II-я МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

"АЛГЕБРАИЧЕСКИЕ, ВЕРОЯТНОСТНЫЕ, ГЕОМЕТРИЧЕСКИЕ, КОМБИНАТОРНЫЕ И ФУНКЦИОНАЛЬНЫЕ МЕТОДЫ В ТЕОРИИ ЧИСЕЛ"

Тезисы докладов
25 - 30 сентября 1995 г.

ВОРОНЕЖ

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МАТЕМАТИЧЕСКИЙ ИНСТИТУТ РАН им.В.А.СТЕКЛОВА

ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНСТИТУТ МАТЕМАТИКИ ВГУ

ВОРОНЕЖСКОЕ ВЫСШЕЕ ВОЕННОЕ АВИАЦИОННОЕ ИНЖЕНЕРНОЕ УЧИЛИЩЕ

ВОРОНЕЖСКАЯ ВЫСШАЯ ШКОЛА МИЛИЦИИ МВД РФ

КОМИТЕТ ПО НАУКЕ И ВЫСШЕЙ ШКОЛЕ
АДМИНИСТРАЦИИ ВОРОНЕЖСКОЙ ОБЛАСТИ

НАУЧНО-ТЕХНОЛОГИЧЕСКОЕ ОБЩЕСТВО
"МАТЕМАТИКА, МЕХАНИКА, ИНФОРМАТИКА" ЧЕРНОЗЕМЬЯ

II-я МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

"АЛГЕБРАИЧЕСКИЕ, ВЕРОЯТНОСТНЫЕ, ГЕОМЕТРИЧЕСКИЕ, КОМБИНАТОРНЫЕ И ФУНКЦИОНАЛЬНЫЕ МЕТОДЫ В ТЕОРИИ ЧИСЕЛ"

Тезисы докладов
25 - 30 сентября 1995 г.

ВОРОНЕЖ
1995

УДК 511.036.054.336

II-я Международная конференция "Алгебраические, вероятностные, геометрические, комбинаторные и функциональные методы в теории чисел": Тезисы докладов. - Воронеж, ВГУ, 1995. -177 с.

В сборнике представлены тезисы докладов и сообщений, состоявшихся на II-й Международной конференции "Алгебраические, вероятностные, геометрические, комбинаторные и функциональные методы в теории чисел", проводимой Воронежским государственным университетом совместно с Московским государственным университетом и Математическим институтом РАН им. В.А.Стеклова.

Тематика докладов охватывает все основные направления современной теории чисел, её приложения к вычислительной математике, теории кодирования, теории передачи и защиты информации, вопросы преподавания теории чисел в высшей школе.

Оргкомитет благодарит Российский фонд фундаментальных исследований за финансовую поддержку.

УДК 5II.54

Аванесов Э.Т. (Кисловодск)

ОБ ОСНОВНЫХ ЕДИНИЦАХ КУБИЧЕСКИХ ПОЛЕЙ ОТРИЦАТЕЛЬНОГО ДИСКРИМИНАНТА

Существуют различные методы определения систем основных единиц алгебраических полей произвольного порядка. К сожалению, расчеты по этим конструкциям для конкретных числовых примеров практически неосуществимы.

В сообщении

I. предлагается эффективизация алгоритма в случае кубических полей отрицательного дискриминанта,

2. рассматривается приложение к решению неопределенного уравнения Делоне-Нагелла

$$x^3+my^3=1.$$

Установлено, что возможное решение его, отличное от тривиального, удовлетворяет неравенствам:

$$|x| \leqslant 1+\left[\frac{1}{\sqrt{3}}\exp\left(\frac{81}{2\pi^2}m^2\right)\right],$$

$$|y| \leqslant 1+\left[\frac{1}{\sqrt{3}\cdot\sqrt[3]{m}}\exp\left(\frac{81}{2\pi^2}m^2\right)\right].$$

Используя известные результаты В.Г.Спиндчука (Об оценке решений уравнения Туэ, ИАН СССР, сер. матем. 36(I972), 7I2-74I), получено уточнение последних оценок:

$$\max\left(|x|,|y|\right)<\exp(Cm),$$

C - вычислимая абсолютная константа.

УДК 621.396

Авсентьев О.С. (г.Воронеж)

Повышение скрытности радиорелейных линий миллиметрового диапазона.

Проблема обеспечения скрытности радиорелейных линий миллиметрового диапазона все более обостряется по мере его освоения и роста технических возможностей "незаконных" пользователей по перехвату сообщений, передаваемых по этим линиям. Повышение защищенности этих сообщений возможно в двух направлениях,- это скрытие факта излучения и создание условий, затрудняющих или делающих невозможным извлечение информации из принятой смеси сигнала и помех (если излучение обнаружено). Применение многих известных традиционных методов (экранирование, засекречивание и др.) в ряде случаев либо невозможно, либо нецелесообразно из-за различных организационно-технических трудностей. Одним из наиболее простых способов решения поставленной задачи является переход для работы на частоты наибольшего затухания (например 60 ГГц) и адаптивное изменение излучаемой мощности при заданной достоверности передачи информации.

Переход на более высокие частоты ранее в большинстве случаев использовался лишь с целью расширения полосы частот, в докладе же в качестве основного результата рассмотрено повышение защищенности информации, причем основное внимание уделено перспективным цифровым системам.

Приведены результаты расчетов, доказывающие значительную эффективность данного способа (особенно на малых расстояниях от 1 до 5 км.). Защищенность информации предложено оценивать по пропускной способности каналов перехвата, в качестве которых приняты боковые и заднее излучения диаграммы направленности передающей антенны.

Показано, что адаптивное изменение излучаемой мощности при заданной достоверности позволяет значительно (на 40% и более) уменьшить расстояния, на которых для "незаконных" пользователей становится невозможным достаточно качественный прием информации, а применение узконаправленных антенн (1,5 - 2 градуса) и переход в диапазон частот наибольшего затухания приводит к тому, что перехват становится возможным практически только на прямой линии между передатчиком и приемником.

УДК 511.3

Абдуллаев С.Б. (УФА)

ОБЗОР РЕЗУЛЬТАТОВ ПО СЧЕТУ ЦЕЛЫХ ТОЧЕК В ВОЗМУЩЕННЫХ КРУГАХ

Одним из обобщений задачи о числе целых точек в круге является задача о числе $N(A)$ целых точек в области A, граница которой в полярных координатах задается уравнением $\rho = R + \tau(R,\varphi)$, где R – неограниченно растущий параметр, функция $\tau(R,\varphi)$ удовлетворяет определенным условиям, ограничивающим ее рост. Пусть $V(A)$ – площадь области A, $H(A) = N(A) - V(A)$, тогда задача сводится к оценке величины $H(A)$. При решении этой задачи возникают двойные тригонометрические суммы, от оценки которых существенно зависит конечный результат.

1) Если использовать оценки Ван дер Корпута тригонометрических сумм с одним индексом суммирования (теорема 6 из [1]), то

$$H(A) \ll R^{\frac{196}{295}} \ln R \text{ при условии, что } \frac{\partial^k}{\partial \varphi^k}\tau(R,\varphi) \ll R^{\frac{289}{295}}, \quad 0 \le K \le 6$$

2) Если применить метод, использованный Е. Титчмаршем в работе [2], то $H(A) \ll R^{\frac{112}{169}} \ln^{\frac{37}{18}} R$ при условии, что

$$\frac{\partial^k}{\partial \varphi^k}\tau(R,\varphi) = o(R), \quad 0 \le K \le 4$$

3) Используя более сильные оценки двойных тригонометрических сумм из работы [3], чем аналогичные оценки из [2], получаем

$$H(A) \ll R^{\frac{80}{121}} \ln^{\frac{15}{8}} R \quad \text{при условии, что} \quad \frac{\partial^k}{\partial \varphi^k}\tau(R,\varphi) = o(R), \quad 0 \le K \le 9$$

Заметим, что полученные оценки для $H(A)$ являются аналогом результата В. Серпинского для числа целых точек в круге.

ЛИТЕРАТУРА

1. Van der Corput J.G. Neue Zahlentheoretishe Abschätzungen // Math Zeitschrift – 1929 – Bd 29 – S. 397 –426.

2. Titchmarsh E.C. The lattice – points in a cizcle // Proc. Lond. Math Soc. – 1934 – 2 – 38 – P. – 115.

3. Колесник Г.А. Об оценке некоторых тригонометрических сумм //Acta Arith. – 1973 – 25 – № 1 – с. 7 – 30

УДК 5II.9

Акрамов У.А. (Самарканд)

ТЕОРЕМА "СИЛЬНОЙ" ИЗОЛЯЦИИ ДЛЯ АЛГЕБРАИЧЕСКИХ РЕШЕТОК

Пусть M – полный модуль алгебраического поля K степени n. Считаем, что среди сопряженных имеется s вещественных и 2t комплексных, так что $n = s + 2t$.

Для любой матрицы $B = (b_{ij})$ символом $\|B\|$ обозначим величину $\|B\| = \max|b_{ij}|$.

Пусть A матрица размера $n\times n$ $(n = s + 2t)$ имеет вид

$$A = \begin{pmatrix} S & \\ & T \end{pmatrix},$$

где $S = (s_{ij})$ – недиагональная матрица размера $s\times s$, а $T = (t_{ij})$– матрица размера $2t\times 2t$, состоящая из блоков размера 2×2: T_{kl} $(k,l = 1, \dots t)$. Обозначим

$(A_\varepsilon) = (A \mid \|S-I\|<\varepsilon,\ \|T_{kk}\|<c\ (1\le k\le t),\ \|T_{kl}\|<\varepsilon\ (k\ne l, 1\le k,l\le t)$,

где I – единичная матрица, c–наперед заданное фиксированное число большее 1, ε – достаточно малая положительная величина.

ТЕОРЕМА. Пусть Λ – любая решетка полного модуля M алгебраического поля K степени $n = s + 2t$. Если $s\ge 3$, то по наперед заданному $\eta > 0$, найдется такое $\varepsilon = \varepsilon(\eta) > 0$, что для любой матрицы A_1 из множество (A_ε) для решетки $\Lambda_1 = A_1\Lambda$ будет выполнено $N(\Lambda_1)<\eta$, где $N(\Lambda_1)$– однородный минимум отвечающий форме

$$x_1 \dots x_s (y_1^2+z_1^2) \dots\dots (y_t^2+z_t^2).$$

Литература

1. Скубенко Б.Ф. О произведении n линейных форм от n переменных// Труды МИ АН СССР, 1981, т.158, с.175–179.

2. Акрамов У.А. Теорема изоляции для форм, отвечающих чисто вещественным алгебраическим полям//Записки науч.семин.ЛОМИ АН СССР, 1990, т.185, N 10, с.5–12.

УДК-511.9

Алутин Н.Н. (Благовещенск)

О ТЕОРИИ ЧИСЕЛ В ШКОЛЬНОЙ МАТЕМАТИКЕ

Следует заметить, что качество подготовки учителя математики проявляется не только в знании школьного курса математики и математических дисциплин высшей школы, но и в умении видеть связь между последними. В высшей школе такую задачу может выполнить спецкурс. Отметим некоторые аспекты содержания предлагаемого спецкурса.

Используя теорию сравнений [1], выводятся признаки делимости на 7, 8, 11, 25 и т.д. (способ Паскаля).

В школьном курсе изучаются правильные многоугольники. Разбирается построение 3, 4, 5, 6 и 2n угольников. Используя понятие характера группы, суммы Гаусса и Якоби можно доказать следующий факт [2]. Если p - простое число вида 2^n+1, то правильный многоугольник с p сторонами, может быть построен с помощью линейки и циркуля. Следует указать, что возможность построения комплексных чисел с помощью циркуля и линейки означает, что они могут быть получены из рациональных чисел конечной последовательностью рациональных операций и операций взятия квадратных корней.

В школе при знакомстве с иррациональными числами упоминаются квадратичные иррациональности, а также говорится об иррациональности чисел e и π. На спецкурсе, следуя [3] доказывается иррациональность чисел e и π, а также их трансцендентность.

В школьном курсе число π вводится как отношение длины окружности к диаметру, но не указывается способ вычисления. Хотя в [4] говорится о таком способе в связи с задачей о квадратуре круга. Доказывается формула Валлиса для получения десятичной записи числа π с требуемой верной цифрой после запятой.

1. Бухштаб А.А. Теория чисел. - М.; Просвещение., 1966.

2. К. Айерлэнд, М. Раузен. Классическое введение в современную теорию чисел. Пер. с английского. - М.; "Мир", 1987.

3. Шидловский А.Б. Трацендентные числа. - М.; Наука. 1987.

4. Глейзер Г.И. История математики в школе. - М.; Просвещение. 1982.

УДК 517.518.+511.

Н.Н.Андреев, А.Ю.Попов (Москва)

ЭКСТРЕМАЛЬНЫЕ ЗАДАЧИ ДЛЯ ФУНКЦИЙ С МАЛЫМ НОСИТЕЛЕМ

В связи с приложениями к теории чисел С.В. Конягин [1] поставил перед авторами следующую задачу. Пусть $0 < h \le 1/2$, $X(h)$ — класс функций таких, что

1. $f(x) = \sum_{n=0}^{\infty} a_n \cos(2\pi n x)$;
2. $a_n \in \mathbb{R}$;
3. $\sum\limits_{n=0}^{\infty} |a_n| = 1$;
4. $supp\ f \subset [-h, h]$.

Требуется оценить величину

$$I(h) = \sup_{f \in X(h)} \int_{-h}^{h} f(x)\,dx.$$

Особую роль в приложениях играет оценка снизу $I(1/4)$.

Очевидно, что $I(h) \le 2h$; и $I(h) \ge h$ (см. [2]).

Теорема 1. *(Н.Н. Андреев)* $I(1/4) \ge 2 - \sqrt{3}$.

С.В.Конягин доказал существование предела

$$L = \lim_{h \to +0} \frac{I(h)}{h}.$$

Мы получили оценки для L.

Теорема 2. *(Н.Н. Андреев)* $L \ge \pi/3$

Теорема 3. *(А.Ю. Попов)* $L < 1.4$.

В докладе будет рассказано и о других экстремальных задачах, примыкающих к рассмотренной.

Работа Н.Н. Андреева поддержана грантом N. MC 5300 Международного Научного Фонда.

Литература:

1. Конягин С.В. О распределении дробных частей членов некоторых геометрических прогрессий. // Тезисы доклада в этом сборнике.

2. Стечкин С.Б. Одна экстремальная задача для тригонометрических рядов с неотрицательными коэффициентами. // Acta Mathematica Academiae Scientiarum Hungaricae, 1972, T. 23 (3–4), p. 289–291.

к.т.н. с.н.с. Анищенко А.В.
Другие авторы

МОДЕЛЬ АНАЛИЗА ИЗОБРАЖЕНИЯ СЛОЖНОГО ОБЪЕКТА

В докладе рассмотрена задача анализа представленного неполного или искаженного изображения сложного объекта в интересах моделирования восприятия его облика - преобразование распределения яркости в картинной плоскости в описание в символьном виде.

Разработан оригинальный алгоритм построения цепочного кода (аналогичного коду Фримана) контура сложного объекта на основе решения обратной задачи разложения в растр отрезка с использованием обобщенного целочисленного алгоритма Брезенхема.

Контур объекта описывается его вершинами. Начальные и конечные точки фрагментов контура, соответствующих элементам конструкции (ЭК) объекта, определяются по правилу: векторное произведение отрезков контура, образующих вершину имеет отрицательный знак в точках нарушения выпуклости сложной геометрической фигуры.

Задача распознавания ЭК решается в два этапа: распознавание формы фрагмента изображения на основе статистических методов; классификация ЭК с использованием структурных методов распознавания.

Определены классы объектов распознавания (формы кривых контура), априорные вероятности их появления, интегральные коэффициенты формы (ИКФ) - признаки распознавания. Алгоритм распознавания строится на последовательном использовании ИКФ по правилу максимума отрицательной корреляционной связи между предыдущим и последующим признаками в случае неоднозначности решения.

На основе логических процедур вывода, базирующихся на эвристических правилах и эмпирических зависимостях устанавливаются отношения "контур - ЭК" и определяются свойства объекта.

Модель реализована с использованием MicroSoft C v.6.0.

УДК 519.68

Аржеухов Л.Б. /Воронеж/

О МОДЕЛИРОВАНИИ ПРОЦЕССОВ ЗАПИСИ ДВОИЧНЫХ ДАННЫХ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ ПАМЯТИ ЗНАКОЧЕРЕДУЮЩИМИСЯ РЯДАМИ

Решение проблемы сверхплотной и сверхнадежной записи информации в интеллектуальных системах памяти /ИСП/ требует создания простых и эффективных математических моделей процессов записи двоичных данных в запоминающие среды. В работе предложены модели таких процессов в форме знакочередующихся числовых рядов вида

$$a_0 \cdot b_0 - a_1 \cdot b_1 + a_2 \cdot b_2 - \dots + a_n \cdot b_n - \dots , \qquad /1/$$

где $a_i; b_i$ –члены ряда, у которых значения a_i и b_i в общем случае определяются значениями соответствующих m_1 и m_2 битов i-ой кодовой группы из m_1+m_2 битов в потоке записываемых данных; $m_1=2,3,4,5,\dots$ и $m_2=2,3,4,5,\dots$; $a_i=a_0+\ell_i^{m_1}$ и $b_i=b^0+\ell_i^{m_2}$; a^0 и b^0 – константы, значения которых определяют исходя из физических особенностей конкретных ИСП; $\ell_i^{m_1}$ и $\ell_i^{m_2}$ – текущие значения кодовых групп из m_1 и m_2 битов исходных данных в пределах $\ell^{m_1}=0,1,2,\dots,2^{m_1}-1$ и $\ell^{m_2}=0,1,2,\dots,2^{m_2}-1$.

Предполагается, что ряд /1/ разбивается на последовательность блоков по r членов и в каждом блоке имеются служебные члены, выделяемые либо тем, что их абсолютное минимальное значение превосходит максимально возможное значение информационных членов, либо определенным местоположением в блоке.

Рассматривается последовательное решение следующих задач: минимизации сумм отдельно нечетных и четных членов ряда; минимизации сумм всех членов ряда; приведения сумм ряда к нулю.

Решение имеет алгоритмическую форму и включает следующие основные операции над членами каждого j-го блока ряда /1/в отдельности: установление предельно допустимых /пороговых/ значений сумм нечетных и четных для всех блоков; вычисление в пределах каждого j-го блока текущих значений сумм нечетных и четных членов, сравнение текущих значений с предельно допустимыми и, если первые превосходят вторые, обращение значений соответствующих членов ряда и, следовательно, значений соответствующих кодов двоичных данных; определение для каждого j-го блока величины и знака разности сумм нечетных и четных членов и минимизация абсолютного значения разности путем последовательного перемещения по блоку первого служебного /маркерного/ члена; дополнение исходного значения маркерного члена блока полученным минимальным значением указанной разности.

УДК 681.3

Афанасьева Н.Ю. (Тула)

ИСПОЛЬЗОВАНИЕ АППАРАТА НЕЧЕТКИХ МНОЖЕСТВ ДЛЯ АНАЛИЗА ПРОИЗВОДИТЕЛЬНОСТИ ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ ПРОЦЕССОВ.

При анализе производительности параллельных вычислительных процессов возникают задачи: необходимость выполнения заданного алгоритма за требуемое время, нахождение плана выполнения заданного алгоритма за минимальное время, и оптимального числа процессоров для реализации графа программы за минимальное число шагов. Существующие методы дискретного программирования позволяют эффективно решать эти задачи рассматривая только информационные связи между частями программы (при этом не учитываются логические связи между операторами) и точное решение задач получено только для простейших моделей.

Для увеличения эффективности анализа предлагается использовать аппарат нечетких множеств. Тогда алгоритм программы можно представить в виде нечеткого множества $G=\{a_i|\mu\}$, где μ-степень принадлежности элемента к нечеткому множеству, характеризующая логические связи между операторами.

Так как присутствует элемент нечеткости (любой алгоритм имеет операторы условного ветвления, что существенно влияет на ход выполнения программы и на время ее решения), то различные задачи оптимизации можно свести не к точному решению, а к нахождению определенного интервала. Для решения экстремальных задач (определение минимального числа процессоров и минимального времени решения) вместо определения экстремума однозначно определенных критериев минимизируется разрыв между заранее заданными целями и соответствующими текущими значениями критериев при заданной системе ограничений. При этом все цели, которые должны быть достигнуты, формулируются как обычные ограничения, в которые вводятся переменные, характеризуют отклонение от цели как в положительную, так и отрицательную сторону. Целевые функции составляются в виде отклонений с соответствующими приоритетами и коэффициентами веса. Из полученного множества решений необходимо выделить оптимальное компромиссное решение. Таким образом в задаче целевого программирования меняется смысл получения задачи. Вместо оптимизации по каким-либо критериям ставится задача оптимального приближения к заранее заданным целевым значениям.

УДК 5II.I9

Баландина Н.Н., Ковердик И.В. (Одесса)

Несимметрическая функция делителей в поле $\Phi(1)$

На целых элементах поля гауссовых чисел $\Phi(1)$ изучается несимметрическая функция делителей

$$\tau_{1,2}(\alpha)=\sum_{\alpha=\delta_1\delta_2^2}^{*} 1$$

(здесь $*$ означает, что суммирование идет по неассоциированным делителям δ_1,δ_2^2 числа α).

Используя оценку тригонометрической суммы

$$\sum_{\substack{\beta \bmod \gamma,\\ (\beta,\gamma)=1\\ \beta\cdot\bar{\beta}\equiv 1(\gamma)}} e^{\pi i \mathrm{Tr}\left(\frac{\alpha_1\beta+\alpha_2\beta^{-2}}{\gamma}\right)} \ll \sqrt{N(\gamma)\cdot N(\alpha_1,\alpha_2,\gamma)}\,\tau(\gamma)$$

(здесь $\alpha_1,\alpha_2,\beta,\gamma$-целые гауссовы числа, $N(\gamma)$-норма γ, $\mathrm{Tr}(\alpha)$-след α из $\Phi(1)$ в Φ)

Мы доказываем теоремы:

Теорема 1 Пусть α_0,γ-целые гауссовы, $(\alpha_0,\gamma)=1$, $x>1$-вещественное. Тогда

$$\sum_{\substack{\alpha\equiv\alpha_0 (\mathrm{mod}\ \gamma)\\ N(\alpha)\le x}} \tau_{1,2}(\alpha) = Z(2)\prod_{\rho/\gamma}\left(1-\frac{1}{N(\rho)^2}\right)\cdot\frac{x}{N(\gamma)} + O\left(\frac{x^{\frac{1}{2}}}{N(\gamma)^{\frac{1}{2}-\varepsilon}}\right)+O\left(x^{\frac{1}{3}+\varepsilon}\right)+$$

$$+O\left(N(\gamma)^{\frac{1}{2}}x^{\varepsilon}\right)$$

с постоянной в символах "O", зависящей только от ε.

(здесь $Z(s)$-дзета-функция Дедекинда поля $\Phi(1)$)

Теорема 2 Для каждого $h\gg\log x$ и всех $m\le x$, за исключением самое большее $o(x)$ из них, имеем

$$\sum_{m\le N(\alpha)<m+h} \tau_{1,2}(\alpha) - Z(2)h$$

УДК 514.17

Барановский Е. П. [1] (Иваново)

Об L-симплексах шестимерных решеток

Получены условия того, что симплекс, взятый в качестве основного для задания 6-мерной решетки евклидова пространства E^6, является L-симплексом, то-есть обладает тем свойством, что описанный вокруг него замкнутый шар не содержит других, кроме вершин симплекса, точек решетки.

Пусть $h_{kl}=A_kA_l^2$ $(k,l=0,1,\dots,6,\ k<l)$- квадраты длин ребер симплекса $S=\langle A_0A_1\dots A_6\rangle$; $x^0,x^1,\dots,x^6$ $(\sum_{k=0}^{6}x^k=1)$- барицентрические координаты относительно симплекса S; и пусть $\Phi(x^0,x^1,\dots,x^6)=-\sum h_{kl}x^kx^l$ $(k,l=0,1,\dots,6,\ k<l)$. Доказана теорема:

Теорема. Неравенства $\Phi(x^0,x^1,\dots,x^6)>0$ для всевозможных перестановок из наборов целочисленных координат
1)(1,1,-1,0,0,0,0), 2)(1,1,1,-1,-1,0,0), 3)(1,1,1,1,-1,-2,0),
4)(2,1,1,-1,-1,-1,0), 5)(1,1,1,1,-1,-1,-1), 6)(2,1,1,1,-1,-1,2),
7)(2,2,1,1,-1,-1,-3), 8)(3,1,1,1,-1,-2,-2), 9)(2,2,1,-1,-1,-1,-1),
10)(3,1,1,-1,-1,-1,-1), 11)(3,2,1,-1,-1,-1,-2),
12)(1,1,1,1,1,-1,-3), 13)(1,1,1,1,1,-2,-2), 14)(2,1,1,1,1,-2,-3)
суть необходимые и достаточные условия того, чтобы основной симплекс 6-мерной решетки был L-симплексом. Названное множество условий минимально.

Работа выполнена при поддержке РФФИ.

УДК 511.5

Баулина Ю.Н. (Москва)

О ЧИСЛЕ РЕШЕНИЙ ДИОФАНТОВА УРАВНЕНИЯ $x_1^2 + \ldots + x_n^2 + a = (a+n)x_1 \ldots x_n$, НЕ ПРЕВОСХОДЯЩИХ ЗАДАННОЙ ГРАНИЦЫ

Пусть $M(x,a,n)$ – число решений $(u_1,\ldots,u_n)$ диофантова уравнения

$$x_1^2 + \ldots + x_n^2 + a = (a+n)x_1 \ldots x_n \; ; \quad a \geqslant 0 \; , \quad n \geqslant 3 \; ,$$

удовлетворяющих условию $1 \leqslant u_n \leqslant \ldots \leqslant u_1 \leqslant x$. В работе [1] доказано, что при $x \to \infty$

$$M(x,0,3) = C\ln^2 x + O(\ln x(\ln\ln x)^2) \; , \quad C \approx 0{,}18$$

Автором получены следующие результаты:

ТЕОРЕМА 1. При $x \to \infty$

$$M(x,a,n) = O(\ln^{n-1} x)$$

ТЕОРЕМА 2. При $x \to \infty$

$$M(x,a,3) = C(a)\ln^2 x + O(\ln x(\ln\ln x)^2) \; ,$$

где

$$C(a) = \frac{3}{\pi^2} \sum\nolimits^{*} \frac{f_a(u_2) + f_a(u_3) - f_a(u_1)}{f_a(u_1) f_a(u_2) f_a(u_3)}$$ – положительная константа, зависящая только от a, символ $\sum^{*}$ означает, что суммирование идет по всем решениям (u_1,u_2,u_3), удовлетворяющим условию $u_1 \geqslant u_2 \geqslant u_3 \geqslant 1$, причем слагаемые, соответствующие решениям $(1,1,1)$ и $(a+2,1,1)$, считаются с множителем $\frac{1}{2}$, $f_a(x) = \ln \frac{(a+3)x + ((a+3)^2x^2 - 4)^{1/2}}{2}$.

Константы в знаках $O()$ зависят только от a.

Литература

1. Zagier D. On the number of Markoff numbers below a given bound / Math. Comput. 1982. V.39. № 160. P.709-723.

УДК 5II.5I2

Белова Н.Н. (Череповец)

ПОВОРОТЫ КВАТЕРНИОНОВ

Рассмотрим порядок целых кватернионов кватернионной алгебры, соответствующей целой положительной квадратичной форме f.

Пусть R, R' - целые кватернионы одной нормы. Будем говорить, что кватернион T управляет целым четырехмерным поворотом (R,R') от кватерниона R к кватерниону R', если $R'=TRT^{-1}$. При этом кватернионы R, R' назовем поворотно эквивалентными, если для любого целого числа $w \neq 0$ найдется кватернион нормы, взаимно простой с w, управляющий поворотом (R,R'). Если T является правым делителем идеала $\mathcal{J} \subset \{x+yR \mid x,y \in \mathbb{Z}\}$, то будем говорить также, что поворот (R,R') управляется идеалом $\mathcal{J}$.

В настоящей работе доказано, что множество кватернионов, управляющих целым четырехмерным поворотом, есть двучленный модуль. Доказано необходимое и достаточное условие поворотной эквивалентности кватернионов. Установлено соответствие между поворотами кватернионов и классами примитивных регулярных идеалов, а также классами целых бинарных положительных квадратичных форм.

Работа является продолжением и обобщением работ Б.А.Венкова, О.В.Линника, А.В.Малышева.

Лит.: I. Белова Н.Н. Теория лучей в порядках Полла / Череповец. гос. пед. ин-т. - Череповец, 1987. - 56с. - Деп. в ВИНИТИ 22.0I.87, № 500 - В87.

УДК 5II.36

Бересневич В.В. (Минск)

Обобщение метрической теоремы Хинчина для неоднородных диофантовых приближений

Исследуя вопрос приближения вещественных чисел рациональными, А.Я.Хинчин установил, что неравенство

$$|\alpha q-p|<\psi(q)$$

имеет конечное или бесконечное число решений для почти всех $\alpha\in\mathbb{R}$ (в смысле меры Лебега на $\mathbb{R}$) в зависимости от сходимости или расходимости ряда $\sum\psi(q)$, где ψ – положительная функция натурального аргумента и $q\psi(q)$ не возрастает [I].

Дальнейшие обобщения этой теоремы были связаны с совместными приближениями точек n-мерного пространства (теорема Хинчина-Грошева). Основную трудность при доказательстве этих теорем составляет случай расходимости ряда ($\sum\psi(q)$ в случае теоремы Хинчина). Когда точка $\alpha=(\alpha_1,\dots,\alpha_n)$ лежит на некоторой поверхности $V\subset\mathbb{R}^n$, то получить аналог теоремы Хинчина непросто даже в случае специальных поверхностей [2].

Получен нелинейный аналог теоремы Хинчина для неоднородных приближений:

Теорема. Пусть ψ – положительная монотонно убывающая функция натурального аргумента, и ряд

$$\sum_{1}^{\infty}\psi(r) \qquad (I)$$

расходится. Тогда неравенство

$$|a_2x^2+a_1x+a_0-y|<H^{-1}\psi(H), \qquad (2)$$

где $H=max(|a_0|,|a_1|,|a_2|)$, имеет бесконечное число решений в целых рациональных a_0,a_1,a_2 для почти всех точек $(x,y)\in\mathbb{R}^2$ (в смысле меры Лебега в $\mathbb{R}^2$); обратно, если ряд (I) сходится, то неравенство (2) имеет бесконечное число решений в целых рациональных a_0,a_1,a_2 на множестве точек $(x,y)\in\mathbb{R}^2$ нулевой меры Лебега в $\mathbb{R}^2$.

Литература. I.Хинчин А.Я. Цепные дроби. Москва,"Наука",1978.
2. Спринджук В.Г. Метрическая теория диофантовых приближений. Москва, "Наука", 1977.

УДК 511.36

Бернік В.І. (Мінск)

ДИОФАНТОВЫ СВОЙСТВА КРИВЫХ С НЕНУЛЕВОЙ КРИВИЗНОЙ

Пусть $f_1(x)$, $f_2(x)$-трижды непрерывно дифференцируемые функции, определенные на некотором интервале $I=[a,b]$ и пусть определитель

$$\begin{vmatrix} f_1' & f_2' \\ f_1'' & f_2'' \end{vmatrix}$$

почти везде на I отличен от нуля. В таких предположениях В.Шмидт [1] доказал, что для почти всех $x \in I$ неравенство

$$|a_2 f_2(x) + a_1 f_1(x) + a_0| < H^{-2-\varepsilon}, \quad \varepsilon > 0, \quad H = \max_{0 \le i \le 2} |a_i| \qquad (1)$$

имеет лишь конечное число решений в целых векторах $\bar{a}=(a_0, a_1, a_2)$. Теорема В.Шмидта была усилена Р.Бейкером [2] установившим, что в правой части неравенства (1) функцию $H^{-2-\varepsilon}$ можно заменить на $\psi^2(H)$, где функция $\psi(x)$ монотонно убывает и ряд $\sum_{H=1}^{\infty} \psi(H)$ сходится.

Теорема. Утверждение теоремы В.Шмидта остается справедливым, если функцию $H^{-2-\varepsilon}$ заменить на $H^{-1}\psi(H)$.

Разница между тремя теоремами становится более наглядной, если положить $\psi(H) = H^{-1}\ell n^{-1-\delta} H$, $\delta > 0$. По-видимому, это окончательный результат, и при условии расходимости ряда $\sum_{H=1}^{\infty} \psi(H)$ соответствующее неравенство будет иметь для почти всех $x \in I$ уже бесконечное число решений.

Литература. I. W. Schmidt, Metrische Sätze über simaltane Approximation abhängiger Grössen // Monatsh. Math. 1964. V.2. PP.154-166.
2. R.C.Baker, Dirichlet's theorem on diophantine approximation // Math.Proc. Cambridge Phil. Soc. 1978. V.83. PP. 37-59.

УДК 5II.36

Берник В.И.(Минск), Переверзева И.А.(Гродно)

ПРИБЛИЖЕНИЯ И ВЕРХНИЕ ОЦЕНКИ РАЗМЕРНОСТИ ХАУСДОРФА

Основной вопрос метрической теории диофантовых приближений состоит в нахождении границы (желательно поменьше), начиная с которой заданную аппроксимацию бесконечно часто выдерживает только множество нулевой меры Лебега. Усиление аппроксимации уже после этой границы естественно сужает множество, что можно уловить с помощью размерности Хаусдорфа. Мы рассматриваем поверхность $G=(x_1,\dots,x_m,f_1(\bar{x}),\dots,f_n(\bar{x}))$, определенную в теореме 4 § 4 главы 2 из [I]. С помощью методов работы [2] доказывается следующая теорема.

Пусть $A(G,v)$ - множество $\bar{x}\in R^m$, для которых система неравенств

$$\max_{1\le i\le m,\ 1\le j\le n}\left(\|x_i q\|,\ \|f_j(\bar{x})q\|\right)<q^{-v},\quad v>(m+n)^{-1}$$

имеет бесконечное число решений в натуральных числах q. Тогда

$$\dim A(G,v)\le\frac{m^2+mn-n}{(m+n)(1+v)}$$

Литература. I. В.Г.Спринджук Метрическая теория диофантовых приближений. М. 1977. 2. N.I.Bernik, N.A.Pereverseva. The method of trigonometrical sums and lower estimates of Hausdorff dimension // (Proc. of the International conf. in honour J.Kubilius. Vilnius, 1992. pp.75-81.

MAHLER'S MEASURE OF CERTAIN CLASSES OF RECIPROCAL POLYNOMIALS

(Marie José BERTIN - University P. M. Curie PARIS 6)

Let P be an irreducible monic polynomial of degree d with integral coefficients. Denote $\alpha_1, \alpha_2, ..., \alpha_d$ the roots of P and

$$M(P) = \Pi_{i=1}^{d} max(1, |\alpha_i|)$$

the Mahler's measure of P

In 1971 Ch. Smyth proved that

$$M(P) \geq \vartheta_0 = 1.32...$$

provided P be non reciprocal (i. e. $P(z) \neq z^d P(1/z)$), where ϑ_0 is a root of $X^3 - X - 1 = 0$.

Till now, very few is known about the measure of reciprocal polynomials.

In 1980 and 1989 D. W. Boyd exhibited some lists of reciprocal polynomials of smallest measure up to degree 32 and we can observe that the roots outside the unit circle of such polynomials are as much as possible non real.

Besides, A. Schinzel proved in 1973 that

$$M(P) \geq ((1 + \sqrt{5})/2)^{d/2}$$

if P is totally real.

Using quite recent results of Matveev (1995), may be not yet published, we propose first to generalize the result of Schinzel for some classes of non totally real reciprocal polynomials and then to explain the observation about the outside conjugates of the lists of D. Boyd.

УДК 519.68

Быковский В. А. (Хабаровск)

КВАДРАТИЧНЫЕ ЦИФРОВЫЕ СИГНАТУРЫ

В работе предложен новый метод формирования цифровых сигнатур сообщений. Как и в криптосистеме *RSA*, в нем используется в качестве личного ключа пара достаточно больших простых чисел (p_1, p_2), а произведение $q = p_1 p_2$ — открытый ключ.

Криптостойкость предложенной конструкции, которую мы называем квадратичной сигнатурой, определяется сложностью задачи разложения q на простые множители p_1, p_2. При этом ее двоичная длина составляет 5/8 длины сигнатуры, сформированной на той же паре (p_1, p_2) по алгоритму *RSA*. В частности, при выборе 512-битовых открытых ключей длина квадратичной цифровой сигнатуры укладывается в 320 бит.

Литература

1. Rivest R. L., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public Key Cryptosystems // Comm.ACM, 1978. 21(2)

2. Rabin M.O. Digital signatures and public-key function as intractable as factorization // Tech.Rep. LCS/TR 212, M.I.T. Lab. for Comp. Sci. 1979. Cambridge, MA.

УДК 511

Влавацкая Л.И., Колявка П.М. (Львов)

ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ В ДОВУЗОВСКОМ ОБРАЗОВАНИИ

Теория чисел, являясь одной из основных ветвей математики, занимает важное место в современном образовании. К сожалению, во многих вузах на ее изучение выделяется очень мало времени, если оно вообще выделяется. В данной работе мы отметим некоторые вопросы теории чисел, которые можно предложить для изучения слушателям подготовительных отделений тех вузов и факультетов, где выделено достаточно времени на элементарную математику. Имеется несколько основных возможностей углубления знаний по теории чисел, и их выбор зависит от специфики вуза и количества часов. Прежде всего, можно рассматривать задачи олимпиадного характера, решения которых, как правило, оригинальны и очень интересны. Кроме того, на следующем этапе можно изложить элементы теории чисел, входящие в программы школ с углубленным изучением математики, физико-математических лицеев и т.д. / диофантовы уравнения, делимость, сравнения, цепные дроби/. Далее, при подготовке специалистов-математиков можно более глубоко изучить природу простых чисел, трансцендентных чисел, рассмотреть вопросы диофантовых приближений.

Независимо от специализации, необходимо рассматривать конечные числовые поля, изучать наиболее простые общие свойства этих полей. Это даст возможность слушателям применять в будущем полученные знания в более сложных разделах математики, в технических науках.

Эта работа была частично поддержана Международной Соросовской программой поддержки образования в области точных наук, грант № АРЦ 051106.

УДК 517.9

Близняков Н.М. / Воронеж /

О СПЕЦИАЛЬНЫХ ДЕФОРМАЦИЯХ МНОГОЧЛЕНОВ

Следующее утверждение развивает теорему Лагерра Э.Н. [1].

Теорема. Пусть числа $k_1, k_2, \dots, k_{n-1} \in \mathbb{N}$ таковы, что для всякого многочлена

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1} \in \mathbb{R}[x]$$

и для всякого числа $q \in (0,1)$ многочлен

$$f_q(x) = a_0 + a_1 q^{k_1} x + a_2 q^{k_2} x^2 + \dots + a_{n-1} q^{k_{n-1}} x^{n-1}$$

имеет не больше мнимых корней / с учетом кратности / чем многочлен $f(x)$. Тогда существует число $k_n \in \mathbb{N}$ такое, что, для любых чисел $a_n \in \mathbb{R}$; $m \in \mathbb{N}$, $m \geq k_n$ и любых чисел $q \in (0,1)$ многочлен $g_q(x) = f_q(x) + a_n q^m x^n$ имеет не больше мнимых корней / с учетом кратности / чем многочлен $f(x) + a_n x^n$.

Работа выполнена при поддержке Российского фонда фундаментальных исследований и программы "Университеты России".

Литература

1. Полиа Г., Сеге Г. Задачи и теоремы из анализа, ч. 2. - М. : Наука, 1978.- 432 с.

2. Том Р., Левин Г. Особенности дифференцируемых отображений // в сб. " Особенности дифференцируемых отображений ".- М.: Мир, 1968.- с. 9-101.

УДК 519.6 + 519.15

Бондаренко Б.А., Туляганов Р.Б. (Ташкент)

РАСПРЕДЕЛЕНИЕ ГАУССОВЫХ БИНОМИАЛЬНЫХ КОЭФФИЦИЕНТОВ ПО МОДУЛЮ P В АРИФМЕТИЧЕСКОМ ТРЕУГОЛЬНИКЕ

Как известно [1], гауссовы биномиальные коэффициенты $\begin{bmatrix} n \\ m \end{bmatrix}_q$ определяются рекуррентным соотношением

$$f(n,m) = af(n-1,m-1) + bf(n-1,m) ,$$

где

$$n = 0,1,\dots , \; m = 0,1,\dots,n, \quad a = 1, \quad b = q^m, \quad \begin{bmatrix} n \\ o \end{bmatrix}_q = 1 \; (n \geq 0).$$

Гауссовы коэффициенты могут быть выписаны в виде арифметического треугольника по аналогии с треугольником Паскаля и его обобщениям, исследованным в [2].

Устанавливаются разнообразные числовые и комбинаторные свойства арифметического треугольника, составленного из гауссовых коэффициентов. Так, установлено, что ни один из коэффициентов, стоящих в строке треугольника, номер которой $N = p^n(p-1)-1$ не делится на простое p, а в следующей за ней строке все коэффициенты, за исключением крайних, делятся на то же p. На основании этого исследуется геометрия арифметического треугольника, составленного из гауссовых коэффициентов, при произвольном простом p.

Методы, разработанные в [2] для исследования обобщенных треугольников Паскаля по модулю p применяются для изучения вопросов распределения гауссовых коэффициентов по модулю $p = 3,5,7$ как в произвольных строках, так и в треугольниках, основаниями которых служат указанные выше строки для любого значения n. Доказано, что $\lim [G(n)/H(n)] = 0$ при $n \to \infty$, где $G(n)$ – количество неделящихся, а $H(n)$ – количество делящихся на p гауссовых коэффициентов в арифметическом треугольнике, с произвольным номером основания n.

