МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

(СГУ)

УТВЕРЖДАЮ

Зав. кафедрой,
к. ф.-м.н., доцент

Л.Б. Тяпаев

ОТЧЕТ О ПРАКТИКЕ

Студента 1 курса факультета КНиИТ, направление 09.04.01 «Информатика и вычислительная техника»

Шарова Александра Вадимовича

учебная

Дискретной математики и информационных технологий

курс 1

семестр 1

продолжительность 17 недель, с 01.09 .2018 г. по 31.12.2018г.

Руководитель практики

заведующий кафедрой, к.ф-м.н. Л.Б.Тяпаев

Саратов 2018

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ

1. $\mathbb{Z}$ – кольцо целых рациональных чисел
2. $\mathbb{Z}_+$ – множество натуральных чисел $\mathbb{N}$
3. $N_0 = \{0, 1, \dots\}$
4. $\mathbb{P}$ – множество простых чисел
5. Сепарабельное пространство – топологическое пространство, в котором можно выделить счётное всюду плотное подмножество
6. Плотное множество – подмножество пространства, точками которого можно сколь угодно хорошо приблизить любую точку объемлющего пространства.
7. Счётное множество – бесконечное множество, элементы которого возможно пронумеровать натуральными числами.
8. Хаусдорфово пространство — топологическое пространство, удовлетворяющее сильной аксиоме отделимости T_2.
9. Множество из $\mathbb{R}^n$ называется компактом, если из любой последовательности его точек можно выделить сходящуюся подпоследовательность, предел которой принадлежит этому множеству.
10. Локально компактное пространство — топологическое пространство, у каждой точки которого существует открытая окрестность, замыкание которой компактно.
11. Размерностью полного метрического пространства X называется наименьшее целое число n такое, что для любого покрытия пространства X существуют вписанное в него подпокрытие кратности $n + 1$.

ВВЕДЕНИЕ

Со времен Ньютона и Лейбница вещественные числа применялись как основной математический объект, который казалось бы отлично подходил для описания окружающего мира. В большинстве практических задач обычно составлялись уравнения и в последствии искалось числовое решение над полем действительных чисел $\mathbb{R}$. Обоснования почему в качестве описательного элемента выбрали именно поле $\mathbb{R}$ даже не стоял. В качестве пространства стандартом де-факто долгое время являлось пространство $\mathbb{R}^3$, а уже после открытий Римана и Эйнштейна $\mathbb{R}^4$.

С течением времени и наращиванием математического аппарата представление о том, что пространство $\mathbb{R}^3$ является наиболее подходящим для описания реального мира все усиливалось, но надо понимать, что евклидово пространство $\mathbb{R}^3$ не более чем удачно выбранная модель описания реального физического пространства.

Так как реальный мир построен на евклидовой геометрии, то получается, что и она очень хорошо описывается вещественными числами, но в случае если бы мы могли отказаться от использования данной геометрии для изучения реального мира мы бы могли отказаться и от вещественной числовой системы. Но какую выбрать систему в данном случае? На этот ответ лучше всего отвечает теория p-адического исчисления, которая является с математической точки зрения более подходящей для описания тех объектов, с которыми приходиться работать в задачах физики, биологии и криптографии.[1]

Целью данной научной работы является изучение основ p-адического анализа на поле $\mathbb{Z}_p$. В данной работе будут рассмотрены такие понятия как p-адическое числа, пространства, функции и p-адическая дифференцируемость. В качестве наглядного примера отличия анализа на $\mathbb{R}$ и на $\mathbb{Z}_p$ будет рассмотрена теорема о среднем значении.

1 p-Адические числа

1.1 p-Адическая норма

Определение 1. Пусть M - некоторое непустое множество, и пусть $d : M \times M \to \mathbb{R}_{\geq 0}$ – функция двух переменных, определенная на этом множестве и принимающая значения во множестве действительных неотрицательных чисел. Функция d называется метрикой (а множество M – метрическим пространством), если d удоволетворяет трем условиям:

1. Для каждой пары $a, b \in M$ справедливо: $d(a, b) = 0$ тогда и только тогда, когда $a = b$.
2. Для каждой пары $a, b \in M$ справедливо равенство $d(a, b) = d(b, a)$.
3. Для каждой тройки $a, b, c \in M$ справедливо неравенство $d(a, b) \leq d(a, c) + d(c, b)$.

