МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра компьютерной алгебры и теории чисел

Функции класса Lip 1 и дифференцирование по модулю в поле p-адических чисел

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студентки 4 курса 421 группы

направление 02.03.01 — Математика и компьютерные науки

механико-математического факультета

Красновой Елизаветы Сергеевны

Научный руководитель
зав. каф., к.ф.-м.н., доцент _____ А.М. Водолазов

Зав. кафедрой
зав. каф., к.ф.-м.н., доцент _____ А.М. Водолазов

Саратов 2022

Введение. P-адическое число — теоретико-числовое понятие, определяемое для заданного фиксированного простого числа p как элемент расширения поля рациональных чисел. Это расширение является пополнением поля рациональных чисел относительно p-адической нормы, определяемой на основе свойств делимости целых чисел на p. P-адические числа были введены Куртом Гензелем в 1897 году.

В настоящее время p-адический анализ является быстро развивающимся направлением в математике. Многочисленные применения p-адических чисел привели к теории p-адических дифференциальных уравнений, p-адической теории вероятностей, p-адической математической физике и так далее. P-адические числа также тесно связаны с диофантовыми уравнениями, т. е. с отысканием всех решений системы полиномиальных уравнений или с оценкой числа ее решений над полем p-адических чисел Q_p. Но одна и та же диофантова задача может иметь разные решения в поле p-адических чисел и в поле действительных чисел из-за различных топологических структур. p-адические числа находят широкое применение в теоретической физике.

Известны p-адические обобщённые функции, p-адический аналог оператора дифференцирования, p-адическая квантовая механика, p-адическая спектральная теория, p-адическая теория струн

Функции, известные в теории автоматов как детерминированные оказываются в точности теми функциями, которые удовлетворяют условию Липшица с коэффициентом 1.

Задачами данной работы являются:

►Рассмотрение p-адических чисел

►Рассмотрение метрики p-адических чисел

►Построение поля p-адических чисел

►Рассмотрение Функции класса Липшица

►Рассмотрение дифференциирования по модулю в поле p-адических чисел

Основное содержание работы. Рассмотрим основные понятия

Пусть X - не пустое множество. Функция d, определенная на множестве всех упорядоченных пар (x,y) элементов X и принимающая неотрицательные вещественные значения d(x,y), называется расстоянием или метрикой в X, если она обладает следующими свойствами:

1. d(x,y) = 0 тогда и только тогда, когда $x = y$;
2. d(x,y) = d(y,x);
3. $d(x, y) \leq d(x, z) + d(z, y) \quad \forall z \in X.$

Множество X вместе с заданной в нём метрикой d называется метрическим пространством. Одно и то же множество X может допускать много различных структур метрического пространства (X,d).

Чаще всего в качестве множеств X будем рассматривать поля. Поле F есть множество с двумя бинарными операциями «+» и «·», такими, что F является коммутативной группой относительно операции «+», а F-0 относительно операции «·», и выполнен закон дистрибутивности. Например это поля рациональных чисел Q и поле вещественных чисел R.

Определение 1.1. Нормой на поле F называется отображение, обозначаемое через || ||, поля F в множество неотрицательных вещественных чисел, такое, что:

1. ||x||=0 тогда и только тогда, когда x=0;
2. ||x·y|| = ||x||·||y||;
3. ||x+y||≤||x||+||y|| (неравенство треугольника). В общем случае вместо аксиомы (2) используется следующая:

2' $||xy|| \leq ||x||||y||$. В этом случае функция $|| \cdot ||$ называется псевдонормой. Норма $|| \cdot ||$ называется неархимедовой, если она удовлетворяет дополнительному условию:

3' $||x + y|| \leq || \max(||x||, ||y||)$ (сильное неравенство треугольника)

Когда говорится, что метрика d «соответствует» норме (или «индуцирована» нормой) || ||, то под этим понимается, что метрика d определяется соотношением d(x,y)= ||x-y||. Легко проверить, что функция d, заданная таким образом по произвольной норме || ||, будет действительно метрикой.