Построены и изучены арифметические фрактальные структуры, составленные из вычетов гауссовых коэффициентов по модулю $p=3,5,7$.

Литература

1. Айгнер М. Комбинаторная теория. – М.: Мир, 1982.

2. Bondarenko B.A. Generalized Pascal Triangles and Pyramids, their Fractals, Graphs, and Applications / Translated by R.C.Bollinger. – USA, Santa Clara: Fibonacci Association, 1993.

УДК. 511.36

Борбат В.Н. (Минск)

ОБ ОДНОМ СВОЙСТВЕ ЦЕЛОЧИСЛЕННЫХ ПОЛИНОМОВ СОВМЕСТНО АППРОКСИММИРУЮЩИХ НУЛЬ С ЗАДАННЫМ ПОРЯДКОМ.

Пусть $P(x)=a_n x^n+\ldots+a_1 x+a_0$ - полином с целыми коэффициентами, H - его высота. В [1] доказана

Теорема 1. Система неравенств

$$\begin{cases} |P(x)|<H^{-n} \\ |P'(x)|<H^{1-\varepsilon} \end{cases} \qquad (1)$$

при любом $\varepsilon>0$ имеет для почти всех $x\in\mathbb{R}$ (в смысле линейной меры Лебега) лишь конечное число решений в полиномах $P(x)\in\mathbb{Z}[x]$.

В настоящей работе производится обобщение указанной теоремы.

Теорема 2. Система неравенств

$$\begin{cases} |P(\omega_1)|<H^{-w_1} \\ |P(\omega_2)|<H^{-w_2} \\ |P'(\omega_1)|<H^{1-\varepsilon} \end{cases} \qquad (2)$$

где $w_1+w_2=n-1$ при любом $\varepsilon>0$ имеет для почти всех $(w_1,w_2)\in\mathbb{R}^2$ лишь конечное решений в полиномах $P(x)\in\mathbb{Z}[x]$.

В [2] доказана метрическая теорема для системы несколько отличной от системы (2). В ней отсутствует условие, налагаемое на производную $|P'(\omega_1)|<H^{1-\varepsilon}$, но $w_1+w_2>n-1$. Теорема 2 позволяет построить регулярную систему векторов с действительными алгебраическими координатами и на основании этого получать оценки снизу для размерности Хаусдорфа.

Литература

1. Берник В.И. // Доклады АН БССР. 1986. Т.30. N 5. С.403-405.
2. Берник В.И. // Известия АН СССР. 1980. Т.44. N 1. С.24-45.

Боровских А.В., Бурлуцкая М.Ш. (Воронеж)

О дифференцировании и интегрировании по мере на абстрактных [illegible]

При относительном дифференцировании функций, имеющих точку разрыва, возникает необходимость "запомнить" в этой точке число – отношение скачков дифференцируемой и дифференцирующей функции (называемой далее мерой) и считать это число значением производной в этой точке: только в этом случае функция будет правильно восстанавливаться по производной с помощью интеграла Лебега-Стилтьеса. Поскольку соответствующая мера (=дифференцирующая функция) в указанной точке будет иметь скачок (мера точки ненулевая), значение интегрируемой функции (производной) не может быть изменено произвольным образом, как в любой другой точке с нулевой мерой, или "забыто". При повторном дифференцировании – таких чисел в одной и той же точке оказывается уже два, при следующем – три и т.д. Считать эти числа значениями производной в одной и той же точке неудобно, т.к. это создает ряд существенных проблем при использовании классической схемы интегрирования Стилтьеса. С другой стороны, игнорировать даже часть из них невозможно – опять же из-за необходимости восстанавливать функцию по её производным.

В докладе возникающая проблема решается путем введения новых "квазичисловых" множеств, строящихся с помощью метода сечений Дедекинда. Именно, производная функции $f(x):M\to R$ (M – линейно упорядоченное множество) определяется не на M, а на новом множестве M' сечений в M. В отличие от классической теории Дедекинда сечения, порождаемые одним и тем же элементом (числом) x, но в которых он входит в разные классы, различаются и обозначаются $x+0$ и $x-0$ соответственно. Оказывается, при таком определении классические понятия предела, непрерывности, производной, меры, интеграла не только не усложняются, но, наоборот, приобретают подчас более естественную, чем в классическом анализе, форму.

Обоснованы аналоги основных результатов анализа: дифференцируемость монотонной функции, абсолютная непрерывность интеграла Лебега-Стилтьеса, восстановление интеграла по производной и т.д. При этом, в случае классической дифференцируемости, точки $x+0$ и $x-0$ отождествляются между собой и с точкой x, а при несовпадении правой и левой производной в точке x эти точки порождают "раздвоение", а при последующем дифференцировании "растроение" и т.д. точки x, создавая естественную область определения для производных.

УДК 511.9

О.Н.Василенко

Московский государственный университет

ТЕСТИРОВАНИЕ НА ПРОСТОТУ И ПОСТРОЕНИЕ БОЛЬШИХ ПРОСТЫХ ЧИСЕЛ

Большие простые числа широко используются в криптографии. Наилучшие общие методы доказательства простоты натуральных чисел в настоящее время состоят из алгоритмов, детерминированно проверяющих простоту n за $O((\log n)^{c \log\log\log n})$ арифметических операций (Аддеман, Ленстра, Коен), и вероятностных алгоритмов типа Лас-Вегас, имеющих полиномиальную сложность и использующих вычисления на эллиптических или гиперэллиптических кривых (Голдвассер-Килиан, Померанс, Аддеман-Хуанг).

Если n имеет специальный вид, или известно полное или частичное разложение $n-1$ или $n+1$ на множители, то доказательство простоты n проводится быстрее. На этом основаны методы построения больших простых чисел, работающие по следующей схеме. Строится возрастающая последовательность простых чисел p_i до тех пор, пока не будет найдено простое число нужной величины. На i -м шаге мы полагаем $n = k \cdot \prod_{j<i} p_j^{\alpha_j} \pm 1$, где k не очень большое натуральное число. Затем тестируем n на простоту с помощью вероятностных тестов (Соловей-Штрассен, Миллер-Рабин), и если n вероятно простое, пытаемся доказать его простоту, пользуясь известным разложением $n \mp 1$ на множители. В случае успеха полагаем $p_i = n$.

В докладе дается обзор описанных выше алгоритмов. См. также [1].

ЛИТЕРАТУРА.

1. Василенко О.Н. Построение больших простых чисел.-М.,МГУ им.М.В.Ломоносова, Лаборатория по математическим проблемам криптографии, 1995, препринт, 32 стр.

УДК 511.36

Васильев Д.В. (Минск)

Интегральное представление дзета-функции Римана в целых точках

Дзета-функция Римана задается рядом $\zeta(s)=\sum_{n=1}^{\infty} n^{-s}$, где Re $s>1$. Еще Л.Эйлер установил, что $\zeta(2k) = q_k\pi^{2k}$, $k\in\mathbb{N}$, $q_k\in\mathbb{Q}$ и, значит, из трансцендентности числа π немедленно следует трансцендентность $\zeta(2k)$. В 1978 г. Р.Апери доказал , что $\zeta(3)$ иррационально. Что касается чисел $\zeta(2k+1)$, то до сих пор не известно рациональны они или нет.

В 1979 г. Ф.Бейкерсом (см [1]) было получено более короткое доказательство иррациональности чисел $\zeta(2)$ и $\zeta(3)$. В качестве приближений рассматривались интегралы

$$I_2=d_n^2\int_{(0,1)^2}\frac{x^n(1-x)^n y^n(1-y)^n}{(1-xy)^{n+1}}\,dxdy \text{ и } I_3=d_n^3\int_{(0,1)^3}\frac{x^n(1-x)^n y^n(1-y)^n z^n(1-z)^n}{(1-z(1-xy))^{n+1}}\,dxdydz,$$

которые равны $A_n+B_n\zeta(2)$ и $C_n+D_n\zeta(3)$ соответственно. Здесь d_n — наименьшее общее кратное чисел $1,\dots,n$, а $A_n,B_n,C_n,D_n\in\mathbb{Z}$.

Интегралы I_2 и I_3 можно обобщить. Пусть

$$I_k(n)=d_n^k\int_{(0,1)^k}\frac{\prod_{i=1}^{n} x_i^n(1-x_i)^n\,dx_1\dots dx_k}{[1-x_k(1-x_{k-1}(1-\dots x_2(1-x_1)\dots))]^{n+1}}$$

Очевидно, что $I_2(n)$ и $I_3(n)$ совпадают с I_2 и I_3 соответственно. Возникает предположение, что $I_k(n)=A_n^k+B_n^k\,\zeta(k)$, где $A_n^k,B_n^k\in\mathbb{Z}$, $k\geq 2$. В случае его истинности немедленно следует иррациональность чисел $\zeta(2k+1)$, $k\geq 2$. Доказана теорема, подтверждающая данное предположение в случае $n=0$.

Теорема: При $k\in\mathbb{N}$ и $k\geq 2$

$$I_k(0)=\begin{cases} 2\zeta(k)(1-2^{1-k}), & \text{при четном } k\\ 2\zeta(k), & \text{при нечетном } k.\end{cases}$$

[1] Beukers F. A note on the irrationality of $\zeta(2)$ and $\zeta(3)$. Bull. London Math. Soc. v.11, n3, 1979, pp. 268-272.

УДК 511.19

Varbanetz P.D.(Odessa)

ON SOME TRIGONOMETRIC SUMS

We study the sum $\sum_{\substack{M\le m\le M'\le 2M\\ N\le n\le N'\le 2N}} e\left(\frac{\varepsilon m^{\beta}}{n^{\alpha}}\right)$ where $e(u)=e^{2\pi iu}$, $\alpha,\beta\in\mathbb{Q}$, $x,M,N\in\mathbb{R}$, $M,N>1$. In particular, we prove the following theorem.

Theorem. *Let $x,M,N\ge 1$, $K=MN\le X^{3/2}$. Let $M_1=X^{-0,0318}K^{0,3417}$, $M_2=X^{0,1809}K^{0,2029}$;*

$$q'=\begin{cases}\left(M^{-904}x^{476}N^{140}\right)^{1/666}, & \text{if } M\ge M_2\\ \left(M^{1348}x^{488}N^{-410}\right)^{1/1208}, & \text{if } M_1\le M\\ \left(M^{334}x^{322}N^{-131}\right)^{1/832}, & \text{if } M_1<M<M_2.\end{cases}$$

Then for $K\ge x^{32/49}$, $M\ge x^{1/15}$, $q=\min(q',x^{1/2}M^{1/4},N^{3/4}$ the estimate

$$\sum_{M\le m\le M'}\sum_{N\le n\le N'} e\left(\frac{\varepsilon m^{1/2}}{n^{1/2}}\right)\ll x^{-1/2}M^{3/4}N^{5/4}+x^{-1/2}M^{-1/4}N^{1/2}\times$$
$$\times\left(xM^{3/4}N^{-3/2}q^{-1/2}+M^{15/8}x^{11/8}N^{-15/16}q^{-1}\min(q^{1/4},x^{1/2}M^{1/4}N^{-1})\right)$$

holds

УДК 511

Вахитова Е.Б. /Стерлитамак/

О ПОЧТИ ПРОСТЫХ В КОРОТКИХ ИНТЕРВАЛАХ И НЕКОТОРЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ

Пусть $p, k, l, n, r \in \mathbb{N}$, $r \geq 2$, $\Lambda_r, x \in \mathbb{R}$, $\Lambda_r > 0$.

Рассмотрим задачи о существовании почти простых чисел P_r, являющихся значениями неприводимого полинома $F(x)$ натуральной степени g с целыми коэффициентами

1/ от натурального аргумента n в коротких интервалах

$$(x - x^{1/\Lambda_r};\ x),$$

2/ от простого аргумента p в коротких интервалах,

3/ от натурального аргумента n из арифметической прогрессии

$$kn + l,$$

4/ от простого аргумента p из последовательности $kp + l$.

Применяя одномерное решето с весами Бухштаба нового типа [1] и результаты работы [2], получим теоремы, позволяющие получить преимущества в выборе параметров одномерного решета с весами в сравнении с теоремами, доказанными автором ранее/1992/ и позволяющие в дальнейшем улучшить оценки для указанных выше задач, а именно, для случаев:

1). $P_r = F(n)$, $n \in (x - x^{1/\Lambda_r};\ x)$, $r = g+1$,

2). $P_r = F(p)$, $p \in (x - x^{1/\Lambda_r};\ x)$, $r = 2g+1$,

3). $P_r = F(n)$, $n \equiv l \pmod k$, $k = [x^{1-g/\Lambda_r};\ x]$, $r = g+1$,

4). $P_r = F(p)$, $p \equiv l \pmod k$, $k = [x^{1-1/\Lambda_r};\ x]$, $r = 2g+1$.

Литература.

1. Бухштаб А.А. Новый тип весового решета // Тезисы докл. всес. конф. "Теория чисел и ее приложения". Тбилиси.- 1985.- С.22-24.

2. Вахитова Е.Б. О приложении функций Бухштаба // Матем.заметки. - 1995.- Т.57, вып. 1. - С. 121-125.

УДК 511

Вереитинов Э.В.(Калуга)

ИССЛЕДОВАНИЕ ДИОФАНТОВЫХ УРАВНЕНИЙ ПРИ ИСПОЛЬЗОВАНИИ ОПЕРАЦИЙ МАТАМАТИЧЕСКОЙ ЛОГИКИ

Операции математической логики и метод математической индукции представляют собою весьма эффективные способы матамати-ческих исследований. Однако оба способа, как правило, применяются независимо друг от друга. Предметом исследования является попытка их комплексного использования в математических доказательствах. Доказаны теоремы для оценки разрешимости уравнений и для оценки истинности высказывательных форм (предикатов) с натуральной переменной, в частности, две теоремы, приведенные ниже.

Т е о р е м а I. Для любых одноместных предикатов $A(n)$ и $B(n)$ с натуральной переменной n истинно утверждение

$$(\forall n\in N)(((A(n)\Rightarrow B(n))\wedge(B(1)\Rightarrow\neg A(1))\wedge(B(n+1)\Rightarrow\neg B(n))\wedge((\exists l)(B(l)=1)))\Rightarrow(B(n)\Rightarrow\neg A(n))).$$

Доказательство проводится методом математической индукции по n. Устанавливается истинность утверждения $B(n)\Rightarrow\neg A(n)$ для любого n при оговоренных в теореме условиях, причём для доказательства истинности утверждения при $n=k+1$ проверяется истинность высказывания для произвольного натурального k

$$(B(k)\wedge(B(k+1)\Rightarrow\neg B(k))\wedge(A(k+1)\Rightarrow B(k+1)))\Rightarrow((B(k)\Rightarrow\neg A(k))\Rightarrow(B(k+1)\Rightarrow\neg A(k+1)))$$

с составлением соответствующей таблицы истинности.

Аналогично выполняется доказательство теоремы 2.

Т е о р е м а 2. Если уравнение $B(n)=0$ с натуральной переменной n является следствием уравнения $A(n)=0$ на множестве натуральных чисел и найдётся такое $n=l$, что уравнение $B(l)=0$ разрешимо, а при $n=1$ при разрешимости уравнения $B(1)=0$ уравнение $A(1)=0$ неразрешимо, и, кроме того, при $n+1$ разрешимость уравнения $B(n+1)=0$ противоречит разрешимости при n уравнения $B(n)=0$, то при разрешимости уравнения $B(n)=0$ уравнение $A(n)=0$ неразрешимо для любого натурального числа n.

УДК 514.17

Власов Е.В. (Иваново)

Дуальные системы
первичных элементов точечных решеток

Теорема 1. Система диагоналей 5-мерного первичного элемента эквивалентна одной из 13 нижеследующих систем

$$1)\ C^5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix},\quad 2)\ \begin{pmatrix} C^5, & & & & 1 \\ & & & & 2 \\ & & & & 2 \\ & & & & 2 \\ & & & & -2 \end{pmatrix},\quad 3)\ \begin{pmatrix} C^5, & & & & 1 \\ & & & & 2 \\ & & & & 2 \\ & & & & 0 \\ & & & & 0 \end{pmatrix},\quad 4)\ \begin{pmatrix} C^5, & & & 1 & 1 \\ & & & 2 & 2 \\ & & & 2 & 0 \\ & & & 0 & 2 \\ & & & 0 & 0 \end{pmatrix},$$

$$5)\ \begin{pmatrix} C^5, & & & 1 & 1 \\ & & & 2 & 0 \\ & & & 2 & 0 \\ & & & 0 & 2 \\ & & & 0 & 2 \end{pmatrix},\quad 6)\ \begin{pmatrix} C^5, & & 1 & 1 & 1 \\ & & 2 & 2 & 2 \\ & & 2 & 0 & 0 \\ & & 0 & 2 & 0 \\ & & 0 & 0 & 2 \end{pmatrix},\quad 7)\ \begin{pmatrix} C^5, & & 1 & 1 & 1 \\ & & 2 & 2 & 0 \\ & & 2 & 0 & 0 \\ & & 0 & 2 & 2 \\ & & 0 & 0 & 2 \end{pmatrix},\quad 8)\ \begin{pmatrix} C^5, & 1 & 1 & 1 & 1 \\ & 2 & 2 & 0 & 2 \\ & 2 & 0 & 2 & 2 \\ & 0 & 2 & 2 & 2 \\ & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$9)\ \begin{pmatrix} C^5, & 1 & 1 & 1 & 1 \\ & 2 & 2 & 0 & 0 \\ & 2 & 0 & 2 & 0 \\ & 0 & 2 & 0 & 2 \\ & 0 & 0 & 2 & 2 \end{pmatrix},\quad 10)\ \begin{pmatrix} C^5, & & 1 & 1 & 1 & 1 & 1 \\ & & 2 & 2 & 0 & 2 & 2 \\ & & 2 & 0 & 2 & 2 & 0 \\ & & 0 & 2 & 2 & 2 & 0 \\ & & 0 & 0 & 0 & 2 & 2 \end{pmatrix},\quad 11)\ \begin{pmatrix} C^5, & & 1 & 1 & 1 & 1 & 1 \\ & & 2 & 2 & 2 & 2 & 2 \\ & & 2 & 0 & 2 & 0 & 2 \\ & & 0 & 2 & 0 & 2 & 2 \\ & & 0 & 0 & -2 & -2 & -2 \end{pmatrix},$$

$$12)\ \begin{pmatrix} C^5, & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ & 2 & 2 & 0 & 2 & 2 & 0 & 2 \\ & 2 & 0 & 2 & 2 & 0 & 2 & 2 \\ & 0 & 2 & 2 & 2 & 0 & 0 & 0 \\ & 0 & 0 & 0 & 0 & 2 & 2 & 2 \end{pmatrix},\quad 13)\ \begin{pmatrix} C^5, & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ & 2 & 2 & 2 & 0 & 0 & 0 & 2 & 2 & 2 & 0 & 2 \\ & 2 & 0 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 \\ & 0 & 2 & 0 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 2 \\ & 0 & 0 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 2 & 2 \end{pmatrix}.$$

Каждый из этих первичных элементов с точностью до эквивалентности относительно преобразований группы $\mathbf{GL}(6, \mathbf{Z})$ реализуется в решетках Γ^5_f с метрической формой $f(x) \in \Phi(\mathbf{R}^*)$, где $\mathbf{R}^*$ – система, дуальная системе $\mathbf{R}$, представляющей соответственно первичный элемент.

Теорема 2. Всякая система диагоналей 6-мерного первичного элемента эквивалентна одной из двух систем

$$1)\ \begin{pmatrix} 1111111111111111111111111111111111 \\ 0200002222000000222222000022220 2 \\ 0020002000222000220002220222022 \\ 0002000200200220200220220222022 \\ 0000200020020202020220220222222 \\ 0000020002002022002022022222222 \end{pmatrix},$$

$$2)\ \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 & 0 & 2 & 2 & 2 & 0 & 0 & 0 & 2 & 2 & 2 & 0 & 2 \\ 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 \\ 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 \end{pmatrix}.$$

АБСТРАКТНАЯ К-АЛГЕБРА

Л.И.Волгин

На множестве функций скалярных произведений (ФСП) $z = V_A(Y) = y_1\alpha_1 + \ldots + y_n\alpha_n$ при наложении ограничения $\alpha_1 + \ldots + \alpha_n = 1$ (условие комплементарности) построена комплементарная алгебра (КА) с базовыми операциями

$$z_1 = V_{(\alpha_1,\alpha_2)}(y_1, y_2) = y_1\alpha_1 + y_2\alpha_2, \quad z_2 = \Lambda_{(\alpha_1,\alpha_2)}(y_1, y_2) = y_1\alpha_2 + y_2\alpha_1, \quad \alpha_1 + \alpha_2 = 1 \qquad (I)$$

(комплементарные дизъюнкция V и конъюнкция Λ) и диаметральной инверсии $\bar{y}_i = M - y_i$, где M есть центр области определения компонент y_i вектора Y. Здесь α_i есть скалярные величины (действительные или комплексные числа), y_i в общем случае являются элементами абстрактного, в частности, векторного линейного пространства. Функции К-алгебры относительно векторов A и Y обладают всеми свойствами линейных пространств. Но дополнительно относительно переменных y_i имеют место: идемпотентность $z(y, \ldots, y) = y$, бисимметричность, распределительные законы, закон спуска инверсии на переменные $\bar{y}_i$, аксиома Клини, вырожденный модулярный закон, вложенность и др.

При $\alpha_i \in \{0, 1\}$ КА вырождается в предикатную алгебру выбора (ПАВ), для которой дополнительно имеют место: свойство согласованности $z_1 z_2 = y_1 y_2$, $z_1 + z_2 = y_1 + y_2$, сочетательный закон, закон булевого поглощения, свойство дуальной инверсии, свойство ортогональности $\alpha_i \alpha_j = 0$ при $i \neq j$, идемпотентность скаляров $\alpha_i \alpha_i = \alpha_i$ и др.

Доказана основная теорема К-алгебры: каждая КА-функция является суперпозиционной функцией от элементарных (бинарных) функций КА.

Условие комплементарности и КА-функции под теми или иными наименованиями находят широкое применение в различных областях науки и техники.

В частности, при $\alpha_1 = 1(x_1 - x_2)$, $\alpha_2 = 1 - \alpha_1 = 1(x_2 - x_1)$ базовые функции ПАВ

$$z_1 = y_1 1(x_1 - x_2) + y_2 1(x_2 - x_1), \quad z_2 = y_1 1(x_2 - x_1) + y_2 1(x_1 - x_2) \qquad (2)$$

воспроизводятся логическими схемными элементами - реляторами, используемых для построения нейронных сетей и коммутационно-логических преобразователей [1,2]. Здесь $1(x)$ есть единичная функция равная нуле при $x < 0$ и единице при $x > 0$. При $y_1 = x_1$, $y_2 = x_2$ выражения (2) воспроизводят базовые операции непрерывной (бесконечнозначной, нечёткой) логики $z_1 = \max(x_1, x_2)$, $z_2 = \min(x_1, x_2)$, которые в свою очередь при $x_1, x_2 \in \{0, 1\}$ вырождаются в булевы дизъюнкцию $z_1 = x_1 \vee x_2$ и конъюнкцию $z_2 = x_1 \wedge x_2$.

Таким образом, свойства и законы булевых алгебр, многозначных и непрерывной логик есть следствие отношений в комплементарной алгебре, вытекающих из дополнительных ограничений, накладываемых в КА на переменные y_i.

1. Волгин Л.И. Комплементарная алгебра и реляторные модели нейронных структур // Электронное моделирование. - 1994. - № 3. - С.15-25.

2. Волгин Л.И. Комплементарная алгебра и предикатная алгебра выбора. - Ульяновск: УлГТУ, 1995. - 66 с.

С. М. Воронин, В. И. Скалыга

О ПОЛУЧЕНИИ АЛГОРИТМОВ ЧИСЛЕННОГО ИНТЕГРИРОВАНИЯ

Пусть p и q – простые числа, $p\equiv 1 \pmod q$, $a\in\mathbb{Z}$, $(a,p)=1$, $a^{(p-1)/q}\not\equiv 1 \pmod p$, $\bar b=(1,a^{(p-1)/q},a^{2(p-1)/q},\dots,a^{(q-1)\cdot(p-1)/q})$,

$$f(\bar x)=\sum_{\bar n\in\mathbb{Z}^{q-1}} C_{\bar n}\cdot\exp(2\pi i(\bar n,\bar x)),\quad \bar x\in\mathbb{R}^{q-1},\quad \|\operatorname{Spec} f\|<\infty.$$

В работах [1-3] на основе теории дивизоров предлагались эффективные методы построения квадратурных формул с малым количеством узлов. При этом возникала необходимость оперировать с нормами целых алгебраических чисел, что накладывало существенное ограничение на размерность интегрируемых функций. Эти затруднения позволяет преодолеть следующая теорема.

ТЕОРЕМА. Найдется $p\ge \ln$ Н. О. К. $(N(n_0+n_1\zeta+\dots+n_{q-1}\zeta^{q-2}))$ такое что для каждого $\bar n\in\operatorname{Spec} f\setminus(\bar 0)$, выполняется $(\bar n,\bar b)\not\equiv 0 \pmod p$. Тогда справедлива формула

$$\int_0^1\int_0^1\dots\int_0^1 f(\bar x)\,dx_1\,dx_2\dots dx_{q-1}=1/p\sum_{\nu=1}^{p} f(\{\bar b/p\cdot\nu\}).$$

Список литературы.

1. Воронин С. М., Темиргалиев Н. О квадратурных формулах, связанных с дивизорами поля гауссовых чисел// Мат. заметки, 1989, т. 46, No. 2, с. 34-41.
2. Темиргалиев Н. Применение теории дивизоров к численному интегрированию периодических функций многих переменных// Мат. сб. 1990, т. 181, No. 4, с. 490-505.
3. Воронин С. М. О квадратурных формулах// Изв. РАН, сер. матем. 1994, т. 58, No.5, с.189-194.

Работа выполнена при финансовой поддержке Российского Фонда Фундаментальных Исследований, грант No. 93-011-16021

УДК 511.334

Воскресенская Г.В. /Самара/

ПАРАБОЛИЧЕСКИЕ ФОРМЫ И РЕГУЛЯРНЫЕ ПРЕДСТАВЛЕНИЯ ГРУПП

Пусть G – конечная группа, представление $\varphi: G \to SL(V)$, $24 \mid \dim V$. Тогда $\forall g \in G$ характеристический многочлен оператора $\varphi(g)$ имеет вид

$$P_g(x) = \prod_k (x^{a_k} - 1)^{t_k}, \quad a_k \in \mathbb{N}, \ t_k \in \mathbb{Z}, \ t_k$$

С элементом g можно связать функцию $\eta_g(z) = \prod_k \eta(a_k z)$, где $\eta(z)$ – эта-функция Дедекинда, определенная на верхней комплексной полуплоскости. Функция $\eta_g(z)$ является параболической формой с характером, веса $\frac{1}{2}\sum_k t_k$.

Автором было доказано [2], что существует ровно 28 параболических форм целого веса с характерами, собственных относительно всех операторов Гекке и не имеющих нулей на верхней комплексной полуплоскости. Все они являются произведениями η-функций от различных аргументов.

ТЕОРЕМА.

Пусть ρ – регулярное представление группы G порядка 24. Тогда $\forall g \in G$ параболическая форма $\eta_g(z)$, ассоциированная с элементом g с помощью представления ρ, является параболической формой целого веса с характером, собственной относительно всех операторов Гекке с дивизором, сосредоточенным в параболических вершинах.

ЛИТЕРАТУРА.

1. Dummit D., Kisilevsky H., Mc Kay J. Multiplicative products of η-functions // Contemp. Math. 1985. - V. 45. - P. 89-98.

2. Воскресенская Г.В. Модулярные формы с дивизором в параболических вершинах : Дисс. канд. физ.-мат. наук. - Самара., 1993. - 114 с.

УДК 511.2, 512.7

Воскресенский В.Е. (Самара)

ЛИНЕЙНЫЕ АЛГЕБРАИЧЕСКИЕ ГРУППЫ И ИХ ЦЕЛЫЕ ФОРМЫ

Пусть O - коммутативное кольцо с единицей без делителей нуля, k - его поле частных, G - линейная алгебраическая группа, определенная над полем k. Целой формой группы G назовем групповую O-схему X такую, что k-группы G и $X \otimes_O k$ изоморфны.

Теорема 1. Пусть $\varphi: G \longrightarrow GL(V)$ - точное линейное представление группы G. Тогда выбор свободной решетки M в пространстве V определяет O-алгебру Хопфа A в алгебре $k[G]$ и $X = \mathrm{Spec}\, A$ является целой формой группы G. Групповая схема X имеет конечный тип над O, она строго плоская и приведенная над O.

Группа X однозначно характеризуется представлением φ и решеткой M, введем обозначение $X = G_{\varphi,M}$. Возникает задача описания подколец A в кольце функций $k[G]$ с условиями:

1) A является O-алгеброй Хопфа конечного типа над O,
2) $A \cap k = O$; $kA = k[G]$,
3) структура алгебры Хопфа в кольце A индуцирована строением алгебры Хопфа $k[G]$.

Подкольца A из $k[G]$, удовлетворяющие условиям 1 - 3, назовем O-порядками Хопфа в $k[G]$.

Важнейшими полями, над которыми естественно возникает вопрос об изучении порядков Хопфа, являются числовые поля и поле p-адических чисел.

Теорема 2. Пусть k - поле p-адических чисел с кольцом целых O, T - алгебраический k-тор. Имеется взаимнооднозначное соответствие между O-порядками Хопфа в $k[G]$ и подгруппами конечного индекса в максимальной компактной подгруппе U группы $T(k)$. Всякая O-форма X конечного типа тора T имеет вид $T_{\varphi,M}$ при некотором точном представлении φ и решетке M в пространстве представления. Среди этих форм имеется минимальная целая модель.

Теорема 2 позволяет описать целые модели для торов, определенных над полем алгебраических чисел, путем склеивания их из локальных моделей.

УДК 511.5

Всемирнов М.А. (С.-Петербург)

О диофантовых представлениях линейных рекуррентных последовательностей

В 1970 г. Ю.В.Матиясевич указал такой многочлен с целыми коэффициентами $P(u, n, x_1, \ldots, x_s)$, что при фиксированных неотрицательных целых значениях параметров u и n уравнение

$$P(u, n, x_1, \ldots, x_s) = 0 \qquad (1)$$

разрешимо в неотрицательных целых числах $x_1, \ldots, x_s$ тогда и только тогда, когда u есть n-ое число Фибоначчи.

Этот результат вместе с предшествующими исследованиями Дж. Робинсон, М. Дейвиса и Х.Патнама доказывал алгоритмическую неразрешимость 10-й проблемы Гильберта.

Позднее аналогичные многочлены были построены для линейных рекуррентных последовательностей 2-го порядка. Вопрос о возможном переносе этих результатов на последовательности более высоких порядков оставался открытым.

Автором получены представления, аналогичные (1), для последовательностей 3-го и 4-го порядков, удовлетворяющих дополнительным арифметическим ограничениям на определяющие коэффициенты. Кроме того, доказано, что для последовательностей более высоких порядков таких представлений получить нельзя. Таким образом полностью решен Открытый вопрос 2.3 из [1].

Применение полученных результатов для нахождения новых диофантовых представлений возведения в степень не только дает еще одно доказательство неразрешимости 10-й проблемы Гильберта, но и может оказаться полезным для ряда приложений.

Литература

[1] Ю. В. Матиясевич, *Десятая проблема Гильберта*. М.,Наука (1993).

[2] М. А. Всемирнов, *Диофантовы представления линейных рекуррентных последовательностей. I* – Записки научных семинаров ПОМИ. 227.

УДК 511.36

Галочкин А.И. (Москва)

О ЛИНЕЙНОЙ НЕЗАВИСИМОСТИ ЗНАЧЕНИЙ ФУНКЦИЙ, УДОВЛЕТВОРЯЮЩИХ ФУНКЦИОНАЛЬНЫМ УРАВНЕНИЯМ МАЛЕРА

Т е о р е м а . Пусть функции $f_1(z), \dots, f_m(z)$ в некоторой окрестности начала координат допускают разложения в ряды Тейлора с коэффициентами из мнимого квадратичного поля I , линейно независимы вместе с 1 над полем $\mathbb{C}(z)$ и составляют решение системы функциональных уравнений

$$\overline{f}(z) = A(z)\overline{f}(z^p) + \overline{B}(z), \quad p \in \mathbb{Z}, \quad p \geq 2,$$

где $\overline{f}(z)$ - столбец, составленный из функций $f_1(z), \dots, f_m(z)$; $A(z)$ - $m \times m$ -матрица, а $\overline{B}(z)$ - столбец с элементами - рациональными функциями. Далее, пусть α и β - целые числа из поля I , $0 < |\alpha|^{m+1} < |\beta|$, такие, что при $z = \alpha/\beta$ сходятся ряды Тейлора функций $f_1(z), \dots, f_m(z)$, определены все матрицы $A(z^{p^k})$ и столбцы $\overline{B}(z^{p^k})$ ($k = 0, 1, 2, \dots$) и определители этих матриц не обращаются в нуль. Тогда числа $1, f_1(\alpha/\beta), \dots, f_m(\alpha/\beta)$ линейно независимы над полем I .

При доказательстве теоремы используются некоторые идеи, связанные с методами Малера и Зигеля. При $\alpha = 1$ подобный результат следует из предложения B статьи [1], которое доказано при помощи Паде-аппроксимаций.

Л и т е р а т у р а . [1]. J.H.Loxton, A.J. van der Poorten. Arithmetic properties of automata: regular sequences J. reine angew. Math. 392, 1988, pp. 57 - 69.

к.т.н. с.н.с. Герасименко В.Г.

МЕТОДЫ ВЫЯВЛЕНИЯ УСТОЙЧИВЫХ ИНФОРМАЦИОННЫХ СТРУКТУР

Принятие решений в условиях неоднозначности и противоречивости исходной информации требует разработки и реализации эффективной процедуры выявления устойчивых информационных структур. В общем случае такая процедура включает :

- структуризацию решения, то есть представление его в виде системы частных информационных решений;

- отображение исходной информации в систему с использованием специальных методов проверки условий сопряжения групп данных (по времени, пространству и алфавиту);

- собственно поиск устойчивых информационных структур и их оценивание на основе методов формальной теории рассуждений (порождения и оценки гипотез, условий их оправдания и фальсификации).

Реализация процедуры в виде проблемно-ориентированной экспертной системы позволяет на 3 - 4 порядка сократить время поиска устойчивых информационных структур и принятия на их основе эффективных решений.

УДК 511

Н.М.Глазунов (Киев)

О ВЕРИФИЦИРОВАННОМ ВАРИАНТЕ МЕТОДА А.В.МАЛЫШЕВА ДОКАЗАТЕЛЬСТВА ГИПОТЕЗЫ МИНКОВСКОГО О КРИТИЧЕСКОМ ОПРЕДЕЛИТЕЛЕ ОБЛАСТИ $|x|^p + |y|^p < 1$, $p > 1$.

Памяти А.В.Малышева

Гипотеза Минковского о критическом определителе области $|x|^p + |y|^p < 1$, $p>1$ исследована в работах Морделла, Дэвиса, Кона и Уотсона и уточнена Дэвисом. В работе А.В.Малышева[1] для уточненной гипотезы Минковского, которую мы и будем называть гипотезой Минковского, предложен метод ее доказательства с применением ЭВМ. Развитие и реализация на ЭВМ метода Малышева позволили полностью доказать гипотезу Минковского [2]. Однако вышеназванный метод требует при его применении проведения некоторых предварительных оценок, которые обусловлены не существом задачи, а способом реализации метода на ЭВМ, а также особенностями некоторых промежуточных шагов метода. Желательно располагать вариантом метода, при реализации которого не требовалось бы проведения предварительных оценок, зависящих от исследуемой функции и области счета. Такой верифицированный вариант метода А.В.Малышева будет представлен в докладе. Он основан (i) на реализации субоптимального включения с автоматической верификацией результатов на всех вычислительных этапах метода, и (ii) на верификации особенностей исследуемых функций и их верифицированном разрешении.

Численные примеры и результаты счета на ЭВМ будут представлены.

Лит.: [1] Малышев А.В. О применении ЭВМ к доказательству одной гипотезы Минковского из геометрии чисел //Модули и представления. Зап. научных семинаров ЛОМИ.- Л., 1977.- Т.71.- С.163-180.
[2] Глазунов Н.М., Голованов А.С., Малышев А.В. Доказательство гипотезы Минковского о критическом определителе области $|x|^p + |y|^p < 1$, $p>1$ // Исследования по теории чисел. (Там же).- Л., 1986.- Т.151.- С.40-53.

УДК 511

Глазунов Н.М. (Киев)

О НЕКОТОРЫХ ТЕОРЕТИКО-ЧИСЛОВЫХ ЗАДАЧАХ НАУЧНЫХ ВЫЧИСЛЕНИЙ

Памяти А.Г.Постникова

Целью научных вычислений является получение точных и надежных численных результатов при компьютерном исследовании задач и гипотез различных разделов науки. В то же время требования точности и надежности таких вычислений, и, особенно, сложность исследуемых задач, а также многообразие арифметических данных, используемых в исследуемых задачах, выдвигают ряд проблем теоретико-числового характера, без решения которых научные вычисления либо не эффективны, либо вообще невозможны.

Мы рассмотрим некоторые из таких теоретико-числовых задач, определяемых верифицированными вычислениями (т.е. такими вычислениями, результаты которых являются такими же строгими, как и математические доказательства). Изложение включает (i) p-адические интервальные арифметики, (ii) верифицированное решение систем алгебраических интервальных уравнений, и звездные тела, (iii) диофантовы приближения для интервалов. Будут предложены решения вышеназванных задач, а также дан обзор некоторых методов эффективных вычислений в конечных полях и целочисленных вычислений.

Глухов М. М. -мл. (г. Москва)

О КАНОНИЧЕСКИХ РАЗЛОЖЕНИЯХ НЕКОТОРЫХ ДВУЧЛЕНОВ НАД $GF(q^n)$

В работе [1] С. А. Степанов указал многочлены над $GF(q^n)$ при нечетном q, $n>1$, на которых достигается известная оценка А. Вейля для сумм символов Лежандра. Используя идею этой работы можно указать многочлены, на которых получаются хорошие оценки сумм характеров произвольного порядка над $GF(q^n)$ при любом q (см. [2]).

Для приложения этих результатов в теории кодов важно знать число $X_m(r)$ неприводимых над $GF(q^n)$ унитарных делителей степени m многочлена $g_r(x)=x+x^{q^r}$ при $r=\frac{n\pm1}{2}$, $\frac{n}{2}\pm1$.

Теорема. а) Если q -четно то

$X_m(r)=a\cdot\Phi_q(m)+2b\cdot\Phi_q(2m)$ если $m\mid r$,

$X_m(r)=0$ если $m\nmid r$;

б) если q -нечетно, $2^c m\mid 2r$, $2^c m\nmid r$, то

$X_m(r)=2^c\sum_{\nu=1}^{\kappa}\frac{1}{2^\nu}\Phi_q(2^c m/2^\nu)$ и $X_m(r)=0$ в других случаях.

Здесь: $\Phi_q(M)$ - число всех неприводимых над $GF(q)$ многочленов степени M при $M>1$ и отличных от X при $M=1$, $\kappa=\exp_2 2^c m$, $a,b,c\in\{0,1\}$; $a=0\Leftrightarrow m,n$ - четно; $b=0\Leftrightarrow(n,r)=1$; $c=0\Leftrightarrow n$ - нечетно.

ЛИТЕРАТУРА.

1. Степанов С. А. О нижних оценках сумм характеров над конечными полями. Дискретная математика т. 3, вып. 2, 1991, стр. 77-86.
2. Глухов М. М. -мл. Нижние оценки сумм характеров от многочленов над конечными полями. Дискретная Математика т. 3, вып. 3, 1994, с. 136-142.

УДК 511.36

Горелов В. А. (Иваново)

Эффективные оценки многочленов от значений E-функций, связанных алгебраическими уравнениями

Пусть $\xi \in \mathbf{A}$; K, K^*, Ω — алгебраические поля над $\mathbf{Q}$, причем K, $K^* \subset \Omega$, $\xi \in \Omega$, $[\Omega : \mathbf{Q}] = d$. Определение класса E-функций $KE(\lambda, c, \mu, q)$, эффективных и неэффективных постоянных см. в книге [1]. Там же изложена история вопроса.

Используя метод Зигеля и его обобщение, полученное в работах А. Б. Шидловского, автором доказывается

Теорема. Пусть функции $f_1(z), \dots, f_m(z)$, $m \geq 2$, принадлежащие классу $KE(\lambda, c, \mu, q)$, составляют решение системы линейных дифференциальных уравнений

$$y_i' = q_{i,0} + \sum_{j=1}^{m} q_{i,j} y_j, \quad q_{i,j} \in \mathbf{C}(z), \quad i = 1, \dots, m,$$

степень трансцендентности множества этих функций над $\mathbf{C}(z)$ равна l, $1 \leq l \leq m-1$, а совокупность старших членов минимальных уравнений (определение см. в [1]) имеет вид

$$A_j(z) f_m^{\varkappa_{m,j}}(z) \dots f_1^{\varkappa_{1,j}}(z), \quad A_j(z) \in K[z], \quad j = 1, \dots, \tau$$
$$\varkappa_0 = \max(\varkappa_{1,1}, \dots, \varkappa_{m,\tau}), \quad \xi T(\xi) A_1(\xi) \dots A_\tau(\xi) \neq 0.$$

Пусть $P = P(z_1, \dots, z_m) \in \mathbf{Z}_K^*[z_1, \dots, z_m]$ — многочлен степени $s > 1$ размера, не превосходящего H.

