ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Л.Н. Гумилев атындағы Еуразия ұлттық университетінің 20 жылдығы және механика-математика факультеті «Механика» кафедрасының құрылғанына 10 жыл толуы аясында өтетін «МЕХАНИКА ЖӘНЕ МАТЕМАТИКАНЫҢ ӨЗЕКТІ МӘСЕЛЕЛЕРІ» атты Республикалық ғылыми-әдістемелік конференциясы

БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ

Республиканской научно-методической конференции «АКТУАЛЬНЫЕ ВОПРОСЫ МЕХАНИКИ И МАТЕМАТИКИ», посвященной 20-летию Евразийского национального университета им. Л.Н. Гумилева и 10-летию основания кафедры «Механика» механико-математического факультета Евразийского национального университета им. Л.Н. Гумилева

2016 жыл 14-15 қазан

Астана

ӘОЖ 531:510 (063)
КБЖ 22
М 49

В подготовке Сборника к печати принимали участие:
Джайчибеков Н.Ж., Ибраев А.Г., Бургумбаева С.К., Бостанов Б.О.

«Механика және математиканың өзекті мәселелері» атты Республикалық ғылыми-әдістемелік конференциясының БАЯНДАМАЛАР ЖИНАҒЫ. Л.Н. Гумилев атындағы Еуразия ұлттық университетінің 20 жылдығы және механика-математика факультеті «Механика» кафедрасының құрылғанына 10 жыл толуына арналған = «Актуальные вопросы механики и математики», посвященной 20-летию Евразийского национального университета им.Л.Н. Гумилева и 10-летию основания кафедры «Механика» механико-математического факультета Евразийского национального университета им. Л.Н. Гумилев. СБОРНИК МАТЕРИАЛОВ Республиканской научно-методической конференции. Қазақша, орысша. – Астана, 2016, 292 б.

ISBN 998-601-301-808-9

Жинаққа студентердің, магистранттардың, докоранттардың және ғалымдардың механика, математика, математикалық және компьютерлік модельдеу, механика және математиканы оқыту әдістемесінің өзекті мәселелері бойынша баяндамалары енгізілген.

В Сборник вошли доклады студентов, магистрантов, докторантов и ученых по актуальным вопросам механики, математики, математического и компьютерного моделирования и методика преподавания механики и математики.

Тексты докладов печатаются в авторской редакции

ISBN 998-601-301-808-9 ӘОЖ 531:510 (063)
КБЖ 22

$$y^2 = x^3 + ax + b(\mathrm{mod}\, p),\ a,\ b \equiv GF(p)$$

Пары *(x,y)* будем называть точкой. Точки эллиптической кривой можно «складывать». «сумма» двух точек, в свою очередь, тоже лежит на эллиптической кривой.

Кроме точек, лежащих на эллиптической кривой, рассматривается также нулевая точка. Считается, что сумма двух точек A с координатами $(X_A,\ Y_A)$ и B с координатами (X_B, Y_B) равна 0, если $X_A = X_B,\ Y_A = -Y_B\ (mod\ p)$. Нулевая точка не лежит на эллиптической кривой, но, тем не менее, участвует в вычислениях; ее можно рассматривать как бесконечно удаленную от кривой.

Ф. Асабаева и Д. Козыбаев [7] доказали

Теорема *Для построения криптографических алгоритмов на основе эллиптических кривых необходимым и достаточным условием является несингулярность эллиптических кривых, т.е.* $\left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2 \neq 0$.

Используя эти результаты мы можем заключить, что алгебра Пуассона, построенная на эллиптических кривых пригодна для применения в криптографических протоколах.

Список использованных источников

1. Одесский А.В., Рубцов В.Н. Полиномиальные алгебры Пуассона с регулярной структурой симплектических листов// ТМФ, 2002, том 133, номер 1, страницы 3–23.
2. Одесский А.В. Эллиптические алгебры// Успехи математических наук, 2002, том 57, номер 6 (348), стр. 87-122.
3. Korovnichenko A., Spiridonov V.P. and Zhedanov A.S. Poisson Algebras on Elliptic Curves// Proceedings of Institute of Mathematics of NAS of Ukraine, 2004, Vol. 50, Part 3, 1116–1123.
4. Макар-Лиманов Л.Г. Об автоморфизмах свободной алгебры с двумя образующими// Функциональный анализ и его приложения, 1970, т. 4, стр. 107-108.
5. Czerniakiewicz A.J. Automorphisms of a free associative algebras of rank 2// Trans. Amer. Math. Soc., 1971, V. 160, P. 393-401.
6. Makar-Limanov L., Turusbekova U., Umirbaev U., Automorphisms and derivations of free Poisson algebras in two variables// Journal of Algebra, Volume 322, Issue 9, 1 November 2009, P. 3318-3330.
7. Асабаева Ф.Б., Козыбаев Д.Х. Применение эллиптических кривых в современных криптографических алгоритмах //Труды международной конференции Валихановские чтения 17. Май – 2013, Кокшетау. С.28-32.