Основной пример нормы на поле рациональных чисел Q даёт абсолютная величина |x|. Индуцированная ею метрика d(x,y)=|x-y| совпадает с обычным расстоянием на числовой прямой

Одна метрика с поля Q известна: она индуцированна обычной абсолютной величиной.

Определение 1.2. Пусть p $\in 2, 3, 5, 7, 11, 13, \ldots$ - некоторое простое число. Для произвольного ненулевого целого числа a положим $ord_p a$ равным

кратности вхождения p в разложение a на простые сомножители, т.е. наибольшему целому неотрицательному числу m, для которого $a \equiv 0(mod p^m)$. Например $ord_5 35 = 1, ord_5 250 = 3$. Теперь, для произвольного рационального числа $x = a/b$ положим $ord_p x$ равным $ord_p a - ord_p b$. Так определенная величина зависит только от x, т.е. из представления $x = ac/bc$ получается то же самое значение для $ord_p x = ord_p ac - ord_p bc$

Кроме того, определим Q на следующее отображение $|\ |_p$:

$$|x|_p = \begin{cases} p^{\frac{1}{ord_p x}}, & \text{если } x \neq 0; \\ 0, & \text{если } x = 0 \end{cases}$$

Предложение 2.1. Функция $|\ |_p$ является нормой на поле Q.

Доказательство. Если x=0 или y=0, или x + y = 0, то свойство (3) очевидно. Поэтому предположим, что числа x,y,x+y отличны от нуля. Пусть x=a/b и y=c/d - несократимые представления. Тогда x+y = (ad+bc)/bd и $ord_p(x+y) = ord_p(ad+bc) - ord_p b - ord_p d$. Заметим теперь, что наибольшая степень p, делящая сумму двух целых чисел, не меньше любой степени p, которая делит одновременно каждое слагаемое. Поэтому

$$ord_p(x+y) \geq \min(ord_p ad, ord_p bc) - ord_p b - ord_p d =$$
$$= \min(ord_p a + ord_p d, ord_p b + ord_p c) - ord_p b - ord_p d =$$
$$= \min(ord_p a - ord_p b < ord_p c - ord_p d) = \min ord_p x < ord_p y.$$

Следовательно, $|x+y|_p = p^{-ord_p(x+y)} \leq \max(p^{-ord_p x}, p^{-ord_p y}) = \max(|x|_p, |y|_p)$, а последнее $\leq |x|_p + |y|_p$.

В действительности получилось более сильное неравенство, чем требуется в условии, и именно это усиленное неравенство приводит нас к одному из основных понятий p-адического анализа.

Теорема 2.2. Отображение $|\cdot|_p$ является неархимедовой нормой на поле рациональных чисел Q, т.е. удовлетворяет аксиомам (1.), (2.), (3.) из определения .

Доказательство. Очевидно, что аксиома (1.) выполнена. В силу того, что $ord_p(xy) = ord_p x + ord_p y$,аксиома (2.) также выполнена.

Проверим аксиому (3.). Если x=0 или y=0, или x+y=0, свойство (3.) тривиально, так что будем считать, что x,y,x+y не равны нулю. Пусть x=a/b, y=c/d. Тогда имеем x+y=(ab+bc)/bd и

$$\begin{aligned} ord_p(x+y) &= ord_p(ad+bc) + ord_p(bd) \\ &\geq min\big(ord_p(ad), ord_p(bc)\big) - ord_p(b) - ord_p(d) \\ &= min\big(ord_p(a) + ord_p(d), ord_p(b) + ord_p(c)\big) - ord_p(b) - ord_p(d) \\ &= min\big(ord_p(a) - ord_p(b), ord_p(c) - ord_p(d)\big) = min\big(ord_p(x), ord_p(y)\big). \end{aligned}$$

Следовательно,

$$|x+y|_p = p^{-ord_p(x+y)} \leq max\left(p^{-ord_p(x)}, p^{-ord_p(y)}\right) = max\big(|x|_p, |y|_p\big) \leq |x|_p + |y|_p.$$

Теорема 2.3. (Теорема Островского) Всякая нетривиальная норма $||\cdot||$ на поле Q эквивалентна либо вещественной норме $|\cdot|$, либо одной из p-адических норм $|\cdot|_p$.