Пример 1. Множество $\mathbb{R}$ всех действительных чисел есть метрическое пространство с метрикой $d(a, b) = |a - b|$, где $|.|$ есть абсолютная величина.

Определение 2. Функция $\|.\|$, определенная на произвольном коммутативном кольце R и принимающая значения в $\mathbb{R}_{\geq 0}$ называется нормой (также, абсолютной величиной), если она удовлетворяет следующим условиям:

1. Для любого $a \in R$ справедливо, что $\|a\| = 0$ тогда и только тогда, когда $a = 0$.
2. Для каждой пары $a, b \in R$ справедливо равенство $\|a \cdot b\| = \|a\| \cdot \|b\|$.
3. Для каждой пары $a, b \in R$ справедливо неравенство треугольника: $\|a + b\| \leq \|a\| + \|b\|$

Из определения следует, что если положить $d(a, b) = \|a - b\|$, то фактически будет задана метрика d на кольце R. Данная метрика называется метрикой, индуцированной нормой $\|.\|$.

Определение 3. Пусть $p \in \mathbb{P}$ – некоторое простое число. В поле $\mathbb{Q}$ введем другую норму $\|.\|_p$ по правилу:

1. $\|0\|_p = 0$,
2. $\|n\|_p = p^{-ord_p n}$,

где $n > 0$ некоторое натуральное число, а $ord_p n$ показатель степени, в которой число p входит в это произведение. В этом случае норма $\|.\|_p$ называется p-адической нормой.

Норма $\|.\|_p$ удовлетворяет всеми характерными свойствами нормы даже в более сильной форме, а именно:

1. $\|x\|_p \geq 0$, причем $\|x\|_p = 0$ если $x = 0$.
2. $\|xy\|_p = \|x\|_p \cdot \|y\|_p$.
3. $\|x + y\|_p \leq \max(\|x\|_p, \|y\|_p)$ [2]

Заметим, что норма $\|x\|_p$ может принимать лишь счетное число значений $p^{-ord_p n}$.

Также, норма $\|x\|_p$ определяет ультраметрику на $\mathbb{Q}$. Данная норма неархимедова, так как $\|nx\|_p \leq \|x\|_p \, \forall n \in \mathbb{Q}_+$.

Теорема 1. *Нормы* $\|.\|$ *и* $\|.\|_p \; \forall p = 2, 3, \ldots$ *исчерпывают все нетривиальные неэквивалентные нормы поля рациональных чисел* $\mathbb{Q}$.

1.2 p-Адические числа

Определение 4. Пополнение поля $\mathbb{Q}$ по p-адической норме образует поле $\mathbb{Q}_p$ p-адических чисел. Поле $\mathbb{Q}_p$ аналогично полю $\mathbb{R} = \mathbb{Q}_\infty$ вещественных чисел, получаемых пополнение поля $\mathbb{Q}$ по норме $\|x\| = \|x\|_\infty$.

Определение 5. Любое p-адическое число $x \neq 0$ однозначно представляется в каноническом виде

$$x = p^\gamma \cdot (x_0 + x_1 \cdot p + x_2 \cdot p^2 + \ldots \tag{1}$$

где $\gamma = \gamma(x) \in \mathbb{Z}$ и x_j – целые числа такие, что $0 \leq x_j \leq p - 1$, $x_0 > 0$, $(j = 0, 1, \ldots)$.

Представление (1) аналогично разложению любого вещественного числа x в бесконечную десятичную дробь:

$$x = \pm 10^\gamma \cdot (x_0 + x_1 \cdot 10^{-1} + x_2 \cdot 10^{-2} + \ldots),$$
$$\gamma \in \mathbb{Z}, x_j = 0, 1, \ldots, 9, x_0 > 0,$$

и доказывается аналогично.

Помимо разложения, представление (1) дает рациональные числа тогда и только тогда, когда, начиная с некоторого номера числа $x_j, j = 0, 1, \ldots$ образуют периодическую последовательность.