Тогда, если $P(\xi) = P(f_1(\xi), \dots, f_m(\xi)) \neq 0$, то существует постоянная σ такая, что

$$|P(\xi)| > CH^{-\frac{(2\varkappa_0)^m (m+1)^l (l+1)}{l!} d^{l+1} s^l},$$

$$C = \begin{cases} 1, & \text{если } \rho < 1, \\ (\exp\exp(\sigma s^{4l} \ln(s+1)))^{-1}, & \text{если } \rho \geq 1, \end{cases}$$

$$\rho = \sigma s^{4l} \ln(s+1) (\ln\ln(H+2))^{-1}.$$

При некоторых дополнительных условиях постоянная σ может быть сделана эффективной.

Литература

1. Шидловский А. Б. Трансцендентные числа. — М: Наука, 1987. — 447 с.

УДК 537.874.35

Головков А.А. (Воронеж)

Синтез комплексированных радиоэлектронных устройств для передачи и защиты информации

В данном докладе излагается методика синтеза комплексированных радиоэлектронных устройств на элементах с сосредоточенными неуправляемыми параметрами (L, C, R) и управляемых полупроводниковых элементах, которые могут быть одновременно использованны для передачи и защиты информации. Методика состоит в замещении схемы такого устройства двумя каскадно соединенными четырехполюсниками, каждый из которых нагружен на иммитанс управляемого элемента, представлении входного иммитанса каждого четырехполюсника в виде дробно-линейного преобразования известного иммитанса управляемого элемента, составлении системы нелинейных алгебраических уравнений, вытекающих из требований к значениям (отношениям) амплитуд и (или) фаз отраженного сигнала в различных состояниях РЭУ, определяемых уровнями управляющего воздействия на управляемом элементе, и решении этой системы относительно выбранных параметров неуправляемых элементов.

Дается техническое обоснование возможности передачи и защиты информации путем модуляции амплитуды и (или) фазы несущего сигнала по закону, соответствующему закону изменения информационного сигнала, источник которого поключен к одному из управляемых элементов, и кодирования промодулированного сигнала посредством дополнительной модуляции амплитуды и (или) фазы по закону, соответствующему закону изменения кодирующего сигнала, источник которого подключен ко второму управляемому элементу [1].

Приводятся результаты лабораторных и натурных испытаний, подтверждающие возможность обеспечения описанных выше и обратных им операций (декодирования и демодуляции) с помощью таких же комплексированных радиоэлектронных устройств в дециметровом диапазоне частот.

ЛИТЕРАТУРА

1. Головков А.А. Синтез многочастотных амплитудных и фазовых манипуляторов отраженного сигнала на элементах с сосредоточенными параметрами. Радиоэлектроника. Изв. ВУЗов, №11, 1991, с. 22...28.

УДК 517.51

Горлов С.К. (Воронеж)

О РЯДАХ С ПОЛОЖИТЕЛЬНЫМИ ЧАСТНЫМИ СУММАМИ ПО СИСТЕМЕ УОЛША

В 50-х годах была поставлена следующая проблема: является ли тригонометрический ряд с неотрицательными частными суммами рядом Фурье? Отрицательный ответ на этот вопрос дал Кацнельсон [1], построив нуль-ряд (но не ряд Фурье), все частные суммы которого неотрицательны. Подобный результат для системы Уолша-Пэли был получен Шиппом [2] и усилен Овсепяном [3] для любых перестановок системы Уолша.

В работе Юдина [4] показано, что тригонометрический ряд с неотрицательными частными суммами при определенном теоретико-числовом ограничении на спектр является рядом Фурье для функции из L_2. В настоящей работе этот результат переносится на ряды по системе Уолша. В частности, для лакунарных рядов Уолша (например, рядов Радемахера) достаточно просто доказывается, что неотрицательность частных сумм гарантирует сходимость ряда к функции из L_2. Это утверждение является более слабым по сравнению с аналогом теоремы Сидона-Зигмунда [5].

Список литературы

1. Katznelson Y. Trigonometric series with positive partial sums //Bull. Amer. Math. Soc. 1965. V. 71. P. 718-719.
2. Shipp F. Über Walsh-Fourierreihen mit nichtnegativen Partialsummen//Ann. Univ. scient. budapest. Sec. math. 1969. V. 12. P. 43-48.
3. Овсепян Р.И. О представлении функций ортогональными рядами// Айкакан ССР Гитутюннери Академиа. Зейкуцнер, Докл. АН АрмССР. 1973. Т. 57, N 1. С. 3-8.
4. Юдин В.А. О тригонометрических рядах с положительными частными суммами//Математические заметки. 1993. Т. 53. вып.3. С.149-152.
5. Голубов Б.И., Ефимов А.В., Скворцов В.А. Ряды и преобразования Уолша: Теория и применения. М.: Наука. 1987.

Regular two-graphs from the even unimodular lattice $E_8 \oplus E_8$

Viatcheslav Grishukhin
CEMI RAN, Moscow, Russia

Each two-graph is in one-to-one correspondence with a set of equiangular lines. This implies that a two-graph is represented by a system of vectors of equal odd norm with mutual inner products ± 1. A construction [1], [2] of two-graphs from doubly even lattices is applied to the even unimodular lattice $E_8 \oplus E_8$ multiplied by $\sqrt{2}$. The construction gives a family of regular two-graphs on 36 points. Many such two-graphs are described in [3]. The system of vectors represented a two-graph generates a sublattice of the lattice $E_8 \oplus E_8$. These sublattices are distinguished by sets of lattice vectors of norm 2. These sets are root systems. Hence the set of all two-graphs from $E_8 \oplus E_8$ is partitioned into families of two-graphs with the same root system. There are 7 families with the following root systems: $\emptyset$, A_1^7, $A_2A_3^3$, A_6A_7, A_1^9, $A_1A_3D_4D_6$, D_7E_7. Two-graphs with the first 4 root systems relate to 23 Steiner triple systems with a head. We do not consider here the hard problem on a number of isomorphism classes of two-graphs in this family, but show that root systems related to two-graphs make possible to distinguish nonisomorphic two-graphs.

References

[1] M.Deza, V.P.Grishukhin. *L-polytopes and equiangular lines*. Discrete Appl. Math 56 (1995) 181-214.

[2] M.Deza, V.P.Grishukhin, *Odd systems of vectors and related lattices*. Rapport de Recherche du LIENS **LIENS-94-5**, 1994. 15pp.

[3] J.J.Seidel, *More about two-graphs*. Fourth Czechoslovakian symposium on Combinatorics. Graphs and Complexity (eds. J.Nešetřil and M.Fiedler) 1992. Elsevier Science Publisher B.V., 287-308.

УДК 511.3

Пузов Л. И. (Саратов)

ОБОБЩЕННЫЕ СУММЫ КЛОСТЕРМАНА

Пусть p – нечетное простое, U_p – группа p-адических единиц; a, b, c – p-адические единицы, l, m, n, α – натуральные, $\alpha \geq 2$, $K = U_p \times U_p$,

$$SK\left(\begin{pmatrix} l & m & n \\ a & b & c \end{pmatrix}; p^\alpha\right) = \sum_{\langle x_\alpha, y_\alpha, z_\alpha \rangle \bmod p^\alpha}^{*} \exp\left(\frac{2\pi i}{p^\alpha}(ax_\alpha^l + by_\alpha^m + cz_\alpha^n)\right),$$

где суммирование проводится по всем наборам $\langle x_\alpha, y_\alpha, z_\alpha \rangle$ таким, что $x_\alpha y_\alpha z_\alpha \equiv 1 (\bmod p^\alpha)$ и $x_\alpha, y_\alpha, z_\alpha \in U_p$.

Теорема. Пусть $\operatorname{ord}_p(lmn(lm + ln + mn)) = 0$ и $R(x,y) = ax^l + by^m + c(xy)^{-n}$. Тогда, в случае разрешимости системы сравнений

$$\frac{\partial R}{\partial x}(x,y) \equiv 0 (\bmod p^\alpha), \quad \frac{\partial R}{\partial x}(x,y) \equiv 0 (\bmod p^\alpha), \quad ((x,y) \in K),$$

в компакте $K_0 = (x_0 + p\mathcal{O}_p) \times (y_0 + p\mathcal{O}_p)$, где (x_0, y_0) произвольное решение системы сравнений

1) существует и притом единственная стационарная точка $\bar{\theta} = (\theta_1, \theta_2) \in K_0$;

2) существует изометрическая эквивалентность ряда Тейлора $T_{\bar{\theta}} R$ функции $R(x,y)$ в точке $\bar{\theta}$ и его второго дифференциала (с точностью до слагаемого $R(\bar{\theta})$):

$$T_{\bar{\theta}} R \simeq R(\bar{\theta}) + d^{[2]}_{\bar{\theta}} R;$$

3) $$SK\left(\begin{pmatrix} l & m & n \\ a & b & c \end{pmatrix}; p^\alpha\right) = \sum_{\nu=1}^{r} \left(\frac{\det(d^{[2]}_{\bar{\theta}_\nu} R)}{p}\right)^\alpha i^{2\left(\frac{p^\alpha - 1}{2}\right)^2} p^\alpha \exp\left(\frac{2\pi i}{p^\alpha} R(\bar{\theta}_\nu)\right),$$

где $\bar{\theta}_\nu = (\theta_{1\nu}, \theta_{2\nu})$ пробегает все стационарные точки функции $R(x,y)$, принадлежащие компакту K.

В противном случае сумма Клостермана равна нулю.

УДК 5II.6

Данилов А.Н. (Череповец)

ИЗОМОРФИЗМ АЛГЕБР КВАТЕРНИОНОВ

Пусть F – поле характеристики $\neq 2$, f – невырожденная тернарная квадратичная форма над F, $\bar{f}$ – алгебраически взаимная с f форма, N_f – норменная форма, $\mathcal{A}_f$ – алгебра обобщенных кватернионов, отвечающая "базисной" форме f [2,3]. Пусть далее $\mathcal{O}_f$ – кольцо целых кватернионов алгебры $\mathcal{A}_f$ над полем Q, где f – целая положительная квадратичная форма [I].

Т е о р е м а I. Алгебры $\mathcal{A}_{f_1}$ и $\mathcal{A}_{f_2}$ над полем F изоморфны тогда и только тогда, когда выполняется любое из трех условий:

а) формы $\bar{f}_1$ и $\bar{f}_2$ эквивалентны над F;

б) норменные формы N_{f_1} и N_{f_2} эквивалентны над F;

в) базисные формы f_1 и f_2 кратно эквивалентны над F.

Т е о р е м а 2. Все изотропные алгебры $\mathcal{A}_f$ над полем F изоморфны. Они изоморфны алгебре $\mathcal{A}_{f_0}$, где $f_0 = x_1^2 + x_2^2 - x_3^2$, и полной алгебре матриц $M_2(F)$ второго порядка над F. Если $\mathcal{A}_f$ – изотропная алгебра, то формы f и $\bar{f}$ изотропны.

Т е о р е м а 3. Пусть $X = SY$, $S = (\gamma_{\mu\nu})$, – целочисленное унимодулярное преобразование переменных, переводящее целую положительную квадратичную форму f_1 в квадратичную форму f_2.

Тогда отображение φ:

$$1 \longrightarrow 1,$$

$$j_\nu \longrightarrow \bar{\gamma}_{1\nu} i_1 + \bar{\gamma}_{2\nu} i_2 + \bar{\gamma}_{3\nu} i_3 \quad (\nu = 1,2,3),$$

где $\bar{S} = (\bar{\gamma}_{\nu\mu})$ – матрица, присоединенная к S, есть изоморфизм алгебр $\mathcal{A}_{f_1} = [1, i_1, i_2, i_3]$ и $\mathcal{A}_{f_2} = [1, j_1, j_2, j_3]$ над Q и изоморфизм колец целых кватернионов $\mathcal{O}_{f_1}$ и $\mathcal{O}_{f_2}$. Этот изоморфизм сохраняет отношение делимости и норму кватерниона.

Лит.: [I] Белова Н.Н., Данилов А.Н. Алгебра и арифметика кватернионов / Череповец. гос. пед. ин-т. – Череповец, I99I. – I0Ic. – Деп. в ВИНИТИ 02.04.92, № II23 – В92. [2] Данилов А.Н. Алгебра кватернионов над полем характеристики $\neq 2$/Череповец. гос. пед. ин-т. – Череповец, I986. – 22с. – Деп. в ВИНИТИ 09.I2.86, № 8369 – В86. [3] Данилов А.Н. Алгебра кватернионов над полем характеристики $\neq 2$.II / Череповец. гос. пед. ин-т. – Череповец, I987. – 25с. – Деп. в ВИНИТИ 03.03.88, № I739 – В88.

УДК 511.6

Данилов А.Н. (Череповец)

О СИСТЕМЕ ДИВИЗОРОВ ПОЛЯ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

Свойства системы дивизоров поля K алгебраических чисел выводятся из ее определения с помощью системы аксиом Гекке [1,2].

Рассмотрены классы дивизоров и группа классов дивизоров по умножению, описан вид дивизоров поля K (через представители базисных классов дивизоров). Введены понятия дивизоров, сопряженных с данным дивизором, и сопряженных систем дивизоров, норма дивизора, классы вычетов $mod\,m$ (m – идеал поля K). Рассмотрены группа классов вычетов $mod\,m$, взаимно простых с m, и группа классов вычетов $mod\,m$ в узком смысле.

Доказаны, в частности, следующие утверждения.

Т е о р е м а 1. Пусть $\mathfrak{b}_i, h_i$ $(i=1,\dots,m)$ – соответственно представители и порядки базисных классов группы классов дивизоров поля K ($h_1 \dots h_m = h$, h – число классов идеалов поля K); $K' = K(\mathfrak{b}_1,\dots,\mathfrak{b}_m)$. Пусть далее поле K содержит все корни четвертой степени из -4 и все корни p – й степени из 1, где p – произвольный простой делитель h. Тогда, если $h_1,\dots,h_m$ попарно взаимно просты, то $[K':K]=h$.

Т е о р е м а 2. В каждом классе дивизоров поля K есть такие целые числа $\omega_1,\dots,\omega_n$, где $n=[K:\mathbb{Q}]$, что любое целое число этого класса единственным способом представимо в виде

$$x_1\omega_1 + \dots + x_n\omega_n \quad (x_i \in \mathbb{Z};\ i=1,\dots,n).$$

При этом

$$\left|det\|\omega_1,\dots,\omega_n\|\right| = |d|^{1/2},$$

где d – дискриминант поля K.

Лит.: [1] Данилов А.Н. Система дивизоров поля алгебраических чисел / Череповец. гос. пед. ин-т. – Череповец, 1995. – 41с. – Деп. в ВИНИТИ 13.04.95, № 1022 – В95. [2] *Hecke E. Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen // Math. Zeitschrift. – 1920. – Bd.6 – S.11–51.*

Bounds on the covering radius of a lattice

M. Deza
Ecole Normal Supérieure, Paris, France

V. Grishukhin
CEMI RAN, Moscow, Russia

This paper leans on results of Baranovskii [1], [2]. The covering radius $R(L)$ of a lattice L is the radius of smallest balls with centers in points of L which cover all the space spanned by L. $R(L)$ is tightly related to minimal vectors of classes of the quotient $\frac{1}{2}L/L$. The convex hull of all minimal vectors of a class Q is a Delaunay polytope $P(Q)$ of dimension $\leq n$,dimension of L. Let $\frac{1}{4}v^2_{max}$ ($\frac{1}{4}u^2_{max}$) be a maximal squared radius of $P(Q)$ of dimension n (of dimension less than n, respectively). If $\frac{1}{3}u^2_{max} \leq \frac{1}{4}v^2_{max}$, then $R^2(L) = \frac{1}{4}v^2_{max}$. This is a case of the well-known Barnes-Wall and Leech lattices. Otherwise, $\frac{1}{4}v^2_{max} \leq R^2(L) \leq \frac{1}{3}u^2_{max}$. This is a refinement of a result of Norton ([3], ch.22).

References

[1] E.P.Baranovskii, *Subdivision of Euclidean spaces into L-polytopes of certain perfect lattices*, Trudy Mat. Inst. Steklov. **196**(1991) 27–46 [=Steklov Inst. Math., **196**(1992)]

[2] E.P.Baranovskii, *The perfect lattices $\Gamma(A^n)$, and the covering density of $\Gamma(A^9)$*, Europ. J. Combinatorics, **15** (1994) 317–323.

[3] J.H.Conway, N.J.A.Sloane, *Sphere Packings, Lattices and Groups*, vol 290 of Grundlagen der mathematischen Wissenshaften Springer-Verlag, Berlin, 1987.

УДК 511.51

Демьяненко В.А. (Екатеринбург)

ОЦЕНКА КРУЧЕНИЯ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Пусть K – алгебраическое числовое поле степени n относительно поля рациональных чисел Q, $\mathcal{F}$ и $\mathcal{G}$ – соответственно кривые $y^2=x^3+rx+s$ и $v^2=u^4+au^2+b$, определённые над K, r, s, a, b – целые, $4r^3+27s^2=\mathcal{D}$, $b^2(a^2-4b)=d$, $\mathcal{D}d\neq 0$.

Пусть, далее, φ – функция Эйлера, p – простое и l – произвольное целое рациональное числа, $\varepsilon(p^l)=e^{2\pi i/p^l}$, $\mathcal{O}_{p^t}$, и $\mathcal{O}'_{p^t}$ (t – натуральное) – примитивные точки порядка p^t на кривых $\mathcal{F}$ и $\mathcal{G}$.

Теорема 1. Если $\mathcal{O}_{p^t}\in K(\varepsilon(p^l))$, то $\varphi(p^t)\le 6n$.

Теорема 2. Если $\mathcal{O}'_{p^t}\in K(\varepsilon(p^l))$, то $\varphi(p^t)\le 4n$.

Из теоремы 1 следует, в частности, ответ на вопрос, поставленный И.Р.Шафаревичем [1, с.86], и результат Мазура по кручению эллиптических кривых над полем Q [2].

Лит.: 1. Демьяненко В.А. О равномерной ограниченности кручения эллиптических кривых над алгебраическими числовыми полями // Тр. МИАН. 1973. Т.132. С.82-87. 2. Mazur B. Rational points on modular curves // Lect. Notes Math. 1977. V.601. P.107-148.

УДК: 621.396.2.018.424

к.т.н.,с.н.с.Денисов В.И. (Воронеж)
Обухов А.Н. (Воронеж)

АЛГОРИТМИЧЕСКИЙ СПОСОБ ОБЕСПЕЧЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ В СИСТЕМАХ ПЕРЕДАЧИ С ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТРОЙКОЙ РАБОЧИХ ЧАСТОТ

Одним из известных способов защиты информации при ее передаче по радиоканалу является режим псевдослучайной перестройки рабочей частоты (ППРЧ) в соответствии с последовательностью номиналов частот (ПНЧ) $\{f_i\}_{i=1}^{\infty}$, которая стороннему наблюдателю неизвестна априори. Типовая структура алгоритма **A**, порождающего такую последовательность, имеет следующий вид: $\mathbf{A} = A_1 \circ A_2 \circ A_3 \circ A_4$, где A_4-алгоритм формирования двоичной псевдослучайной последовательности (ДПСП); A_3-комбинационно-числовое преобразование (КЧП) ДПСП в многоуровневую числовую последовательность (МЧП) с параметрами выборки (m) и смещения (c) вида $r_i = \sum_{k=0}^{m-1} 2^k x_{[c(i-1)+m-k]}$; A_2 -правило перенумерации членов МЧП, задаваемое транзективной переменной ключа; A_1 - правило соответствия членов последовательности номеров частотных каналов (ПНК) и ПНЧ.

С целью преодоления такой меры защиты сторонний наблюдатель сталкивается с необходимостью построения эквивалентного алгоритма $\tilde{\mathbf{A}}$, порождающего ПНЧ $\{\tilde{f}_i\}_{i=1}^{\infty}$, такую, что $\tilde{f}_i = f_i$ при $i \leq N$, где N достаточно большое число.

Предлагаемый способ решения этой задачи включает следующую последовательность действий:

использование произвольного соответствия членов ПНК и ПНЧ - $\tilde{A}_1$;

использование разработанных методов направленного перебора, основанных на корреляционных свойствах комбинационных МЧП (метод "хвостов") или структурных свойствах матрицы смежности (МС) наблюдаемой ПНЧ (матричный метод), для построения правила $\tilde{A}_2$;

определение параметров $m=\log_2 K$ и $c=\log_2 E$, где K-объем используемой адресной группы частот (АГЧ), E- количество единиц в строках МС, для построения КЧП $\tilde{A}_3$;

использование алгоритма Берлекэмпа-Месси (или его модификаций) для построения алгоритма $\tilde{A}_4$.

При исследовании алгоритмов **A**, основанных на использовании ДПСП, имеющих невысокую линейную степень, и скользящего режима КЧП ($c<m$), разработанный способ показал положительные результаты. Например, при использовании матричного метода построения $\tilde{A}_2$ применительно к системам с объемом АГЧ 32 частоты трудоемкость вычислений снижается на 25-35 порядков (в зависимости от соотношения параметров m и c) по сравнению с методом полного перебора, что по оценкам позволит снизить общие временные затраты до единиц - десятков секунд (в зависимости от характеристик технических средств наблюдателя).

Добровольский Н.М., Ванькова В.С.(Тула.)

Об отклонении q-регулярных сеток

В работе [1] были введены понятия р-ичных сеток I и II рода и определены группы преобразований G - арифметических сдвигов и G^* - поразрядных сдвигов классов этих сеток.

Для q - регулярных р - ичных сеток в работе [2] были получены оценки среднего арифметического квадратичного отклонения по орбитам указанных групп преобразований.

Через $D_{s+1}(X(\vec{t}))$ и $D_{s+1}(CX(\vec{t}))$ обозначим отклонения образов сетки X под действием преобразований $g(\vec{t})\in G$ и $g^*(\vec{t}) \in G^*$, соответственно.

Теорема. Для любой q - регулярной р-ичной сетки X справедливы оценки отклонения

$$D_{s+1}(X(\vec{t})) = O\ (\ln^{s} N)$$

$$D_{s+1}(CX(\vec{t})) = O\ (\ln^{s} N)$$

Литература.

1. Ванькова В.С., Добровольский Н.М., Есаян А.Р. О преобразованиях многомерных сеток." Деп. ВИНИТИ. N 447 - 91

2. Ванькова В.С. О квадратичном отклонении q-регулярных р- ичных сеток. Тезисы докладов международной конференции " Современные проблемы теории чисел". Россия, Тула, 20 сентября-25 сентября 1993 года.

511.9

Добровольский Н.М., Рощеня А.Л. (Тула)

О ЧИСЛЕ ТОЧЕК РЕШЕТКИ В ГИПЕРБОЛИЧЕСКОМ КРЕСТЕ

Пусть $s \geqslant 2$ и Λ - полная решетка в R^s. Рассмотрим гиперболический крест $K(T) = \{ \vec{x} \mid \bar{x}_1 \dots \bar{x}_s < T \}$, где $\bar{x} = \max(1, |x|)$. Обозначим через $D(T|\Lambda)$ - количество точек решетки в гиперболическом кресте $K(T)$.

Теорема. Для любой полной решетки Λ справедлива асимптотическая формула

$$D(T|\Lambda) = \frac{2^s T \ln^{s-1} T}{(s-1)!\det\Lambda} + O(T \ln^{s-2} T). \qquad (1)$$

Следствие. Для $\alpha = \delta + it$, при $\delta > 1$ для гиперболической дзета-функции полной решетки Λ справедливо интегральное представление

$$\zeta_H(\alpha|\Lambda) = \sum'_{\vec{x}\in\Lambda} (\bar{x}_1 \dots \bar{x}_s)^{-\alpha} = (\alpha+1) \int_{q(\Lambda)}^{\infty} \frac{D(x|\Lambda)}{x^{\alpha+1}}, \qquad (2)$$

где $q(\Lambda) = \min_{\vec{x}\in\Lambda\setminus\{\vec{0}\}} \bar{x}_1 \dots \bar{x}_s$.

Как известно, для $\Lambda = Z^s$ существует полином $P_{s-1}(x)$ степени $s-1$ такой, что

$$D(T|Z^s) = TP_{s-1}(T) + o(T).$$

Интересно выяснить, имеет ли место аналогичный результат для произвольной полной решетки.

Литература

1. Титчмарш. Теория дзета-функции Римана. М., 1953

УДК 511.9

Домбровский И.Р. (Минск)

О ПРЕДСТАВЛЕНИИ ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ U_n -ЧИСЛАМИ

Число $a \in \mathbb{R}$ называется U_n – числом, если неравенство

$$0 < |P(a)| < H_P^{-w}$$

имеет при любом w бесконечное число решений в полиномах $P(x) \in \mathbb{Z}[x]$, $\deg P \le n$, $H(P) = H_P$, однако, для любого $k < n$ существует w_k, что

$$|Q(a)| > H_Q^{-w_k},$$

для всех $Q(x) \in \mathbb{Z}[x]$, $\deg Q \le k$, $H(Q) = H_Q$.

Известные числа Лиувилля являются U_1 числами.

В 1962 г. П. Эрдеш опубликовал работу [1], в которой доказал возможность представления любого действительного числа в виде как суммы, так и произведения двух чисел Лиувилля. Развитие данной работы на случай U_2 чисел проведено К. Алнячиком [2].

Предлагаемый в данных тезисах результат обобщает упомянутые выше в двух направлениях :
во-первых, любое действительное a представимо в виде

$$a = f(u_1, u_2),$$

где f принадлежит довольно широкому классу алгебраических кривых (например, $f(x,y) = x^p + y^q$, $p,q \in \mathbb{N}$),
во-вторых, для произвольного $n \in \mathbb{N}$, u_1 и u_2 являются U_n -числами.

1. Erdös P. – Michigan Math. J.,1962, Vol. 9, p. 59-60.
2. Alnjacik K. – Acta Arith., 1990, Vol. 55, N4, p.301-310.

УДК 511

Дубицкас А. (Вильнюс)

О РАЗМЕРЕ ВПОЛНЕ ВЕЩЕСТВЕННЫХ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

Пусть α–целое алгебраическое число, n – его степень и $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ его сопряжённые. Через $\overline{|\alpha|} = \max_{1\leqslant i\leqslant n} |\alpha_i|$ и $M(\alpha) = \prod_{1\leqslant i\leqslant n} \max(1, |\alpha_i|)$ обозначим соответственно размер и меру Малера этого алгебраического числа.

По теореме Кронекера, если α не корень из единицы, то $\overline{|\alpha|} > 1$ и, следовательно, $M(\alpha) > 1$. Если α – вполне вещественное (т.е. все $\alpha_i \in \mathbb{R}$) и не имеет вида $2\cos(\pi r)$, $r \in \mathbf{Q}$, то $\overline{|\alpha|} > 2$. Таким образом существуют такие положительные функции $c_1(n)$, $c_2(n)$, $c_3(n)$ что для целого алгебраического числа α степени n

1.) $M(\alpha) = 1$ или $M(\alpha) \geqslant 1 + c_1(n)$;

2.) $\overline{|\alpha|} = 1$ или $\overline{|\alpha|} \geqslant 1 + c_2(n)$;

3.) в случае вполне вещественного алгебраического числа не имеющего вида $2\cos(\pi r)$, $r \in \mathbf{Q}$, $\overline{|\alpha|} \geqslant 2 + c_3(n)$.

Задача о нахождении точного вида функции c_1 известна под названием "вопрос Лемера" [1], а функций c_2, c_3 – "гипотеза Шинцеля-Цассенхауза" [2]. В настоящее время обе эти проблемы остаются открытыми, а наиболее сильная оценка c_1 при $n > n_0$ принадлежит Лубутену [3] и c_2 при $n > n_0$ автору [4]. Для c_3 имеет место следующая оценка:

Теорема. Пусть α – целое вполне вещественное алгебраическое число степени n и $\alpha = 2\cos(\pi r)$, $r \in \mathbf{Q}$. Тогда для любого $\epsilon > 0$ существует такое эффективное $n_0(\epsilon)$, что при $n > n_0$

$$\overline{|\alpha|} > 2 + \left(\frac{81k}{32\pi} - \epsilon\right)\frac{(\log\log n)^6}{n(\log n)^2},$$

где $k = \sum_{m\geqslant 0}(-1)^m/(2m-1)^2 = 0.916\ldots$ постоянная Каталана.

ЛИТЕРАТУРА

1. D.H.Lehmer. Factorization of certain cyclotomic functions, *Ann. of Math.* **34**(1933), 461–479.
2. A.Schinzel and H.Zassenhaus. A refinement of two theorems of Kronecker. *Michigan Math. J.* **12**(1965), 81–85.
3. R.Louboutin. Sur la mesure de Mahler d'un nombre algébrique, *C.R.Acad. Sci. Paris* **296**(1983), 707–708.
4. A.Dubickas, On a conjecture of A.Schinzel and H.Zassenhaus, *Acta Arith.* **63**(1993), 15–20.

Дубовицкий А.Я. (Черноголовка)

СРАВНЕНИЕ ИНФОРМАТИВНОСТИ s И v ВАРИАЦИИ

Принцип максимума (ПМ) возникает как эквивалент стационарности экстремали x^0,u^0 в выбранном классе недокальных вариаций. Для задач со смешанными ограничениями выделены, в сущности, лишь два таких класса: s и v вариации. Класс v богаче, но предполагает гладкость по t ограничений равенства тогда, как s вариации требуют лишь их непрерывности. s ПМ (ПМ, отвечающий s вариациям) оптимали w^0 содержит условия: а. Сопряженная функция ψ_x имеет ограниченное изменение на Δ. б. функция Понтрягина $H[u,t]=\psi_x f(x^0,u,t)$ достигает max на множестве V[t] допустимых значений управления при всех t из Δ. в. $M(t)=\psi_x f(x^0,u^0,t)$ п.в. на Δ, где $M(t)=\max\limits_{V[t]} H[u,t]$.

Сравнительно с s ПМ v ПМ содержит два дополнительных условия: г. $\psi_t(t)=-M(t)$ имеет ограниченное изменение на Δ. д. ψ_t удовлетворяет сопряженному уравнению. v ПМ даже формально более сильное условие экстремума чем s ПМ. В классической задаче оптимального управления г.,д. выполняются для любого s ПМ экстремали w^0 и, поэтому, s ПМ ~ v ПМ. Как показано в [1] для нерегулярных задач это не так. Бытовала гипотеза, что в общем случае регулярной задачи s ПМ ~ v ПМ. Однако, как показали наши совместные с А.А.Милютиным исследования, дело обстоит сложнее. Оказывается в регулярных задачах условие г. выполняется для любого s ПМ. В то же время существует пример регулярной задачи, не удовлетворяющей условию независимости смешанных ограничений, которая обладает континуумом бесконечно гладких s экстремалей, не являющихся v экстремалями.

Теорема 1. В задачах с независимыми смешанными ограничениями s ПМ ~ v ПМ. (Результат новый уже для задач с фазовыми ограничениями.)

Теорема 2. Для счетно липшицевой экстремали w^0 регулярной задачи, не содержащей Понтрягинского ограничения, s ПМ ~ v ПМ .

В условиях теоремы 2. существует пример задачи, обладающей s экстремалью, не удовлетворяющей никакому v ПМ.

1 А.Я.Дубовицкий, А.А.Милютин Теория принципа максимума "Наука" 1981 ЦЭМИ Методы теории экстремума в экономике.

УСТОЙЧИВОСТЬ ОБОБЩЕННЫХ ПОЛОЖИТЕЛЬНЫХ РЕШЕНИЙ ИНТЕГРАЛЬНЫХ УРАВНЕНИЙ ПЕРВОГО РОДА

В.А.Дубовицкий (Москва)

Рассматривается экстремальная задача

$$J(\mu) = \| \int_Y a(y)d\mu(y) - z \| \to \min, \quad \mu \in M(Y) \qquad (1)$$

Здесь Y метрический компакт, $a: Y \to Z$ непрерывное отображение из Y в гильбертово пространство Z, z есть вектор Z, M(Y) совокупность неотрицательных мер Радона на Y. Минимум в (1) называется оптимальным интегральным представлением (ОИП) вектора z на компакте Y с ядром a. Если ядро $a(y)$ отделено от 0, т.е. $0 \notin \mathrm{co}\, a(Y)$, то существует непустое слабо компактное выпуклое множество $D(a,z)$ решений (1) и возникает вопрос о его устойчивости относительно возмущений a,z. Актуальность этой проблемы обусловлена тем, что ОИП является формализацией понятия неотрицательного обобщенного решения линейного интегрального уравнения первого рода. Эта формализация в естественном смысле снимает проблему некорректности этих уравнений. Наиболее общий результат об устойчивости выражается следующей теоремой.

Теорема. Пусть $a_n \to a_0$ равномерно и $z_n \to z_0$ слабо в Z. Тогда $D(a_n, z_n) \to D(a_0, z_0)$.

Сходимость множеств $D(a,z)$ понимается в смысле сходимости компактов. Аналитически типичная структура минимума (1) и устойчивость ОИП описывается в терминах функционала уклонения графиков (гистограмм) мер. Эти результаты составляют теоретическую базу приложений, использующих восстановление неотрицательных обобщенных решений интегральных уравнений первого рода. Численное решение (1) сводится к минимизации квадратичного функционала высокой размерности на конусе неотрицательных векторов. Как показала наша практика, редукция интегральных уравнений к ОИП (метод гистограмм) является эффективным средством решения обратных задач спектроскопии. Уникальной особенностью ОИП является их нечувствительность к белому шуму в "экспериментальном" векторе z и непрерывная зависимость ошибки восстановления от систематической ошибки математической модели, т.е. нормы уклонений a,z. Для сильно некорректных обратных задач, метод гистограмм служит альтернативой традиционной технике регуляризации.

УДК 511.3

Евликов В.В. /Владимир/

ОЦЕНКА ОСТАТКА В ЗАДАЧЕ ЭРДЕША

В 1946 г. П.Эрдеш [1] высказал предположение о существовании предельного закона $F_\beta(u)$ для последовательности функций распределения /п.ф.р./ с аддитивной функцией $g_\beta(n)$: $g_\beta(p^l)=\log^\beta p^l$, где $\beta>0$ и $\beta\neq1$, т.е. что существует $F_\beta(u)$ такая, что

$$\frac{1}{x}\sum_{n\le x,\ g_\beta(n)\le u\log^\beta x} 1 \to F_\beta(u) \quad \text{при } x\to\infty$$

в каждой точке непрерывности $F_\beta(u)$. Им было показано, что $F_\beta(u)$ не может быть тривиальным [1]. В работах Левина Б.В. и Тимофеева Н.М. [2], в случае $\beta>1$, П.Эрдеша и П.Эллиотта [3] в случае $0<\beta<1$, было доказано, что предельный закон $F_\beta(u)$ не является безгранично делимым. В работе [4] автором с помощью метода урезания аддитивной функции была найдена оценка отклонения от предельного закона $F_\beta(u)$ порядка $(\log x)^{\frac{\theta}{1+\beta}}$, где $\theta=\min\{1,\beta\}$. С использованием не усовершенствованной аналитической техники Халоса [5] удалось получить скорость сходимости п.ф.р. к предельной функции $F_\beta(u)$ порядка $\log^{-\Delta} x$, где $\Delta=\min\{\frac{1}{2},\beta\}$.

[1] P.Erdös On the distribution function of additive functions. // Ann. of Math. – 1946. – v.47. – N 2. – S. 1-20.

[2] Левин Б.В. Тимофеев Н.М. Распределение значений аддитивных функций //Успехи мат. наук.–1973.– т.28. №1/169/.– с.243-244.

[3] P.D.T.A.Elliott P.Erdös The tails of infinitelly divisible laws and problem in number theory. // J. of Number Theory. – 1978. – v.11. – S. 542-551.

[4] Евликов В.В. Новый вид урезания аддитивных функций //Литовский мат.сборник.–1981.– №.4.– с.211-213.

[5] Halasz G. Über die Mittelwerte multiplikativer zahlen theoretischer Funktionen. // Acta Math. Acad. Sci. Hungar. – 1968. – B.19. – S. 365-404.

УДК 511

О НЕКОТОРЫХ НЕОПРЕДЕЛЕННЫХ УРАВНЕНИЯХ

Г.В.Евстратов

В докладе исследуются различные методы и подходы к решению широкого класса диофантовых уравнений в целых числах.

Например, до сих пор неизвестен алгоритм, распознающий по данному целому a, имеет ли система уравнений (см. / I /, стр. I54)

$$\left.\begin{aligned} z^2 + av^2 &= x^2 \\ z^2 - av^2 &= y^2 \end{aligned}\right\} \qquad (I)$$

целочисленные решения или нет. Такая задача для $a=1$ была поставлена еще Леонардо Пизанским по прозвищу Фибоначчи около I220 г.

Алгоритм для решения системы (I) определяется следующей теоремой.

Теорема I. Пусть Ω - есть множество натуральных чисел определяемых отношением $|f(m,n)|/v^2$, где $f(m,n)$ - многочлен, а m,n,v - любые целые рациональные числа. Тогда система(I) имеет целочисленные решения только при тех целых a, которые принадлежат множеству Ω, т.е. если $a\in\Omega$. При этом многочлен $f(m,n)$ и соответствующее решение системы (I) находятся по формулам

$$\begin{cases} f(m,n) = 4mn(2m^2+n^2-3mn); \\ x = n^2-2m^2; \\ y = 4mn-2m^2-n^2; \\ z = 2mn-2m^2-n^2. \end{cases}$$

Нижеприведенная теорема 2 опровергает теорему, доказанную

Дж.Касселсом (см. / 2 /, с. 328), где утверждается, что уравнение

$$x^2 - y^2 + z^2 = N$$

имеет конечное число решений в целых числах.

Теорема 2. Пусть N - целое рациональное число и пусть f - целая форма, которая эквивалентна над областью целых рациональных чисел R форме $x^2 - y^2 + F(z_i)$, где $F(z_i) = F(z_1, \ldots, z_n)$ - любая целочисленная функция от $n \geq 1$ переменных. Тогда целых представлений B числа N формой f будет конечное число или бесконечное в зависимости от того, конечную или бесконечную последовательность целых чисел вида $4m$ и /или/ $2k+1$ образует $N - F(z_i)$ при изменении переменных z_i, при этом все решения находятся по формуле:

1) если $N - F(z_i) = 4\omega\beta$, то

$$x = \omega + \beta; \quad y = \omega - \beta;$$

2) если $N - F(z_i) = (2\omega+1)(2\beta+1)$, то

$$x = \omega + \beta + 1; \quad y = \omega - \beta.$$

ЛИТЕРАТУРА

1. Давенпорт Г. Высшая арифметика. - М., Наука, 1965.

2. Дж. Касселс. Рациональные квадратические формы (перевод с английского) - М., Мир, 1982, 438 с.

Еровенко В.А. (Минск)

СУЩЕСТВЕННЫЕ СПЕКТРЫ ОБЫКНОВЕННЫХ ДИФФЕРЕНЦИАЛЬНЫХ ОПЕРАТОРОВ С ПОЧТИ ПОСТОЯННЫМИ КОЭФФИЦИЕНТАМИ В L^p

В математической литературе встречаются различные определения существенных спектров. В докладе обсуждается как, пользуясь первой и второй теоремами устойчивости для полуфредгольмовых операторов, можно получить явные формулы для вычисления наиболее известных существенных спектров дифференциальных операторов с почти постоянными коэффициентами, получаемых относительно малыми по норме или относительно компактными возмущениями обыкновенных дифференциальных операторов с постоянными коэффициентами или дифференциальных операторов Эйлера в соответствующих пространствах Лебега $L^p(a,\infty)$ для всех $1\le p\le\infty$.

В методе, использующем первую теорему устойчивости Като для полуфредгольмовых операторов, по-существу, реализуется идея метода расщепления, восходящая к И.М.Глазману, и состоящая в том, что для дифференциального оператора на полуоси $[a,\infty)$ можно пренебрегать поведением коэффициентов вне окрестностей бесконечно удаленной точки. При этом существенно используются полученные автором результаты об инвариантности существенных спектров относительно сдвига полуоси изменения переменной.

Для получения явных формул существенных спектров Голдберга $\sigma_{e1}(T)$, Като $\sigma_{e2}(T)$, Фредгольма $\sigma_{e3}(T)$, Вейля $\sigma_{e4}(T)$, Браудера $\sigma_{e5}(T)$ возмущенных операторов, где например,

$\sigma_{e2}(T):=\mathbb{C}\setminus\{\lambda\in\mathbb{C}: T-\lambda I$ - полуфредгольмов оператор$\}$,

$\sigma_{e4}(T):=\mathbb{C}\setminus\{\lambda\in\mathbb{C}: T-\lambda I$ - фредгольмов оператор индекса $0\}$,

используются результаты осущественных спектрах обыкновенных дифференциальных операторов, полученные в работах автора [I-3].

Отметим, что при использовании техники относительно компактных возмущений пришлось, вообще говоря, накладывать разные условия на коэффициенты возмущающего дифференциального оператора, различая случаи $p=1,\infty$ и $1<p<\infty$.

I. Еровенко В.А.// Докл. АН Беларуси. 1992. Т.36, №6.
2. Еровенко В.А.// Докл. АН Беларуси. 1994. Т.38, №I.
3. Еровенко В.А.// Докл. АН Беларуси. 1995. Т.39, №2.

