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

Қолданылған әдебиеттер тізімі

1. Азбелев Н. В. и Рахматуллина Л. Ф. Функционально-дифференциальные уравнения.- Дифференц.уравнения, 1978, т.14, № 5, с.771-797.
2. Максимов В. П. Вопросы общей теории функционально-дифференциальных уравнений.- Дис.д-ра физ.-мат.наук, Киев, 1984,- 275 с.
3. Треногин В.А. Функционалный анализ: Учебник.- 4-е изд.,испр.-М.: ФИЗМАТЛИТ, 2007.
4. Ибатов А. О нормально разрешимых задачах для функционально-дифференциальных уравнений.- В кн.: Тезисы докладе конференции молодых ученых КазГУ им.С.М.Кирова, посвященной 40-детию победы Советского народа в Великой Отечественной войне, 1985, с..241-242.

УДК 512.55

ПРИЛОЖЕНИЯ ЭЛЛИПТИЧЕСКИХ АЛГЕБР ПУАССОНА

Козыбаев Д.Х., Жолмаганбет А.А
akerke_17093@mail.ru, kozybayev_dkh@enu.kz
ЕНУ им. Л.Н. Гумилева, Астана, Казахстан

Одним из актуальных направлений в современной математике являются приложения пуассоновых структур к различным проблемам матеамтики и теоретической механики. Эти задачи возникают в динамике твердого тела, небесной механике, теории вихрей, космологических моделях. Алгебры Пуассона играют ключевую роль в гамильтоновой механике, симплектической геометрии.

Векторное пространство B над полем k, снабженное двумя билинейными операциями $x \cdot y$ (умножение) и $\{x, y\}$ (скобка Пуассона), называется алгеброй Пуассона, если B является асоциативно-коммутативной алгеброй относительно $x \cdot y$, алгеброй Ли относительно $\{x, y\}$ и B удовлетворяет тождеству Лейбница:

$$\{x \cdot y, z\} = \{x, z\}y + x\{y, z\}.$$

До последнего времени алгебраическая теория пуассоновых структур была мало изучена. В настоящее время алгебры Пуассона исследуются многими математиками Европы, США и т.д. В работе [1] исследуются полиномиальные алгебры Пуассона с определенными условиями регулярности. Алгебрами такого класса являются, в частности, линейные структуры (структуры Ли–Березина–Кириллова) на дуальных пространствах полупростых алгебр Ли, квадратичные эллиптические алгебры Склянина, а также полиномиальные алгебры, недавно описанные Бондалом, Дубровиным и Угальей. Приводятся примеры таких алгебр и показано, что некоторые из них естественным образом возникают в гамильтоновых интегрируемых системах. В [2] рассматриваются примеры эллиптических алгебр, зависящие от двух непрерывных параметров: эллиптической кривой и точки на ней и являющиеся плоской деформацией кольца многочленов от n переменных. Описываются свойства этих алгебр, а также их связи с интегрируемыми системами, деформационным квантованием, многообразиями модулей и другимии направлениями современных исследований. В работе [3] рассмотрены элиптические алгебры Пуассона.

Известно [4, 5], что группы автоморфизмов алгебр многочленов $k[x,y]$ и свободных ассоциавтиынх алгебр $k\langle x,y\rangle$ от двух переменных над произвольным полем k являются изоморфными, т.е.

$$Aut_k k[x,y] \cong Aut_k k\langle x,y\rangle.$$

Аналог этого результата для свободной алгебры Пуассона $k\{x,y\}$ получен в [6], т.е.

$$Aut_k k[x,y] \cong Aut_k k\langle x,y\rangle \cong Aut_k k\{x,y\}.$$

Также описана группа автоморфизмов эллиптических алгебр Пуассона над полем характеристики 0.

Эллиптические кривые – один из самых перспективных инструментов для построения криптографических алгоритмов. Кроме того, аппарат теории эллиптических кривых оказывается полезным и при анализе криптографических алгоритмов, основанных на задачах разложения и дискретного логарифмирования в конечном поле.

На сегодняшний день математики уже давно работают не только с числами. Алгебра имеет дело с «объектами», их «свойствами» и операциями, определенными на множестве данных объектов. Примерами могут служить множество комплексных чисел, поле многочленов с рациональными коэффициентами и т. д. Так вот, группа точек эллиптической кривой, являясь первоначально абстрактным алгебраическим объектом, оказалась удобной для построения алгоритмов цифровой подписи.

Согласно общей теории эллиптических кривых над полями характеристики > 3, эллиптической кривой E над F_p является множество решений (x, y) уравнения

$$Y^2 + a_1XY + a_2Y = X^{2n+1} + b_{2n}X^{2n} + b_{2n-1}X^{2n-1} + ... + b_1X + b_0 \pmod p$$

над полем F_p вместе с дополнительной точкой O, называемой точкой в бесконечности или нулевой точкой (так как эта точка играет роль нейтрального элемента в группе точек), где $a, b \in F_p$.

Покажем теперь, что с заданной операцией сложения множество точек эллиптической кривой образуют абелеву группу. Введем для данной кривой бинарную операцию сложения в дальнейшем обозначаемую символом $\oplus$. Возьмем множество всех точек данной кривой и еще один дополнительный элемент O, которым является бесконечна удаленная точка.

Вкратце приведем аналог известного алгоритма Диффи-Хеллмана, который можно реализовать на данной кривой. Заметим, что алгоритм Диффи-Хеллмана является основой для подавляющего большинства современных алгоритмов с открытыми ключами, безопасность которых основана на сложности решения проблемы дискретного логарифма.

1) Берем произвольную точку P;
2) Алиса задумывает число k_1 и находит точку $k_1 \cdot P = A$;
3) Боб задумывает число k_2 и находит точку $k_2 \cdot P = B$;
4) Они обмениваются точками A и B и оба находять общую секретную точку

$$k_2 \cdot P \cdot k_1 = k_1 \cdot P \cdot k_2 = T.$$

При рассмотрении данного алгоритма в конечных полях, его безопасность будет эквивалентна проблеме дискретного логорифмирования в конечном поле. Построение аналога системы Диффи-Хелмана влечет возможность построения всех остальных криптосистем на этой платформе. Для этого мы упаздняем определение эллиптических кривых. Эллиптическую кривую над конечным простым полем *GF(p)* определяем как множество пар *(x,y)*, таких что *x,y* ≡ *GF(p)*, удовлетворяющих уравнению:

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

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,* *m.e.* $\left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2 \neq 0$.

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