Определение 6. Поле $\mathbb{Q}_p$ является коммутативно-ассоциативной группой по сложению;

Определение 7. Поле $\mathbb{Q}_p^* = \mathbb{Q}_p \setminus \{0\}$ является коммутативно-ассоциативной группой по умножению;

Определение 8. Поле $\mathbb{Q}_p^*$ называется мультипликативной группой поля $\mathbb{Q}_p$[3];

Определение 9. p-адические числа x, для которых $\|x\|_p \leq 1$ (т.е. $\gamma(x) \geq 0$ или $\{x\}_p = 0$), называются целыми p-адическими числами, и их множество обозначается $\mathbb{Z}_p$. Множество $\mathbb{Z}_p$ является подкольцом кольца $\mathbb{Q}_p$; $\mathbb{Z}_+$ плотно в $\mathbb{Z}_p$. Целые числа $x \in \mathbb{Z}_p$, для которых $\|x\|_p = 1$, называютсяются единицами в $\mathbb{Z}_p$. [4]

Совокупность элементов x из $\mathbb{Z}_p$, для которых $\|x\|_p < 1$ (т.е. $\gamma(x) \geq 0$ или $\|x\|_p \leq \frac{1}{p}$) образуют главный идеал кольца $\mathbb{Z}_p$; Данный идеал имеет вид $p\mathbb{Z}_p$. Поле вычетов $\mathbb{Z}_p \setminus p\mathbb{Z}_p$ состоит из p элементов. В мультипликативной группе поля $\mathbb{Z}_p \setminus p\mathbb{Z}_p$ существует единица $\eta \neq 1$ порядка $p-1$ такая, что элементы $0, \eta, \eta^2, \ldots, \eta^{p-1} = 1$ образуют полный набор представителей классов вычетов поля $\mathbb{Z}_p \setminus p\mathbb{Z}_p$.

1.3 Пространство p-адических чисел $\mathbb{Q}_p$

В силу свойств p-адической нормы норма в поле $\mathbb{Q}_p$ удовлетворяет неравенству треугольника:

$$\|x+y\|_p \leq \max(\|x\|_p, \|y\|_p) \leq \|x\|_p + \|y\|_p, x, y \in \mathbb{Q}_p.$$

Следовательно в $\mathbb{Q}_p$ можно ввести метрику:

$$\rho(x,y) = \|x-y\|_p. \tag{2}$$

При этом $\mathbb{Q}_p$ становится полным метрическим пространством. Из представления (1) следует сепарабельность $\mathbb{Q}_p$.

Определение 10. $B_\gamma(a)$ – круг радиуса p^{γ^p} с центром в точке $a \in \mathbb{Q}_p$:

$$B_\gamma(a) = \left\{ x : \|x-a\|_p \leq p^\gamma \right\}, \gamma \in \mathbb{Z} \tag{3}$$

Определение 11. $S_\gamma(a)$ – граница радиуса p^{γ_p}.

$$S_\gamma(a) = \left\{ x : \|x - a\|_p = p^\gamma \right\}, \gamma \in \mathbb{Z} \tag{4}$$

Лемма 1. *Если $b \in B_\gamma(a)$, то $B_\gamma(b) = B_\gamma(a)$.*

Замечание 1. *Круг $B_\gamma(a)$ и окружность $S_\gamma(a)$ – открыто-замкнутые множества в $\mathbb{Q}_p$.*

Замечание 2. *Всякая точка круга $B_\gamma(a)$ является его центром.*

Замечание 3. *Любые два круга в $\mathbb{Q}_p$ либо не имеют общих точек, либо один содержится в другом.*

Замечание 4. *Всякое открытое множество в $\mathbb{Q}_p$ есть объединение не более чем счетного числа кругов без общих точек.*

Лемма 2. *Если множество $M \subset \mathbb{Q}_p$ содержит две различные точки a и b, $a \neq b$, то его можно представить в виде объединения непересекающихся открыто-замкнутых (в M) множеств M_1, M_2 таких, что $a \in M_1, b \in M_2$.*

Лемма (2) утверждает, что всякое множество пространства $\mathbb{Q}_p$, состоящее из более чем одной точки, несвязно. Другими словами, связная компонента любой точки совпадает с самой точкой. Из этого следует, что $\mathbb{Q}_p$ является вполне несвязным пространством.