УДК 511.19

Жанбырбаева У.Б., Тараненко Н.В. (Одесса)

АДДИТИВНАЯ ФУНКЦИЯ В СЕКТОРИАЛЬНОЙ ОБЛАСТИ

Зафиксируем целое гауссово число γ и определим для каждого $r = 0, 1, 2, \ldots$ аддитивную функцию следующими соотношениями:

$$\mathcal{A}_\gamma^{(r)}(p) = \begin{cases} k^r, & \text{если } \gamma^k \| (p+1), \\ 0, & \text{если } (\gamma, p+1) = 1, \end{cases} \qquad \mathcal{A}_\gamma^{(r)}(d) = \sum_{p^a \| d}^{*} a\, \mathcal{A}_\gamma^{(r)}(p).$$

(знак $*$ означает, что суммирование производится по неассоциированным числам). Эта функция является аналогом функций $\omega(d), \Omega(d)$ и на множестве натуральных чисел рассматривались в [1].

Положим

$$A_m^{(r)}(x; \varphi_1, \varphi_2) = \sum_{\substack{\mathcal{A}_\gamma^{(r)}(d) = m \\ N(d) \le x,\ \varphi_1 < \arg d \le \varphi_2}}^{*} 1, \qquad B_m^{(r)}(x, h; \varphi_1, \varphi_2) = \sum_{\substack{\mathcal{A}_\gamma^{(r)}(d) = m \\ x < N(d) \le x+h,\ \varphi_1 < \arg d \le \varphi_2}}^{*} 1$$

Нами доказаны теоремы о распределении значений функции $\mathcal{A}_\gamma^{(r)}(d)$. Приведем некоторые из них:

ТЕОРЕМА 1. Существует постоянная $a > 0$ такая, что при

$$\varphi_2 - \varphi_1 \ge \exp\left(-a\, \frac{(\log x)^{3/5}}{\log\log x}\right)$$

справедлива асимптотическая оценка (при $x \to \infty$):

$$\sum_{m=1}^{\infty} \left(\frac{A_m^{(r)}(x; \varphi_1, \varphi_2)}{x} - \frac{B_m^{(r)}(x, h; \varphi_1, \varphi_2)}{h} \right)^2 \ll (\varphi_2 - \varphi_1)^2 (\log x)^{-2} (\log\log x)^{-\frac{1}{2}},$$

если только $\begin{cases} x^{\frac{3}{12}+\varepsilon} \le h \le x & \text{, для } \varphi_2 - \varphi_1 \gg 1, \\ x^{\frac{2}{3}+\varepsilon} \le h \le x & \text{, в остальных случаях.} \end{cases}$

ТЕОРЕМА 2. Для каждого вещественного z

$$\frac{2}{\varphi_2 - \varphi_1} \cdot \frac{1}{h} \# \left\{ \lambda \in \mathbb{Z}[i] \;\middle|\; x < N(\lambda) \le x+h,\ \varphi_1 < \arg \lambda \le \varphi_2,\ \frac{\mathcal{A}_\gamma^{(r)}(\lambda) - c_1^{(r)} \log\log x}{z\,(c_2^{(r)} \log\log x)^{1/2}} \right\} \to \Phi(z) \qquad (\text{при } x \to \infty).$$

Литература

1. Wijsmuller M. The value distribution of an additive function // Ann. Univ. Sci. Bud. - T. XIV - 1994. - P. 279-291.

УДК 511

Жукова А.А. (Владимир)

РАСПРЕДЕЛЕНИЕ АРИФМЕТИЧЕСКИХ ФУНКЦИЙ ПО ПРОГРЕССИЯМ.

Пусть $f(n)$ - мультипликативная функция из рассмотренного в [1] класса $M_\alpha(D)$. Грубо говоря, это означает, что среднее значение $|f(n)|^t$ равно $O(\ln^\alpha x)$ и для $f(p)$ справедливы оценки типа теоремы Зигеля-Вальфиша.

В работе [1] доказано (см. теорему 4) что, если $f(p)\ln p$ хорошо распределена в среднем по прогрессиям модуля d, $d \le Q \le \sqrt{x}$, то и для $f(n)$ справедлива теорема типа А.И.Виноградова-Бомбьери.

Целью работы является получение подобных оценок, когда n пробегает числа, имеющие ровно k простых делителей, то есть будут найдены равномерные по k оценки следующей суммы:

$$\sum_{d\le Q}\max_{y\le x}\max_{(a,d)=1}\left|\sum_{n\le y,\,\Omega(n)=k,\,n\equiv a(\mathrm{mod}\,d)} f(n)-\frac{1}{\varphi(d)}\sum_{n\le y,\,\Omega(n)=k,\,(n,d)=1} f(n)\right|,$$

где $\Omega(n)$ - число простых делителей с учетом их кратности, $f(n)$ принадлежит классу $M_\alpha(D)$.

Литература

[1] Левин Б.В., Тимофеев Н.М. Распределение арифметических функций в среднем по прогрессиям (теоремы типа Виноградова-Бомбьери) // Математический сборник. 1984. Т. 125 (167) N 4 (12), С. 558-572.

УДК 511.9

Журавлев В.Г. (Владимир)

ПРЕДСТАВЛЕНИЕ ФОРМ РОДОМ КВАДРАТИЧНЫХ ФОРМ.

Весом представлений $n(A, F)$ формы A родом положительно определенных квадратичных форм F называется число всех решений $X \in M_{n,m}(Z)$, где $n = \dim Q$ и $m = \dim A$, матричных уравнений ${}^tXQX = A$, когда $\{Q\}$ пробегает все классы рода F и решения берутся с весом $|Aut\, Q|^{-1}$. С помощью масс-формулы Конвейя-Слоэна и техники дискриминантных форм В.В.Никулина доказана

Теорема. Если ступень a матрицы A бесквадратна и $m \leq n-2$, то

$$n(A, F) = std(A, Q) \prod_{p|2ad} \alpha_p(A, Q),$$

где $std(A, Q)$ - произведение ζ - функций Римана и L - функции Дирихле, зависящие от $n-m$, a и определителя d формы Q, а множители $\alpha_p(A, Q)$ определяются через p-адические инварианты форм A, Q и являются рациональными функциями от степеней $p^{i}(i = 1, ..., [(n-m)/2])$.

Как приложение приведем формулы числа решений двух диофантовых квадратичных систем, связанных с представлениями форм. Пусть $xy = x_1y_1 + ... + x_ny_n$, $|x| = xx$ и $a > 0$ - нечетное бесквадратное число. Тогда число решений системы уравнений

$$|x| = |y| = a,\ xy = 0\ (x,\ y \in \mathbf{Z}^4)$$

равно

$$r(a) = 3 \cdot 2^{\omega(a_+)+2} \cdot a_- \sigma(a_-),$$

где $\omega(a)$ - число простых p делителей $a = a_+ \cdot a_-$, любое $p|a_\pm$ удовлетворяет сравнению $p \equiv \pm 1 (mod\, 4)$ и $\sigma(a_-)$ - сумма делителей a_-.

Если $a_1,\ a_2 > 0$ - нечетные бесквадратные взаимно простые числа, то число решений системы уравнений

$$|x| = a_1,\ |y| = a_2,\ xy = 0\ (x,\ y \in \mathbf{Z}^5)$$

равно

$$r(a_1,\ a_2) = c \prod_{p|a_1} \left(p + \left(\frac{a_2}{p}\right)\right) \prod_{p|a_2} \left(p + \left(\frac{a_1}{p}\right)\right)$$

с коэффициентом $c = 80$, если a_1 или $a_2 \equiv 1 (mod\, 4)$, и $c = 240$ в противном случае.

УДК 511.34+519.67

Зенкин А.А. (Москва)

ОБОБЩЕННАЯ ПРОБЛЕМА ВАРИНГА: ОБ ОДНОМ НОВОМ СВОЙСТВЕ НАТУРАЛЬНЫХ ЧИСЕЛ.

Рассматривается задача о представлении натуральных чисел $n \geq 1$ суммами вида:

$$n = \sum_{i=1}^{s} n_i^r , \qquad (1)$$

где $r \geq 2$, $s \geq 1$ - целые, и основания степени подчинены условию:

$n_i \geq m$, $i = 1, 2, 3, ..., s$,

где $m \geq 0$ - произвольное фиксированное целое число.

Полное решение этой задачи дает следующая теорема [1].

ТЕОРЕМА 1. *При любых* $m \geq 0$, $r \geq 2$ *существуют:*

1) *конечное число слагаемых* $g(m, r)$ *и*

2) *конечное инвариантное множество* $Z(m, r)$

такие, что для всех $s \geq g(m, r)$

$N(m, r, s) = \{s \cdot m^r + z : z \in Z(m, r)\}$,

где, по определению, положено

$$N(m,r,s) = \{ n \geq s \cdot m^r + 1 : n \neq \sum_{i=1}^{s} n_i^r , \ n_i \geq m \},$$

$$Z(m,r) = \{n \geq 1 : n \neq \sum_{i=1}^{s} (n_i^r - m^r) \ \textit{для всех}\ s \geq 1, \ n_i \geq m \},$$

$$G(m,r) = \operatorname{Arg}\min_{s} \{ |N(m,r,s)| < \infty \},$$

$$g(m,r) = \operatorname{Arg}\min_{s} \{ |N(m,r,s)| = |Z(m,r)| \}.$$

Опираясь на эти результаты, можно доказать следующее общее утверждение об одном новом общем свойстве натуральных чисел.

ТЕОРЕМА 2. *При любых* $m \geq 1$, $r \geq 2$ *любое натуральное число*

$$n > g(m, r) \cdot m^r + \bar{z} , \quad \bar{z} = \max\{Z(m, r)\},$$

представимо *суммами* (1) *ОДНОВРЕМЕННО ПРИ ВСЕХ* s, $1 \leq s \leq [n/m^r]$, *ЗА ИСКЛЮЧЕНИЕМ тех значений* s, *при которых* $s \cdot m^r = n - z$, $z \in Z(m, r)$, *и, быть может, некоторых значений* $s < g(m,r)$.

Так, например, знаменитое число 169 есть сумма вида (1) при r=2, m=1 и ПРИ ВСЕХ s=1,2,3,....169, КРОМЕ $s = 169 - z$, $z \in Z(1, 2) = \{1, 2, 4, 5, 7, 10, 13\}$, где $Z(1, 2)$ - известное множество Г.Полла [3].

ЛИТЕРАТУРА. 1.А.А.Зенкин, Когнитивная компьютерная графика. - М.: Наука,1991. 2.А.А.Зенкин, Проблема Варинга для сумм биквадратов положительных целых чисел: $g(1,4) = 21$. - Математические заметки, т.54, вып.5, 45 -56 (1993). 3. G.Pall, On sums of squares. - Amer. Math. Monthly, vol. 40, 10-18 (1933).

УДК 511.9+519.67

Зенкин А.А. (Москва)

"О ДОКАЗАТЕЛЬСТВЕ ОБЩИХ МАТЕМАТИЧЕСКИХ УТВЕРЖДЕНИЙ С ПОМОЩЬЮ КОМПЬЮТЕРА".

В работе предложен новый метод компьютерного доказательства *общих* математических утверждений ***ДОУ-2*** [1]. Суть метода заключается в том, что *прямое* доказательство общего утверждения С (типа " $\forall$ n≥1 P(n), *кроме* $\forall n \ni N'$ ", где P(n) - некоторый теоретико-числовой предикат, а N' - как правило, конечное, так называемое *исключительное* множество натуральных чисел) *заменяется* на доказательство *условного* утверждения $A \rightarrow B$, где А - некоторое *частное* утверждение вида $\exists n^* Q(n^*)$, В - *общее* утверждение вида $\forall n > n^* P(n)$. Из истинности условного утверждения $A \rightarrow B$ (доказывается аналитически) и истинности частного утверждения А (проверяется на компьютере) следует истинность общего утверждения В. Далее, как правило, с помощью компьютера проверяется истинность предиката P(n) для всех $n \le n^*$ чем и завершается полное доказательство общего утверждения С.

В ряде случаев истинность частного (нередко - единичного) утверждения А может быть установлена посредством предъявления так называемой *шифограммы*, - *когнитивного визуального изображения*, - соответствующего *абстрактного* математического объекта [1]. Приведены примеры доказательства ряда нетривиальных теоретико-числовых теорем в рамках ***обобщенной проблемы Варинга*** с помощью метода ***ДОУ-2*** [2,3].

ЛИТЕРАТУРА. 1. А.А.Зенкин, *Когнитивная компьютерная графика*. - М.: Наука,1991. 2. А.А.Зенкин, *Проблема Варинга для сумм биквадратов положительных целых чисел: g(1,4) = 21*. - Мат. заметки, т.54, вып.5, 45 - 56(1993). 3. A.A.Zenkin, *Waring's problem from the standpoint of the cognitive interactive computer graphics*. - "Mathematical and Computer Modelling", vol.13, No. 11, pp. 9 - 25, 1990.

О рациональных приближениях значений G-функций

В.В. Зудилин

С помощью метода "градуированных приближений Паде" [1] доказываются следующие утверждения.

ТЕОРЕМА 1. *Пусть функция* $f(z) \in \mathrm{G}(\mathbb{Q}, C, \Phi)$ *(определение см. в* [2]*) является решением линейного дифференциального уравнения*

$$A_m(z)y^{(m)} + \cdots + A_1(z)y' + A_0(z)y = B(z), \quad B, A_j \in \mathbb{Q}[z], \quad j = 0, 1, \ldots, m, \quad m \geqslant 2,$$

порядка m *и не удовлетворяет никакому*

а) *линейному в случае* $m = 2$, б) *алгебраическому в случае* $m > 2$

дифференциальному уравнению с коэффициентами из $\mathbb{Q}(z)$ *меньшего порядка. Пусть, кроме того,* $a \in \mathbb{Z}$, $b \in \mathbb{N}$ *таковы, что* $aA_m(a/b) \neq 0$, *и* $\varepsilon < \frac{1}{m+t+1}$ *– произвольная положительная постоянная. Обозначим через* $k \in \mathbb{N}$ *наименьший общий знаменатель коэффициентов многочленов* $B, A_0, \ldots, A_m \in \mathbb{Q}[z]$ *и положим*

$$t = \max\Big\{\deg B, \max_{0 \leqslant j < m}\{\deg A_j\}, \deg A_m - 1\Big\}, \quad E = e \cdot \max\Big\{H(B), \max_{0 \leqslant j \leqslant m}\{H(A_j)\}\Big\}.$$

$$C_0 = \Big(2e(t+1)^2 H(C\Phi)^{6(m+1)^2(t+1)(1+\log m)}\Big)^{e(1-\log\varepsilon)} \Phi^{1+te}(C\Phi)^{\frac{2-(m-1)\varepsilon}{\varepsilon^m(m-1)!}},$$

$$\eta_0 = \frac{(1+t\varepsilon)\log b + \log C_0}{(1-(m+t+1)\varepsilon)\log b - \log C_0 - (2-(m+1)\varepsilon)\log(C|a|)}.$$

Если для заданных a, b *выполнено условие* $b > C_0 \cdot (C|a|)^{2+e(m+2t+1)\left(1+\frac{e}{1/(m+t+1)-\varepsilon}\right)}$, *иными словами, если* $\eta_0 > 0$, *то число* $f(a/b)$ *иррационально и для любых* $\eta > \eta_0$, $p, q \in \mathbb{Z}$ $|q| > q_*(f; a, b, \varepsilon, \eta)$, *справедливы оценки* $|f(a/b) - p/q| > |q|^{-1-\eta}$.

Через $\operatorname{den}\lambda \in \mathbb{N}$ обозначим знаменатель несократимой дроби рационального числа λ. Введем в рассмотрение следующие функции натурального аргумента n:

$$\varphi(n) = \sum_{1 \leqslant i \leqslant n \atop (i,n)=1} 1 \text{ – функция Эйлера}, \quad \rho(n) = \frac{n}{\varphi(n)} \sum_{1 \leqslant i \leqslant n \atop (i,n)=1} \frac{1}{i}, \quad \chi(n) = \sum_{p \mid n} \frac{\log p}{p-1}.$$

Так, $\rho(1) = 1$, $\chi(1) = 0$; $\rho(2) = 2$, $\chi(2) = \log 2$; $\rho(3) = \frac{3}{2}$, $\chi(3) = \frac{1}{2}\log 3$ и т.д.

ТЕОРЕМА 2. *Рассмотрим обобщенную полилогарифмическую функцию*

$$f(z) = \sum_{\nu=1}^{\infty} \frac{z^\nu}{(\nu+\lambda)^m}, \quad m \geqslant 2, \quad \lambda \in \mathbb{Q} \setminus \{-1, -2, \ldots\}.$$

Пусть $a \in \mathbb{Z} \setminus \{0\}$, $b \in \mathbb{N}$ *и* $\varepsilon < \frac{1}{m+2}$ *– произвольная положительная постоянная. Положим* $\rho = \rho(\operatorname{den}\lambda)$, $\chi = \chi(\operatorname{den}\lambda)$, $H = \operatorname{den}\lambda \cdot \max\{1, |\lambda|\}$.

$$C_0 = \exp\Big\{\big(\log(8H) + \chi + m\big)\varepsilon(1 - \log\varepsilon) + m\rho\big(1 + \varepsilon + \tfrac{2-(m-1)\varepsilon}{\varepsilon^m(m-1)!}\big)\Big\}.$$

$$\eta_0 = \frac{(1+\varepsilon)\log b + \log C_0}{(1-(m+2)\varepsilon)\log b - \log C_0 - (2-(m+1)\varepsilon)\log|a|}.$$

Если для заданных a, b *выполнено условие* $b > C_0 \cdot (C|a|)^{2+e(m+3)\left(1+\frac{e}{1/(m+2)-\varepsilon}\right)}$, *то число* $f(a/b)$ *иррационально и для любого* $\eta > \eta_0$ *и произвольных* $p, q \in \mathbb{Z}$, $|q| > q_*(a, b, \lambda, \varepsilon, \eta)$, *справедливы оценки* $|f(a/b) - p/q| > |q|^{-1-\eta}$.

[1] *Зудилин В.В.* Мат. сборник. 1995. Т. 186. №4. С. 89–124.

[2] *Галочкин А.И.* Мат. сборник. 1974. Т. 95 (137). №3 (11). С. 396–417.

Московский государственный университет им. М.В. Ломоносова

Кафедра теории чисел

УДК 510.22

Игнатьев В.М., Данилкин Ф.А. (Тула)

ПРИМЕНЕНИЕ ОБЪЕКТНО-ОРИЕНТИРОВАННОГО ПРОГРАММИРОВАНИЯ ПРИ ИСПОЛЬЗОВАНИИ ТЕОРИИ НЕЧЕТКИХ МНОЖЕСТВ.

В настоящее время применение теории нечетких множеств находит все большее распространение. Одна из сфер его применения – использование в компьютерных программах. В литературе приводятся примеры программной реализации теории нечетких множеств. Однако, они написаны с использованием обычных стилей программирования. Это значительно усложняет их применение в связи с тем, что не позволяет решать поставленные задачи в общем виде. Выходом из такой ситуации может послужить использование объектно-ориентированного программирования.

Наиболее полное описание нечетких множеств достигается с использованием основных концепций объектно-ориентированного программирования (инкапсуляция, наследование, полиморфизм). Инкапсуляция, или сокрытие данных, обеспечивает возможность работы с множеством как с одним элементом. Наследование позволяет создавать новые классы множеств. Полиморфизм обеспечивает возможность переопределять семантику операций, тем самым позволяя пользователю записывать математические выражения над нечеткими множествами в привычном виде.

Рассмотрены вопросы применения библиотеки классов нечетких множеств. Разработанная библиотека дополнена рядом новых операций для нечеткими множеств с константами, такие как умножение, сложение, конъюнкция, дизъюнкция, импликация, симметрическая разность. Приведены примеры их использования.

Таким образом, соединяя последние достижения в объектно ориентированном программировании с теорией нечетких множеств, появляются новые возможности для создания программ.

В.М.Игнатьев, Е.В.Ларкин (Россия, Тула)

ОПТИМАЛЬНОЕ РАСПАРАЛЛЕЛИВАНИЕ ВЫЧИСЛИТЕЛЬНЫХ АЛГОРИТМОВ

Одной из основных при реализации вычислительных алгоритмов на параллельных ЭВМ со структурами MISD и MIMD является проблема распараллеливания обработки информации, включающая не только разделение последовательного алгоритма на одновременно и параллельно выполняемые фрагменты, но и оптимизацию временой сложности вычислений. На настоящий момент существует целый ряд параллельных алгоритмов, реализующих информационные технологии теории чисел и смежных областей математики, однако в общем виде проблема разделения произвольного алгоритма на параллельно выполняемые отдельными процессорами фрагменты весьма далека от разрешения.

Предлагается метод распараллеливания, основанный на семантическом анализе исходного последовательного алгоритма A моделируемого управляющей сетью Петри $G = \{P, T, I(T), O(T), \iota\}$, где P - множество позиций; совпадающее со множеством операторов алгоритма A; T - множество переходов; $I_P(T)$ и $O_P(T)$ - входная и выходная функции, соответственно, причем для переходов $t_{i(t)}$ выполняются условия: $\mu[I(t_{i(t)})] \leqslant 1$ и $\mu[O(t_{i(t)})] \leqslant 1$; ι - наложенные на сеть Петри характеристики информационного потока. Цель анализа заключается в выявлении структурных особенностей информационного потока и выделении в нем фрагментов $\iota_{i(I)}$, удовлетворяющих условиям $\varkappa(\lambda)$ для таких отношений, как отношения связности $\lambda(\iota_{i(I)})$, независимости $\lambda[\iota_{i(I)} \neq \iota_{i(I)}(\iota_{j(I)})]$, предшествования $\lambda(\iota_{i(I)} \leftarrow \leftarrow \iota_{j(I)})$ и т.п.

В результате анализа формируется раскраска $C(G)$, основанная на выделении в алгоритме A информационно-независимых связных фрагментов, которая используется для преобразования исходной сети в сеть $\Upsilon = \{\pi, \tau, I(\tau), O(\tau), \theta\}$, где $\{\pi, \tau, I(\tau), O(\tau)\}$ - структура с непустым множеством переходов $\tau_{\sim}$, для которых выполняется одно из условий $\mu[I(\tau_{\sim i(t)})] > 1$ или $\mu[O(t_{\sim i(t)})] > 1$, а θ - наложенные временные характеристики. Производная сеть Петри является моделью параллельного вычислительного процесса. Одной из операций при ее генерации является оценка и минимизация таких характеристик алгоритма, как временная сложность или простой компонентов вычислительного комплекса во время вычислений.

УДК.5II

Исмоилов Д. (Душанбе)

О методе Хуа оценок полных рациональных тригонометрических сумм.

В докладе рассматривается проблемы оценок полных рациональных тригонометрических сумм (ПРТС), предложенный в 40-ые годы Хуа - Локенгом [I]. В последнее время автором обобщен и развит метод работы [I] для более общих ПРТС [2]. Пусть

$f(x) = a_k x^k + \dots + a_1 x + a_0$; $g(x) = b_r x^r + \dots + b_1 x + b_0$;

q - натуральное число; $(a_k, \dots, a_1, a_0, q) = 1$; $i^2 = -1$;

$(b_r, \dots, b_1, b_0, q) = 1$; $R(x) = f(x)/g(x)$;

$$S(R,q) = \sum_{x=1}^{q} e_q(R(x)); \quad e_q(R(x)) = \exp(2\pi i R(x)/q);$$

где суммирование ведется по всем $x = 1,2, \dots, q$; для которых $g(x) \not\equiv 0 \pmod q$ и $e_q(R(x)) \not\equiv \text{const}$. При $r = 0$ сумма $S(R,q)$ совпадает с классической ПРТС [I]. В работе [2] построен алгоритм с помощью которого удается доказать точное равенство для $S(R;p^n)$;

Теорема. Пусть $h(x) = f'(x)\cdot g(x) - f(x)\cdot g'(x)$; $q = p^n$; p - простое число, $n \geq 2$; $kr \geq 2$; $\xi = \xi^{(1)}$ - пробегает все корни сравнения $p^{-\tau} h(x) \equiv 0 \pmod p$; $0 \leq \tau \leq W$; m - максимум кратности корней $\xi = \xi^{(1)}$. Тогда существуют целые числа $u_1, u_2, \dots, u_t$ такие, что

$$(1)\quad S(R,p^n) = \sum_{(\xi^{(1)},\dots,\xi^{(t)})} p^{u_t - t} \sum_{y=1}^{p^{n-u_t}} \exp\Big(R(\xi^{(1)}) + \sum_{\nu=1}^{t-1} p^{U_\nu} R_\nu(\xi^{(\nu+1)}) + p^{u_t} R_t(y)\Big)$$

где $\xi^{(2)}$ определяется по $\xi^{(1)}$, $\xi^{(3)}$ определяется по $(\xi^{(1)}, \xi^{(2)})$ и т.д.; U_ν зависит от $\xi^{(\nu)}$; $R_\nu(\xi^{(\nu+1)})$ и $R_t(y)$ однозначно определяется по $R(x)$ t - наибольшая длина цепочек набора $(u_1, \dots, u_t)$. $U_0 = 0$; $U_t = u_1 + \dots + u_t$; $2t \leq U_t \leq (m+1)t + \tau$; $0 \leq n - U_t \leq 2W + 1 \leq n - U_{t-1}$.

Из (1) (с учетом результата А.Вейля при $q = p$) выводятся неулучшаемые оценки снизу и сверху для величины $|S(R,q)|$ при любом натуральном q.

[1] Hua L.K. Journ. Chinese Math.Soc. (1940), 2., p. 301 - 312.

[2] Ismailov D.China,Advansec in mathematics,(1994),vol 23,N1,p.153-171

УДК. 5II.

Исмоилова Н.Д. (Душанбе)

Об одном обобщении суммы Гаусса.

В сообщении рассматривается одно обобщение классической суммы Гаусса для дробно-линейных функций с целыми коэффициентами. Известно, что точное значение суммы Гаусса найдено для любого вещественного характера модуля q. Для невещественных примитивных характеров модуля $q = p^n$, p – простое число, $n \geq 2$ на основании p-адического представления числа и явной формулы А.Г.Постникова для $\chi(1 + pn)$, n –целое число [1], недавно Д.Исмоилов [2] нашел точное значение Гауссовых сумм. Здесь мы будем рассматривать следующую сумму Гаусса: пусть $\chi(n)$ – примитивный характер Дирихле модуля q, $h_1(x) = (a_1x + b_1)/(c_1x + d_1)$; $h_2(x) = (a_2x + b_2)/(c_2x + d_2)$ дробно – линейные функции с целыми коэффициентами a_1, b_1, c_1, d_1; a_2, b_2, c_2, d_2;

$e(\alpha) = \exp(2\pi i\alpha)$, $i^2 = -1$; $\alpha \in R$;

$$S_q(\chi, h_1, h_2) = \sum_{x=1}^{q}{}' \chi(h_1(x))e(h_2(x)/q),$$

где суммирование ведется по всем x, для которых $(c_1x + d_1, q) = 1$; $(c_2x + d_2, q) = 1$. Приведем один результат для случая когда $h_1(x) = h_2(x)$, $q = p$ – простое число и $\chi(n) = (n/p)$ символ Лежандра.

Теорема. При $(ac, p) = 1$ имеет место равенства

$$S_p(\chi, h) = \begin{cases} (p-1)\left(\frac{ac'}{p}\right)e(ac'/p), & ad \equiv bc \pmod p \\ i^{\left(\frac{p-1}{2}\right)^2}\sqrt{p} - \left(\frac{ac'}{p}\right)e\left(\frac{ac'}{p}\right); & ad \not\equiv bc \pmod p. \end{cases}$$

Здесь $\left(\frac{ac'}{p}\right)$ – символ Лежандра, $cc' \equiv 1 \pmod p$.

Используя этот результат можно выписать явное значение величины $S_q(\chi, h)$ для любого натурального q.

[1] Постников А.Г. О сумме характеров по модулю, равному степени простого числа. Изв. АН СССР, сер. матем. (I9), (I955), с. II-I6.

[2] Исмоилов Д. Точное значение Гауссовых сумм. В кн: Тез. научн. конф. по комплексному анализу. Душанбе I992 с 24-25

УДК 5II.9

Истамов А.М. (Самарканд)

О ЧИСЛЕ КЛАССОВ БИНАРНЫХ КВАДРАТИЧНЫХ ФОРМ ОТРИЦАТЕЛЬНОГО ДИСКРИМИНАНТА

Рассматривается известное соотношение между числами классов бинарных квадратичных форм отрицательного дискриминанта, отличающихся на множитель - квадрат простого числа.

Пусть h - число приведенных бинарных форм с дискриминантом $D<0$, а H - число таких форм с дискриминантом $D'=D\,p^{2k}$. Тогда имеет место соотношение

$$H = h\,p^{k-1}\left(p-\left(\frac{D}{p}\right)\right),\quad \text{где } \left(\frac{D}{p}\right) - \text{символ Лежандра } \langle 1\rangle.$$

Пользуясь понятиями арифметики матриц второго порядка гораздо проще вывести это соотношение. Для этого сопоставим каждой форме (a, b, c) с дискриминантом D матрицу $L_j = \begin{pmatrix} b_j & a_j \\ c_j & b_j \end{pmatrix}$. Рассмотрим все неассоциированные примитивные матрицы с определителем p^k:

$$A_i = \begin{pmatrix} p^{k_1} & 0 \\ \xi_i & p^{k_2} \end{pmatrix};\quad 0 \le \xi_i < p^{k_1};\quad (\xi_i, p)=1;\quad k_1+k_2=k, k_1=\overline{0,k}.$$

Известно, что их количество равно $p^k(p+1)$. Составим всевозможные произведения матриц $\bar{A}_i L_j A_i$ $(i=\overline{0,p^k(p+1)};\ j=\overline{1,h})$. Можно показать, что все формы соответствующие эти матрицам будут неэквивалентны. Поэтому, достаточно вычислить их количество. В случае, когда $\left(\frac{D}{p}\right)=1$ их будет $p^{k-1}(p-1)$, а в случаях, когда $\left(\frac{D}{p}\right)=0$ или $\left(\frac{D}{p}\right)=-1$ их будет соответственно p^k или $p^{k-1}(p+1)$. Во всех случаях верна формула (I).

I. Лежен-Дирихле И.Г. Лекции по теории чисел. ОНТИ НКТП СССР, 1936, 403 с.

2. Венков Б.А. Элементарная теория чисел. ОНТИ НКТП СССР, 1937, 218 с.

3. Истамов А. О классах смежности матриц. Труды СамГУ, 1970, 191, с.84-89.

УДК 681.3

Ильин А.А. (Тула)

ПАКЕТ ПРИКЛАДНЫХ ПРОГРАММ ДЛЯ ИССЛЕДОВАНИЯ ТОЧНОСТИ РЕАЛИЗАЦИИ ГНЕЗДОВЫХ АЛГОРИТМОВ ЦИКЛИЧЕСКОЙ СВЕРТКИ С ФИКСИРОВАННОЙ АРИФМЕТИКОЙ

Представлена методика исследования точности реализации гнездовых алгоритмов циклической свертки с фиксированной арифметикой и структура программного обеспечения (ПО) их моделирования на 16 и 32-разрядных (на основе микропроцессоров i80386, i80486, i80586 и аналогичных) ПЭВМ. При моделировании на 16-разрядных ПЭВМ (на основе микропроцессоров i8086/88, i80186, i80286 и аналогичных) в состав ПЭВМ должен входить арифметический сопроцессор. Разрядность операндов не более 32.

Формат представления операндов с фиксированной арифметикой: запятая фиксирована левее самого старшего разряда. То есть операнды должны быть меньше единицы по модулю.

В ПО реализован метод масштабирования, заключающийся в следующем: при возникновении переполнения разрядной сетки представления операндов все элементы данных сдвигаются на один разряд вправо.

ПО реализовано на языке высокого уровня C++. Разработан класс вещественных чисел с фиксированной запятой меньших единицы по модулю. Набор операторов и функций класса позволяют легко моделировать гнездовые алгоритмы циклической свертки с задаваемой разрядностью операндов.

ПО позволяет формировать исходные данные в виде входного сигнала и импульсной характеристики цифрового фильтра, задавать схему гнездового алгоритма циклической свертки, задавать разрядность операндов, реализовывать гнездовые алгоритмы циклической свертки как с фиксированной, так и с плавающей арифметикой, определять стандартное отклонение ошибки реализации гнездовых алгоритмов циклической свертки по оригинальной методике. Предлагаемая методика за точный результат циклической свертки принимает результат реализации с плавающей арифметикой.

Представленная методика и ПО позволяют оценивать ошибку реализации гнездовых алгоритмов циклической свертки и выбирать при проектировании разрядность спецпроцессора, обеспечивающую заданную точность реализации, с учетом априорных сведений об исходном сигнале.

УДК 511.

Ильясов М.И. (г.Уральск.)

ПЕРЕХОД ОТ ОБЫКНОВЕННОЙ БЕСКОНЕЧНОЙ ЦЕПНОЙ ДРОБИ К ПОЛУРЕГУЛЯРНОЙ БЕСКОНЕЧНОЙ ЦЕПНОЙ ДРОБИ

Известно, что всякое иррациональное число единственным образом представляется в виде обыкновенной бесконечной цепной дроби вида:

$$q+\cfrac{1}{q_1+\cfrac{1}{q_2+\cfrac{1}{\ddots}}} \qquad (1)$$

где q -целое, $q_1, q_2, \ldots$ натуральные числа.

В теории чисел наряду с бесконечной цепной дробью (I) рассматривается бесконечные цепные дроби вида:

$$a+\cfrac{1}{q_1-\cfrac{1}{a_2-\cfrac{1}{\ddots}}} \qquad (2)$$

где a-целое, $a_1, a_2, \ldots$ натуральные числа, большие единицы. Это выражение называется бесконечной полурегулярной цепной дробью (частный случай).

Здесь верна теорема: всякое иррациональное число единственным образом представляется в виде (2).

Нередко удается представить значения какой-либо функции в определенных точках в виде (2). Например, отношение двух соседних функций Бесселя. Отсюда легко установить, что это отношение является иррациональным числом в специально выбранных точках.

В докладе указывается правило перехода от представления (I) к представлению (2) и обратно.

Доказана теорема:

Если бесконечные цепные дроби (I) и (2) представляют одно и то же иррациональное число, то

$$a = q\,,\ q_1 = q_1+1\,,\ a_{q_2+1} = q_3+2\,,$$

$$a_{q_2+q_4+1} = q_5+2\,,\ \ldots,\ a_{q_2+q_4+\ldots+q_{2k}+1} = q_{2k+1}+2\,,\ldots$$

а остальные a_i равны двум.

УДК 681.142

Ирхин В.П. (Воронеж), Краснобаев В.А. (Москва)

АЛГОРИТМЫ РЕАЛИЗАЦИИ ОПЕРАЦИЙ МОДУЛЯРНОЙ АРИФМЕТИКИ

Исследования, проводимые в области улучшения основных характеристик вычислительных средств, указывают на целесообразность применения методов теории чисел для кодирования информации в ЭВМ с целью распараллеливания процесса ее обработки. Этот принцип наиболее полно реализован при использовании системы счисления в остаточных классах (СОК) с применением операций модулярной арифметики. Широкому распространению СОК препятствует, в частности, отсутствие эффективных алгоритмов реализации операций в этой системе.

Предлагается алгоритм, в котором реализуются свойства симметрии арифметической таблицы, что позволило использовать 1/8 часть полной таблицы для осуществления всех операций модулярной арифметики. Дальнейшим развитием этого подхода является разработка алгоритмов сокращения таблиц, основанных на использовании внутреннего модуля и деления таблицы на функционально законченные части. Определены оптимальные характеристики внутреннего модуля и коэффициента деления таблицы.

Рассматривается алгоритм, связанный с увеличением ступеней СОК, и предлагается методика выбора их числа. Для реализации операции целочисленного деления в СОК возникает необходимость в получении обратной мультипликативной величины числа. Приводятся варианты ее определения, основанные на использовании малой теоремы Ферма и теоремы Вильсона.

Для перевода числа из СОК в двоично-позиционную систему (ДПС) разработаны два эффективных алгоритма. Первый основан на расширении диапазона представления числа в СОК, где в качестве дополнительного основания выбирается модуль равный исходному диапазону представления, либо взаимно-простой с ним. Второй случай более предпочтителен для определения обратных мультипликативных величин оснований СОК. Второй алгоритм перевода базируется на разложении числа, рассматриваемого в виде вектора, по ортогональным проекциям системы оснований с последующим суммированием позиционных характеристик этих проекций. Приводится алгоритм для сравнения чисел в СОК, суть которого состоит в разбиении диапазона представления чисел на два интервала с последующим анализом операндов.

Карташева Л.В., Радченко Т.Н. (Ростов-Дон)

АНАЛИТИЧЕСКИЕ ПРЕДСТАВЛЕНИЯ КОШИ ОБОБЩЕННЫХ ФУНКЦИЙ ИЗ $\widetilde{\Phi}_+'$ НА ПОЛУОСИ И ИХ ПРЕДЕЛЬНЫЕ СВОЙСТВА

Пространство основных функций $\widetilde{\Phi}_+$ состоит из функций $\varphi(x)$, удовлетворяющих условиям:

$\varphi(x) \in \overset{\infty}{C}(R_+)$ и $\lim_{x \to 0,\infty} x^{\ell} \varphi^{(m)}(x) = 0$, $\forall \ell \in R$ $(m = 0, 1, 2, \dots)$

кроме того, $\int_0^\infty x^{\ell_n(x)} \varphi(x)\, dx = 0$ $(n = 0,1,2,\dots,\ \ell = 0,1,2\dots)$

Топология в $\widetilde{\Phi}_+$ вводится с помощью системы норм:

$$\|\varphi;\ \widetilde{\Phi}_+\|_k = \sup_{m \le k} \sup_{x \ge 0} (1+x)^k |\varphi^{(m)}(x)|, \quad k = 0, 1, 2, \dots.$$

Рассмотрим сингулярный оператор

$$S\varphi = F.P. \frac{1}{\pi i} \int_0^\infty \frac{\varphi(t)}{t - x}\, dt \qquad (I)$$

и изучим его действие на функции $\varphi(x) \in \widetilde{\Phi}_+$.

ТЕОРЕМА 1: сингулярный оператор, определенный (I), отображает $\widetilde{\Phi}_+$ в себя.

Аналитическим представлением Коши, обобщенной функции $f \in \widetilde{\Phi}_+'$, назовем функционал $\hat{f}(z) = \frac{1}{2\pi i} \left(f_t, \frac{1}{t - z}\right)$

Положим $f^*(x+ih) = \hat{f}(x+ih) - \hat{f}(x-ih)$, $\tilde{f}(x+ih) = \hat{f}(x+ih) + \hat{f}(x-ih)$.

Теорема 2: если $f \in \widetilde{\Phi}_+'$, $\varphi \in \widetilde{\Phi}_+$, то

$$F.P. \int_0^\infty f^*(x+ih)\, \varphi(x)\, dx = (f_t, \varphi^*(t+ih))$$

и $\lim_{h \to +0} (f_t, \varphi^*(t+ih)) = (f_t, \varphi(t))$, где

$$\varphi^*(t+ih) = \frac{h}{\pi} F.P. \int_0^\infty \frac{\varphi(x)}{(x-t)^2 + h^2}\, dx$$

Теорема 3: Если $f \in \widetilde{\Phi}_+'$, $\varphi \in \widetilde{\Phi}_+$, то

$$F.P. \int_0^\infty \tilde{f}(x+ih)\, \varphi(x)\, dx = (f_t, -\widetilde{\varphi}(t+ih))$$

$$\lim_{h \to +0} (f, -\widetilde{\varphi}(t+ih)) = (f, -S\varphi)$$

где $S\varphi$ определяется формулой (I)

Теорема 4: В условиях теорем 3 и 4 существуют $\lim_{h \to +0} \hat{f}(x \pm ih) = f^{\pm}(x)$ и выполняются соотношения

$$f^+(x) + f^-(x) = Sf, \quad f^+(x) - f^-(x) = f(x)$$

УДК 519.6

Киселев В.Д., Румянцева И.И., Корелин Д.С. (Тула)

Двойственность в задачах целочисленного квадратичного программирования

Рассматривается следующая задача целочисленного квадратичного программирования (ЦКП). Необходимо максимизировать

$$f(x) = \sum_{j=1}^{n} c_j x_j + \sum_{j=1}^{n} \sum_{k=1}^{n} d_{kj} x_k x_j$$

при ограничениях

$$\sum_{j=1}^{n} a_{ij} x_j \le b_i, \qquad i=1,2,\ldots,m.$$

$$x_j = \{0,1\}, \qquad j=1,2,\ldots,n,$$

где $D=\|d_{kj}\|$ -неотрицательная матрица порядка n, $A=\|a_{ij}\|$- матрица размерности $m \times n$, $C=\|c_j\|$ и $B=\|b_i\|$ - неотрицательные вектора размерности n и m соответственно.

Предлагаются два новых эффективных алгоритма решения задачи ЦКП с булевыми переменными, основанные на линеаризации целевой функции с использованием теории двойственности.

Выбор этого подхода объясняется тем, что даже большого размера линейные задачи могут быть решены относительно легко. В этом случае процесс решения задачи ЦКП состоит из двух этапов. На первом этапе решением n линейных задач определяются коэффициенты линейной функции, на втором- а) при использовании метода ветвей и границ определяются порядок ветвления переменных и оценки границ решения задачи ЦКП на основе двойственной по отношению к линеаризированной задачи; б) при использовании метода встречного решения функциональных уравнений динамического программирования определяется множество допустимых решений линеаризированной задачи и на полученном множестве проводится анализ значений квадратичной функции.

Приводятся результаты вычислительного эксперимента, подтверждающие преимущество предлагаемых алгоритмов по сравнению с существующими.