УДК 517.51

ПОРЯДОК УБЫВАНИЯ КОЭФФИЦИЕНТОВ ФУРЬЕ В СМЫСЛЕ СРЕДНИХ АРИФМЕТИЧЕСКИХ

Муканова А.М., Игенберлина А.Е.

Aimira-814@mail.ru

ЕНУ им. Л.Н.Гумилева, Астана, Казахстан

Пусть $f(t) \in L_1[-1,1]$ и a_n ее косинус коэффициенты Фурье

$$a_n = \int_{-1}^{1} f(t)\cos n\pi t dt$$

Лемма Римана-Лебега говорит о том, что $a_n \to 0$ при $n \to \infty$ [1]. Но скорость сходимости может быть как угодно медленной, поскольку для любой последовательности (k_n), такой, что $|k_n| \to \infty$ при $n \to \infty$ мы имеем

$$k_n a_n = \int_{-1}^{1} f(t) k_n \cos n\pi t dt = T_n f \ ,$$

где T_n линейный функционал на $L_1[-1,1]$, имеющий норму

$$\|T_n\| = \max_{|t|\le 1} |k_n \cos n\pi t| = |k_n|,$$

Поэтому $k_n a_n \to 0$ для каждой $f(t) \in L_1[-1,1]$, что противоречит принципу равномерной ограниченности [2]. Для $f(t) \in C[-1,1]$ также верны подобные рассуждения.

Однако, оказывается, можно сделать точное утверждение о порядке убывания косинус коэффициентов Фурье, если трактовать, например, $na_n \to 0$ в более слабом смысле. Конкретно мы покажем, что если $f(t) \in L_2[-1,1]$, то $n^{\frac{1}{2}} a_n \to 0$ в смысле чезаровских средних, т.е.

$$\frac{a_1 + 2^{\frac{1}{2}} a_2 + \ldots + n^{\frac{1}{2}} a_n}{n} \to 0 \ ,$$

и во-вторых, что если $f(t) \in C[-1,1]$, то $na_n \to 0$ в смысле чезаровских средних второго порядка, т.е. если

$$u_n = \frac{a_1 + 2a_2 + \ldots + na_n}{n},$$

$$v_n = \frac{u_1 + u_2 + \ldots + u_n}{n},$$

то $v_n \to 0$. Из этого возможно сделать вывод, например, что если $a_n \ge a_{n+1} \ge 0$ для всех $n \ge 0$, то имеет место сходимость в обычном смысле в обоих случаях.

Мы также докажем подобные результаты для синус коэффициентов Фурье

$$b_n = \int_{-1}^{1} f(t) \sin n\pi t dt$$

хотя в некоторых случаях доказательства разные.

Для оценивания скорости сходимости коэффициентов Фурье $f(t) \in L_2[-1,1]$ нам понадобятся теорема Рисса-Фишера и две леммы о сходимости по Чезаро.

Лемма 1. Для любого сходящегося ряда $\sum_{n=1}^{\infty} a_n$, мы имеем, что $na_n \to 0$ в смысле Чезаро.

Доказательство. Пусть $S_n = a_1 + a_2 + \ldots + a_n \to S$. Тогда

$$\frac{a_1 + 2a_2 + \ldots + na_n}{n} = \frac{S_1 + 2(S_2 - S_1) + \ldots + n(S_n - S_{n-1})}{n} = S_n - \frac{S_1 + S_2 + \ldots + S_{n-1}}{n} \to S - S = 0$$

Лемма 2. Если $a_n \ge 0$ и $a_n \to 0$ в смысле Чезаро, то $a_n^{\frac{1}{2}} \to 0$ в смысле Чезаро.

Доказательство. Мы имеем

$$\frac{a_1^{\frac{1}{2}} + \ldots + a_n^{\frac{1}{2}}}{n} \le \frac{(n(a_1 + \ldots + a_n))^{\frac{1}{2}}}{n}$$

по неравенству Коши

$$=\left[\frac{a_1+...+a_n}{n}\right]^{\frac{1}{2}}\to 0.$$

Теорема 1. Если

$$a_n=\int_{-1}^{1} f(t)\cos n\pi t dt,\quad n=1,2,...,$$

– косинус коэффициенты Фурье функции $f(t)\in L_2[-1,1]$, то $n^{\frac{1}{2}}a_n\to 0$ в смысле Чезаро.