Известно, что поле рациональных чисел Q не является полным ни по одной нетривиальной норме. При этом все нетривиальные нормы даются теоремой Островского. Поле вещественных чисел R является пополнением Q по вещественной норме $|\cdot|$. Определим поле Q_p p-адических чисе как пополнение поля Q по p-адической норме $|\cdot|_p$. Таким образом, пространство Q_p - ультраметрическое. По теореме Островского, существуют два «универсума»: вещественный и p-адический.

Мы строим Q_p посредством процедуры поплнения. Элементами Q_p являются классы эквивалентности последовательностей Коши Q по p-адической норме. Q можно отождествить с подполем Q_p, состоящим из классов эквивалентности, содержащих постоянные последовательности Коши.

Пусть $x \in Q_p$ и x_n - последовательность Коши рациональных чисел, представляющая a. Тогда по определению

$$|x|_p \stackrel{def}{=} \lim_{n\to\infty} |x_n|_p. \tag{1}$$

Если $|x|_p \neq 0$, то последовательность норм x_n стабилизируется в смысле $|x_n|_p = |x|_p$ для достаточно большого n. Этот факт следует также из сильного неравенства треугольника. Действительно, так как $|x_n - x|_p < |x|_p$ для достаточно большого n, то согласно сильному неравенству треугольника для достаточно большого n будем иметь:

$$|x_n|_p = |(x_n - x) + x|_p = \max(|x_n 0 x|_p, |x|_p) = |x|_p. \tag{2}$$

Таким образом p-адическая абсолютная величина продолжается Q_p, и имеем

$$\{|x|_p : x \in Q_p\} = \{|x|_p : x \in Q\} = \{p^\gamma : \gamma \in Z\} \cup \{0\}$$

В этом смысле, поведение p-адических чисе. При расширении Q и R, евклидова абсолютная величина принимает все неотрицательные действительные значения

P-адическая норма $|\cdot|_p$ на Q_p, заданная соотношением 1, обладает следующими свойствами:

Предложение 3.1. Если x,y $\in Q_p$, то

1 $|x|_p \geq 0, |x|_p = 0 \Longleftrightarrow x = 0$;

2 $|xy|_p = |x|_p|y|_p$;

3 $|x + y|_p \leq \max(|x|_p, |y|_p)$; Более того, если $|x|_p \neq |y|_p$ то

3' $|x + y|_p = \max(|x|_p, |y|_p)$

Таким образом норма на Q_p удовлетворяет сильному неравенству треугольника, т.е. является неархимедовой. Для любого $n \in N|nx|_p \leq |x|_p$.

Теперь можем распространить p-адическую аддитивную абсолютную величину (порядок) с Q на Q_p : для каждого $x \in Q_p$
$\{0\}$ положим

$$\upsilon_p(x) = ord_p(x) = -\log_p |x|_p, \upsilon_p(0) = ord_p(0) = \infty$$

Ясно, что соотношение

$$ord_p(xy) = ord_p(x) + ord_p(y), ord_p(x + y) \geq \min\big(ord_p(x), ord_p(y)\big).$$

верно для Q_p.

Операции, являющиеся в определенном смысле «элементарными» операциями-командами-для большинства процессов (такие как арифметические - сложение и кмножение, логические - OR, XOR, AND и другие - например, левый и правый сдвиги SHL, SHR, а также маскирование) и их различные композиции трактуются, как если бы они были непрерывными и могли бы быть аппроксимированы дифференцируемыми функциями. Они на самом деле являются непрерывными и могут быть аппроксимированы дифференцируемыми функциями, но в неархимедовой метрике.

Оказалось, что большая часть (если не все множество) таких «элементарных» для процессора операций (т.е. его команд) допускают простые и естественные продолжения на множество N_0 неотрицательных рациональных чисел. Но последнее по отношении к 2-адической метрике является всюду плотным подмножеством в компактном пространстве Z_2 всех целых 2-адических чисел. Примечательное заключается в том, что соответствующие продолжения вышеупомянутых операций являются непрерывными (а значит, равномерно непрерывными) функциями на Z_2.