УДК 621.396

Климов А. И. (г. Воронеж)

Приемопередатчик ИК-диапазона.

В частоящее время существенно обостряются проблемы электромагнитной совместимости различных радиосредств, и, в частности, помехоустойчивости передачи информации. Одним из путей решения этих проблем является использование для целей связи инфракрасного (ИК) излучения с длинами волн, соответствующими окнам прозрачности атмосферы / 1 /.

В докладе приводятся результаты разработки и экспериментальных исследований приемопередатчика ИК-диапазона, предназначенного для осуществления одноканальной телефонной связи по атмосферному каналу в симплексном режиме.

Доказывается целесообразность применения частотно-импульсной модуляции сигнала поднесущей частоты. В качестве излучателя применяется диод ближнего ИК-диапазона.

Показывается, что от известной аппаратуры аналогичного назначения, работающей в оптическом (или СВЧ и КВЧ диапазонах), данный приемопередатчик отличается малыми габаритами и массой (может быть смонтирован в монокуляре бинокля), низким энергопотреблением и обеспечивает телефонную связь при нормальных метеоусловиях на расстоянии до 1 км. При этом достигается высокая помехоустойчивость и скрытность связи. Ширина диаграммы направленности оптической антенны составляет 1 градус, поэтому перехват сообщения возможен фактически только на линии визирования.

ЛИТЕРАТУРА

1. Гауэр Дж. Оптические системы связи. -М.: Мир, 1990 г.

УДК 511.36

Ковалевская Э.И. (Минск)

ПРИМЕНЕНИЕ МЕТОДА ТРИГОНОМЕТРИЧЕСКИХ СУММ К ЭФФЕКТИВИЗАЦИИ ТЕОРЕМЫ О СОВМЕСТНЫХ РАЦИОНАЛЬНЫХ ПРИБЛИЖЕНИЯХ

Пусть на конечных отрезках $[a_j, b_j]$ заданы действительные, $(n+1)$-раз непрерывно дифференцируемые функции $f_{j1}(x_j), \dots, f_{jn}(x_j)$ $(1 \le j \le m,\ m \ge n \ge 2)$, такие, что вронскианы $W_j(f_{j1}(x_j), \dots, f_{jn}(x_j)) \ne 0$ почти всюду (в смысле меры Лебега) на $[a_j, b_j]$. В [1] доказано, что для почти всех $\bar{x} = (x_1, \dots, x_m) \in [a_1, b_1] \times \dots \times [a_m, b_m]$ неравенство

$$\max_{1 \le j \le m} \left(\|q f_{j1}(x_j)\|, \dots, \|q f_{jn}(x_j)\| \right) < q^{-1/mn) - \varepsilon}, \qquad (1)$$

где $\varepsilon > 0$ как угодно мало, имеет только конечное число решений в целых числах $q > 0$ (Здесь $\|\alpha\|$ - расстояние от числа α до ближайшего целого). Получен эффективный вариант этого результата.

Теорема. Пусть $Q > 0$ - достаточно большое число, $m \ge n \ge 2$; числа δ, δ удовлетворяют условиям $\delta > 1/mn$, $0 < \delta < \delta/n$. Пусть I_j - интервал из $[a_j, b_j]$ $(1 \le j \le m)$ длиной $Q^{-\delta}$; M - множество тех $\bar{x} \in I_1 \times \dots \times I_m$, для которых (1), где правая часть заменена на $Q^{-\varepsilon}$, имеет хотя бы одно решение в целых числах q, когда $1 \le q \le Q$; μM - его мера Лебега; $|W_j(x_j)| > \alpha > 0$ для $x_j \in [a_j, b_j]$ $(1 \le j \le m)$. Тогда

$$\mu M < c \begin{cases} Q^{-m(n\delta - \delta + 1)}, & \text{если } \delta < n(1 - m\delta)/m(n^2 - 1), \\ Q^{-m\delta/n} \ln Q, & \text{если } \delta \ge n(1 - m\delta)/m(n^2 - 1), \end{cases}$$

где $c = c(\alpha, m, n) > 0$ - абсолютная константа.

Теорема доказывается методом тригонометрических сумм. Оценки такого вида с явной зависимостью от параметров задачи находят применение в математической физике при разрешении так называемой проблемы малых знаменателей.

Литература. 1. Берник В.И., Ковалевская Э.И. // Матем.заметки. 1974. Т.15, вып.2. С.247-254.

УДК 514+531.8

Ковалев М.Д.(Москва)

О ВОССТАНОВИМОСТИ ШАРНИРНИКОВ ПО ВНУТРЕННИМ НАПРЯЖЕНИЯМ

Простейшая плоская шарнирная конструкция (шарнирник [1]) состоит из двух стержней (рычагов) одними концами скрепленных между собой шарниром p_1, а другими концами закрепленных в плоскости с помощью шарниров p_2 и p_3. Ненулевой набор $\{\omega_{12},\omega_{13}\}$ вещественных чисел, сопоставленных рычагам p_1p_2 и p_1p_3 нашего шарнирника, называют его внутренним напряжением, если выполнено условие равновесия сил

$$\omega_{12}(\mathbf{p}_1-\mathbf{p}_2)+\omega_{13}(\mathbf{p}_1-\mathbf{p}_3)=\mathbf{0}, \quad (1)$$

где $\mathbf{p}_1,\mathbf{p}_2,\mathbf{p}_3$- радиус векторы шарниров. Наш шарнирник, очевидно, допускает внутреннее напряжение лишь если $\mathbf{p}_1$ лежит на прямой $\mathbf{p}_2\mathbf{p}_3$. Легко установить, что задание комбинаторной схемы этого шарнирника, положений $\mathbf{p}_2$ и $\mathbf{p}_3$ его закрепленных шарниров и внутреннего напряжения $\omega=\{\omega_{12},\omega_{13}\}$ однозначно определяет положение $\mathbf{p}_1$ свободного шарнира, а значит, и весь шарнирник.

В общем случае пусть $\mathcal{M}=\mathcal{M}(P,G)$ - множество всех шарнирников евклидова пространства $\mathbf{R}^d$ с данной схемой G соединения рычагов и с заданными положениями P закрепленных (шаровых) шарниров. Если шарнирник $\mathbf{p}\in\mathcal{M}$ допускает внутренние напряжения, то они вместе с нулевым напряжением как решения системы вида (1) образуют линейное подпространство $\mathbf{W}(\mathbf{p})$ пространства $\mathbf{W}^r$ всех мыслимых напряжений (r-число рычагов шарнирника). Когда в множестве $\mathcal{M}$ нет иных, кроме $\mathbf{p}$, шарнирников, обладающих подпространством внутренних напряжений $\mathbf{W}(\mathbf{p})$?

Решая этот вопрос, разумно на шарнирник $\mathbf{p}$ наложить условие неравенства нулю длин его рычагов; и условие полной напрягаемости, то есть существования внутреннего напряжения ненулевого на всех рычагах. Полное решение поставленного вопроса удалось получить лишь для шарнирников на прямой. Уже в $\mathbf{R}^2$ ситуация намного сложнее чем на прямой. Один из интересных открытых вопросов: для любого ли шарнирника $\mathbf{p}$, восстановимого по своему $\mathbf{W}(\mathbf{p})$, существует напряжение $\omega\in\mathbf{W}(\mathbf{p})$ по которому (одному) можно восстановить шарнирник $\mathbf{p}$?

1. Ковалев М.Д. Геометрическая теория шарнирных устройств // Известия РАН. Серия Математическая. 1994 т.58. №1. С.45-70.

УДК 511. 9

Ковальчик Ф.Б. (Одесса)

ОБ ОДНОЙ АСИМПТОТИЧЕСКОЙ ФОРМУЛЕ

Доказана

ТЕОРЕМА. Для любого натурального m при $x \to \infty$, $\theta > \exp\left(-c(\log x)^{3/5}(\log\log x)^{-1}\right)$ справедлива асимптотическая формула

$$\sum_{\substack{\alpha\in\mathcal{O}\\ N\alpha\le x\\ \omega(\alpha)=k\\ \alpha\in S}}{}' \tau_n^{\beta}(\alpha) = \theta\left(\frac{2\pi h}{g\sqrt{d}}\right)^{n^{\beta}} \frac{x\left(n^{\beta}\log\log x\right)^{k-1}}{(k-1)!\,\log x}\left\{H_{\beta}\left(\frac{k-1}{n^{\beta}\log\log x}\right) + \sum_{q=2}^{2m}\frac{1}{q!}H_{\beta}^{(q)}\left(\frac{k-1}{n^{\beta}\log\log x}\right)\frac{P_{q-1}(k)}{(n^{\beta}\log\log x)^{q}} + O\left(\frac{2^{3m}\,P_{2m}(k)(k-2m)^{7/2}}{(2m+1)!\,(n^{\beta}\log\log x)^{2m+1}}\right)\right\}$$

равномерно по $1 \le k \le \log\log x + a(x)\sqrt{\log\log x}$.

Здесь $\mathcal{O}$ система целых идеальных чисел мнимого квадратичного поля $\mathbb{Q}(\sqrt{-d})$, g число единиц, h число классов идеальных чисел, $\tau_n(\alpha)$ число представлений $\alpha \in \mathcal{O}$, $\alpha \neq 0$ в виде произведения n различных неассоциированных сомножителей из $\mathcal{O}$, $\omega(\alpha)$ число различных простых делителей $p \in \mathcal{O}$ числа α, $N\alpha$ норма α, S сектор единичного круга раствора θ, $\beta \in (0,1]$. $P_j(k)$ некоторые многочлены с коэффициентами из $\mathbb{Z}$ степени j, например, $P_{2m}(k) = (k-1)^2(k-2)\cdots(k-(2m-1))$,

$$H_{\beta}(z) = \frac{n^{\beta}}{\Gamma(1+n^{\beta}z)}\prod_{p}\left(1-\frac{1}{Np}\right)^{n^{\beta}}\left(1+\frac{n^{\beta}z}{Np}+\frac{\left(\frac{n(n+1)}{2}\right)^{\beta}z}{Np^2}+\dots\right),$$

$H_{\beta}^{(q)}(z)$ – q-я производная, $\sum'$ означает, что суммирование ведется по неассоциированным α, c положительная постоянная, $a(x)$ вещественная функция, стремящаяся к ∞ медленнее $\sqrt{\log\log x}$. Эта теорема улучшает полученный ранее автором результат.

УДК 511.5

Л.А. Коган (Ташкент)

ПРЕДСТАВЛЕНИЕ ЧИСЕЛ КВАДРАТИЧНЫМИ ФОРМАМИ

В докладе будет рассказано о современном состоянии проблемы нахождения формул типа Якоби, Гиургилля, Булыгина-Морделла, Вейля, Клостермана для количества представлений чисел квадратичными формами. Автор [I-7] связал решение указанной проблемы с гипотезой А.Вейля, обобщенной гипотезой А.Вейля, результатами автора по доказательству обобщенной гипотезы А.Вейля, с подъемом автора в теории модулярных форм и функциональных уравнений, результатами Эйхлера о представимости параболических форм в виде обобщенных кватернарных тэта-рядов, результатами автора о представимости параболических форм в виде обобщенных бинарных тэта-рядов, исследованиями И.М. Виноградова и Бердхеса о распределении квадратичных невычетов, проблемой Мамфорда о представимости параболических форм в виде линейной комбинации произведений тэта-функции с рациональными характеристиками. Благодаря установленной связи удалось в основном решить проблему о формулах первых четырех типов. Автор, используя вышеуказанные результаты Эйхлера недавно решил проблему Мамфорда для некоторых классов параболических форм типа $(\kappa, N, 1)$, $\kappa \geq 2$.

Литература

I. Коган Л.А. Теория модулярных форм и проблема нахождения формул для количества представлений чисел положительными квадратичными формами. ДАН СССР 1968, т.182, № 2 259-261.

2. Коган Л.А. Гипотеза И.М. Виноградова о наименьшем квадратичном невычете и представление чисел квадратичными формами. ДАН СССР 1971, т.198 №6. 1263-1264.

3. Коган Л.А. Эллиптические кривые и модулярные формы. ДАН СССР 1972, т.204 №2. 275-278.

4. Коган Л.А. О представлении целых чисел положительно определенными квадратичными формами. Ташкент ФАН, 1971.

5. Коган Л.А., Ташпулатов Б.Т., Фазиев С.Р. Представление чисел квадратичными формами. Ташкент ФАН, 1980.

6. Коган Л.А., Ташпулатов Б.Т., Дусумбетов А.Д. Представление чисел квадратичными формами. Ташкент ФАН, 1989.

7. Ташпулатов Б.Т., Коган Л.А. Представление чисел квадратичными формами. Ташкент ФАН. 1993.

УДК 511.5

Коган Л.А., Ташпулатов Б.Т., Кулматов А.К. (Ташкент)

О ФОРМУЛАХ ТИПА ВЕЙЛЯ

Коган Л.А. [1,2] доказал обобщенную гипотезу А.Вейля для эллиптических кривых с комплексным умножением, относящуюся к построению модулярных форм веса К ($K \geqslant 2$).

В доказанной теореме Коган Л.А. [3] выписал множители у ряда $L_K(s)$ кроме хороших простых Р , также для плохих Р. Идея подъема Коган Л.А. [1,2,3] в теории модулярных форм нашла практическую реализацию, а именно Коган Л.А. и Кулматов А.К. получили формулы типа Вейля для некоторых квадратичных форм с шестью и восемью переменными, причем, А.К. Кулматов исследовал квадратичные формы, отличные от рассматриваемых Л.А. Коганом, а Ташпулатов Б.Т. [3] получил формулу типа Вейля для квадратичных форм с десятью и более переменными.

Литература

1. Коган Л.А. Эллиптические кривые и модулярные формы ДАН СССР, 1972, т. 204 №2, с. 275-278

2. Коган Л.А., Ташпулатов Б.Т., Дусумбетов А.Ф. Представление чисел квадратичными формами, - Ташкент: ФАН, 1989, - 132 с.

3. Ташпулатов Б.Т., Коган Л.А. Представление чисел квадратичными формами. - Ташкент: ФАН, 1993. - 112 с.

УДК 511.5 Кожегельдинов С.Ш. (Семипалатинск)

К РЕШЕНИЮ СИСТЕМЫ УРАВНЕНИЙ ГЕРОНА

При отыскании всех решений системы уравнений Герона

$$16S_1^2=(x_1-y_1+z)(x_1+y_1-z)(-x_1+y_1+z)(x_1+y_1+z),$$
$$16S_2^2=(x_2-y_2+z)(x_2+y_2-z)(-x_2+y_2+z)(x_2+y_2+z), \qquad (1)$$

где

$$S_1,x_1,y_1,z,x_2,y_2,S_2\in\mathbb{N},\quad x_1<y_1+z,\quad y_1<z+x_1, \qquad (2)$$
$$z<x_1+y_1,\quad x_2<y_2+z,\quad y_2<z+x_2,\quad z<x_2+y_2,$$

используются результаты и методы работ [1-4]. В дальнейшем для удобства совокупность формул , которая дает все решения системы (1) с условием (2), называется формулой. Имеют место не менее восьми эквивалентных формул, каждая из них является формулой всех решений системы (1) с условием (2). В частности, доказана

Теорема. Все решения системы (1) с условием (2) получаются из формулы

$$S_1=k^2\frac{abcd(a+b)(ac-bd)(a^2\gamma^2+\beta^2\delta^2)^2}{\Delta^2},$$

$$x_1=k\frac{(a+b)(ac-bd)(a^2\gamma^2+\beta^2\delta^2)}{\Delta},\qquad y_1=k\frac{ab(c^2+d^2)(a^2\gamma^2+\beta^2\delta^2)}{\Delta},$$

$$z=k\frac{(a^2c^2+b^2d^2)(a^2\gamma^2+\beta^2\delta^2)}{\Delta},$$

$$x_2=k\frac{(\alpha+\beta)(\alpha\gamma^2-\beta\delta^2)(a^2c^2+b^2d^2)}{\Delta},\qquad y_2=k\frac{\alpha\beta(\gamma^2+\delta^2)(a^2c^2+b^2d^2)}{\Delta},$$

$$S_2=k^2\frac{\alpha\beta\gamma\delta(\alpha+\beta)(\alpha\gamma^2-\beta\delta^2)(a^2c^2+b^2d^2)^2}{\Delta^2},$$

где $k,a,b,c,d,\alpha,\beta,\gamma,\delta\in\mathbb{N},\quad (a,b)=(c,d)=(\alpha,\beta)=(\gamma,\delta)=1,$

$ac>bd,\ \alpha\gamma^2>\beta\delta^2,\ \Delta=((a^2c^2+b^2d^2)(\alpha\gamma^2-\beta\delta^2,\beta\delta^2(\alpha+\beta)),(a^2\gamma^2+\beta^2\delta^2)(ac^2-bd^2,bd^2(a+b)))$.

Тем же путем, каким мы получили все решения системы (1) с условием (2), могут быть получены и все решения того же типа системы с большим числом уравнений.

Литература: [1] Кожегельдинов С.Ш. Об основных героновых треугольниках//Мат. заметки. 1994. Т.55, вып.2.С.72-79. [2] Его же. Отыскание основных героновых треугольников/МИЭТ. М.,1990. No.4613. Деп. ВИНИТИ. [3] Его же. Параметризация основных героновых треугольников со взаимно простыми сторонами//Тез. докл. Межвуз. конф. посвящ. 70-летию со дня рожд. проф. Т.И. Аманова.-Семипалатинск. 1993. С.21-23. [4] Кожегельдинов С.Ш., Кожатаева М.Ж. К вопросу решения системы уравнений Пифагора//Там же. С.30-31.

УДК 511.5 Кожегельдинов С.Ш. (Семипалатинск)

ОБ ИСПОЛЬЗОВАНИИ АРИФМЕТИЧЕСКИХ ФУНКЦИЙ

В докладе рассматривается использование арифметических функций, имеющих фундаментальное значение при отыскании всех основных (а следовательно, и всех) решений некоторых диофантовых уравнений, ибо среди них существуют и такие (к таковым относится и уравнение Герона), все основные решения которых параметризировать алгебраическим образом, насколько нам известно, не удается [1-3], [4 а-з]. В нем рассматривается также использование арифметических функций и при отыскании всех основных решений некоторых систем таких уравнений с общей переменной. Например, использование арифметических функций позволяет параметризировать двенадцатью целыми параметрами все основные решения в натуральных числах следующей системы диофантовых уравнений с общей переменной z :

$$S^2=xyz(x+y+z),\quad z^2+t^2=z^2,\quad \frac{1}{f^2}+\frac{1}{g^2}=\frac{1}{z^2},\quad \ell^2+2h^2=z^2,\quad u^2-v^2+w^2=z^2,$$

для которой решение

$$S=13938365952000,\ x=6064800,\ y=4851840,$$

$$z=574560,\ Z=459648,\ t=344736,\ f=2052000,\ g=598500,$$

$$\ell=446880,\ h=255360,\ u=302400,\ v=131440,\ w=453600$$

является основным.

Использование арифметических функций значительно упрощает отыскание треугольника Ферма, т.е. пифагорова треугольника, у которого, гипотенуза и сумма катетов - квадраты.

Литература: [1] Dickson L.E. History of the Theory of Numbers. V.2. New York, 1966. [2] Оре О. Приглашение в теорию чисел. М.,1980. [3] Серпинский В. Пифагоровы треугольники. М., 1959. [4] Кожегельдинов С.Ш. а) Некоторые элементы теории диофантовых уравнений в упражнениях и задачах. М.,1993. б) Отыскание основных героновых треугольников (ГТ)//Изв. АН Республ. Казахстан. Сер. физ.-мат. Алма-Ата, 1992. No.3.-С.48-51. в) Об основных ГТ//Мат. заметки. 1994. Т.55, вып.2, С.72-79 . г) О тиановых треугольниках//Там же. Т.53, вып. 5.-С.155-157. д) О решении уравнений в натуральных числах//Тез. докл. Межвуз. конф., посвящ. 70-летию со дня рождения проф. Т.И.Аманова.-Семипалатинск, 1993.-С.17-19; е) О задаче Курциуса//Там же.-С.19-21. ж) Параметризация ГТ со взаимно простыми сторонами//Там же.-С.21-23. з) Об отыскании треугольника Ферма//Улылык онегеси: сб.материалов Республ. конф. "Абай. Современная культура и язык".-Семипалатинск, 1994.-С.361-367.

Несколько замечаний о форме Картана-Титца

Колмыков В.А.

1. Рассмотрим конечное дерево Кокстера T с весами ребер 3 (см.[1], гл.4, параграф 1, п.4) и его квадратичную форму Картана-Титца $B = B_T$ ([1], гл.5, параграф 4). Множество рассматриваемых деревьев Кокстера обозначим Γ. Множество $\hat{\epsilon}$ и графы Z_{pqr} определены в тезисах Колмыкова В.А., Кущова В.С., Субботина В.Ф., публикуемых в этом сборнике.

2. Введем меру отклонения нулевого конуса B^0 от диагонали координатного пространства: $\omega B = sup\{\alpha | (\forall i\ 1 \le x_i \le \alpha) \to B(x) > 0\}$.

В указанных выше тезисах и в работе [2] вычислено ωB как функция геометрических инвариантов дерева. Это позволяет доказать ряд содержательных утверждений о форме Картана-Титца. Определим $* : \Gamma \to \Gamma$ так: $Z^*_{pqr} = Z_{p+1,q+1,r+1}$, далее $T^* = T$, если $T \notin \hat{\epsilon}$. Множество деревьев, удовлетворяющих условию U, обозначается $\{U\}$.

3. *ТЕОРЕМА.*

1) $\{\omega B = \infty\} = \{B > 0\}$

2) $\{\omega B > 2\} = \{B > 0\} \cup \{B > 0\}^*$

3) $\{\omega B \in \mathbf{Z}\} = \{B \ge 0\} \cup \{B \ge 0\}^*$

ЛИТЕРАТУРА

1. Бурбаки Н. Группы и алгебры Ли. М., Мир, 1972.

2. Колмыков В.А. Топологическое строение множества отклонений форм Картана-Титца деревьев и схемы Дынкина. // Тезисы докладов 26 Воронежской зимней математической школы, Воронеж, изд-во ВГУ, 1994, с.57.

УДК 512.519.46

Колмыков В.А., Кущов В.С. (Воронеж)

ОБ ОДНОЙ КВАДРАТИЧНОЙ ФОРМЕ НА ЦЕЛОЧИСЛЕННЫХ КУБАХ

Рассматриваются конечные связные графы Кокстера с весами ребер, равными 3. Форма Картана-Титца графа Кокстера определена в [1], гл.У, § 4. Положим $K(n,m)=\{x\in R^5 \mid n\le x_i\le m\}$, $n,m\in N$. Мы уже решили графовое неравенство $B|_K>0$ для $m/n\ge 4$, см. [2]. Для дальнейшего исследования нам понадобится

ЛЕММА. Пусть $3{,}5<m/n<4$, $n\neq 3$,

$B=x_1^2+\dots+x_{10}^2-(x_1x_2+x_2x_3+\dots+x_8x_9)-x_3x_{10}$.

Тогда $B|_K\neq 0$.

Доказательство. Положим $n, m, c, x_1, x_2, c_1, c_2, \dots, c_5$ как указано в таблице, $x_3=m$, $x_{10}=[m/2]$, $x_4=x_3-c$, $x_{i+4}=x_{i+3}-c_i$, $1\le i\le 5$. Соответствующие значения $B(x)$ указаны в последнем столбце таблицы

n	m	x_1	x_2	c	c_1	c_2	c_3	c_4	c_5	$B(x)$
12e+1	42e+4	14e+1	28e+3	5e+1	c	c	c-1	c-1	c-1	1-e
12e+2	42e+8	14e+2	28e+5	5e+1	c	c	c	c	c	-2e
12e+3	42e+11	14e+3	28e+7	5e+1	c	c	c	c+1	c+1	1-e
12e+4	42e+15	14e+5	28e+10	5e+2	c	c	c	c	c-1	-2e
12e+5	42e+18	14e+6	28e+12	5e+2	c	c	c	c	c+1	- e
12e+6	42e+22	14e+7	28e+14	5e+2	c	c+1	c+1	c+1	c+1	-2e
12e+7	42e+25	14e+8	28e+16	5e+3	c	c	c	c	c	- e
12e+8	42e+29	14e+9	28e+19	5e+3	c	c	c+1	c+1	c+1	-2e
12e+9	42e+32	14e+10	28e+21	5e+4	c	c	c	c	c-1	- e
12e+10	42e+36	14e+12	28e+24	5e+4	c	c	c	c+1	c+1	-2e-1
12e+11	42e+39	14e+13	28e+26	5e+5	c	c	c	c-1	c-1	- e
12e+12	42e+43	14e+14	28e+28	5e+5	c	c	c	c	c+1	-2e-1

ЛИТЕРАТУРА

1. Бурбаки Н. Группы и алгебры Ли. М., Мир, 1972.
2. Колмыков В.А., Кущов В.С., Субботин В.Ф. О поведении формы Картана-Титца на целочисленных кубах //Тез.докл. школы "Современные методы теории функций и смежные проблемы математики и механики", Воронеж, 1995, С.126.

УДК 512.519.46

Колмыков В.А., Кущов В.С., Субботин В.Ф.(Воронеж)

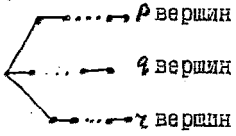
О РАСПОЛОЖЕНИИ НУЛЕВОГО КОНУСА ФОРМЫ КАРТАНА-ТИТЦА

I. Пусть G – конечный связный граф Кокстера [I], гл. IV, § I, п.9. Квадратичная форма Картана-Титца B_G определена в [I], гл.У § 4, п.I. Мы будем рассматривать только графы Кокстера с весами ребер 3 (в этом случае B_G – целочисленная).

2. Для дерева T введем меру отклонения нулевого конуса B_G^0 от диагонали координатного пространства:

$$\omega(T) = \sup\{\alpha \mid (\forall i \quad 1 \le x_i \le \alpha) \Rightarrow B_T(x) > 0\}$$

3. Определим класс $\hat{\mathcal{E}}$: он состоит из графов, не содержащих $\hat{A}_n$, $\hat{\mathcal{D}}_n$; или по-другому: он состоит из деревьев, не содержащих $\hat{\mathcal{D}}_n$; или так: он состоит из графов Z_{pqr} $0 \le p \le q \le r$:



Гармонией Z_{pqr} назовем число $\gamma = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1 \in \mathbb{R}$. Положим

$\hat{\mathcal{E}}_6 = \{T \in \hat{\mathcal{E}} \mid \hat{E}_6 \le T\} = \{Z_{pqr}\}_{2 \le p}$, $\hat{\mathcal{E}}_7 = \{T \in \hat{\mathcal{E}} \setminus \hat{\mathcal{E}}_6 \mid (\hat{E}_7 \le T) \vee (\hat{E}_8 \le T$

и число вершин $\sigma(T) \ge 12)\} =$

$= \{Z_{pqr}\}$, (ГДЕ $p=1, q \ge 3$ или $p=1, q=2, r \ge 8$), $\hat{\mathcal{E}}_8 = \{T \in \hat{\mathcal{E}} \setminus$

$\setminus \hat{\mathcal{E}}_6 \setminus \hat{\mathcal{E}}_7 \mid \hat{E}_8 \le T\} = \{Z_{122}\}_{r=5,6,7}$. $\mathcal{P} = \hat{\mathcal{E}} \setminus \hat{\mathcal{E}}_6 \setminus \hat{\mathcal{E}}_7 \setminus \hat{\mathcal{E}}_8 = \{A_n, D_n, E_6, E_7, E_8\}$

– схемы Дынкина.

ТЕОРЕМА. а) $T \in \hat{\mathcal{E}}_6 \Rightarrow \omega = (\gamma+1)/(\gamma+1-\sqrt{1-2\gamma})$

б) $T \in \hat{\mathcal{E}}_7 \Rightarrow \omega = (\gamma+2)/(\gamma+\sqrt{1-3,5\gamma})$

в) $T \in \hat{\mathcal{E}}_8 \Rightarrow \omega = (2\gamma+1)/(2\gamma-1+\sqrt{7/3-10\gamma/3})$

г) $T \in \mathcal{P} \Rightarrow \omega = \infty$.

Работа [2] состоит из доказательства этой теоремы.

ЛИТЕРАТУРА

I. Бурбаки Н. Группы и алгебры Ли. М., Мир, 1972.

2. Колмыков В.А., Кущов В.С., Субботин В.Ф. Об одном инварианте формы Картана-Титца. Деп. в ВИНИТИ, № 122-В.94, 15 с.

УДК 511.336

С.В. Конягин (Москва)

О РАСПРЕДЕЛЕНИИ ДРОБНЫХ ДОЛЕЙ ЧЛЕНОВ НЕКОТОРЫХ ГЕОМЕТРИЧЕСКИХ ПРОГРЕССИЙ

Для простых r и $l \equiv 1 \pmod r$ фиксируем такой вычет $g = g_{l,r}$ по модулю l, что $g \not\equiv 1 \pmod l$ и $g^r \equiv 1 \pmod l$. Для $u \in \mathbb{R}$ обозначим $\|u\| = \inf_{n\in\mathbb{Z}} |u - n|$. Величина $I(h)$ при $0 < h \le 1/2$ определена в [1].

Теорема. *Пусть $0 < h \le 1/2$, $r \to \infty$. Тогда для всех l, за исключением не более $(I(h) + o(1))^{-r}$ значений, для любых действительных $u_0, u_1, \dots, u_{r-1}$ найдется такое целое число a, что $\|ag^j/l - u_j\| < h$ при $j = 0, 1, \dots, r-1$.*

В связи с рассмотрением суперсингулярности над F_p гиперэллиптических кривых вида $y^2 = x^l + \lambda$, $\lambda \ne 0$ интерес в теореме представляет случай $h = u_0 = u_1 = \dots = u_{r-1} = 1/4$[2].

Теорема доказывается аналогично теореме 4.5 из [3].

Работа поддержана грантом N. MC5300 Международного Научного Фонда.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[1] Н.Н. Андреев, А.Ю. Попов, 'Экстремальные задачи для функций с малым носителем', наст. сборник.

[2] T. Washio and T. Kodama, 'A Note on a Supersingular Function Fields', *Sci. Bull. Fac. Education Nagasaki Univ.*, **37** (1986), 9–15.

[3] S. Konyagin and I. Shparlinski, 'On the distribution of residues of finitely generated multiplicative groups and some their applications', *Macquarie Math. Report 95-172C, Macquarie Univ.*, 1995.

ОБ ОДНОЙ ЭКСТРЕМАЛЬНОЙ ЗАДАЧЕ ТЕОРИИ ЧИСЕЛ

Копылов Г.Н.
Волгоградский госуниверситет

Пусть n — натуральное число. Множество натуральных чисел, меньших n, называется *хорошим*, если какая-то сумма его элементов делится на n без остатка. Через $f(n)$ обозначим минимальное k, гарантирующее, что любое множество из k натуральных чисел меньших n наверняка является хорошим для данного n.

Очевидно, что множество чисел от 1 до k не будет хорошим, если

$$(k+1)k/2 < n,$$

так как сумма этих чисел меньше n.

С другой стороны, из пары p, $n-p$ в нехорошее множество может входить только одно число. Таким образом,

$$(\sqrt{1+8n}-1)/2 < f(n) \le n/2+1. \tag{1}$$

Доказано (см. [1]), что существует абсолютная постоянная $C > 0$, такая что $f(n) \le C\sqrt{n}$ для любого n. Известно

Предположение. Асимптотика функции f определяется нижней оценкой неравенства (1).

При $n = 100$ оценки (1) дают

$$13 < f(n) \le 51.$$

Теорема.

$$f(nk) \le nf(k).$$

Для решения задачи с помощью ЭВМ В. Бонелисом была написана переборная программа, позволившая получить точные результаты при $n < 53$. Все полученные результаты совпадали с нижней оценкой или отличались от нее на 1. Не подтвердилось предположение о монотонности функции f ($f(42) = 10 > f(43) = 9$).

Назовем пример *стандартным*, если числа 1, 2, ..., k образуют максимальное возможное при данном n плохое множество.

Приведем результаты, полученные с помощью ЭВМ. Стандартные примеры: 5, 7, 8, 11–13, 16–19, 22–24, 29–33, 37–41, 43, 46–51; нестандарные примеры: 6, 9, 10, 14, 15, 20, 21, 25–28, 34–6,42, 44, 45, 52.

Удалось несколько улучшить оценки для $f(100)$. Так как $f(50) = 10$, то $f(100) \le 2f(50) = 20$.

С другой стороны, числа 1, 2, 3, 4, 5, 6, 7, 50, 51, 52, 53, 54, 55, 56 образуют плохой набор из 14 чисел.

Таким образом,

$$14 < f(100) \le 20.$$

Литература

1. П. Эрдеш. Некоторые проблемы теории чисел // В книге "Вычисления в алгебре и теории чисел". М.: Мир. 1976. с. 202–212.

ОБ ОДНОЙ ЭКСТРЕМАЛЬНОЙ ЗАДАЧЕ ТЕОРИИ ЧИСЕЛ

Копылов Г.Н., Бонелис В.Д.
Волгоградский госуниверситет

Пусть n - натуральное число. Множество натуральных чисел, меньших n, называется хорошим, если какая-то сумма его элементов делится на n без остатка. Через f(n) обозначим минимальное k, гарантирующее, что любое множество из k натуральных чисел меньших n наверняка является хорошим для данного n.

Очевидно, что множество чисел от 1 до k не будет хорошим, если

$$(k+1)*k/2 < n,$$

так как сумма этих чисел меньше n.

С другой стороны из пары p, n-p в нехорошее множество может входить только одно число. Таким образом

$$(\mathrm{sqrt}(1+8n) - 1)/2 < f(n) <= n/2 + 1 \qquad (1)$$

Известно (см.[1]), что существует константа c, что

$$f(n)<=c\ n$$

При n = 100 оценки (1) дают

$$13 < f(n) <= 51.$$

Теорема. $f(n*k) <= n*f(k)$.

Для решения задачи с помощью ЭВМ написана переборная программа, позволившая получить точные результаты при n < 53. Все полученные результаты совпадали с нижней оценкой или отличались от нее на 1. Не подтвердилось предположение о монотонности функции f. f(42) = 10 > f(43) = 9.

Назовем пример стандартным, если числа 1, 2, ..., k образуют максимальное возможное при данном n плохое множество.

Приведем результаты, полученные с помощью ЭВМ.
Стандартные примеры: 5,7,8,11-13,16-19,22-24,29-33,37-41,43,46-51;
нестандартные примеры: 6,9,10,14,15,20,21,25-28,34-36,42,44,45,52.

Удалось несколько улучшить оценки для f(100).
Так как f(50) = 10, то f(100) <=2f(50) = 20.

С другой стороны, числа 1,2,3,4,5,6,7,50,51,52,53,54,55,56 образуют плохой набор из 14 чисел.
Таким образом

$$14 < f(100) <= 20.$$

Литература

1. П.Эрдеш. Некоторые проблемы теории чисел. // В книге "Вычисления в алгебре и теории чисел", М.,"Мир",1976,с.202-212.

УДК 5II.8

Е.Г. КОЦАРЕВ (МОСКВА)

О СРЕДНЕМ ЗНАЧЕНИИ МОДУЛЯ ТРИГОНОМЕТРИЧЕСКИХ СУММ

Пусть n, t, s, P – натуральные числа. Хуа Ло-Кен [I] доказал, что при $t \geqslant t_0$, $s \geqslant s_0$ для любого $\varepsilon > 0$ имеют место неравенства

$$\int_0^1 \dots \int_0^1 \left| \sum_{x=1}^{P} \exp 2\pi i (\alpha_1 x + \dots + \alpha_n x^n) \right|^{2t} d\alpha_1 \dots d\alpha_n \ll \ll P^{2t - \frac{1}{2}n(n+1)+\varepsilon},$$

$$\int_0^1 \dots \int_0^1 \left| \sum_{x=1}^{P} \exp 2\pi i (\alpha_1 x + \dots + \alpha_{n-2} x^{n-2} + \alpha_n x^n) \right|^{2s} d\alpha_1 \dots d\alpha_n \ll \ll P^{2s - \frac{1}{2}(n^2 - n + 2)+\varepsilon},$$

где числа t_0, s_0 определяются таблицей

n	2	3	4	5	6	7	8	9	I0
t_0	3	8	28	55	I20	207	336	540	
s_0		5	I6	43	I04	I75	272	4I2	629

На основе новых результатов в теореме Виноградова о среднем /см. [2] и цитированную там литературу/ получено усиление результата Хуа Ло-Кена при $n \geqslant 6$.

ТЕОРЕМА [3]. Величины t_0, s_0 могут быть определены следующей таблицей:

n	6	7	8	9
t_0	II7	200	326	522

n	6	7	8	9	I0
s_0	I0I	I68	262	394	607

Литература

I. Hua Loo-Keng. Additive Primzahltheorie // Leipzig, 1959.

2. Тырина О.В. Новая оценка тригонометрического интеграла И.М. Виноградова Изв.АН СССР.Сер.мат., I987.-Т.5I,№ 2,с.363-378.

3. Коцарев Б.Г. О среднем значении модуля сумм Вейля невысокой степени М., I994. – 28 с. – Деп. в ВИНИТИ, № I656 – В 94.

УДК 007.5:535:681.518

Коржик Ю.В., Костылев В.И. (Воронеж)

МЕТОДЫ ТЕКСТУРНОЙ ПАРАМЕТРИЗАЦИИ ИЗОБРАЖЕНИЙ В СИСТЕМАХ ОБРАБОТКИ И ХРАНЕНИЯ ВИДЕОИНФОРМАЦИИ

При решении многих задач, связанных с разработкой автоматизированных систем анализа сложноструктурных изображений, все большее применение находят статистические методы. Они позволяют оперативно формировать признаки для сегментации изображения, распознавания его фрагментов и могут быть использованы в системах обработки и хранения информации для представления сложноструктурных изображений в виде пространственной совокупности статистически однородных фрагментов. Получаемое при подобной параметризации сокращенное описание сложноструктурного изображения может быть использовано для оперативной классификации больших массивов изображений в системах анализа и хранения видеоинформации.

В докладе предлагается и исследуется новый метод текстурной параметризации изображений, основанный на формировании структурно-статистических функционалов при сканировании изображения. Теоретически найдено оптимальное число текстурных признаков, позволяющих проводить анализ сложной информации и дающих ее достаточно полное описание. В качестве функционалов рассматривается число локальных экстремумов функции яркости, число выбросов за заданный опорный уровень и площадь опорной поверхности текстурного фрагмента изображения. Проведено сравнение предлагаемого метода текстурной параметризации с наиболее эффективными из известных методов.

Особенностью предложенного метода параметризации является то, что он сохраняет высокую эффективность при частичном или даже полном отсутствии априорной информации об анализируемых фрагментах изображения. Теоретически сделаны оценки среднего значения и дисперсии признаков-функционалов для фрагментов изображений с различными статистическими свойствами. Сделана оценка эффективности предложенного метода в зависимости от относительных размеров фрагмента изображения. Проведено исследование возможности сегментации изображений, обладающих сильными анизотропными свойствами.

Работа выполнена в Воронежском государственном университете при финансовой поддержке Российского фонда фундаментальных исследований (проект N 94-01-01503).

УДК 511

Кочетков К.П., Пантелеева Е.И. /Москва, МПУ/

О ЧИСЛЕ ЦЕЛЫХ ТОЧЕК В ЭЛЛИПСЕ

Начиная с проблемы Гаусса о числе целых точек в круге и проблемы делителей Дирихле /о числе целых точек под гиперболой/, проблема о числе целых точек в некоторой замкнутой области принадлежит к ряду классических задач теории чисел.

В работах Гаусса для числа $K(R)$ целых точек в круге радиуса R с центром в начале координат была получена асимптотическая формула с главным членом πR^2 и остаточным членом $\Delta(R)=O(R^\kappa)$, $\kappa=1$

Метод И.М.Виноградова оценки тригонометрических сумм позволил улучшить оценку $\Delta(R)$, именно, заменить $\kappa=1$ на $\kappa=\frac{2}{3}+\varepsilon$ и даже на $\kappa=\frac{2}{3}-\frac{1}{132}+\varepsilon$. Точнее, для $\Delta(R)$ верна оценка $O(R^\kappa \ln R)$, $\kappa=\frac{2}{3}-\frac{1}{132}$.

Рассмотрим эллипс с центром в начале координат и полуосями a и b, ориентированными по осям координат. Для числа целых точек $\Im(a,b)$ в указанном эллипсе нами получена асимптотическая формула с главным членом πab и остаточным членом $\Delta(a,b)=O((ab)^\kappa)$, где метод Гаусса дает значение $\kappa=\frac{1}{2}$, а метод И.М.Виноградова - значение $\kappa=\frac{1}{3}-\frac{1}{264}+\varepsilon$. Точнее, для $\Delta(a,b)$ верна оценка $O((ab)^\kappa \ln(ab))$, $\kappa=\frac{1}{3}-\frac{1}{264}$, что является обобщением результата, полученного для числа целых точек в круге.

Литература: [1] Карацуба А.А. Основы аналитической теории чисел. М., Наука, 1983. [2] Виноградов И.М. Особые варианты метода тригонометрических сумм. М., Наука, 1976.

УДК 621.3

Кравец О.Я., Мачтаков С.Г. (Воронеж)

О НЕКОТОРЫХ АЛГОРИТМИЧЕСКИХ СРЕДСТВАХ, ОБЕСПЕЧИВАЮЩИХ ПОВЫШЕННЫЙ УРОВЕНЬ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ ЭВМ

Развитие современных сетей интегрального обслуживания, разнородный характер информации, циркулирующей в них, различный уровень ее конфиденциальности предопределяют необходимость решения проблем, связанных с защитой данной информации. Традиционные криптографические методы, по видимому, целесообразно дополнить некоторыми алгоритмическими средствами поиска, идеей фрагментирования блоков данных и принципом стохастического местоположения информации в сети, снижающим вероятность ее несанкционированного обнаружения.