Доказательство. Из Теоремы Рисса-Фишера мы имеем, что $\sum_{n=1}^{\infty}a_n^2<\infty$, т.е. ряд $\sum_{n=1}^{\infty}a_n^2$ – сходится. Тогда по лемме 1, $na_n^2\to 0$ в смысле Чезаро, и поэтому из леммы 2, $n^{\frac{1}{2}}a_n\to 0$ в смысле Чезаро.

Для оценивания скорости сходимости коэффициентов Фурье $f(t)\in C[-1,1]$ нам понадобится теорема Фейера и лемма 3.

Лемма 3. Если $\sum_{n=1}^{\infty}a_n$ сходится в смысле Чезаро, то $na_n\to 0$ в смысле Чезаро второго порядка.

Доказательство. Пусть $S_n=a_1+a_2+...+a_n$

$$\sigma_n=\frac{S_1+S_2+...+S_n}{n}$$

и предположим $\sigma_n\to\sigma$.

Если

$$u_n=\frac{a_1+2a_2+...+na_n}{n}$$

$$v_n=\frac{u_1+u_2+...+u_n}{n},$$

Тогда

$$u_n=\frac{S_1+2(S_2-S_1)+...+n(S_n-S_{n-1})}{n}=\frac{nS_n-S_1-S_2-...-S_{n-1}}{n}=S_n-\frac{n-1}{n}\sigma_{n-1}=S_n-t_n,$$

где

$$t_n=\frac{n-1}{n}\sigma_{n-1}\to\sigma$$

и следовательно

$$v_n=\sigma_n-\frac{t_1+t_2+...+t_n}{n}\to\sigma-\sigma=0.$$

Контрпример $\sum_{n=1}^{\infty}(-1)^n$ показывает, что при тех же условиях на ряд $\sum_{n=1}^{\infty}a_n$ не вытекает сходимость $na_n\to 0$ в простом чезаровском смысле.

Теорема 2. Если

$$a_n = \int_{-1}^{1} f(t)\cos n\pi t dt, \quad n = 1,2,...,$$

– косинус коэффициенты Фурье функции $f(t) \in C[-1,1]$, то $na_n \to 0$ в смысле Чезаро второго порядка.

Доказательство. По теореме Фейера $\sum_{n=0}^{\infty} a_n$ сходится в смысле Чезаро (к f(0)). Поэтому, результат следует из леммы 3.

Заметим, что мы предположили f(t) непрерывной при t=0.

Принцип равномерной ограниченности показывает, что существует $f(t) \in C[-1,1]$, для которой $na_n \not\to 0$ в обычном смысле Чезаро.

Список использованных источников

1. Бари Н.К. Тригонометрические ряды. – М: Физматгиз, 1961. – 936 с.
2. Ready J. On the order of magnitude of Fourier coefficients // SIAM J.Math.Anal. – 1986. – N 17. – P. 469–476.

УДК 517.51

ФУНКЦИИ ОГРАНИЧЕННОЙ СРЕДНЕЙ ОСЦИЛЛЯЦИИ И ПРОСТРАНСТВО БЕСОВА

Муканов Ж.Б., Байсалбаева Л.Е.

lbaisalbayeva@mail.ru

ЕНУ им. Л.Н.Гумилева, Астана, Казахстан

В данной работе рассматриваются пространство Бесова для функций многих переменных и класс функций, связанный с функциями ограниченной средней осцилляции.

Приведём необходимые определения и обозначения. Пусть $\{p_{k_j}^{(j)}\}_{k_j=1}^{\infty}$ - последовательности целых чисел $p_{k_j}^{(j)} \ge 2$, j=1, 2, …, n; $k_j = 1,2,...,$ и пусть

$$G^{(j)} = \{x = \{x_{k_j}^{(j)}\}_{k_j=1}^{\infty}, 0 \le x_{k_j}^{(j)} \le p_{k_j}^{(j)} - 1\}, j = 1,2,...,n,$$

- соответствующие группы Виленкина целочисленных последовательностей с групповой операцией $(\dot{+})$ покоординатного сложения по модулю $p_{k_j}^{(j)}$; $G^n = \prod_{j=1}^{n} G^{(j)}$ - прямое произведение групп $G^{(j)}$. Множества

$$G_{v_l}^{(j)} = \{x = \{x_{k_j}^{(j)}\}_{k_j=1}^{\infty} \in G^{(j)} : x_{k_j}^{(j)} = 0, 0 \le k_j < v_l\}, \ j = 1,...,n; v_l = 1,2,...,$$

являются подгруппами группы $G^{(j)}$, и система подгрупп $G(v_l) = \prod_{j=1}^{n} G_{v_l}^{(j)}$ $(v_l = 1,2,...)$ группы G^n задаёт систему окрестностей нуля в G^n. Относительно введённой операции сложения и топологии группа G^n является компактной абелевой нуль-мерной группой (в одномерном случае см. [1]). Положим