Такой подход позволяет установить соответствия между «дискретными» и «непрерывными» свойствами некоторых классов функций. Например, с этой точкой зрения функции, известные в теории автоматов как детерминированные оказываются в точности теми функциями, которые удовлетворяют условию Липшеца с коэффициентом 1. также соответствие между биективными функциями на кольцу вычетов $Z/2^n$ и 2-адическими функциями, сохраняющими меру Хаара; между последовательностями максимального периода, порожденного конгруэнтными генераторами и равномерно распределенными последовательностями целых 2-адических чисел; между конгруэнтными генераторами максимального периоа и эргодическими относительно меры Хаара функциями.

Похоже, эти соотвествия не являются чем-то внешним, а демонстрируют неархимедову сущность компьютерных операций. Список команд процессора (или значительную его часть) обычо едается рассмотреть как множество равномерных 2-адических функций и, доказав средствами неархимедова анализа некоторое утверждение относительно определенной композиции этих

функций, тем самым получить утверждение относительно соответствующей компьютерной программы. В данной работе этот подход демонстрируется на примере программ - датчиков случайных чисел.

Упомянутые задачи изучаются в работе для произвольного простого p, однако в связи с ограничениями объема приведены доказательства лишь части результатов, в первую очередь относящихся к случаю p = 2, который наиболее важен для приложений, а с точки зрения техники доказательств стоит несколько особняком.

Определение 4.1. Пусть S и T - пространства с мерами μ и τ соответственно, f:S$\to$ T - измеримая функция (т.е. каждое множеств f^{-1} (U)μ-измеримо при τ-измеримом U $\subseteq$ T). Функцию f назовем пропорциональной, если для любых двух τ-измеримых можеств U, V $\subseteq$ T выполняется $\mu(f^{-1}(U)) = \mu(f^{-1}(V))$ как только τ (U) = τ (V). Если $\mu\tau$ - вероятностные меры (например, меры Хаара), то пропорциональная функция называется равновероятной. В случае, когда S=T и $\mu(U)$ для каждого измеримого множества U. Наконец, если f сохраняют меру и f^{-1}(U), говорим, что f эргодична.

Пропорциональные, сохраняющие меру и эргодические отображения, представляют собой полезные инструменты для конструирования равномерно распределенных последовательностей на топологических группах. Именно, справедливо следующее

Предложение 4.2. Пусть S и T - компактные топологические группы, f: S$\to$ T - непрерывная, измеримая относительно меры Хаара функция. Если $\{a_n\}_{n=0}^{\infty}$ - равномерно распределенная последовательность над S, а f - пропорциональная функция, то последовательность $\{f(a_n)\}_{n=0}^{\infty}$ равномерно распределена. Если, сверх того, f эргодична, то $\{f^n(a)\}_{n=0}^{\infty}$ равномерно распределена для почти всех a $\in$ S (по определению, $f^n(a) = f(f^{n-1}(a))$, $f^0(a) = a$.

Пусть A - компактная топологическая группа. В первую очередь нас интересуют равномерно распределенные последовательности целых p-адических чисел, т.е. случай, когда A изоморфна аддитивной группе кольца целых p-адических чисел Z_p. Общее опрееление равномерно распределеннойй последовательности над A в данном случае принимает следующий вид.

Определение 4.3. Последовательность $\{a_n\}_{n=0}^{\infty}$ называется равномерно распределенной над Z_p, если

$$\lim_{N\to\infty} \frac{\nu N^{a+p^k Z_p}}{N} = p^{-k}$$

для всех k = 1,2,..., a $\in Z_p$. (Здесь $\nu_N(U)$ - число тех $a_0, \ldots, a_N$, которые лежат в U).

Если вышеприведенное равенство выполняется лишь для некоторого $k = k_0$ говорим, что последовательность $\{a_n\}_{n=0}^{\infty}$ равномерно распределена по модулю p^{k_0}.