Однако стохастическое расположение информации требует наличия специальных алгоритмических средств поиска и транспортировки данных. Наиболее приемлемыми оказались средства, основанные на использовании класса лавинных алгоритмов как наиболее быстрых в смысле поиска информации с недетерминированным положением. Вместе с тем лавинные алгоритмы обладают существенным для сетей интегрального обслуживания недостатком - большой избыточностью служебной информации. В докладе рассматриваются методы уменьшения избыточности, основанные на принципе "обратной волны" и порожденные следующей задачей оптимального управления поиском в распределенных системах:

$$\sum_{m=0}^{N-1}\sum_{i=1}^{N}\sum_{j=1}^{N} S_{ij}*|\mathrm{sign}(\vartheta_{ij,m})| \longrightarrow \min ,$$

$$\sum_{i=1}^{N}\sum_{j=1}^{N} S_{ij} = \mathrm{const},$$

где

$$\vartheta_{ij,m+1}=\begin{cases}\xi_{j,m+1}, & \text{если } i\in\Omega_j\setminus\Gamma_{j,m+1},\\ 0, & \text{если } i\in\Gamma_{j,m+1};\end{cases} \qquad \xi_{j,m+1}=\sum_{i=1}^{N} S_{ij}*\vartheta_{ij,m} ;$$

$\xi_{j,1}=\Psi_-$; $\xi_{i,1}=0\ \forall i\neq j, i=1..N$; $\exists(j,m):(\xi_{j,m}=\Psi_-)\rightarrow(\xi_{j,m+1}=\Psi_+)$;

$\Gamma_{j,m+1}=\{i\in\Omega_j:\vartheta_{ij,m}=\xi_{j,m+1}\}$; $\Gamma_{j,0}=\varnothing$; $\Omega_i=\{k:S_{ik}\neq 0, k=1..N\}$;

$\{S_{ij}\}$ - матрица смежности N-узлового графа; const - количество каналов связи; Ψ_- и Ψ_+ - аксиоматически определенные объекты со свойствами поглощения нуля и единицы, причем $\Psi_-+\Psi_+=\Psi_+$.

Работа выполнялась при поддержке РФФИ.

УДК 511.9

Крылов В.Е. (Владимир)

О ПРЕДСТАВЛЕНИИ ЧИСЕЛ БИНАРНЫМИ ЦИКЛИЧЕСКИМИ ФОРМАМИ

Пусть группа собственных классов положительно определённых целочисленных бинарных квадратичных форм дискриминанта $D<0$ будет циклической, f_1 -её образующая и пусть $f_i=f_1^i\ (i=1,2,\dots,h-1)$ Обозначим $r(f_i,m)$ количество целых представлений натурального числа m формой f_i и разложим m в произведение чисел m_0, m_-, m_+ состоящих из простых сомножителей p со значениями характера $\chi_1(p)$ поля $Q(\sqrt{D})$ соответственно $0,-1,+1$. Для любого p с $\chi_1(p)=+1$ положим $a(p)=i$, если $r(f_i,p)>0$.

Теорема 1. Число m представляется какой-то формой $f_i, i=1,2,\dots,h-1$, тогда и только тогда, когда m_--квадрат. Если $D<-4$, то в этом случае

$$r(f_i,m)=2r(i,m),$$

при этом $r(i,m)$ -число решений сравнения

$$\sum_{j=1}^{n} a(p_j)(2x_j-d_j)+\sum_{t=1}^{\ell} a(q_t)\delta_t \equiv i \pmod h,\quad 0\le x_j\le d_j,$$

где $m_+=p_1^{d_1}p_2^{d_2}\dots p_n^{d_n}$, $m_0=q_1^{\delta_1}q_2^{\delta_2}\dots q_\ell^{\delta_\ell}$ -разложения в произведения степеней различных простых делителей.

Теорема 2. Существует натуральное число m с условиями

$$r(f_0,m)=r(f_1,m)=\dots=r(f_{h-1},m)>0$$

в том и только в том случае, если порядок h группы классов нечётен.

Литература

[1]. Боревич З.И., Шафаревич И.Р. Теория чисел, М; Наука, 1984.

[2]. Крылов В.Г. Элементарная теория чисел Гекке, Владимир, 1988.

УДК 621.33 Крючков А.Н.,Абузова И.В. (Россия,Тула)

Обеспечение требуемой надежности при передаче сигнала во времени

В настоящее время увеличивается объем информации, подлежащей хранению, это и медицинская информация, так как меняется среда жизнедеятельности человека, и технологическая документация, и оборонная информация. На фоне этого резко возрастают требования по надежности восстановления полезной информации после окончания сроков хранения.

Основной особенностью передачи сигнала во времени является большая вероятность мощных непредсказуемых помех. Поэтому доклад посвящен разработке основных принципиальных подходов и инструментальных средств для обеспечения максимальной надежности восстановления полезной информации в системах длительного хранения.

Сущность математического аппарата заключается в использовании традиционных средств борьбы с помехами, таких как помехоустойчивое кодирование, в комбинации с методами распознавания образов. Причем обратная связь осуществляется с помощью самообучения систем распознавания, где в качестве обучающей выборки используются результаты декодирования. Представлено практическое применение предложенных теоретических положений.

Обосновывается целесообразность применения кода Файра при хранении двоичной информации на микрофильме. Распознавание образов осуществляется на основе критерия Байеса, а декодирование по теореме Меггита. Разработанный программный комплекс самонастраивается в зависимости от характеристик носителя информации.

Программное обеспечение разработано для ЭВМ типа IBM PC AT, операционная среда WIDOWS, на языке высокого уровня Си ++. При проведении экспериментов надежность восстановления полезной информации была достигнута 0,99999.

УДК 511.9

Кубенский М.Н. / С.-Петербург/

Об индексе подпорядка.

Пусть $\mathcal{A}$ простая центральная алгебра размерности n^2 над алгебраическим числовым полем k ; R – кольцо целых поля k . Будем через $N\mathfrak{m}$ обозначать абсолютную норму идеала $\mathfrak{m}$ кольца R .

ТЕОРЕМА. Если $\mathcal{O} \subset \mathcal{O}_1$ два порядка в $\mathcal{A}$ и $\nu = [\mathcal{O}_1 : \mathcal{O}]$ – индекс одного порядка в другом. Пусть $\mathfrak{p}$ простой идеал в R и $N\mathfrak{p}^{n^2-n+1} \mid \nu$ . . Тогда существует такой порядок $\mathcal{O}_2$, что $\mathcal{O} \subset \mathcal{O}_2 \subset \mathcal{O}_1$ и $[\mathcal{O}_2 : \mathcal{O}] \mid N\mathfrak{p}^{n^2-n}$

Эта теорема обобщает лемму из работы Лолла [2]. Она может быть использована для последовательного перечисления порядков в простых центральных алгебрах, как это делается для случая когда $\mathcal{A}$ – алгебра кватернионов над $\mathbb{Q}$ – поле рациональных чисел.

Лит.: 1 Пирс Р. Ассоциативные алгебры. М.: Мир, 1986г.
2 Pall G. On Generalized Quaternions Trans. Amer. Math. Socien., 1946, N2, pp. 280-332
3 Reiner I. Maximal Orders, A.P, 1975

УДК 511.3

Кудинов А. Ф. (Воронеж)

О РЕШЕТЕ ЭРАТОСФЕНА

В работе получены формулы, аналогичные формуле решета Эратосфена. ОБОЗНАЧЕНИЯ: $\overline{\Pi}(x)$ - количество простых чисел $p_k \le x$; $\varphi(n,x)$ - количество натуральных чисел $k \le x$ взаимно простых с n; $[\beta]$ - целая часть β; $[n,m]$ - н.о.к. натуральных чисел n и m.

$$\overline{\Pi}(x) - \overline{\Pi}(\sqrt{x}) + 1 = x + \sum_{k \ge 1} (-1)^k \sum_{2 \le i_1 < \dots < i_k \le \sqrt{x}} \left[\frac{x}{[i_1, \dots, i_k]} \right];$$

$$\overline{\Pi}(x) = \sum_{k \ge 1} (-1)^{k-1} k \sum_{2 \le i_1 < \dots < i_k \le x} \left[\frac{x}{[i_1, \dots, i_k]} \right];$$

$$\left[\frac{x}{p_1 p_2 \cdots p_{\overline{\Pi}(\beta)}} \right] = x + \sum_{k \ge 1} (-1)^k \sum_{2 \le i_1 < \dots < i_k \le \beta} \varphi(i_1, i_2 \cdots i_k, x)$$

Литература

Бухштаб А.А. Теория чисел, М., 1960.

УДК 511.3

Кудрявцев М.В. (Саратов)

МОДИФИКАЦИЯ ЛЕММЫ ХУА О РАЗБИЕНИИ

Пусть p – простое, $\mathbb{O}_p$ – кольцо целых p-адических единиц; $\chi(\bar{x}) = \chi(x_1,\dots,x_n) = \chi_1(x_1)\dots\chi_n(x_n)$, где $\chi_i(x_i)$ – либо характер Дирихле по модулю p, либо χ_i – тождественная единица,

$$F = F(x_1,\dots,x_n) = \sum_{\langle i_1,\dots,i_n\rangle} a_{i_1,\dots,i_n} x_1^{i_1}\dots x_n^{i_n} \in \mathbb{O}_p[[x_1,\dots,x_n]]$$

– аналитическая функция от n переменных $x_1,\dots,x_n$ (см. [1]), такая, что $F(\bar{x}) - F(\bar{0})$ – локально примитивная функция. Обозначим

$$\tau_i = \min_{i_j \ge 1} \operatorname{ord}_p(i_j a_{i_1,\dots,i_j,\dots,i_n}) \ (1 \le i \le n), \quad h_i(\tau_i) = \begin{cases} 0, & \text{если } \tau_i = 0, \\ 1, & \text{если } \tau_i \ge 1 \end{cases}$$

$$\nu_i = \nu_i(F',p) = 1 + h_i(\tau_i)\operatorname{ord}_p 2, \quad f_i(\bar{x}) = p^{-\tau_i}\frac{\partial F}{\partial x_i}(\bar{x}) \quad (1 \le i \le n).$$

Обозначим множество решений системы сравнений

$$\begin{cases} f_1(x_1,\dots,x_n) \equiv 0 \ (\mathrm{mod} p^{s_1}), \\ \dots\dots\dots\dots\dots\dots \\ f_n(x_1,\dots,x_n) \equiv 0 \ (\mathrm{mod} p^{s_n}), \end{cases} \quad \begin{cases} x_1 \equiv 0 \ (\mathrm{mod} p^{s_1}), \\ \dots\dots\dots\dots \\ x_n \equiv 0 \ (\mathrm{mod} p^{s_n}) \end{cases} \qquad (1)$$

через $K = K(\bar{x}, s_1,\dots,s_n)$, где $s_1 \ge 1, \dots, s_n \ge 1$ – целые. Положим

$$S(F;\chi;p^\alpha) = \sum_{\langle x_1,\dots,x_n\rangle \bmod p^\alpha} \chi(x_1,\dots,x_n)\exp\left\{\frac{2\pi i}{p^\alpha}F(x_1,\dots,x_n)\right\},$$

где суммирование проводится по всем наборам $\langle x_1,\dots,x_n\rangle$ таким, что x_i пробегает НСВ по $\mathrm{mod} p^\alpha$. Положим $\tau = \max\limits_{1\le i\le n} \tau_i$, $\nu = \max\limits_{1\le i\le n} \nu_i$.

Теорема. Пусть $\alpha \ge \tau + \nu + 1$ – целое, $1 \le s_i \le \alpha - 1$ $(1 \le i \le n)$. Тогда

$$S(F;\chi;p^\alpha) = \sum_{\langle x_1,\dots,x_n\rangle \bmod p^\alpha:\ \bar{x}\in K} \chi(\bar{x})\exp\left\{\frac{2\pi i}{p^\alpha}F(\bar{x})\right\}.$$

Причем, если система сравнений (1) неразрешима, то $S(F;\chi;p^\alpha) = 0$.

Литература.

1. Серр Ж.П. Алгебры Ли и группы Ли.–М.:Мир, 1969.
2. Гусев Г.И. К гипотезе о рядах Пуанкаре // Математ. заметки.–1973.–Т.14, N 3.–С.453-463.

Кузнецов Н.В.

РИМАНОВА ДЗЕТА-ФУНКЦИЯ И АВТОМОРФНЫЕ ФОРМЫ

В 80-х - 90-х годах XX века сформировалось новое направление в теории Римановой дзета-функции, в основе которого лежат "формулы следа Петерсона-Кузнецова". Открытие этих формул стало возможным после установления классической "формулы следа Сельберга"; они суть праэлементы сельберговской формулы следа, которая в случае модулярной группы и ее конгруенц-подгрупп является их следствием.

Формулы следа Петерсона-Кузнецова послужили основой новых методов, с помощью которых Г.Иванец, Ж.Дезуйе, П.Сарнак, М.Хаксли В.Быковский, И.Мотохаши и многие другие получили блестящие результаты в аналитической теории чисел и в теории параболических форм.

Главные результаты этого направления пока еще принадлежат будущему (возможно, не очень далекому). Здесь впервые открывается реальная возможность установить истинный порядок дзета-функции Римана на критической прямой и одновременно доказать аналог гипотезы Линделефа для рядов Гекке, ассоциированных с параболическими формами веса нуль.

ЛИТЕРАТУРА

N.V.Kuznetsov, Sums of Kloosterman sums and the eigth power moment of the Riemann zeta-function, in: Number theory and related topics, Oxford Univers. press, 1989, p.57-117

УДК 511

КУЛМАТОВ А.К. (Ташкент)

О КОНЕЧНОСТИ ЧИСЛА КЛАССОВ КВАДРАТИЧНЫХ ФОРМ ТИПА ЛИУВИЛЛЯ И ТИПА А.ВЕЙЛЯ

Автором доказаны теоремы :

I. О конечности числа классов примитивных положительных квадратичных форм $Q(x_1,\dots,x_n)$ типа Лиувилля с целочисленной симмет - ричной матрицей порядка n ($n\geqslant 4$; n - четное), определителя $d=2^{\alpha}\Delta_1^2$ ($\alpha\geqslant 0$ - целое , Δ_1 - нечетное) с условием $(x_1,\dots,x_n)\equiv \equiv(b_1,\dots,b_n)(mod\, g)$.

2. О конечности числа классов примитивных положительных квадратичных форм $Q(x_1,\dots,x_n)$ типа Лиувилля с целочисленной симмет - ричной матрицей порядка n ($n\geqslant 5$, n - нечетное) с условием $(x_1,\dots,x_n)\equiv(b_1,\dots,b_n)(mod\, g)$.

3. О конечности числа классов примитивных положительных квaтернарных квадратичных форм $Q(x_1,x_2,x_3,x_4)$ типа А.Вейля в узком смысле , определителя $d=2^{\beta}\Delta_2^2$ ($\beta\geqslant 0$ - целое , Δ_2 - нечетное), с условием $(x_1,x_2,x_3,x_4)\equiv(b_1,b_2,b_3,b_4)(mod\, g)$.

Эти теоремы обобщают некоторые соответствующие известные результаты Когана Л.А.[1].

ЛИТЕРАТУРА

I. Коган Л.А. , Тошпулатов Б.Т. , Дусумбетов А.Д. Представление чисел квадратичными формами , Ташкент ; Фан , 1989 . - 131 с.

УДК 511

Лауринчикас А. (Вильнюс)

РАВНОМЕРНЫЕ ОЦЕНКИ ДЛЯ ВТОРОГО МОМЕНТА ДЗЕТА-ФУНКЦИИ РИМАНА

Пусть $\zeta(s)$, $s = \sigma + it$, обозначает дзета-функцию Римана и для $\sigma > \frac{1}{2}$

$$E_\sigma(T) = \int_0^T |\zeta(\sigma + it)|^2 dt - \zeta(2\sigma)T - (2\pi)^{2\sigma-1}(2-2\sigma)^{-1}\zeta(2-2\sigma)T^{2-2\sigma}.$$

К. Матсумото [1] для фиксированных σ, $\frac{1}{2} < \sigma < \frac{3}{4}$, получил оценку

$$E_\sigma(T) = O(T^{\frac{1}{1+2\sigma}} \log^2 T).$$

Имеются более точные оценки для $E_\sigma(T)$ во всей полосе $\frac{1}{2} < \sigma < \frac{3}{4}$. Мы получили равномерную оценку для $E_\sigma(T)$. Пусть $\delta = 2\sigma - 1$ и $\beta_T = \min(\delta^{-1}, \log T)$.

ТЕОРЕМА 1. Равномерно по σ, $\frac{1}{2} < \sigma < \frac{3}{4}$,

$$E_\sigma(T) \ll O(T^{\frac{1}{3+2\delta}} \beta_T^{\frac{4(1+\delta)}{3+2\delta}} (\log T)^{\frac{2(1+\delta)}{3+2\delta}}).$$

Теперь пусть опять для $\sigma > \frac{1}{2}$

$$\int_2^T E_\sigma^2(t)\,dt = \frac{2}{5-4\sigma}(2\pi)^{2\sigma-\frac{3}{2}} \frac{\zeta^2\left(\frac{3}{2}\right)}{\zeta(3)} \zeta\left(\frac{5}{2} - 2\sigma\right) \times \zeta\left(\frac{1}{2} + 2\sigma\right) T^{\frac{5}{2}-2\sigma} + F_\sigma(T).$$

Известно [1], что для фиксированных σ, $\frac{1}{2} < \sigma < \frac{3}{4}$,

$$F_\sigma(T) = O(T^{\frac{3}{4}-\sigma} \log T).$$

Имеет место следующая равномерная оценка.

ТЕОРЕМА 2. Равномерно по σ, $\frac{1}{2} < \sigma < \frac{3}{4}$,

$$F_\sigma(T) = O(T^{\frac{3}{4}-\delta} \beta_T \log T).$$

Литература

1. K. Matsumoto, The mean square of the Riemann zeta-function in the critical strip, Japan J. Math., 15, No 1, 1989, 1-13.

DEPRESSION AND ESTIMATES OF EXPONENTIAL SUMS

C.L. Liu

1. Estimates of trigonometric Sums and Character Sums.

For a trigonometric sum modulo a power of a prime number, it is observed that the classical induction process goes further when the prime number is less than the degree of the polynomial in the sum. Sharper estimates for these sums are then established. Parallel results for complete character sums are established.

2. Depression of Lifting of a Exponential Sum

For each natural number m a trigonometric sum S modulo a power of a prime number can be lifted to a trigonometric sum $S(m)$ in the unramified extension of degree m over the p-adic completion of the field of rational number According to A. Weil, we code $S(1)$, $S(2)$, $S(3), \ldots$ into an L-series $L(t, S)$. It is proved that $L(t, S)$ is a radical of a rational function when the degree of the polynomial in S is less that the prime number in S and the prime number is prime to the greatest common divisor of the nonconstant coefficients of the polynomial. Parallel results for complete character sums are established.

УДК 511.37

Манставичюс Э.* (Вильнюс, Литва)

ВЕРОЯТНОСТНЫЕ АСПЕКТЫ РАСПРЕДЕЛЕНИЯ НАТУРАЛЬНЫХ ДЕЛИТЕЛЕЙ

В работах автора [1], [2] исследованы проблемы распределения значений арифметических объектов, определяемых через натуральные делители $d_k(m)$ чисел $m \in \mathbb{N}$. В основе лежит идея, что последовательность

$$1 = d_1(m) < d_2(m) < \ldots < d_{\tau(m)}(m) = m$$

представляет собой случайный процесс дискретного времени, когда $m \leqslant n$ выбирается "случайно". Он является процессом восстановления для $\tau(m,u) := \#\{d|m : d \leqslant u\}$, $u \geqslant 1$. Используя функциональные предельные теоремы мы определили множество предельных кривых последовательностей

$$\frac{\log_2 \tau\left(m, \exp\left\{(Lk)^t\right\}\right) - tLLk}{\sqrt{2(LLk)LLLLk}} \qquad \frac{LLd_{[k^t]}(m) - t\log_2 k}{\sqrt{2(\log_2 k)LLLk}},$$

где $t \in [0,1]$, $k \geqslant 2$, $Lu = \log\max\{u, e\}$, "для почти всех" $m \in \mathbb{N}$. Эти результаты имеют вид закона повторного логарифма Штрассена. Слабые функциональные предельные теоремы показывают, что

$$\frac{\log_2 \tau\left(m, \exp\left\{(Ln)^t\right\}\right) - tLLn}{\sqrt{LLn}}, \qquad t \in [0,1]$$

для больших n является арифметической моделью броунóвского движения.

В докладе будут обсуждаться следствия, имеющие явный теоретико-числовой смысл.

ЛИТЕРАТУРА

1. E.Manstavičius. Functional approach in the divisor distribution problems. *Acta Math. Hungarica*. 1995. **67**(1-2), 1–17.
2. E.Manstavičius. Natural divisors and the Brownian motion. *Journal de Théorie des Nombres de Bordeaux* (to appear).

* Работа выполнена в рамках Объединенной программы правительства Литвы и Международного фонда Науки, Грант No *LI* 2100

УДК 511.2

Мануилов Н.Ф. (Смоленск)

К ТЕОРИИ ДЕЛИМОСТИ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

Элементарными методами доказана

Теорема. Для любых алгебраических чисел α, β существуют натуральные числа $k, l\ (k \neq l)$, такие, что

$$\beta^k - \beta^l = \alpha t, \quad t \in Z[\alpha, \beta],$$

где $Z[\alpha, \beta]$ - кольцо чисел, полученное присоединением к кольцу целых чисел элементов α и β.

Доказательство теоремы конструктивное и основывается на следующем факте о делимости многочленов с целыми коэффициентами.

Лемма. Пусть элементы $f, g \in Z[x]$ взаимно просты (не имеют общего необратимого в $Z[x]$ делителя). Тогда для $\forall h \in Z[x]$ существуют натуральные k и l ($k \neq l$) такие, что

$$h^k - h^l \in I,$$

где I идеал в $Z[x]$, порожденный элементами f и g.

Доказательство леммы конструктивное.

УДК 511

Маренич А.С. /Мурманск/

РЕШЕНИЕ УРАВНЕНИЙ В КОЛЬЦЕ ФОРМАЛЬНЫХ СТЕПЕННЫХ РЯДОВ.

Пусть $\mathcal{K}$ -область целостности, содержащая подкольцо действительных чисел. Под формальным степенным рядом,/ф.с.р./, от переменных $T = (T_1, \dots, T_m)$; $m = 1,2,3,\dots$ над кольцом $\mathcal{K}$ будем понимать бесконечное выражение $\Phi : \Phi = F_0(\Phi) + F_1(\Phi) + F_2(\Phi) + \dots$ где $F_i(\Phi) \in \mathcal{K}[T]$, $F_i(\Phi)$ - форма степени i от переменных T или нуль. Кольцо ф.с.р. от переменных T с коэффициентами из $\mathcal{K}$ обозначается $\mathcal{K}[[T]]$. Решение уравнений в кольце $\mathcal{K}[[T]]$ имеет прикладное значение. Например, в теории чисел, в комбинаторике и теории вероятностей при применении метода производящих функций приходится решать системы дифференциальных и функциональных уравнений в кольце ф.с.р. Существование решений этих уравнений рассматривается в алгебре. Следующие теоремы являются конструктивным доказательством существования решения таких уравнений. Теоремы доказаны методом рядов Ли, перенесённым в кольцо ф.с.р.

Теорема I. Если система уравнений относительно $X = (X_1, \dots, X_n)$:

$$\frac{\partial}{\partial y_k} X_i = \Phi_{k,i}(X); \qquad \begin{matrix} k = 1, \dots, m \\ i = 1, \dots, n \end{matrix} \qquad /1/$$

с начальными условиями:

$$F_0(X_i) = 0; \quad \Phi_{k,i} \in \mathcal{K}[[T]] \quad ; X_i \in \mathcal{K}[[Y]] \qquad /2/,$$

где $Y = (y_1, \dots, y_m)$, имеет решение, то оно единственно. Если операторы $\mathcal{D}_k$: $\mathcal{D}_k = \sum_{i=1}^{n} \Phi_{k,i} \frac{\partial}{\partial T_i}$; $k = 1, \dots, m$ коммутативны, то есть $\mathcal{D}_k \mathcal{D}_l = \mathcal{D}_l \mathcal{D}_k$ для $k, l = 1, \dots, m$ то система /1/ с начальными условиями /2/ имеет решение, которое выражается ф.с.р.:

$$X_i = \sum_{r_1, \dots, r_m \geq 0} \frac{y_1^{r_1} \dots y_m^{r_m}}{r_1! \dots r_m!} F_0\left(\mathcal{D}_1^{r_1} \dots \mathcal{D}_m^{r_m} T_i\right)$$

Следующая теорема - это теорема Бормана-Лагранжа для нескольких переменных в кольце ф.с.р.

Теорема 2. Уравнение относительно X: $X = \sum_{i=1}^{n} T_i \Phi_i(X)$ с начальными условиями: $F_0(X) = 0$; $\Phi_i \in \mathcal{K}[[T_{n+1}]]$, $X \in \mathcal{K}[[T]]$ $i = 1, \dots, n$; $T = (T_1, \dots, T_n)$ имеет единственное решение, которое выражается ф.с.р. Лагранжа:

$$X = \sum_{\substack{r_1, \dots, r_n \geq 0 \\ r_1 + \dots + r_n \geq 1}} \frac{T_1^{r_1} \dots T_n^{r_n}}{r_1! \dots r_n!} F_0\left(\frac{\partial^{r_1 + \dots + r_n - 1}}{\partial T_{n+1}^{r_1 + \dots + r_n - 1}} \Phi_1^{r_1} \dots \Phi_n^{r_n}\right).$$

УДК 511

Матвеев Е.М. (Москва)

О РАСШИРЕННОЙ ЛОГАРИФМИЧЕСКОЙ ВЫСОТЕ АЛГЕБРАИЧЕЕСКИХ ЧИСЕЛ

Пусть $\mathbb{K}$ – алгебраическое поле, $[\mathbb{K}:\mathbb{Q}]=D$, $\alpha \in \mathbb{K}^*$. Абсолютной логарифмической высотой α называется сумма по всем нормализованным нормированиям $h(\alpha) = \sum |\log|\alpha|_v|/2D$, при этом $h(\alpha)$ не зависит от поля $\mathbb{K}$. Из теоремы Кронекера следует, что существует такая константа $C(D)>0$, для которой из неравенства $h(\alpha)<C(D)$ следует, что α – корень из 1, т.е. это граница, отделяющая корни из 1 от остальных чисел. Для приложений важно иметь возможно более точную оценку $C(D)$. Не доказанная гипотеза Лемера утверждает, что можно взять $C(D)=C_1/D$ с абсолютной константой $C_1>0$.

В ряде приложений важно уметь отделять алгебраические числа (в том числе и корни из 1) от 1. Это встречается, когда работают с логарифмами алгебраичских чисел. Пусть выбран некоторый набор $\mathcal{S}$ вложений $\mathbb{K}$ в $\mathbb{C}$ (и соответственно, архимедовских нормирований $\mathbb{K}$) и определены значения $\log \alpha^{(\sigma)}$, $\sigma \in \mathcal{S}$. Положим

$$S = |\mathcal{S}|, \qquad \lambda = \sum_{\sigma\in\mathcal{S}} |\log \alpha^{(\sigma)}|/S, \qquad \mu = \sum_{v\notin\mathcal{S}} |\log|\alpha|_v|/2.$$

Тогда имеет место утверждение: если $\alpha \in \mathbb{K}^*$, $\alpha \neq 1$, то

$$\max\{\lambda,\ \mu/S\} \geq 1/(2.5\ \delta\ \log(4.8\ \delta)), \qquad \delta = D/S.$$

Эта граница близка к предельно возможной. По крайней мере для α – корня из 1 и $S=1$ мы имеем $\mu=0$ и

$$\lambda = |\log \alpha| \geq \pi/2D\ \log\log(6D).$$

УДК 511

Матвеев Е.М. (Москва)

СПОСОБ ПОСТРОЕНИЯ ХОРОШО РАСПРЕДЕЛЕННЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Опишем простейшую модификацию разработанного автором метода. Пусть дано вероятностное пространство Ω и функция $f\colon \Omega \longrightarrow \Omega$, удваивающая объемы. Тогда имеются две обратные функции g_0 и g_1, удовлетворяющие условиям:

а) $\forall\, x\in\Omega : g_0(x)\neq g_1(x)$, б) $x = f\circ g_0(x)$, $x = f\circ g_1(x)$.

Пусть имеется также неподвижная точка $\xi = \xi_0$ отображения f.

Предлагаемая последовательность $\{\xi_n\}$ строится следующим образом: пусть $n = (\delta_m, \ldots, \delta_1)_2$ - двоичное разложение n и $\delta_k = 1$ - младший ненулевой разряд. Тогда

$$\xi_n = g_{\delta_1}\circ g_{\delta_2}\circ \cdots \circ g_{\delta_m}\circ f^m(\xi_0) = g_0^{k-1}\circ g_1\circ f^k(\xi_{n-1}),$$

(второе равенство позволяет быстрее рассчитывать очередную точку по предыдущей точке).

На отрезке $\Omega = \mathbb{R}/\mathbb{Z}$, взяв $f(x)=2x \pmod{\mathbb{Z}}$, получим известную последовательность ван дер Корпута. В квадрате $\Omega = \mathbb{C}/\mathbb{Z}[i]$ хорошо взять $f(z) = (1+i)z \pmod{\mathbb{Z}[i]}$. Возможны и многомерные обобщения. Вообще, отметим, что для построения хорошо распределенных последовательностей оказывается можно брать довольно простые функции. Такое построение обобщает идею ван дер Корпута, которую можно назвать "обращением", а именно, если взять какое-либо разложение n, то при построении точки ξ_n знаки разложения n будут встречаться в обратном порядке.

Приведем еще пример обращения. Пусть F_m - m-е число Фибоначчи ($F_0=1$, $F_1=1$). Натуральные числа можно разлагать по основанию Фибоначчи $n = (\delta_m, \ldots, \delta_1)_F = \delta_1 F_1 + \ldots \delta_m F_m$, тогда конечная последовательность $\xi_n = (\delta_1, \ldots, \delta_m)_F / F_{m+1}$, $0 \le n < F_{m+1}$, будет хорошо распределена на единичном отрезке.

УДК 511

Матвеев Е.М. (Москва)

УСИЛЕНИЕ ОЦЕНКИ ОДНОРОДНОЙ РАЦИОНАЛЬНОЙ ЛИНЕЙНОЙ ФОРМЫ ОТ ЛОГАРИФМОВ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

Пусть дано поле $\mathbb{K} \subseteq \mathbb{C}$, $[\mathbb{K}:\mathbb{Q}]=D$, числа $\alpha_1,\dots,\alpha_n \in \mathbb{K}^*$ ($n \geq 2$), фиксированы некоторые значения логарифмов $\log \alpha_j$,

$$A_j = \max\{1,\ D\,h(\alpha_j),\ |\log \alpha_j|\},\quad j=1,\dots,n;\qquad \Omega = A_1 \dots A_n .$$

Здесь $h(\alpha)$ – абсолютная логарифмическая высота α. Предположим также, что выполняется условие сильной независимости чисел α_j:

$$[\mathbb{K}(\sqrt{\alpha_1},\dots,\sqrt{\alpha_n}):\mathbb{K}] = 2^n. \qquad (1)$$

Рассматривается линейная форма от логарифмов

$$\Lambda = b_1 \log \alpha_1 + \dots + b_n \log \alpha_n,\quad b_1,\dots,b_n \in \mathbb{Z},\quad b_n \neq 0.$$

Тогда существует такая абсолютная константа $C>0$, что имеет место неравенство

$$|\Lambda| > \exp(-C^n D^2 \Omega \log(C^n D^2 \Omega/A_n) \log(eB)), \qquad (2)$$

где $B = \max\{|b_j| A_j/A_n:\ j=1,\dots,n\}$.

Примечания. 1. Константа C явно вычисляется и сравнительно невелика.

2. Основное отличие оценки (2) от предшествующих в том, что зависимость от n показательная, а не вида n^{Cn}.

3. В настоящее время имеются оценки $|\Lambda|$ без параметра (Ω/A_n) и условия (1), однако, совместить это с устранением множителя n^{Cn} пока не удается. Отметим, что имеется много приложений оценок линейных форм, где устранение n^{Cn} даст значительный эффект.

4. Прием устранения n^{Cn} использован автором в схеме Гельфонда-Бейкера, но применим и в других методах (Шнайдера, интерполяционные определители Лорана и т.д.). Во всех случаях он дает значительное усиление оценок.

УДК 511.9+519

Т.И.МАТИКАШВИЛИ
Тульский государственный технический университет

ПРЕДСКАЗАНИЕ ЭВОЛЮЦИИ КЛЕТОЧНОГО АВТОМАТА

Постановка задачи предсказания эволюции одномерного клеточного автомата фон-Неймана и методы её решения близки к теории чисел. Для определения состояния автомата с правилом перехода

$$a(t+1) = \sum_{k} a_j(t) \oplus_k C \; ; \quad a \in \{0,1,2,\dots k-1\}$$

(в дальнейшем $\oplus$-автомат), на шаге $t = 0,1,2,\dots$ использованы t-мерные массивы I_t индексов, отсчитываемых от произвольно выбранной клетки a_0. Массив I_t получается поэлементным сложением I_{t-1} и I_1. Например, если $I_1 = |-1.0,1|$, то

$$I_2 = \begin{vmatrix} -2 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & 1 & 2 \end{vmatrix}.$$

Длина массива-строки I_1 равна n и соответствует величине анализируемой при переходе окрестности клетки a_i. Все элементы I_t, кроме стоящих на главной пространственной диагонали, встречаются в массиве кратное t число раз.

При вычислении нового состояния $a_i(t+1)$ каждой клетки складываются целые числа, изображающие состояния соответствующих клеток. Сопоставление t-ых поколений автомата и массивов I_t позволяет доказать следующие теоремы.

Теорема 1. В бесконечном $\oplus$-автомате исходное поколение A_0, в котором только одна клетка a_0 находится в ненулевом состоянии, превращается на шаге $t = k^h$; $h = 1,2,3,\dots$ в поколение A_t из n клеток в состоянии $a_0(0)$, расположенных на расстоянии t одна от другой.

Теорема1 обобщается на пару клеток с ненулевыми начальными состояниями, а затем на любую начальную конфигурацию автомата, закономерным образом трансформирующуюся в моментам $t = k^h$.

Теорема 2. В замкнутом $\oplus$-автомате из m клеток с простыми m и k длина l цикла развития между повторяющимися конфигурациями равна

$$l = t_{1+l} - t_1 = k^h - 1, \text{ при } k^h - pm = \pm 1 \; ; \quad p \in \{1,2,3,\dots\}$$

О разрешимости обобщенной смешанной задачи

С.П. Митин (Владимир), А.П. Солдатов (Новгород)

Для эллиптической системы

$$\sum_{i,j=1}^{2} a_{ij} \frac{\partial^2 u}{\partial x_i \partial x_j}(x) = 0, \quad x \in D,$$

с постоянными коэффициентами $a_{ij} \in R^{l \times l}$ рассматривается обобщенная смешанная задача

$$(d_1 u)(x) = f_1(x), \ (d_2 \delta u)(x) = f_2'(x), \quad x \in \Gamma,$$

где δ является граничной конормальной производной $\sum a_{ij} n_i \partial u / \partial x_j$, штрих означает производную по длине дуги, а d_1 и d_2 представляют собой прямоугольные матрицы-функции порядков соответственно $r \times l$ и $(l-r) \times l$, причем целочисленная величина $0 \le r \le l$ кусочно-постоянна на границе Γ области D.

В работе показывается, что при некоторых предположениях условия разрешимости этой задачи в классической постановке [1] можно описать как условия ортогональности к решениям формально сопряженной задачи. Основное предположение заключается в том, чтобы слабое (в $L_2(D)$) решение этой однородной задачи совпадало с сильным.

Для классической смешанно-контактной задачи плоской теории упругости [2] аналогичный вопрос был изучен в [3].

Литература

[1] Солдатов А.П. // Изв. РАН. Сер. матем. 1992, Т. 56,

[2] Мусхелишвили Н.И. Некоторые основные задачи математической теории упругости. М., 1966. N 3, С. 566–604.

[3] Митин С.П., Солдатов А.П. // Дифференц. уравнения. 1993, Т. 29, N 5, С. 885–889.

УДК 511

Митькин Д.А. /Москва/

Об оценке коэффициентов ряда Лорана для дзета-функции Римана

Один из способов оценки коэффициентов γ_n ряда Лорана для $\zeta(s)$ в окрестности ее полюса $s=1$,

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=0}^{\infty} \gamma_n (s-1)^n,$$

состоит в применении к формуле

$$\gamma_n = \frac{(-1)^n}{n!} \lim_{N\to\infty} \left(\sum_{k=1}^{N} \frac{\ln^n k}{k} - \frac{\ln^{n+1} N}{n+1} \right)$$

методов частного суммирования. В частности, таким способом выводится равенство /см.[1]/

$$\gamma_n = \frac{(-1)^{n+m-1}}{n!\,m!} \int_1^{\infty} B_m^*(x) f_n^{(m)}(x)\,dx,$$

где $f_n(x) = \frac{\ln^n x}{x}$, $1 \le m \le n$, $B_m^*(x) = B_m(\{x\})$ - периодизированный полином Бернулли. В работе [1] оптимальный выбор параметра m при всех n не проводился. На самом деле выбор $(n \ge 2)$ $m = [n/\ln n]$ приводит к оценке $\gamma_n \ll \exp(-n\ln n + O(n\ln\ln n))$ которая порождает способ аналитического продолжения $\zeta(s)$ на всю плоскость, исключая ее полюс $s=1$.

Отметим, что аналогичная оценка для γ_n получается /но при этом используются аналитические свойства $\zeta(s)$ на всей плоскости/ и из интегральной формулы

$$\gamma_n = \frac{1}{2\pi i} \oint_{\{|s-1|=\tau\}} \frac{\zeta(s)}{(s-1)^{n+1}}\,ds, \quad \tau > 0,$$

если выбрать $\tau \sim n/\ln n$ $(n\to\infty)$.

Литература : [1]. Исраилов М.И. О разложении Лорана дзета-функции Римана. //Труды МИАН.1981.т.158.с.98-104.

УДК 621.391.7

Михайлов Г.Д., Кутищев С.Н. (Воронеж)

СПОСОБ УПРАВЛЕНИЯ ДИАГРАММОЙ НАПРАВЛЕННОСТИ АНТЕННОЙ РЕШЕТКИ

В целях управления передачей информации в пространстве и ее защиты от несанкционированного доступа формулируется проблема синтеза диаграмм направленности (ДН) антенных решеток специального вида [1]. При этом синтезированная ДН имеет минимальный уровень излучения в направлении, защищаемом от несанкционированного доступа, с сохранением основных характеристик максимумов ДН.

В данной работе рассматривается методика амплитудно-фазового синтеза ДН линейной антенной решетки N эквидистантно расположенных изотропных излучателей.

Алгоритм амплитудно-фазового синтеза ДН состоит из двух основных этапов.

1) Выбирается исходная ДН $P_0(u)$, обеспечивающая в первом приближении низкий уровень излучения в требуемом секторе углов Δu и заданные положения максимумов ДН.

2) Находится искомая ДН $P(u)$ из условия минимизации среднеквадратической разности искомой и исходной ДН [2, 3] при заданных ограничениях на положения нулей ДН, формирующих сектор углов Δu.

Результаты численных расчетов показали, что, например, для линейной антенной решетки, состоящей из четырех элементов может быть синтезирована ДН с уровнем мощности излучения менее -40 дБ в секторе углов $\pm 15^{\circ}$.

Литература

1. Хоффман Л.Дж. Современные методы защиты информации. М.: Сов. радио, 1980.

2. Steyskal H. Wide-band nulling performance versus number of pattern constraints for an array antenna./ IEEE Trans. Ant. and Prop., 1983, vol. AP-31, pp. 159-163.

3. Михайлов Г.Д., Кутищев С.Н. Электромагнитное рассеяние апертурными атеннами./ В сб. трудов 27-й Международной конференции "Теория и техника антенн". М.: АО "Радиофизика", 1994, с. 125-127.

УДК 5II.36

Морозова И.М. (Минск)

МЕТРИЧЕСКАЯ ОЦЕНКА ПРИБЛИЖЕНИЯ НУЛЯ МОДУЛЯМИ ЗНАЧЕНИЙ АНАЛИТИЧЕСКИХ ФУНКЦИЙ

Пусть n – некоторое натуральное число и $f_1(z), f_2(z), \dots, f_n(z)$ – аналитические функции комплексной переменной z в области Ω и

$$\Delta = \begin{vmatrix} f_1'(z) & \dots & f_n'(z) \\ \dots & \dots & \dots \\ f_1^{(n)}(z) & \dots & f_n^{(n)}(z) \end{vmatrix} \not\equiv 0$$

Пусть далее

$$F(z) = a_0 + a_1 f_1(z) + \dots + a_n f_n(z), \quad a_i \in \mathbb{Z}, \quad H = \max_{0 \le i \le n} |a_i|$$

Теорема. Для почти всех z (в смысле меры Лебега) неравенство

$$|F(z)| < H^{-w}$$

имеет лишь конечное число решений в целых векторах $a = (a_0, \dots, a_n)$ при $w > \frac{n^2}{8} + \frac{3n}{4} + \frac{1}{8}$.