Если рассматривать лемму для случая, когда множество M состоит только из двух точек a и b, убеждаемся, что существует непересекающиеся окрестности этих точек. Из этого можно сделать вывод, что пространство $\mathbb{Q}_p$ хаусдорфово.

Лемма 3. *Для того чтобы множество $K \subset \mathbb{Q}_p$ было компактом, необходимо и достаточно, чтобы оно было замкнутым и ограниченным в $\mathbb{Q}_p$*

Замечание 5. *Всякий круг $B_\gamma(a)$ является и окружность $S_\gamma(a)$ компакты.*

Замечание 6. *Пространство $\mathbb{Q}_p$ локально компактное.*

Замечание 7. *Всякий компакт можно покрыть конечным числом кругов фиксированного радиуса без общих точек.*

Замечание 8. *В пространстве $\mathbb{Q}_p$ справедлива лемма Гейне-Бореля: из каждого бесконечного покрытия компакта K можно выбрать конечное покрытие K.*

Теорема 2. *Размерность пространства $\mathbb{Q}_p$ равна* 0.

2 p-Адический анализ в $\mathbb{Z}_p$

Так как компакт $\mathbb{Z}_p$ есть пополнение множества $\mathbb{N}_0$ по метрике $d_p(x,y) = \|x-y\|_p$, то любое число из $\mathbb{Z}_p$ есть предел последовательности чисел из $\mathbb{N}_0$.

Определение 12. p-адическое целое z является пределом последовательности $\{z_i\}_{i=0}^{\infty}$, если если для любого $\epsilon > 0$ найдется N такое, что $\|z_i - z\|_p < \epsilon$ как только $i > N$. [5]

Определение 13. p-адическое целое z есть предел последовательности $\{z_i\}_{i=0}^{\infty}$, если для любого (достаточно большого) положительного рационального целого K найдется N такое, что $z_i \equiv z \pmod{p}^K$ при всех $i > N$. [5]

Замечание 9. *По определению p-адической метрики* $\|z_i - z\|_p \leq p^{-K}$ *тогда и только тогда, когда* $z_i \equiv z \pmod{p}^K$. *[5]*

Определение 14. Функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$ называется непрерывной в точке $z \in \mathbb{Z}_p$, если для любого (достаточно большого) положительного рационального целого M найдется положительное рациональное целое L такое, что $f(x) \equiv f(z) \pmod{p}^M$ как только $x \equiv z \pmod{p^L}$. [5]

Определение 15. Функция f называется равномерно непрерывной на $\mathbb{Z}_p$, если f непрерывна в каждой точке $z \in \mathbb{Z}_p$, и L зависит только от M и не зависит от z.[6]

2.1 p-адическая дифференцируемость

Определение 16. Функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$ называется дифференцируемой в точке $z \in \mathbb{Z}_p$, если существует p-адическое число $f'(x) \in \mathbb{Q}_p$ такое, что для любого $M \in \mathbb{N}$ справедливо

$$\left\| \frac{f(x+h) - f(x)}{h} - f'(x) \right\|_p \leq \frac{1}{p^M}, \tag{5}$$

если h достаточно мало, т.е. когда $\|h\|_p \leq p^{-K}$, где $K = K(M)$ достаточно велико.

Определение 17. Функция f называется равномерно дифференцируемой (на $\mathbb{Z}_p$), если неравенство (5) выполняется одновременно для всех $x \in \mathbb{Z}_p$ как только h достаточно мало. [7]

Лемма 4. *Если совместимая функция* $f : \mathbb{Z}_p \to \mathbb{Z}_p$ *дифференцируема в точке* $x \in \mathbb{Z}_p$, *то* $f'(x) \in \mathbb{Z}_p$.

Определение 18. Функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$ называется дифференцируемой в точке $x \in \mathbb{Z}_p$, если существует p-адическое число $f'(x) \in \mathbb{Q}_p$ такое, что для любого $M \in \mathbb{N}$ справедливо

$$f(x+h) \equiv f(x) + h \cdot f'(x) \pmod{p}^{M+ord_p h} \tag{6}$$

Определение 19. Функция f называется равномерно дифференцируемой (на $\mathbb{Z}_p$), если неравенство (6) выполняется одновременно для всех $x \in \mathbb{Z}_p$ как только h достаточно мало, т.е. когда $ord_p h \geq K = K(M)$ для достаточно большого $K \in \mathbb{N}$.