В соответствующем определении n-мерной равномерно распределенной последовательности $\{a_n \in Z_p^{(n)}\}_{n=0}^{\infty}$ вышеприведенное равенство меняется на

$$\lim_{N\to\infty} \frac{\nu N^{a+p^k Z_p^{(n)}}}{N} = p^{-kn}.$$

Далее, пусть функция f удовлетворяет условию Липшеца с коэффициентом 1: $||f(a) - f(b)||_p \leq ||a - b||_p$ для всех $a, b \in Z_p$, где $||\cdot||_p$ есть p-адическая норма. Последнее условие, очевидно, эквивалентно системе включений $f(a + p^k Z_p) \subseteq f(a) + p^k Z_p$ для всех открытых шаров $a + p^k Z_p$ в Z_p. В алгебре функция $g : A \to A$ называется консервативной, если для любой когруэнции η универсальной алгебры A и каждой пары $a, b \in A$ конгруэнтных по модулю η элементов их образы относительно g также конгруэнтны по модулю η. заметим, что каждая функция, индуцированная полиномом над универсалной алгеброй A консервативна. Такие функции называются полиномиальными функциями над универсальной алгеброй A. Поскольку $p^k Z_p$ есть идеал кольца Z_p и все идеалы в Z_p имеют такой вид, то сказанное означает, что f консервативна, и наоборот. Аналогичное верно и для n-мерных (n>1) функций, удовлетворяющих условию Липшеца с коэффициентом 1. Поэтому везде далее для простоты употребляется термин «консервативная функция» вместо «функция, удовлетворяющая условию Липшеца с коэффициентом 1». Стоит отметить, что такие функции представляют самостоятельный интерес для теории автоматов, где они известны под названием детерминированных.

Предложение 4.4. Пусть A - конечная группа, η - ее конгруэнция, $F : A^{(n)} \to A^{(m)}$ (где $m \leq n$) - пропорциональная (соответственно, биективная, транзитивная) консервативная функция. Тогда F пропорциональна (соответственно, биективна, транизитивна) по модулю η. Более того, если A есть прямое произведение групп B и C, $A = B \times C$, то F пропорциональна на A, если и только если она пропорциональна и на B и на C (т.е. по модулю каждой конгруэнции, соответствующей проектированию на прямой сомножитель). Наконец, $F : A \to A$ транзитивна тогда и только тогда, когда она транзитивна и на B и на C, и порядки |B| и |C| взаимно просты.

Предложение 4.5. Функция $f(x) = m + nx$ с рациональными целыми коэффициентами m, n транзитивна на Z/p^k тогда и только тогда, когда m и p взаимно просты и либо $n \equiv 1(mod p)$, либо p=2, k>1 и $n \equiv 1(mod 4)$.

Рассмотрим некоторый специальный класс p-адических функций, тесно связанных с равномерно дифференцируемыми функциями на Z_p.

Определение 5.1. Функцию $F = (f_1, \ldots, f_m) : Z^{(n)_p} \to Z_p^{(m)}$ назовем дифференцируемой по модулю p^k, в точке $u = (u_1, \ldots, u_n) \in Z_p^{(n)}$, если найдутся положительное рационально целое число N и матрица $F'_k(u)$ над Q_p размера $n \times m$ (которая называется матрицей Якоби по модулю p^k функции F в точке u) такие, что для каждого положительного целого $K \geq N$ и каждого $h = (h_1, \ldots, h_n) \in Z_p^{(n)}$ из системы неравенств $||h_1||_p \leq p^{-K} (i =, 1, 2, \ldots, n)$ следует, что

$$d_p^m(F(u+h), F(u) + hF'_k(u)) \leq p^{-k-K},$$

где d_p^m есть метрика на $Q_p^{(m)}$, индуцированная метрикой d_p на Q_p:

$$d_p^m(a, b) = max\{d(a_i, b_i) : i = 1, 2, \ldots, m\}$$

для всех $a = (a_1, a_2, \ldots, a_m), b = (b_1, \ldots, b_m \in Q_p^{(m)}$. Напомним, что по определению $d(u, v) = ||u - v||_p$ для всех $u, v \in Q_p$.

Предложение 5.2. Если функция $F = (f_1, \ldots, f_m) : Q_p^{(n)} \to Q_p^{(m)}$ дифференцируема в точке $u \in Q_p^{(n)}$, то она дифференцируема по модулю p^k в этой точке для всех $k = 1, 2, \ldots$.