Настоящая теорема является комплексным аналогом теоремы Пяртли [1] и усиливает результат работы [2].

Литература

I.Пяртли А.С. Функциональный анализ. I969. т.3, вып. 4. с.59–62.
2.Ковалевская З.И., Сакович Н.В. Весці АН Беларусі. Серыя фіз.-мат. навук. I994. №4. с. I7–20.

О СОВМЕСТНЫХ ДИОФАНТОВЫХ ПРИБЛИЖЕНЯХ

Н. Г. Мощевитин

Пусть $\psi(y)$– некоторая вещественнозначная функция вещественного аргумента. Натуральное число p мы будем называть совместным ψ–приближением к числам $\alpha_1, ..., \alpha_s \in R$, если

$$\max_{j=1,...,s} ||p\alpha_j|| = \max_{j=1,...,s} \min_{a \in Z} |p\alpha_j - a| \le \psi(p).$$

ТЕОРЕМА 1

Пусть $\psi(y) = y^{-1/s}\omega(y)$, где $\omega(y)$ монотонно убывает (не обязательно строго монотонно) при $y \ge 1$ и

$$\omega(1) \le 2^{-(s+1)(s+2)}(s!)^{-1/s}. \qquad (1)$$

Тогда найдутся числа $\alpha_1, ..., \alpha_s$, допускающие бесконечную последовательность совместных ψ–приближений, но не допускающих ни одного совместного $2^{-(s+3)}\psi$–приближения.

ТЕОРЕМА 2

Пусть в условии теоремы 1 соотношение (1) заменено на более сильное требование

$$\omega(1) \le 2^{-(s+1)(s+3)}(s!)^{-1/s}.$$

Тогда найдется континуальное семейство векторов $\alpha = (\alpha_1, ..., \alpha_s)$, допускающих бесконечно много совместных ψ–приближений, но не допускающих ни одного совместного $2^{-(s+3)}\psi$–приближения.

Будем говорить, что числа $\alpha_1, ..., \alpha_s$ обладают ψ–свойством, если они допускают бесконечно много ψ–приближений, но не допускают ни одного $c\psi$–приближения с некоторой константой c, зависящей от $\alpha_1, ..., \alpha_s$.

ТЕОРЕМА 3

Пусть $\psi(y) = y^{-1/s}\omega(y)$, где $\omega(y)$ монотонно убывает. Тогда в любой s–мерной области Ω с объемом $Vol\ \Omega > 0$ найдется континуальное семейство векторов α, обладающих ψ–свойством.

Теоремы 1, 2, 3 обобщают известные теоремы Касселса и Ярника

УДК 5I2.7

Нарзуллаев У.Х. (Самарканд)

КОГОМОЛОГИИ СЕРРА ДЛЯ ГРУППЫ ТРЕУГОЛЬНЫХ МАТРИЦ

В ряде вопросов алгебраической теории чисел появляется следующая задача: пусть k-поле алгебраических чисел, A-алгебраическая группа над k, требуется описать ядро гомоморфизма локализации для когомологий:

$$H^q(k, A) \longrightarrow \sum_v H^q(k_v, A).$$

На этом языке могут быть описаны задачи поведения группы классов идеалов, группы Шафаревича-Тэйта над абелевым многообразием и другие. Алгебраическая сторона этого вопроса связана с описанием пересечения ядер отображения ограничения на группы разложения.

Ж.-П. Серром [1] было предложено изучать соответствующую конструкцию для общей алгебраической ситуации, в которой ограничения берутся на все циклические подгруппы.

Пусть G-конечная группа, A - G-модуль. Через $Ш^q_*(G, A)$ обозначим подгруппу группы когомологий $H^q(G, A)$, состоящую из элементов, аннулирующихся при ограничении на любую циклическую подгруппу группы G.

Пусть G_p - силовская p-подгруппа группы $GL_2(\mathbb{Z}/p^n\mathbb{Z})$, T - подгруппа треугольных матриц из G_p.

Теорема. Если $A = \mathbb{Z}/p^n\mathbb{Z} + \mathbb{Z}/p^n\mathbb{Z}$, $T \subset G$, то группа $Ш^1_*(G, A)$-циклическая.

Отметим, что при этом можно дать оценку порядка группы $Ш^1_*(G, A)$ через параметры группы G.

ЛИТЕРАТУРА

I. J.-P. Serre. Sur les groupes de congruence des varietes abeliennes. Изв. АН СССР, сер.матем., I964, 28, № I, с.3-20.

2. Башмаков М.И., Нарзуллаев У.Х. Об одной когомологической конструкции Серра. В сб.: Кольца и матричные группы. Орджоникидзе, I984, с.II-I9.

УДК 5II.9

Нарзуллаев Х.Н. (Самарканд)

ЭФФЕКТИВИЗАЦИЯ DOTU-ОКРЕСТНОСТЕЙ ТРЕУГОЛЬНЫХ МАТРИЦ

В связи с попыткой решения гипотезы Минковского о произведении линейных неоднородных форм возникла так называемая DOTU-тематика, которая заключается в следующем: если любая вещественная матрица A представима в виде DOTU (D-диагональная, O-ортогональная, T-треугольная с единицами по диагонали, U-целочисленная унимодулярная матрицы), то верна гипотеза Минковского.

А. Макбет [I] доказал, что всякая матрица второго порядка представима в виде DOTU. Он же доказал представимость в виде DOTU достаточно малой окрестности рациональной матрицы порядка n.

В [2] доказана представимость в виде DOTU матриц второго и третьего порядков.

ТЕОРЕМА I. Пусть T - вещественная треугольная матрица порядка n. Тогда всякая матрица T_δ из δ-окрестности матрицы T представима в виде

$$T_\delta = DOT, \text{ где } \delta \le \frac{1}{100n!2^n}.$$

ТЕОРЕМА 2. Пусть B-невырожденная матрица порядка n. Тогда существует целочисленная матрица S такая, что BS есть DOTU-матрица.

Отсюда непосредственно следует, что у произвольной решетки A из R^n существует DOTU-подрешетка ограниченного индекса.

ЛИТЕРАТУРА

1. Macbeath A.M. Factorization of matrices and Minkowski's conjecture. Proc. Glasgow math. Ass.,5(1961), 86-89.
2. Нарзуллаев Х.Н. О представлении унимодулярной матрицы в виде DOTU для n=3. Мат.заметки., т.I8, № 2 (I975), 2I3-22I.

УДК 511.9

Нечаев В.И. (Москва)

Суммы квадратов и криптография

Предлагается криптосхема, основанная на применении теоремы ***Эйлера-Ферма***. Чтобы её реализовать, необходимо иметь в виду следующее:

1. Пусть **p** - натуральное число, сравнимое с 1 по модулю 4. Уравнение

$$p=x^2+y^2 \qquad (1)$$

разрешимо и притом единственным способом в целых и взаимно простых числах **x, y** с условием $0<x<y$, тогда и только тогда, если **p** - простое или квадрат простого числа.

2. Если дано простое число **p**, то задача решения уравнения (1) в числах, удовлетворящих указанным условиям, сводится к решению сравнения

$$t^2 \equiv -1 \pmod p \qquad (2)$$

3. Если **p** велико, то пока нет способа, кроме простого перебора, отыскания решения сравнения (2).

4. При составлении таблицы простых, необходимых для работы криптосхемы, следует иметь в виду, что точки комплексной плоскости **(x,y)** с условием что $(x,y)=1$, а сумма x^2+y^2 есть простое число, распределены равномерно в её первом квадранте.

5. Описание криптосхемы. Пользователь **A** заблаговременно заготавливает тройки $(p,x,y), (p_1,x_1,y_1), \ldots$ с условием (1) и сообщает адресату **B** их третьи компоненты $y, y_1, \ldots$. Сообщение v $(0<v<p)$ пользователь **A** шифрует следующим образом:

$$v \cdot x \equiv \xi \pmod p, 0<\xi<p \qquad (3)$$

и передает телеграмму (p,ξ) адресату **B**. Адресат **B**, извлекая квадратный корень из выражений

$$p-y^2,\ p-y_1^2,\ldots$$

находит **x**, а затем и сообщение **v** из сравнения (3).

Литература.

Дэвенпорт Г., Высшая арифметика, пер.с англ., М., 1965.

Манин Ю.И., Панчишкин А.А., Введение в теорию чисел. М., 1990.

Zarzycki P. Distribunion of Primes of Imaginfry Quadratic Fiields in Sectors, Journal of Number Theory 37. 152-160, 1991.

УДК 517.968

Новикова Л.В. /г.Ростов-на-Дону /

Об инвариантных многообразиях эволюционных уравнений.

Исследуется вопрос о рождении инвариантных асимптотически устойчивых многообразий уравнения

$$\frac{du}{dt} = A_\delta u + \Phi(u) \qquad /1/$$

гомеоморфных прямому произведению $T_n \times S_\kappa$, где T_n - n - мерный тор, S_κ - κ - мерная сфера, для всюду плотного на отрезке $(0, \varepsilon)$ параметрической оси $/ \delta \in R_1 /$ множества N_ε значений параметра δ.

Уравнение /1/ рассматривается в банаховом пространстве U, A_δ - производящий оператор сильно непрерывной полугруппы операторов в банаховом пространстве U со всюду плотной в U областью определения D_A, единой для всех операторов A_δ, зависящих от вещественного параметра $\delta \in R_1$. $\Phi(u)$ - нелинейная часть уравнения /1/ с областью определения $D_\Phi \supseteq D_A$.

Рассматривается случай, когда n пар комплексно - сопряженных собственных значений, имеющих общую суммарную кратность $n + \kappa$, переходит из левой полуплоскости в правую при переходе вещественного параметра δ через критическое значение.

Литература :

1. Николенко Н.В. Инвариантные, асимптотически устойчивые торы возмущенного уравнения КдФ, УМН, т. 36, вып.5 /125/, 1980, 121-188.

УДК 511

Осипян О.Н.
Кубанский госуниверситет

Об одной процедуре в многостепенном диофантовом анализе

Пусть $(x,y,z)=(u,v,w)=1$, $z\neq x+y$, $w\neq u+v$, $x,y,z,u,v,w\in N$ и

$$\begin{cases} x^2+y^2+z^2=u^2+v^2+w^2, \\ x^4+y^4+z^4=u^4+v^4+w^4, \end{cases} \qquad (A)$$

тогда из каждого решения этой системы можно получить соответствующие решения следующих многостепенных систем:

1^0. $x^n_1+x^n_2+\ldots+x^n_6=y^n_1+y^n_2+\ldots+y^n_6$, $n=1,2,3,4,5$ или в символической записи $x_1,x_2,\ldots,x_6 \overset{5}{=} y_1,y_2,\ldots,y_6$.

Для этой системы требование $z\neq x+y, w\neq u+v$ излишне.

2^0. $x^n_1+x^n_2+\ldots+x^n_7=y^n_1+y^n_2+\ldots+y^n_7$, $n=1,2,4,6,8$.

3^0. $x^n_1+x^n_2+\ldots+x^n_{14}=y^n_1+y^n_2+\ldots+y^n_{14}$, $n=1,2,3,4,5,6,7,8,9$.

Из параметрического решения системы (A)

$x=a^2-ab+3b^2$, $y=|2a^2+4ab-b^2|$, $z=|3a^2-2b^2|$; $u=3a^2+ab+b^2$,

$v=|a^2+4ab-2b^2|$, $w=|2a^2-3b^2|$ получаем

$d+x,d+y,d+z,d-x,d-y,d-z, \overset{5}{=} d+u,d+v,d+w,d-u,d-v,d-w$, где d-произвольное целое число. Для получения соответствующего решения системы 2^0, используем тождества Отто Бирка. Тогда

$x_1=x+y+z$, $x_2=-x+y+z$, $x_3=x-y+z$, $x_4=x+y-z$, $x_5=2u$, $x_6=2v$, $x_7=2w$;

$y_1=u+v+w$, $y_2=-u+v+w$, $y_3=u-v+w$, $y_4=u+v-w$, $y_5=2x$, $y_6=2y$, $y_7=2z$.

Из решений системы 2^0 получаем решения системы 3^0:

$d+x_1,d+x_2,\ldots,d+x_7,d-x_1,d-x_2,\ldots,d-x_7 \overset{9}{=} d+y_1,d+y_2,\ldots,d+y_7,d-y_1,d-y_2,\ldots,d-y_7$, где d- произвольное целое число.

Для каждой из перечисленных систем получены по несколько новых многопараметрических решений.

У Д К 519.1:612

В.О. Осипян
Кубанский госуниверситет

Подсчет числа перестановочных целых функций полей Галуа

Пусть $N_{p,n}(f(x))$- число перестановочных целых функций

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$$

степени $n\geqslant 1$ с коэффициентами из поля Галуа $GF(p)$, $g_f(x)$-целая функция степени не выше $p-1$, порождённой $f(x)$.

В докладе рассматриваются необходимые и достаточные условия существования перестановочных целых функций, на основе которых можно находить все перестановочные целые функции поля $GF(p)$ заданной степени.

Для малых p, в частности, получены следующие формулы относительно числа $N_{p,n}(f(x))$ (в общем случае получена рекуррентная формула):

1. $N_{2,n}(f(x))=2\sum\limits_{u=0}^{m}\left\{\begin{matrix}n-1\\2u\end{matrix}\right\}$, где $m=[(n-1)/2]$;

2. $N_{3,n}(f(x))=\begin{cases}6 & \text{при } n=1,\\ 0 & \text{при } n=2,\\ 4*3^{n-2} & \text{при } n\geqslant 3;\end{cases}$

3. $N_{5,n}(f(x))=\begin{cases}20 & \text{при } n=1,\\ 0 & \text{при } n=2,4,\\ 100 & \text{при } n=3,\\ 4*5^{n-3} & \text{при } n\geqslant 5\end{cases}$

Литература

1.Р. Лидл, Г.Нидеррайтер. Конечные поля, т.2.-М.: Мир,1988.

УДК 511.9

Е.В.Орловская (С.-Петербург)

К ТЕОРИИ ζ-ФУНКЦИИ ЭПШТЕЙНА ОТ ТРЕХ ПЕРЕМЕННЫХ

Пусть $\mathcal{P}_f$ – пространство положительно определенных квадратичных форм

$$f(x_1, x_2, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$$

с вещественными коэффициентами $a_{ij} = a_{ji}$ и с определителем $\Delta = \Delta(f) > 0$. Для функции f и вещественного параметра $s > 0$ определена дзета-функция Эпштейна, задаваемая при $s > 1$ сходящимся рядом

$$\zeta(f, s) = \sum_{\bar{x} \in \mathbb{Z}^n / \{0\}} [f(\bar{x})]^{-\frac{ns}{2}}$$

а для $0 < s < 1$ – аналитическим продолжением ($s = 1$ – простой полюс).

Теорема I. Для каждого $s > \frac{1}{2}$, $s \neq 1$ класс формы $\varphi_0^{(3)} \lambda$, где $\lambda \in \mathbb{R}$, $\lambda > 0$

$$\varphi_0^{(3)} = x_1^2 + x_1 x_2 + x_2^2 + x_1 x_3 + x_2 x_3 + x_3^2$$

суть единственные формы, дающие абсолютный минимум функции $\zeta(f, s)$ как функции от f на топологическом пространстве $\mathcal{P}_f$. Для каждого $0 < s < \frac{1}{2}$ класс формы $(\varphi_0^{(3)})^{\mu}$, где $\mu \in \mathbb{R}$, $\mu > 0$, $[\varphi_0^{(3)}]^*$ – форма, взаимная к $\varphi_0^{(3)}$, суть единственные формы, дающие абсолютный минимум функции $\zeta(f, s)$ как функции от f на топологическом пространстве $\mathcal{P}_f$. При $s = \frac{1}{2}$ абсолютный минимум $\zeta(f, s)$ достигается на формах из классов форм $\varphi_0^{(3)} \lambda$ и $[\varphi_0^{(3)}]^* \mu$, где $\lambda, \mu \in \mathbb{R}$, $\lambda > 0$, $\mu > 0$.

Теорема I устраняет упущения, содержащиеся в работе [2].

Лит.: I. Montgomery H. Minimal theta functions // Glasgo Math J., 1988, v. 30, p. 75-85. 2. Орловская Е.В. Минимум тета-функции трех переменных и решение проблемы Монтгомери в трехмерном пространстве// Зап. научн. семин. ПОМИ, 1994, т.211, с.150-157. 3. Рышков С.С. К вопросу о финальной ζ-оптимальности решеток, дающих наиплотнейшую решетчатую упаковку n-мерных шаров// Сибирск.мат.ж., 1973, т.14, с.1065-1075.

УДК 517.5

А.И.ПАВЛОВ

Математический институт им.В.А.Стеклова РАН

ИРРАЦИОНАЛЬНЫЕ СТЕПЕННЫЕ РЯДЫ

Пусть Ψ – множество функций ψ, удовлетворяющих условиям:

1. ψ определена на множестве $\mathcal{N}$ всех натуральных чисел; при любых m_1 и m_2 таких, что $(m_1, m_2)=1$, выполняется равенство $\psi(m_1 m_2)=\psi(m_1)\psi(m_2)$; $\psi(1)=1$;

2. ψ принимает только значения $-1, 0, 1$;

3. при некотором целом $\kappa \geq 2$ функция $\chi(m)=\sum_{d^\kappa | m} \psi(d)$ принимает только значения 0 и 1;

4. существует бесконечная последовательность $\{p_i\}$ простых чисел такая, что $\psi(p_i)\neq 0$.

Пусть далее $M = M(\psi, \kappa)$ – множество тех $m \geq 1$, для которых $\chi(m)=1$. Можно показать, что плотность множества M равна $\gamma=\sum_{d=1}^{\infty} \frac{\psi(d)}{d^\kappa}$. Причем, $\gamma>0$ и если $M\neq\mathcal{N}$, то $\gamma<1$.

ТЕОРЕМА. Если целая функция $G(z)\not\equiv 0$ имеет порядок $\sigma<\frac{1}{2}\left(1-\frac{1}{2\kappa-1}\right)$ и её тейлоровские коэффициенты неотрицательны, то степенной ряд $f(z)=\sum_{m\in M} G(m) z^m$, имеющий радиус сходимости 1, не может быть аналитически продолжен в область $|z|>1$ через любую дугу, лежащую на окружности $|z|=1$.

ЗАМЕЧАНИЕ. Если $\psi(m)\equiv\mu(m)$ – функция Мёбиуса, то множество M состоит из κ-чисел. При этом натуральное число m называется κ-числом, если для любого простого p выполняется условие $p^\kappa \nmid m$.

Сформулированная теорема продолжает исследования, проводившиеся в работах Гекке, Кантора, Кэррола и Кэмпермана, Дэвенпорта, Морделла, Салема, Шварца и Валлисера и других. Соответствующие ссылки можно найти в книге Л.Кейперс и Г.Нидеррейтер, Равномерное распределение, М., Наука, 1985.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований/проект 94-01-00002/.

УДК 511.512

Пачев У.М. (Нальчик)

АСИМПТОТИЧЕСКОЕ РАСПРЕДЕЛЕНИЕ СМЕЖНЫХ КЛАССОВ ГРУППЫ ГЛАВНОГО РОДА БИНАРНЫХ КВАДРАТИЧНЫХ ФОРМ

Пусть G - группа классов главного рода положительных бинарных квадратичных форм определителя m и K - ее подгруппа индекса $(G:K) \ll m^{\varepsilon}$ при сколь угодно малом $\varepsilon > 0$. Обозначим через $h_{G/K}(\Lambda_m; g, b_1, b_2, b_3)$ - число классов собственно примитивных положительных бинарных квадратичных форм определителя m, принадлежащих заданному смежному классу группы главного рода G по ее подгруппе K, для которых представители $(x_1, x_2, x_3) = x_1x^2 + 2x_2xy + x_3y^2$ классов квадратичных форм удовлетворяют условиям

$$(x_1, x_2, x_3) \in \Lambda_m, \quad (x_1, x_2, x_3) \equiv (b_1, b_2, b_3) \pmod g,$$

где Λ_m - ограниченная квадрируемая область на поверхности двуполостного гиперболоида $x_1x_3 - x_2^2 = m$, $x_1 > 0$; b_1, b_2, b_3 - целые числа, удовлетворяющие сравнению $b_1b_3 - b_2^2 \equiv m \pmod g$; g - нечетное число, взаимно простое с m. Тогда, исходя из теоремы 3 и ее следствии 2 работы [1] дискретным эргодическим методом получается следующий асимптотический результат.

Теорема. Пусть q - нечетное квадратное число с условием $\left(\frac{-m}{p}\right) = 1$ для всех простых делителей p числа q. Тогда при $m \to \infty$

$$h_{G/K}(\Lambda_m; g, b_1, b_2, b_3) = \frac{\lambda(\Lambda_m)}{\lambda_0} \cdot \frac{1}{\rho(g,m)} \cdot \frac{h(-m)}{t(G:K)} \left(1 + \alpha(q,g,m)\right),$$

где $\lambda(\Lambda_m)$ - гиперболическая мера области Λ_m; $\lambda_0 = \frac{2\pi}{g}$; $\rho(g,m)$ - число решений сравнения $x_1x_3 - x_2^2 \equiv m \pmod g$; $h(-m)$ - порядок группы классов положительных бинарных квадратичных форм определителя m; t - число гауссовых родов; $(G:K)$ - индекс подгруппы K в группе главного рода G; $\alpha(q,g,m) \to 0$ при $m \to \infty$.

Литература: I. Малышев А.В. О применении дискретного эргодического метода в аналитической арифметике неопределенных тернарных квадратичных форм//Зап. науч. семинаров ЛОМИ.-1980.-Т.93, с.5-24.

УДК 511.5

Пензин Ю.Г. **(Иркутск)**

ДИОФАНТОВ РАНГ МНОЖЕСТВА ПРОСТЫХ ЧИСЕЛ

Последние десятилетия характеризуются активным проникновением формально-логических и алгоритмических методов в классическую теорию чисел (см.обзор[3]), что дает возможность по-новому взглянуть на некоторые старые проблемы[4].

В 1970г. было завершено доказательство теоремы, что любое рекурсивно перечислимое множество M представимо диофантовым полиномом $F(x, y_1, ..., y_r)$, т.е. натуральное число n принадлежит M , если и только если уравнение $F(n, y_1, ..., y_r) = 0$ имеет решение в натуральных числах [1]. Диофантовым рангом множества M назовем наименьшее возможное число r среди всех таких представлений для множества M. Из определения следует, что множества ранга 0 есть в точности все конечные множества. Важно получить точные значения ранга для наиболее интересных множеств, например, для множества простых чисел P. В работе [2] показано, что диофантов ранг P не превосходит 9, хотя по предположению он не больше трех. В настоящей работе мы даем оценку снизу для ранга P.

ТЕОРЕМА. Диофантов ранг множества всех простых чисел, принадлежащих любой арифметической прогрессии - в частности, ранг множества всех простых чисел больше 1.

Литература

[1] Ю.В.Матиясевич. *Диофантовость перечислимых множеств*. ДАН СССР, 1970, т.191, N2, 279-282.

[2] Ю.В.Матиясевич. *Простые числа перечисляются полиномом от 10 переменных*, в сб."Теоретические применения методов математической логики:II", Ленинград, Наука, 1977, 62-82.

[3] Ю.Г.Пензин. *Алгоритмические вопросы в теории чисел*, в сб."Алгебраические системы", Иркутск, 1976, 122-148.

[4] Ю.Г.Пензин. *Проблема близнецов в формальной арифметике*, Математические заметки, т.26, N4, 1979, 505-511.

УДК 511.9

Подсыпанин Е.В. (С.-Петербург)

РАЦИОНАЛЬНЫЕ ПРИБЛИЖЕНИЯ ТАНГЕНСА

В работе доказывается следующая теорема о рациональных приближениях чисел вида $\operatorname{tg}\frac{1}{a}$, $a \in \mathbb{N}$.

ТЕОРЕМА. Пусть a - натуральное число. Тогда существуют такие постоянные C_1 и C_2, зависящие только от a, что во-первых, имеется бесконечно много решений неравенства

$$\left|\operatorname{tg}\frac{1}{a} - \frac{p}{q}\right| < \frac{C_1 \ln\ln q}{q^2 \ln q}$$

в натуральных числах p, q и во-вторых, для любых натуральных значений p и q справедливо неравенство

$$\left|\operatorname{tg}\frac{1}{a} - \frac{p}{q}\right| > \frac{C_2 \ln\ln q}{q^2 \ln q}$$

В доказательстве используется известное разложение $\operatorname{tg} x$ в цепную дробь. Аналогичное утверждение для показательной функции см. [1].

[1]. Попов А.Ю. Приближения некоторых степеней числа e. Сб."Диофантовы приближения", Изд-во Моск.Ун-та, 1985, 77-85.

А.Ю. Попов, С.Б. Стечкин* (Москва)

Асимптотическое распределение простых чисел в среднем

Пусть $\psi(x)$ — функция Чебышева, $R(x) = \psi(x) - x$. Положим $\theta = \sup\{\operatorname{Re} s \mid \zeta(s) = 0\}$, где $\zeta(s)$ — дзета-функция Римана. Если для всех s_0: $\zeta(s_0) = 0$, $\operatorname{Re} s_0 < \theta$, то говорим, что θ недостижимо. Имеем

$R(x) = O_\theta(x^\theta)$ $(\theta > 1/2)$,
$R(x) = O(\sqrt{x}\ln^2 x)$ $(\theta = 1/2$, фон Кох),
$R(x) = o(x^\theta)$, если θ недостижимо,
$R(x) = \Omega_\pm(\sqrt{x}\ln\ln\ln x)$ (Литтльвуд).

Для различных средних от R, $|R|$ и R^2 даются оценки сверху и снизу в зависимости от значения θ, а также безусловные оценки. Например.

(I) $\int_1^X R^2(u)\,du = O(X^{2\theta+1})$ *равномерно относительно* θ*: константа в* O *эффективна.*

(II) $\int_X^{2X} |R(u)|\,du \geq 10^{-3}X^{3/2}$*: если* $\theta = 1/2$*, то оценка эффективна.*

(III) *Если* $\theta = 1/2$*,* $H = H(x) = o(x)$*, то* $H^{-1}\int_x^{x+H} R(u)\,du \neq O(\sqrt{x})$.

Соответствующие результаты справедливы и для функции $P(x) = \pi(x) - \operatorname{li} x$.

УДК 517.5

Резцов А.В. (Москва)

Об одном функционале на множестве неотрицательных многочленов

Рассматривается множество $P^+(n)$ неотрицательных на отрезке $[-1; 1]$ многочленов $p(x)$ степени не выше $n \in \mathbb{N}$. Для произвольных k точек $x_1, \dots, x_k \in [-1; 1]$ и многочлена $p=p(x) \not\equiv 0$ из $P^+(n)$ изучается следующий функционал.

$$F(n, k; x_1, \dots, x_k; p) = \left(p(x_1)+ \dots +p(x_k)\right) \Big/ \left(\int_{-1}^{1} p(x)\,dx \right)$$

Величина

$$M(n, k; x_1, \dots, x_k) = \max \left\{ F(n, k; x_1, \dots, x_k; p) \;\Big|\; 0 \not\equiv p \in P^+(n) \right\}$$

возникает в ряде задач дискретной математики, теории информации, а также при изучении упаковок и кубатурных формул. Так, например, задача о вычислении $M(n; 1; x_1)$ является классической и решена для всех $n \in \mathbb{N}$ (с помощью аппарата многочленов Лежандра и Якоби).

Очевидно $M(n, k; x_1, \dots, x_k) \geq \max \left\{ M(n, 1; x_1), \dots, M(n, 1; x_k) \right\}$, однако поставить здесь знак строгого неравенства для $k>1$ нельзя. Нами получен следующий результат.

Для $n=2s$, $s \in \mathbb{N}$, $k=s+1$ *существует* [illegible] *таких наборов точек* $x_1, \dots, x_k \in [-1; 1]$, *что*

$$M(n, k; x_1, \dots, x_k) = \max \left\{ M(n, 1; x_1), \dots, M(n, 1; x_k) \right\} = M(n, 1; x^*),$$

где $x^* = \max \left\{ |x_1|, \dots, |x_k| \right\}$.

В частности, для $n=2=k$ $(s=1)$ *точки* x_1, x_2 *определяются условием*

$$1+3x_1x_2=0, \quad x_1 \in [-1; -\sqrt{1/3}\,] \cup [\sqrt{1/3}; 1].$$

The research described in this publication was made possible in part by Grant No MC5300 from the International Science Foundation.

УДК 511.9+514.174

С.С.Рышков, К.А.Рыбников (мл) (Москва)

Теория переноса свойства и ее приложения

В сообщении мы рассматриваем достаточно большой класс односвязных комплексов, включающий, например, произвольные грань-в-грань разбиения на выпуклые многогранники евклидова пространства E^n (которые мы ниже обозначаем через $\mathfrak{T}$), и полиэдральной сферы S^n. Мы также считаем заданным так называемое "множество свойств" $\mathfrak{P}$. Это множество, например может быть множеством линейных функций на E^n или каким-нибудь конечным множеством (цветов). Если каждая пара клеток, смежных по $(n-1)$-мерной грани, снабжена парой взаимно обратных элементов группы всех взаимно-однозначных отображений множества $\mathfrak{P}$ на себя, то можно переносить свойство с одной клетки на другую по цепочке последовательно смежных клеток. Наша главная теорема состоит в том, что для однозначности такого переноса достаточно, чтобы он был однозначен в пределах звезды каждой $(n-2)$-мерной грани. Как следствия этой теоремы мы даем доказательство теорем, обобщающих известные теоремы Максвелла ([1],[2]) и Вороного [3].

Теорема 1. Если разбиение $\mathfrak{T}$ имеет выпуклый дуальный граф [4], то оно имеет и женератриссу, то есть в E^{n+1} существует выпуклая полиэдральная поверхность, дающая в проекции разбиение $\mathfrak{T}$.

Теорема 2. Если разбиение $\mathfrak{T}$ таково, что для звезды каждой $(n-3)$-мерной грани существует дуальный многогранник со всеми гранями - треугольниками, то разбиение $\mathfrak{T}$ имеет женератриссу.

Теорема 3. В условиях теоремы 2 одномерный остов разбиения $\mathfrak{T}$ есть паучья сеть [5].

Приведем также один простой пример. Рассмотрим разбиение $\mathfrak{T}$ и множество $\mathfrak{P}$, состоящее из двух элементов: черного и белого цветов. Мы фиксируем цвет для одной из клеток и пытаемся так раскрасить все разбиение, чтобы каждые два смежных многогранника имели разные цвета. Легко видеть, что это невозможно, если в звезде какой-нибудь $(n-2)$-мерной грани содержится нечетное число многогранников разбиения. Оказывается, что если в звезде каждой $(n-2)$-мерной грани содержится по четному числу многогранников разбиения, то требуемая "шахматная" раскраска возможна (см. [6]).

ЛИТЕРАТУРА. 1. J.C.Maxwell, On Reciprocal Diagrams and Diagrams of Forces *Philosophical Magazine*, ser. 4. **27** (1864), 250-261. 2. J.C.Maxwell, On Reciprocal Diagrams, Frames and Diagrams of Forces *Transactions of the Royal Society of Edinburgh*, **26** (1869-72), 1-40. 3. G.F.Voronoi, Nouvelles applications des parameters continus a la theorie des formes quadratiques, Deuxieme memoire, J. Reine Angew. Math., **134** (1908), 198-287; **136** (1909), 67-178. 4. С.С.Рышков, К.А.Рыбников, Женератрисса. Задачи Максвелла и Вороного *Доклады РАН*, (1995), в печати. 5. P.Ash, E.Bolker, H.Crapo and W.Whitely, Convex Polyhedra, Dirihle Tesselations, and Spider Webs, *Shaping space: a polyhedral approach. Eds: Seneshal M., Fleck G.* Boston (1988), 231-250. 6. S.S.Ryshkov, K.A.Rybnikov, The theory of quality translation and its applications in the tiling theory, *Europ.J.Combinatorics*, in print.

Авторы поддержаны ISF, гранты M3D000 и M3D300.

УДК 511

Родосский К. А. (Воронеж)

О существовании элементарных доказательств частных случаев Великой теоремы Ферма

Произвольно фиксируем в кольце Z целых рациональных чисел простое число $p \geqslant 3$. Частным случаем Великой теоремы Ферма является утверждение: для каждой тройки попарно взаимно простых чисел $a, b, c \in Z$ имеет место отрицание равенства

$$a^p + b^p + c^p \neq 0.$$

Метод доказательства от противного сводит проблему доказательства отрицания равенства к опровержению предположения, которое обозначим символом F_p: существуют попарно взаимно простые числа $x, y, z \in Z$ такие, что имеет место равенство

$$x^p + y^p + z^p = 0.$$

Предположение F_p распадается на два случая: в одном из них (первом) предполагается, что ни одно из чисел x, y, z не делится на p; во втором случае предполагается, что одно из этих чисел делится на p. Первый случай обозначим символом $1F_p$, второй случай - символом $2F_p$. Для опровержения предположения F_p достаточно опровергнуть каждый его случай.

Опровержение любого случая предположения F_p называется элементарным, если оно проводится над кольцом рациональных чисел, содержащим кольцо Z в качестве подкольца; в частности, если опровержение проводится над кольцом Z.

Софи Жермен нашла элементарное доказательство условия для каждого $p \geqslant 3$, выполнение которого влечет ложность случая $1F_p$; это достаточное условие называется теоремой Жермен. С помощью теоремы Жермен опровергнуты случаи $1F_p$ для всех $p < 193$ и еще для некоторых других простых чисел, составляющих конечное множество. Других элементарных методов опровержения случаев $1F_p$ не было предложено ни для одного конкретного значения p.

Что касается элементарных опровержений случаев $2F_p$, то в литературе отмечается их полное отсутствие.

В статье автор, с помощью найденного им элементарного метода, опровергает случай $2F_3$. Так как случай $1F_3$ элементарно опровергнут с помощью теоремы Жермен, то предположение F_3 опровергнуто элементарно. Метод автора может быть распространен на другие вторые случаи, например на случай $2F_5$.

УДК 5II.3

Рузимурадов Х.Х. (Самарканд)

ОЦЕНКА СВЕРХУ НОРМЫ МАТРИЧНОГО БАЗИСА РЕШЕТКИ

Пусть $\Lambda = A\mathbb{Z}^n$ решетка в $\mathbb{R}^n$ с матричным базисом $A = (a_{ij})$ Положим $\|A\| = n \max|a_{ij}|$, $\mu = N(\Lambda) = \inf|x_1 x_2 \dots x_n|$ - однородный минимум решетки Λ, где $0 \neq (x_1, x_2, \dots, x_n) \in \Lambda$.

Во многих задачах геометрии чисел появляются оценки сверху нормы матричных базисов решетки (см., например, [I], глава Y, §3). В данной работе получена следующая теорема, в котором норма матричного базиса решетки оценивается при помощи ее однородного минимума.

ТЕОРЕМА. Пусть Λ унимодулярная решетка (т.е., $d(\Lambda) = I$) в $\mathbb{R}^n$ с однородным минимумом μ. Тогда существует постоянная $c(\mu)$, зависящая только от μ и n, такая, что при $\Lambda = A\mathbb{Z}^n$ имеет место следующая оценка $\|A\| \leq c(\mu)$.

ЛИТЕРАТУРА

I. Дж.В.С. Касселс. Введение в геометрию чисел. М.: Мир, I965.

УДК 511.36

Сакович Н.В. (Могилев)

МАЛЫЕ ЗНАЧЕНИЯ МОДУЛЕЙ ПОЛИНОМОВ КОМПЛЕКСНОЙ ПЕРЕМЕННОЙ И РАЗМЕРНОСТЬ ХАУСДОРФА

Пусть $P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 y + a_0$ – многочлен с целыми рациональными коэффициентами и $N_n(w)$ – множество действительных чисел x, для которых неравенство $|P(x)| < H^{-w}$ имеет бесконечное число решений в целочисленных полиномах $P(x) \in \mathbb{Z}[x]$. При $w > n$, как показал Спринджук, это неравенство имеет бесконечное число решений только для множества нулевой меры. В 1970 г. А.Бейкер и В.Шмидт ввели понятие регулярной системы и указали метод, позволяющий с помощью таких систем получать оценки снизу размерности Хаусдорфа. В 1983 г. В.И.Берник в /1/ доказал их гипотезу, состоящую в том, что $\dim N_n(w) = \frac{n+1}{w+1}$.

Мы рассматриваем аналог гипотезы Бейкера-Шмидта для комплексных чисел. Оказывается и в случае поля комплексных чисел можно построить регулярную систему комплексных алгебраических чисел. Получены оценки снизу и сверху размерности Хаусдорфа множества $\mathcal{L}_n(v)$ – множества комплексных чисел z, для которых неравенство $|P(z)| < H^{-v}$ имеет бесконечное число решений в целочисленных полиномах $P(z)$.

Теорема. При $\frac{n-1}{2} < v < 8n+7$ имеем

$$\dim \mathcal{L}_n(v) = \frac{n+1}{v+1}$$

Полученный результат усиливает теорему из /2/.

1. Берник В.И. Acta Arithmetica. – 1983 - Т. 42, №3. – С. 219-253.
2. Берник В.И., Сакович Н.В. Регулярные системы комплексных чисел. //Докл. Акад. наук Беларуси. - 1994. - Т.38, № 5. - С.10-13.

УДК 5II.36

Салихов В.Х. (Брянск)

КРИТЕРИЙ АЛГЕБРАИЧЕСКОЙ НЕЗАВИСИМОСТИ ЗНАЧЕНИЙ ГИПЕРГЕОМЕТРИЧЕСКИХ Е-ФУНКЦИЙ ОДНОГО КЛАССА (ЧЕТНЫЙ СЛУЧАЙ)

Рассмотрим обобщенную гипергеометрическую Е-функцию

$$\varphi(z)=\sum_{n=0}^{\infty}\frac{(\gamma_1)_n\cdots(\gamma_\ell)_n}{(\lambda_1)_n\cdots(\lambda_{t+\ell})_n}\left(\frac{z}{t}\right)^{tn},$$

где $\ell\geq 0$, $t\in\mathbb{N}$, $\gamma_i,\lambda_j\in\mathbb{Q}$, все $\lambda_j\neq 0,-1,-2,\ldots$.

Одной из классических задач в методе Зигеля–Шидловского является доказательство алгебраической независимости чисел

$$\varphi(\alpha),\varphi'(\alpha),\ldots,\varphi^{(t+\ell-1)}(\alpha),\quad \alpha\in\mathbb{A}\setminus\{0\}. \qquad (1)$$

В решении этой задачи в последнее десятилетие достигнут существенный прогресс. В частности, получены достаточные условия, наложенные на параметры γ_i,λ_j при произвольных t,ℓ. В работе [1] эти условия в случае t – нечетно, $\ell=0$, доведены до необходимых. В настоящем докладе получен соответствующий критерий в случае t –четно, $3\nmid t$, $\ell=0$.

Теорема. Пусть $\ell=0$, $t=2\tau$, $\tau\in\mathbb{N}$, $3\nmid\tau$. Числа (1) алгебраически зависимы тогда и только тогда, когда выполнены условия

1) существует $i\in\{1,\ldots,t\}$ такое, что $\lambda_i\in\mathbb{N}$;

2) существуют d –делитель τ, $d\geq 1$, $\chi_0,\ldots,\chi_{d-1}\in\mathbb{Q}$, где $\tau=\frac{\tau}{d}$, такие, что

$$\{\lambda_1,\ldots,\lambda_t\}\equiv\bigcup_{i=0}^{d-1}\left\{\frac{\beta_i}{d},\frac{\beta_i+\frac{1}{2}}{d},\frac{\beta_i+\chi_1}{d},\frac{\beta_i-\chi_1}{d},\ldots,\frac{\beta_i+\chi_{d-1}}{d},\frac{\beta_i-\chi_{d-1}}{d}\right\}\pmod{\mathbb{Z}},$$

$\beta_i=\chi_0+i$.

ЛИТЕРАТУРА

I.Салихов В.Х. Критерий алгебраической независимости значений одного класса гипергеометрических Е-функций //Мат.сб.1990.Т.181, № 2. с.189-211.

И.А.СЕМАЕВ / Москва /

МЕТОД РАЗЛОЖЕНИЯ ЦЕЛЫХ ЧИСЕЛ НА МНОЖИТЕЛИ

Пусть $R(f,g)$ результант многочленов

$$f(x) = a_0x^2 + a_1x + a_2\ ,\quad g(x) = b_0x^2 + b_1x + b_2$$

$R(f,g)$ абсолютно неприводимый многочлен степени 4 от 6 неизвестных. Пусть N произвольное целое число. Предлагается метод решения диофантова уравнения $R(f,g) = N$ относительно целых коэффициентов многочленов $f(x), g(x)$, не превосходящих по модулю величины порядка $O(N^{1/4})$.

Отсюда следует метод разложения числа N.

1. Находим решение уравнения $R(f,g) = N$ - многочлены $f(x)$, $g(x)$ с целыми коэффициентами, модули которых ограничены величиной порядка $O(N^{3/4})$.

2. Вычисляем $d = b_1^2 - 4b_0b_2$ - дискриминант многочлена $g(x)$. Если d есть квадрат целого числа, то переходим к п.3, в противном случае возвращаемся к п.1.

3. Найдем рациональный корень β многочлена $g(x)$, а затем наибольший общий делитель N_1 чисел N и числителя рационального числа $b_0f(\beta)$.

Число N_1 - нетривиальный делитель N. Модуль дискриминанта d многочлена $g(x)$ ограничен величиной $O(N^{1/2})$. Предполагается, что эта величина равномерно распределена в указанных границах. Тогда число шагов алгоритма до выделения нетривиального делителя числа N равно в среднем $O(N^{1/4})$.