Замечание 10. *Правила дифференцирования не зависят от метрики: для вычисления производных суммы, частного и сложной функции в p-адическом анализе используются те же формулы, что и в действительном.*

Замечание 11. *Между действительным и p-адическим анализом существует резкое различие например в том, что в и в том, и в в другом случае производная константы равна* 0, *однако в p-адическом анализе в отличии от действительного равенство нулю производной некоторой функции не означает, что эта функция константа.*

2.2 теорема о среднем

Теорема 3. *(в* $\mathbb{R}$*) Если функция* $f(x)$ *непрерывна на отрезке* $[a, b]$ *и дифференцируема на интервале* (a, b), *то в этом интервале найдется хотя бы одна точка* ξ, *такая, что* $f(b) - f(a) = f'(\xi)(b - a)$.

Ключевая проблема в доказательстве данной теоремы на поле $\mathbb{Q}_p$ в том, что поле $\mathbb{Q}_p$ неупорядоченное. Но эта трудность может быть устранена[8]. В $\mathbb{R}$ мы можем переопределить среднее так, что:

$$\xi = at + b(1-t) \quad \forall 0 \leq t \leq 1;$$

такое преобразование, к примеру, делается когда данная теорема доказывается в поле $\mathbb{C}$. Теперь мы можем написать p-адический аналог теоремы о среднем.

Теорема 4. *(в $\mathbb{Q}_p$)[9] Если функция $f(x)$ дифференцируема и производная непрерывна на $\mathbb{Q}_p$, то для любых двух чисел a и b из множества $\mathbb{Q}_p$ найдется такой элемент $\xi \in \mathbb{Q}_p$, что:*

$$\xi = at + b(1-t) \quad \forall t : |t| \leq 1$$

для которого:

$$f(b) - f(a) = f'(\xi)(b-a).$$

Доказательство. Возьмем $f(x) = x^p - x, a = 0, b = 1$, тогда производная $f'(x) = px^{p-1} - 1$ и $f(a) = f(b) = 0$. Теорема предполагает, что существует такое число $\xi : p\xi^{p-1} - 1 = 0$. В свою очередь любое $\xi = at + b(1-t) = (1-t)$, где $t \in \mathbb{Z}_p$ (это значит, что $t| \leq 1$), должно принадлежать $\mathbb{Z}_p$. В свою очередь $p\xi^{p-1} - 1$ принадлежит $\mathbb{Z}_p$ (а это принадлежит $1 + p\mathbb{Z}_p$) и из-за этого не может быть нулем. □

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Козырев, С. В. Методы и приложения ультраметрического и p-адического анализа: от теории всплесков до биофизики / С. В. Козырев // Совр. пробл. матем. 2008. Т. 12. С. 3–168.

2 И.В., Волович. p–Адическая математическая физика: основные конструкции, применения к сложным и наноскопическим системам / [Волович И.В., Козырев С.В. : б. и.], 2008. 30 с.

3 Baker, A. An Introduction to p-adic Numbers and p-adic Analysis / [A. Baker : s. n.], 2017. 64 p.

4 Владимиров, В.С. p-Адический анализ и математическая физика / [В.С. Владимиров, Волович И.В., Зеленов Е.И.] : М.:Физматлит, 1994. 352 с.

5 Анашин, В.С. Введение в прикладной p-адический анализ / [В.С. Анашин : б. и.].

6 Ciocan, N. P-adic Functions - Part 1 / [N. Ciocan : s. n.], 2011. 11 p.

7 Anashin, V. The p-adic ergodic theory and applications / [V. Anashin : s. n.], 2014. 221 p.

8 Gouvea, F.Q. p-adic Numbers: An Introduction / [F.Q. Gouvea] : Springer, 2011. 306 p.

9 Alain, M.R. A Course in p-adic Analysis / [M.R. Alain] : Springer-Verlag New York, 2000. 438 p.