Определение 5.3. Скажем, что функция $F = (f_1, \ldots, f_m) : Z_p^{(n)} \to Z_p^{(m)}$, дифференцируема по модулю p^k во всех точках $u \in Z_p^{(n)}$, имеет целочисленные производные по модулю p^k, если матрица $F_k'(u)$ есть матрица над Z_p.

Теорема 5.6. Если функция $F = (f_1, \ldots, f_m) : Z_p^{(n)} \to Z_p^{(m)}$ равномерно дифференцируема по модулю p и имеет целозначные производные по модулю p во всех точках из $Z_p^{(n)}$, то ее можно представить в виде

$$F(x_1, \ldots, x_n) = P(x_1, \ldots, x_n) + C(x_1, \ldots, x_n),$$

где P есть периодическая функция с периодом $p^{N_1(F)}$, а C - консервативная функция. Следовательно, F асимптотически консервативна, а C равномерно дифференцируема по модулю p.

Доказательство. Рассмотрим p-адическое представление функции F:

$$F(x_1, \ldots, x_n) = \left(\sum_{i=0}^{\infty} \delta_i(f_i(x_1, \ldots, x_n)))p^i, \ldots, \sum_{i=0}^{\infty} \delta_i(f_m(x_1, \ldots, x_n)))p^i \right),$$

и положим

$$P(x_1, \ldots, x_n) = \left(\sum_{i=0}^{N_1(F)-1} \delta_1(f_1(x_1, \ldots, x_n)))p^i, \ldots \right.$$
$$\left. \ldots, \sum_{i=0}^{N_1(F)-1} \delta_1(f_m(x_1, \ldots, x_n)))p^i \right),$$

$$C(x_1, \ldots, x_n)F(x_1, \ldots, x_n) - P(x_1, \ldots, x_n).$$

Для $l \geq N_1(F)$ и всех $s_1, \ldots, s_n \in Z_p$ из определения следует, что

$$F(x_1 + s_1 p^l, \ldots, x_n + s_n p^l) \equiv F(x_1, \ldots, x_n) \pmod{p^l}, \tag{3}$$

поскольку $F_1'(x_1, \ldots, x_n)$ есть матрица над Z/p и, следовательно,

$$(s_1 p^l, \ldots, s_n p^l) F_1'(x_1, \ldots, x_n) \equiv (0, \ldots, 0) \pmod{p^l}.$$

В частности, 3 означает, что F ассимптотически консервативна. Это в свою очередь означает, что $\delta_i(f_j(x_1, \ldots, x_n))$ зависит лишь от

$$\delta_0(x_1), \ldots, \delta_0(x_n), \ldots, \delta_i(x_1), \ldots, \delta_i(x_n),$$

если $i \geq N_1(F)$ (т.е. периодична с периодом p^{i+1}) и следовательно, C консервативна. С другой стороны, из 3 следует, что если $i < N_1(F)$, то $\delta_i(f_j(x_1, \ldots, x_n))$ не зависит от $\delta_r(x_t)$ при $r = N_1(F), N_1(F)+1, \ldots, t = 1, 2, \ldots, n, ..\delta_i(f_j(x_1, \ldots, x_n))$ периодична с периодом $p^{N_1(F)}$ для $i = 0, 1, \ldots, N_1(F) - 1, j = 1, 2, \ldots, m$. Значит функция $P(x_1, \ldots, x_n)$ также имеет период $p^{N_1(F)}$. Поскольку $P(x_1, \ldots, x_n)$ как периодическая функция с примарным по p периодом есть псевдоконстанта (либо константа), то соответствующие произвдные по модулю p у функций C и F совпадают, т.е. C равномерно дифференцируема по модулю p.

Заключение. В представленной бакалаврской работе были изучены и рассмотрены p-адические числа с соответствующей метрикой, поле p-адических чисел, а также функции класса Липшеца и дифференцирование в поле p-адических чисел по модулю p^k.

На языке C++ изучен генератор равномерно распределенной последовательности и представлен программный код его реализации в приложении А.