только тогда, когда

1. $b_0(f), b_1(f), \ldots, b_{p-1}(f)$ устанавливают поный набор вычетов по модулю p;
2. $b_{a+p^k}(f), \ldots, b_{a+p^k(p-1)}(f)$ все ненулевые вычеты по модулю p.

Тогда первое условие эквивалентно биективности φ_0, а второе условие — биективности $\varphi_{k,[a]_k}$. □

Заключение. Изучение эргодичности мономиальных динамических систем на p-адических сферах было важно для развития p-адической теории динамических систем. С точки зрения приложений, потребность изучения эргодичности p-адических динамических систем возникает при решении задачи генерации псевдослучайных чисел: p-адические эргодические 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. Изучение p-адических динамических систем мотивировано их применениями в различных областях математики, физики, генетики, биологии, когнитивной науки, нейрофизиоло-

гии, информатики, криптологии и т.д. В частности, p-адические динамические системы нашли применение в криптографии, что стимулировало интерес к негладким динамическим отображениям. Важный класс (в общем случае) негладких отображений задается липшицевыми функциями класса 1. В настоящей работе приводится краткий обзор результатов о липшицевых функциях класса 1 и описывается сохранение меры (для меры Хаара на кольце целых p-адических чисел) и эргодических функций. Основным математическим инструментом, используемым в этой работе, является представление функции рядом Ван дер Пута, который активно используется в p-адическом анализе. Основным моментом в построении базиса Ван дер Пута является непрерывность характеристической функции p-адического шара. Также мы используем алгебраическую структуру (перестановки), индуцированную координатными функциями с частично замороженными переменными.