И.А.СЕМАЕВ / Москва /

О ВЫЧИСЛЕНИИ ЛОГАРИФМОВ НА НЕКОТОРЫХ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Пусть E эллиптическая кривая над конечным простым полем F_p. Предположим, что мощность множества $E(p)$ F_p-точек кривой E равна p. Т.о. группа $E(p)$ изоморфна аддитивной группе F_p^+. Доказывается

УТВЕРЖДЕНИЕ. Сложность вычисления дискретных логарифмов в группе $E(p)$ не больше сложности $O(\ln p)$ операций в поле F_p.

Доказательство основано на алгоритме быстрого вычисления изоморфизма $E(p) \to F_p^+$. Пусть $Q \in E(p)$. Существует функция f_Q на E, дивизор которой равен $p((Q) - (\infty))$. Рассмотрим разложение f_Q в точке $R \in E(p)$:

$$f_Q = a_0 + a_1 t_R + a_2 t_R^2 + \dots$$

где t_R локальный параметр в т. R. Нетрудно найти точку R т.о., чтобы $a_0, a_1 \neq 0$. Из результатов теории обобщенных якобианов [1] следует, что отображение $Q \to a_1 a_0^{-1}$ устанавливает изоморфизм $E(p)$ и F_p^+. Пользуясь тождеством работы [2], легко можно определить, что значения функции f_Q и производной функции f_Q в т. R могут быть вычислены со сложностью не более $O(\ln p)$ операций в поле F_p.

Этот результат обобщается на случай якобианов над конечными полями.

1. Серр Ж. Алгебраические группы и поля классов.-М.:Мир,1968
2. Семаев И.А. Быстрый алгоритм вычисления спаривания А.Вейля на эллиптических кривых. Международная конференция " Современные проблемы теории чисел" , Тула, 1993, Тезисы докладов.

УДК 511.337

Сенчуков В.Ф. (Харьков)

РЕКУРСИВНЫЕ ФОРМУЛЫ ПРОСТЫХ ЧИСЕЛ-БЛИЗНЕЦОВ

Рассматривается приложение конструктивных средств последовательностной интерпретации алгебры логики [1] к аналитическому описанию последовательности простых чисел-близнецов.

Обозначим: $D_\kappa = p_1 p_2 \dots p_\kappa$, $\kappa = 1,2,\dots$, p_κ -простые числа, $\varphi_\kappa(a)$ -число чисел, взаимно простых с D_κ и не превышающих a, $\varphi_\kappa(D_\kappa) = T_\kappa = (p_1-1)\dots(p_\kappa-1)$; $S_\kappa(n)$-последовательность приведенных систем вычетов по модулю D_κ, $S_0(n) = n$; $\psi_\kappa(a)$-число пар чисел, взаимно простых с D_κ, разность между которыми равна 2 и первый элемент пары не превышает a, $\psi_\kappa(D_\kappa) = \Gamma_\kappa = (p_1-1)(p_2-2)\dots(p_\kappa-2)$; $\Gamma_0 = T_0 = p_0 = 1$.

Пусть $\{(\beta_\kappa(n), \gamma_\kappa(n))\}$ -последовательность пар чисел, взаимно простых с D_κ и таких, что $\gamma_\kappa(n) - \beta_\kappa(n) = 2$. Установлено, что последовательность $\beta_\kappa(n)$ как функцию натурального аргумента можно представить в виде:

$$\beta_\kappa(n) = \beta_{\kappa-1}(\mathcal{U}_\kappa(n)), \quad \beta_0(n) = n, \tag{1}$$

где

$$\mathcal{U}_\kappa(n) = \sum_{i=1}^{p_\kappa \Gamma_{\kappa-1}} \left[\frac{1}{\Gamma_\kappa} \left(n + \Gamma_\kappa - 1 - \psi_\kappa(\beta_{\kappa-1}(i)) \right) \right] + 1,$$

$[\cdot]$ -функция антье.

Другое описание $\beta_\kappa(n)$ получаем исходя из $S_\kappa(n)$ [2]:

$$\beta_\kappa(n) = S_\kappa(\nu_\kappa(n)), \tag{2}$$

где

$$\nu_\kappa(n) = \sum_{i=1}^{T_\kappa} \left[\frac{1}{\Gamma_\kappa} \left(n + \Gamma_\kappa - 1 - \psi_\kappa(S_\kappa(i)) \right) \right] + 1.$$

Для каждого κ в (1) и (2) функция $\beta_\kappa(n)$ при $1 \le n \le \psi_\kappa(p_{\kappa+1}^2 - 2)$ дает один и тот же отрезок последовательности простых чисел-близнецов.

Лит.:[1] Сенчуков В.Ф. Последовательностная модель булевой алгебры //Докл.АН УССР.Сер.А.-1988.-№2.-С.20-23.

[2] Сенчуков В.Ф. Логические операции над последовательностями и закон простых чисел //Докл.АН УССР.Сер.А.-1988.-№6.-С.21-24.

Синюкова Е. Н. (Одесса)

НЕКОТОРЫЕ ГЛОБАЛЬНЫЕ АСПЕКТЫ ТЕОРИИ HP-ОТОБРАЖЕНИЙ H-ПРОСТРАНСТВ

Вещественное риманово C^r-пространство V^n четной размерности ($n>2$, $r>1$) с метрическим тензором g_{ij} называется H-пространством H^n, если на нем определен аффинор F_i^h, удовлетворяющий соотношениям

$$F_\alpha^h F_i^\alpha = -\delta_i^h \qquad F_{ij}^h = -F_{\alpha\beta}^h F_i^\alpha F_j^\beta \qquad g_{\alpha\beta} F_i^\alpha F_j^\beta = g_{ij} \qquad F_{(h,ij)} = 0,$$

где $F_{hi} = g_{h\alpha} F_i^\alpha$.

C^2-кривая C^r-пространства H^n ($n>2$, $r>1$), в локальной системе координат заданная уравнениями $x^h = x^h(t)$, называется HP-кривой, если в каждой точке $M \in H^n$ для нее справедливы соотношения $\eta_\alpha^h \eta^\alpha = a(t)\eta^h + b(t)\eta^{\bar h}$, где $\eta^h = dx^h/dt$, $\eta^{\bar h} = \eta^\alpha F_\alpha^h$. Для H-пространств изучают отображения, сохраняющие почти комплексную структуру и HP-кривые. Они называются HP-отображениями (HPO) [1].

На основе исследования формул типа Таллини для HP-отображений H-пространств доказана теорема 1.

Теорема 1. HPO компактного C^r-пространства H^n ($r>2$) на пространство $\bar H^n$ тривиально (является аффинным), если в общей по отображению системе координат инвариант $g^{\alpha\beta}(\bar R_{\alpha\beta} - R_{\alpha\beta})$ не изменяет знак на всем H^n.

Теорема 2. Компактные с положительно определенной метрикой C^r-пространства H^n($r>2$), в которых для произвольного симметричного тензора $b^{\alpha\beta}$ имеет место неравенство

$$T_{\alpha\beta\sigma\rho} b^{\alpha\beta} b^{\gamma\sigma} \geqslant 0, \qquad (1)$$

в целом не допускают нетривиальных HPO. Здесь $T_{\alpha\beta\sigma\rho}$ - тензор, специальным образом выражающийся через тензоры Римана и Ричи пространства H^n.

Условию (1) удовлетворяют, к примеру, голоморфно-плоские пространства H^n с $R \geqslant 0$.

Следствие. Компактные с положительно определенной метрикой C^r-пространства H^n($r>2$), в которых для произвольного симметричного тензора b^{ij}

$$R_{\alpha\beta\sigma\rho} b^{\alpha\beta} b^{\gamma\sigma} \leqslant 0 \qquad R_{\bar\alpha\bar\beta\sigma\rho} b^{\alpha\beta} b^{\gamma\sigma} \leqslant 0,$$

в целом не допускают нетривиальных HPO.

1. Синюков Н. С., Курбатова И. Н., Микеш Й., Голоморфно-проективные отображения келеровых пространств. Учебное пособие, Одесса, 1985.

УДК 517.524

Скоробогатько В. Я. (Львов)

О ПРЕДСТАВЛЕНИИ ИРРАЦИОНАЛЬНОСТЕЙ ВЫСШИХ СТЕПЕНЕЙ ВЕТВЯЩИМИСЯ ЦЕПНЫМИ ДРОБЯМИ

В [1] построен алгоритм разложения действительного числа в ветвящуюся цепную дробь и указаны его приложения (в частности, в электростатике). Тут приводится модифицированная модель этого алгоритма и ее применения в теории иррациональностей высших степеней.

Ветвящейся цепной дробью называется выражение

$$\alpha = \sum_{k_1=1}^{N} \cfrac{a_{k_1}}{b_{k_1} + \sum\limits_{k_2=1}^{N} \cfrac{a_{k_1k_2}}{b_{k_1k_2} + \ddots + \sum\limits_{k_n=1}^{N} \cfrac{a_{k_1k_2\ldots k_n}}{b_{k_1k_2\ldots k_n} + \ddots}}}. \qquad (1)$$

В алгоритме числа $a_{k_1k_2\ldots k_s}$ равны единице, $b_{k_1k_2\ldots k_s}$ — некоторые натуральные числа. Если число α можно представить периодической дробью вида (1) (определение периодичности дроби дается, а алгоритм получения чисел $b_{k_1k_2\ldots k_s}$ указан), то значение α является алгебраической иррациональностью высшей степени. Эта степень зависит от числа ветвления N.

Литература

[1] В. Я. Скоробогатько. Разложение действительного числа в ветвящуюся цепную дробь, препринт ИППММ НАН Украины, Львов, 1993.

УДК 511.9

А.А.СНЕГОВОЙ (ВНИИГеосистем)

ИСПОЛЬЗОВАНИЕ ВВЕДЕНИЯ МЕРЫ ДЛЯ АНАЛИЗА ВЫЧИСЛИТЕЛЬНОЙ ЭФФЕКТИВНОСТИ КВАДРАТУРНЫХ И КУБАТУРНЫХ ФОРМУЛ ЧИСЛЕННОГО ИНТЕГРИРОВАНИЯ.

В работах [1-3] был предложен новый подход к оценке "качества" различных алгоритмов вычисления интегралов, позволяющий эффективно сравнивать, как детерминированные, так и стохастические (метод Монте-Карло) алгоритмы. При таком подходе, за меру качества алгоритма интегрирования предлагается принять среднеквадратическое значение погрешности между точным значением интеграла и его значением полученным с помощью данного алгоритма, при этом, средний квадрат погрешности усредняется по некоторой мере (называемой мерой введения) определяемой на классе функций, разложимых по базису Фабера-Шаудера. Показано, что предлагаемый подход удобен для оценки сравнительной эффективности различных квадратурных и кубатурных формул.

Л И Т Е Р А Т У Р А

1. Воронин С.М., Скалыга В.И. О квадратурных формулах // Доклады АН СССР. 1984, т.276, No.5, с.1038-1041.

2. Smale S. On the efficiency of algorithms of analysis // Bull. Amer. Math. Soc., 1985, vol.13, No.2, p.p. 87-121.

3. Снеговой А.А., Тищенко С.А. Использование введения меры для анализа вычислительной эффективности квадратурных и кубатурных формул численного интегрирования. // Мат. заметки (в печати)

Работа выполнена при финансовой поддержке Российского Фонда Фундаментальных Исследований, грант No. 93-011-16021

УДК 511.216

Станкус Э.* (Вильнюс, Литва)

ОБОБЩЕННЫЕ ЧИСЛА

Элементы последовательности $\{q_n\}$, удовлетворяющей условиям $1 < q_1 \leqslant q_2 \leqslant \ldots q_n \to \infty$, называются обобщенными простыми числами (g-простыми) [2]. Рассмотрим мультипликативную полугруппу B, порожденную этими g-простыми числами. Как известно, элементы $\nu_1 = 1 < \nu_2 < \nu_3 < \ldots$ (g-целые) полугруппы B g-простыми числами представляются неоднозначно. Обозначим соответственно через $\beta_1 = 1, \beta_2, \beta_3, \ldots$ числа таких представлений. Тогда сумма $B(x) = \sum_{\nu_i \leqslant x} \beta_i$ есть число g-целых, не превосходящих x.

Теорема. Пусть $q_n = p_{N+n} - r$, $n = 1, 2, \ldots$ последовательность g простых, где $r \geqslant 1$, $N = \pi(r) + 1$, p_n nое рациональное простое число, $\pi(r)$ как обычно, число простых чисел, не превосходящих r. Тогда существует постоянная $c = c(r) > 0$, что, при $x \to \infty$,

$$B(x) = B_r x + O_r\left(x \exp\left\{-\left(1 - \frac{c}{\log\log x}\right)\sqrt{\frac{1}{2}\log x \log\log x}\right\}\right), \qquad (1)$$

где

$$B_r = \prod_{p \leqslant p_N} \left(1 - \frac{1}{p}\right) \prod_{p > p_N} \left(1 + \frac{r}{p(p-r-1)}\right).$$

Теорема доказана аналитическим методом применяя контурное интегрирование.

При $r = 1$ из формулы (1) следует (см. [1]) асимптотическая формула для суммы $A(x) = \sum_{\varphi(n) \leqslant x} 1$, где $\varphi(n)$ – функция Эйлера. В этой формуле оценка остатка более точна по порядку роста чем в эффективной теореме А.Смати [3], доказанной элементарным методом.

ЛИТЕРАТУРА

1. P. T. Bateman, The distribution of values of the Euler function. *Acta Arith.*. **21**(1972). 329-344.

2. A. Beurling, Analyse de la loi asymptotique de la distribution des nombres premiers généralisés, *Acta Math.* **68**(1937), 255-291.

3. A. Smati, Evaluation effective du nombre d'entiers n tels que $\varphi(n) \leqslant x$, *Acta Arith.* **61.2**(1992), 143-159.

* Работа выполнена при поддержке фонда науки и студий Литвы

УДК 511.251; 512.94

Стахов С.В. (С.-Петербург)

ПОЗИЦИОННЫЕ СИСТЕМЫ СЧИСЛЕНИЯ В ТЕЛЕ КВАТЕРНИОНОВ

Построены три инъективных отображения алгебры кватернионов $\mathbb{R}^{\mathbb{H}}$ во множество кодовых последовательностей $(g_n)_{n\in\mathbb{Z}}$

$$Code_\sigma : \mathbb{R}^{\mathbb{H}} \to \{ (g_n)_{n\in\mathbb{Z}} \mid g_n \in G\cup\{0\} \}$$

$$q \longmapsto (g_n)\Big|_{\sum \delta_\sigma^n \cdot g_n = q} = Code_\sigma(q) \qquad (1)$$

с ненулевыми цифрами g_n из бинарной группы $G \in \{T^*, O^*, I^*\}$, $G\subset\mathbb{H}_1$ правильного многогранника (тетраэдра, октаэдра, икосаэдра) [1] и основанием δ_σ из евклидова подкольца $\mathbb{Z}G$, аддитивно порожденного группой G в алгебре $\mathbb{R}^{\mathbb{H}}$ [2]. Эти отображения названы позиционными системами счисления, индуцированными группой G в $\mathbb{R}^{\mathbb{H}}$.

Инъекция (1) переносит структуру тела кватернионов $(\mathbb{H},+,\cdot)$ на свой образ $\mathcal{R}_\sigma = Code(\mathbb{R}^{\mathbb{H}})$

$$Code_\sigma : (\mathbb{H},+,\cdot) \to (\mathcal{R}_\sigma,+,\cdot). \qquad (1')$$

ТЕОРЕМА 1. Подмножество кодов

$$\mathcal{R}_0 = \{ (g_n)_{n=M}^{N} \mid M,N \in \mathbb{Z} \} \subset \mathcal{R}_\sigma \qquad (2)$$

с конечными носителями (нулевые начало и конец отброшены) образуют кольцо $(\mathcal{R}_0,+,\cdot)$, вложимое в тело кватернионов $(\mathbb{H},+,\cdot)$

$$Qu_\sigma : \mathcal{R}_0 \to \mathbb{H}\ ,\ (g_n) \mapsto \sum_M^N \delta_\sigma^n \cdot g_n = Qu_\sigma((g_n)). \qquad (3)$$

Образ кольца $(\mathcal{R}_0,+,\cdot)$ конечных кодов при этом вложении совпадает с кольцом $\mathbb{Z}[1/2]\cdot T^*$ для $G = T^*$ или $\mathbb{Z}G$ для $G \in \{O^*, I^*\}$ и всюду плотен в $(\mathbb{R}^{\mathbb{H}}, |\ |^2)$. Группа единиц $\mathcal{R}_\sigma^\times = G \rtimes \langle\delta_\sigma\rangle$ (полупрямое).

Для группы $G = T^*$ тетраэдра построены алгоритмы сложения и умножения конечных кодов (g_n) без вычисления вложения (3) в $\mathbb{R}^{\mathbb{H}}$. Временная вычислительная сложность этих алгоритмов в $\mathcal{R}_2$ зависит линейно и квадратично (соответственно) от длины $L=N-M+1$ складываемых и перемножаемых кодов.

Гипотеза. Подмножество $\mathcal{P}_\sigma$ периодических кодов из $\mathcal{R}_\sigma$ является телом $(\mathcal{P}_\sigma,+,\cdot)$, изоморфным $Qu_\sigma(\mathcal{P}_\sigma) = \mathbb{Q}G$ рациональной подалгебре $(\mathbb{Q}G,+,\cdot)$ с делением [2], порождаемой группой G в $\mathbb{R}^{\mathbb{H}}$.

Литература

1. Кострикин А.И. Введение в алгебру. М., "Н.", 1977, с.375.
2. Стахов С.В. Евклидовость подколец тела кватернионов, порожденных некоторыми конечными подгруппами. Деп. ВИНИТИ №398-85 26с. РЖМат, 1985, 5 А467.

УДК 51

Степанова Л.Л. (Москва)

Дополнительные главы элементарной математики (Арифметика)

Переход на многоуровневую систему подготовки специалистов для средней школы, открытие магистратуры образования, введение элементарной математики на старших курсах математического факультета педвузов и университетов открывает новые возможности улучшения арифметической подготовки учителя-магистра. Предлагаемая ниже программа курса "дополнительные главы элементарной математики"раздел **"Арифметика"**нацелена на решение этой задачи и была апробирована в течение 3-х лет на **матфаке МПГУ**.

I. Арифметические функции. (1). **Функция Мёбиуса** и точные формулы для $\pi(x)$. **Функция $\Phi(x,\sqrt{x})$. Теорема Лежандра. Формула Мейселя** для $\pi(x)$. (2). Числа, свободные от квадратов. **Бесквадратные числа** и $\pi(x)$. Расходимость ряда Σp^{-1}. **Функция $[\sqrt{x}]$. Функция $Q(x)$.** Значение суммы $\Sigma Q(x/k^2)$. (3). Суммы по делителям. **Формулы обращения Мёбиуса** и их применение к нахождению арифметических функций и вычислению различных сумм. Теорема о среднем значении суммы по делителям и её применение к функциям $\tau(n)$, $\sigma(n)$, $\sigma_k(n)$, $\lambda(n)$. (4). Точные формулы для **суммы Дирихле**. Преобразования сумм.

II. Факторизация натуральных чисел. Факторизация натуральных чисел с помощью деления на простые $p\le\sqrt{n}$. Критерии простоты: теорема **Эйлера** о разности двух квадратов, построение рекуррентной последовательности, представление чисел квадратичными формами, теорема о представлении натурального числа квадратичной формой вида $ax^2 + by^2$. Удобные числа. **Числа Ферма и Мерсенна. Теоремы Евклида и Эйлера** о четных совершенных числах. Проблемы. Числа избыточные и недостаточные. Факторизация чисел **Мерсенна** и чисел **Ферма**. Задача построения правильных многоугольников Числа **Ферма** и бесконечность простых в некоторых арифметических прогрессиях. **Разложение на множители и шифрование**.

III. Диофантовы уравнения. Уравнения первой степени. Теорема **Ламэ**. Общий метод решения диофантова уравнения первой степени. Уравнения второй степени. **Пифагоровы тройки. Треугольные числа**. Уравнение **Пелля-Ферма**. Диофантовы уравнения выше второй степени. Неразрешимость некоторых уравнений.

IY. Суммирование числовых последовательностей. Степенные суммы. Преобразование **Абеля**. Применение формулы **Муавра**. Теорема о числе бесквадратных чисел. **Числа Бернулли.**

Y. Средние значения некоторых арифметических функций. Точки с целыми координатами. Точки под гиперболой и в круге. Среднее значение функции **Эйлера** и функции $\delta(n)$. **Фареевы дроби.**

УДК 511.335

Стяпанаускас Г.* (Вильнюс, Литва)

СРЕДНИЕ ЗНАЧЕНИЯ МУЛЬТИПЛИКАТИВНЫХ ФУНКЦИЙ СО СДВИНУТЫМИ АРГУМЕНТАМИ

Пусть $g_1, g_2 : \mathbb{N} \to \mathbb{C}$ - мультипликативные функции, $|g_i| \leqslant 1$, $i = 1,2$.

Немало работ посвящено ассимптотикам средних значений таких функций на разных множествах. В исследованиях применяются также средние значения со сдвинутыми аргументами

$$\sum_{n \leqslant x} g_1(n+a) g_2(n). \tag{1}$$

Автор, используя некоторые идеи недавных работ А.Хильдебранда и Р.Варлимонта, получил новые результаты о поведении сумм вида (1) и аналогичных сумм по более "редким" множествам.

Сформулируем один из результатов.

Теорема. Пусть

$$P(x) = \prod_{p \leqslant x} \left(1 - \frac{2}{p} + \left(1 - \frac{1}{p}\right) \sum_{m=1}^{\infty} \frac{(g_1 + g_2)(p^m)}{p^m}\right),$$

$$Q(x) = \prod_{p \leqslant x} \left(1 - \frac{2}{p-1} + \sum_{m=1}^{\infty} \frac{(g_1 + g_2)(p^m)}{p^m}\right),$$

$$R(r,x) = \sum_{r < p \leqslant x} \frac{|g_1(p) - 1|^2 + |g_2(p) - 1|^2}{p} + \frac{1}{r \log r}.$$

Пусть далее $x \geqslant r \geqslant 2$, $A > 0$, $\varepsilon > 0$. Тогда $\exists c$ и $c_1 = c_1(\varepsilon)$ такие, что

$$\frac{1}{x} \sum_{n \leqslant x} g_1(n+1) g_2(n) = P(x) + O\left(e^{cr^{2/3}} x^{-1/3} + \left(R(r,x)\right)^{1/2}\right),$$

$$\frac{1}{\pi(x)} \sum_{p \leqslant x} g_1(p+2) g_2(p+1) = Q(x) + O_{\varepsilon,A}\left(e^{cr^{\varepsilon}} (\log x)^{-A} + \left(R(r,x)\right)^{1/2}\right).$$

Пусть φ - функция Эйлера, σ - сумма делителей, I_k - индикатор множества $A_k = \left\{n \,\middle|\, p^m \| n \Rightarrow m < k\right\}$ $(k \geqslant 2)$. Тогда теорему можно применять разным комбинациям произведений функций

$$\frac{\varphi(n)}{n}, \quad \frac{n}{\sigma(n)}, \quad \frac{\varphi(n)}{\sigma(n)}, \quad I_k(n).$$

Причем, остаточные члены для этих функций удается получить немного лучше чем дает теорема.

* Работа выполнена при поддержке фонда науки и студий Литвы

УДК 511.9

Таммела П.П. (Таллинн)

О НЕКОТОРЫХ АЛГОРИТМАХ ТЕОРИИ ПРИВЕДЕНИЯ ПОЛОЖИТЕЛЬНЫХ КВАДРАТИЧНЫХ ФОРМ

Пусть $f = f(x) = f(x_1, x_2, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} \cdot x_i \cdot x_j$ — n-арная положительно определенная квадратичная форма с вещественными коэффициентами a_{ij}, причём $a_{ij} = a_{ji}$, $(i, j = 1, \ldots, n)$. Множество всех положительных квадратичных форм определяет в пространстве коэффициентов R^N, $N = n(n+1)/2$ так называемый конус положительности $\mathfrak{R}$. В этом пространстве каждой квадратичной форме отвечает точка $f = (a_{11}, \ldots, a_{nn}, a_{12}, \ldots, a_{n-1,n})$.

Пусть f_1 и f_2 — две вещественные квадратичные формы. Говорят, что формы f_1 и f_2 эквивалентны, если найдутся целочисленные подстановки S_1 и S_2 для которых

$$f_1 \cdot S_1 = f_2 \text{ и } f_2 \cdot S_2 = f_1.$$

Решение многих вопросов теории чисел требует исследования эквивалентности положительных квадратичных форм. При этом рассматриваются задачи: 1. эквивалентности двух форм; 2. нахождения всех преобразований эквивалентности; 3. нахождения всех автоморфизмов данной квадратичной формы. Эти проблемы решаются при помощи теории приведения положительных квадратичных форм. Среди положительных квадратичных форм теми или иными условиями выделяются формы, называемые приведёнными. При этом каждая приведённая форма должна быть эквивалентна хотя бы одной приведённой форме, и должен быть более или менее удобный алгоритм, переводящий заданную форму f в приведённую φ и одновременно строящий целочисленную матрицу S преобразования f в φ, $f \cdot S = \varphi$.

В докладе рассматриваются различные алгоритмы и их реализации на ЭВМ, в том числе алгоритмы из [1] и [2].

ЛИТЕРАТУРА

[1] Afflerbach L. Die Gütebewertung von Pseudo-Zufallszahlen-Generatoren aufgrund theoretischer Analysen und algorithmischer Berechnungen, Grazer Mathematische Berichte Nr.309, (1990).

[2] Lenstra A.K., Lenstra H.W. Jr., Lovasz L. Factoring Polynomials with Rational Coefficients, Math. Ann., 261, 515-534 (1982).

УДК 517 + 511

Гашбаев В.Х. (Душанбе)

О вероятностных методах в p-адических полях.

В предлагаемом докладе рассматриваются некоторые проблемы теории вероятностей в p-адических полях Q_p, (p - простое число) в связи с оценками тригонометрических сумм. Известно, что оценки тригонометрических сумм Г. Вейля, полученные И.М. Виноградовым дали значительные результаты в теории кодирования, распознавания образов, линейных рекурсивных последовательностей и т.д. ; которые широко применяются в решении вопросов прикладной математики.

В последнее время происходит бурное развитие применения p-адического анализа в различных областях математики [1,2] (дифференциальные уравнения, спектральной теории, теории обобщенных функций и в теории вероятностей) с одной стороны. С другой стороны достаточно глубоко развивается теория оценок тригонометрических сумм на основе p-адического анализа [3].

В сообщении дается обзор круга вопросов, связанных с применением новейших оценок тригонометрических сумм к задачам теории вероятностей (статстабилизации, закона больших чисел, центральных предельных теорем) в p-адических полях Q_p. Изучаются связи, статистические модели, алгоритмы и функциональные отображения вероятностных показателей в полях вещественных чисел и в поле Q_p для различных систем.

Цитированная литература:

1. Владимиров В.С. Волович И.В. , ДАН СССР, 1988 Т.302 N 2 . С. 320-322

2. Безгин В.В. , Хренников А.Ю. , Эндо М. , Юко О. ДАН РА. 1994. Т.334 N 1, С. 5-8

3. Постников А.Г. . Изв. АН СССР. Сер. мат. 19 (1955) С. 11-16

УДК 511

Тимофеев Н.М. (Владимир)

АДДИТИВНАЯ ПРОБЛЕМА ДЕЛИТЕЛЕЙ С РАСТУЩИМ ЧИСЛОМ СОМНОЖИТЕЛЕЙ.

Пусть $\tau_k(n)$-число представлений n в виде произведения k-сомножителей.
Обозначим

$$S_k(x) = \sum_{n \le x} \tau_k(n)\, \tau_2(n+1).$$

С помощью дисперсионного метода Ю.В.Линник [1] доказал, что

$$S_k(x) = k!\, A_k\, S_k\, x(\ln x)^k + O(x(\ln x)^{k-1}(\ln_2 x)^{k^4}),$$

где $\ln_2 x = \ln\ln x$, A_k, S_k - постоянные зависящие от k. Мотохаши [2] доказал асимптотическую формулу для $S_k(x)$ с остатком равным $O(x(\ln_2 x)^c/\ln x)$, где c-постоянная зависящая от k. В работах [1] и [2] предполагается, что k-фиксированное число.

Основной результат работы следующий:

Теорема. Равномерно по k, при $80k^{10}(\ln_2 x)^3 \le \ln x$

$$S_k(x) = \frac{x(\ln x)^k}{(k-1)!} \prod_p \left(1 - \frac{1}{p} + \frac{1}{p}\left(1 - \frac{1}{p}\right)^{k-1}\right)\left(1 + O\left(k^{5/2}(\ln x)^{-1}\right)\right)$$

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (93-01-00260).

Литература

[1] Линник Ю.В. Дисперсионный метод в бинарных аддитивных задачах. Издательство Ленинградского университета, 1961.

[2] Motohashi Y. An asymtotic series for an addititve divisor problem// Math. Zeitschrift. 1980. Bd. 179. s. 43-63.

УДК 5II.5

Ташпулатов Б.Т. (Ташкент)

ПРОБЛЕМА Д.МАМФОРДА И ФОРМУЛЫ ТИПА КЛОСТЕРМАНА ДЛЯ КОЛИЧЕСТВА ПРЕДСТАВЛЕНИЙ ЧИСЕЛ КВАДРАТИЧНЫМИ ФОРМАМИ

В книге Д. Мамфорда [I, с.98] поставлена следующая проблема: верно ли, что любая параболическая форма веса $\ell \geq 3$ равна полиному степени 2ℓ от тэта - функций с рациональными характеристиками?

Эта проблема решена нами [2] для параболических форм вида

$$\sum_{x_1, \ldots, x_n = -\infty}^{+\infty} q^{a_1^2 x_1^2 + \ldots + a_n^2 x_n^2} = \frac{1}{2} + \sum_{m=1}^{+\infty} \left(a_1^2 x_1^2 + \ldots + a_n^2 x_n^2, m \right) q^m,$$

где $\left(a_1^2 x_1^2 + \ldots + a_n^2 x_n^2, m \right)$ - сингулярный ряд Харди-Литтлвуда [2, с.56], $q = e^{\pi i \tau}$, x_i - любые целые числа, $\operatorname{Im} \tau > 0$.

Эти результаты применены нами для получения формул типа Клостермана для некоторых классов квадратичных форм с тремя и более переменными.

ЛИТЕРАТУРА

I. Мамфорд Д. Лекции о тэта-функциях (пер. с англ.) - М., Мир, I988. - 448 с.

2. Ташпулатов Б.Т., Коган Л.А. Представление чисел квадратичными формами. - Т., Фан, I993. - II2 с.

УДК 5II.36

Тищенко К.И. (Минск)

ПРИБЛИЖЕНИЕ ЦЕЛЫХ p-АДИЧЕСКИХ ЧИСЕЛ АЛГЕБРАИЧЕСКИМИ ОГРАНИЧЕННОЙ СТЕПЕНИ

В I96I году Е.Вирзинг [I] доказал следующую теорему: для любого действительного числа α, не являющегося алгебраическим числом степени $\le k$, существует бесконечное множество действительных алгебраических чисел β степени $\le k$ таких, что

$$|\alpha-\beta| \ll H(\beta)^{-k/2-\nu} \qquad (1)$$

при $\nu=3/2$. В [2] получено усиление этого результата: показатель ν в (I) заменён на γ_k, где $\lim\limits_{k\to\infty} \gamma_k=3$.

Нами получено p-адическое обобщение этого результата: для любого целого p-адического α существует бесконечное множество действительных алгебраических чисел β степени $\le k$ таких, что

$$\|\alpha-\beta\|_p \ll H(\beta)^{-(k+3)/2}.$$

литература. I. В.Шмидт. Диофантовы приближения. М.,I983.
2. В.И.Берник, К.И.Тищенко. Целочисленные полиномы с перепадом величин коэффициентов и теорема Вирзинга // ДАН Беларуси, I993, т.37, № 5, с.9-II.

О.В.ТЫРИНА

МГТУ им. Н. Э.Баумана

О ЧИСЛЕ ПЕРЕМЕННЫХ В АСИМПТОТИЧЕСКОЙ ФОРМУЛЕ В ПРОБЛЕМЕ ВАРИНГА

Одной из наиболее известных проблем аддитивной теории чисел является проблема Варинга для числа I_N представлений натурального числа N в виде $N = x_1^n + \ldots + x_\tau^n$ с натуральными $x_1, \ldots, x_\tau$.

В следующей теореме уменьшается число переменных в проблеме Варинга, при котором справедлива обычная асимптотическая формула для числа I_N.

Теорема. Пусть $\bar{\tau} = 1820$ при $n = 11$, $\bar{\tau} = 2224$ при $n = 12$, $\bar{\tau} = [2n^2(2\ln n + \ln\ln n + 2{,}3)]$ при $n \geqslant 13$. Тогда при $\tau \geqslant \bar{\tau}$ для числа I_N представлений натурального числа N в виде $N = x_1^n + \ldots + x_\tau^n$ с натуральными $x_1, \ldots, x_\tau$ справедлива асимптотическая формула

$$I_N = \frac{\left(\Gamma\left(1+\frac{1}{n}\right)\right)^\tau}{\Gamma\left(\frac{\tau}{n}\right)} N^{\frac{\tau}{n}-1} \mathfrak{S} + O\left(N^{\frac{\tau}{n}-1-\frac{1}{20n\ln n}}\right),$$

где Γ – гамма-функция Эйлера, $\mathfrak{S}$ – особый ряд проблемы Варинга.

Эта теорема при $n \geqslant 11$ улучшает результаты Р.Вона [1] и И.М.Виноградова [2].

ЛИТЕРАТУРА

1. Vaughan R.C. On Waring's problem for smaller exponents II // Mathematika. 1986. V.33, N1 P.6-22.

2. Виноградов И.М. Метод тригонометрических сумм в теории чисел. М.: Наука, 1971.

3. Тырина О.В. Средние значения тригонометрических сумм. Кандидатская диссертация. МГУ. М. 1989.

УДК 511

Толстиков А.В. (Череповец)

ОБ ИНТЕГРАЛЬНОМ КОРНЕ В КОЛЬЦЕ АРИФМЕТИЧЕСКИХ ФУНКЦИЙ

Пусть S – коммутативная полугруппа с единицей e и однозначным разложением на простые множители, P – множество всех ее простых элементов. Тогда для любого $m \in S$ имеем $m = p_1^{d_1} p_2^{d_2} \dots$, где все $p_i \in P$, а среди целых чисел $d_i \geq 0$ есть лишь конечное число, отличных от нуля. Обозначим через $\Omega(m) = d_1 + d_2 + \dots$. Рассматривается арифметическая свертка (интегральное произведение) функций f и g из S в произвольное числовое поле K:

$$(f \circ g)(m) = \sum_{d_1 d_2 = m} f(d_1)\, g(d_2),$$

где суммирование ведется по всем различным решениям уравнения $d_1 \cdot d_2 = m$ в полугруппе S. В работе [1] находится явная формула для решения функционального уравнения $f = g \circ h$, где f, g – данные функции, $g(e) \neq 0$, h – искомая функция.

Функция g называется интегральным корнем n – й степени из функции f, если f есть n – я интегральная степень функции g: $f = g \circ g \circ \dots \circ g = g^{(n)}$ (n – сомножителей).

ТЕОРЕМА. Пусть $f(e) \neq 0$. Тогда функция g, являющаяся квадратным интегральным корнем из функции f, имеет следующее явное выражение:

$$g(m) = \sqrt{f(e)} \sum_{k=1}^{\Omega(m)} (-1)^{k-1} \cdot 2^{1-2k} \cdot f^{k}(e) \cdot a(k,0) \cdot f^{(k)}(m),$$

где $\sqrt{f(e)}$ – один из квадратных корней из числа $f(e)$, $f^{(k)}$ – k – я интегральная степень f, коэффициенты $a(k,0)$ вычисляются по следующим рекуррентным формулам: $a(1,0) = 1$, $a(k,k) = 1$ $(k \geq 1)$,
$a(k,0) = a(k-1,1)$ $(k \geq 2)$, $a(k,1) = 2a(k-1,1) + a(k-1,2)$ $(k \geq 2)$,
$a(k,i) = a(k-1,i-1) + 2a(k-1,i) + a(k-1,i+1)$; $i = 2,3,\dots,k-2$ $(k \geq 3)$.
$a(k,k-1) = a(k-1,k-2) + 2a(k-1,k-1)$ $(k \geq 3)$, $k \in \mathbb{N}$.

Вычисление коэффициентов $a(k,i)$ удобно вести методом аналогичным треугольнику Паскаля для биноминальных коэффициентов.

Лит.: [1] Данилов А.Н., Толстиков А.В. Об одном функциональном уравнении полугруппы. 27 Герценовские чтения. Математика. – Л., 1973. – С.3–8.

УДК 511.5

Трелина Л.А. (Минск)

О СУПЕРЭЛЛИПТИЧЕСКОМ УРАВНЕНИИ

Пусть K – конечное расширение поля $\mathbf{Q}$, $\mathcal{O}_K$ – кольцо его целых элементов, S – конечное подмножество множества точек поля K, содержащее все архимедовы точки, $\mathcal{O}_S$ – кольцо S-целых элементов поля K, U_S – группа S-единиц в K. В работах А.Бейкера, а затем и других авторов (см. [1]) получены эффективно вычислимые границы для высот решений $(x, y) \in \mathcal{O}_S^2$ уравнения

$$f(x) = ay^m \qquad (*)$$

где $f \in \mathcal{O}_K[X]$ – сепарабельный многочлен, $a \in \mathcal{O}_K$, $a \neq 0$, $m \in \mathbf{Z}$, $m \geq 2$, $\deg f - m \geq 5$. Известно также, что существование решения $(x, y) \in \mathcal{O}_S^2$ означает ограниченность показателя m сверху вычислимой величиной, зависящей от K, S, высоты и степени f. Обозначим через h_f и $h(\alpha)$ высоту многочлена f и высоту алгебраического числа α, через s и P – число неархимедовых точек в S и наибольшее из соответствующих им рациональных простых чисел.

Следующая теорема полезна для приложений.

Теорема. *Если показательное диофантово уравнение (*) имеет по крайней мере два решения $(x_i, y_i, m_i) \in U_S \times K \times \mathbf{Z}$, $i = 1, 2$, то все решения с $x \in \mathcal{O}_S$ удовлетворяют неравенству $\max(h_f, h(x)) < C$, где C – положительное число, эффективно определяемое по степени и дискриминанту поля K, степени, дискриминанту и старшему коэффициенту многочлена f, a, s и P.*

1. Спринджук В.Г. Классические диофантовы уравнения от двух неизвестных. М.: Наука, 1982.

А.П.Трифонов, М.Б.Беспалова

ВЛИЯНИЕ РАНДОМИЗАЦИИ ИМПУЛЬСНОЙ НЕСУЩЕЙ НА СКРЫТНОСТЬ ПЕРЕДАЧИ ИНФОРМАЦИИ

В системах передачи информации в качестве несущего колебания часто используют периодические последовательности импульсов. Для повышения скрытности передачи информации предлагается рандомизировать импульсную несущую введением мультипликативных гауссовских искажений. Тогда принимаемая на фоне аддитивного гауссовского белого шума последовательность импульсов представляет собой нестационарный гауссовский случайный процесс. Исследовано влияние мультипликативных искажений на эффективность оценки максимального правдоподобия периода следования, синтезированной в предположении, что мультипликативные искажения отсутствуют. При наличии мультипликативных искажений эту оценку можно назвать квазиправдоподобной. Методом локально-марковской аппроксимации [I] найдена дисперсия оценки. Получен проигрыш в точности оценки из-за наличия мультипликативных искажений, который характеризует повышение скрытности передачи информации вследствие рандомизации несущей.

Точность оценки периода следования повышается, если при синтезе оценки максимального правдоподобия учесть наличие мультипликативных гауссовских искажений. Выполнен статистический синтез и анализ алгоритма оценки по методу максимального правдоподобия. Методом локально-марковской аппроксимации найдена дисперсия оценки. Показано, что применение алгоритма максимального правдоподобия вместо квазиправдоподобного алгоритма может привести к существенному выигрышу в точности оценки. При этом выигрыш быстро возрастает с увеличением отношения дисперсии мультипликативных искажений к квадрату их математического ожидания и с увеличением средней энергии одного импульса. Тем самым повышается скрытность передачи информации по отношению к квазиправдоподобному алгоритму обработки.

Приведенные результаты получены при поддержке Российского фонда фундаментальных исследований.

Литература

I. Трифонов А.П., Шинаков Ю.С. Совместное различение сигналов и оценка их параметров на фоне помех. – М.: Радио и связь, 1986.– 264 с.

А.П. Трифонов. С.В. Ролдугин

ПРИМЕНЕНИЕ СОСТАВНОЙ ШУМОВОЙ НЕСУЩЕЙ ДЛЯ ПОВЫШЕНИЯ СКРЫТНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ

Идея применения шумовой несущей для передачи информации предложена довольно давно [1]. Установлено, что системы передачи информации при использовании шумовой несущей имеют ряд полезных свойств, в частности более высокую степень скрытности, чем при использовании традиционных несущих.

Различные виды модуляции шумовой несущей обычно сводятся к изменению параметров ее спектра мощности при сохранении стационарности случайного сигнала. Отказ от сохранения стационарности случайной несущей в результате ее модуляции позволяет существенно расширить возможности применения шумовой несущей.

Составную шумовую несущую можно представить в виде двух расположенных последовательно во времени независимых стационарных гауссовских случайных процессов, отличающихся какими-либо параметрами. Следовательно, стационарность составной шумовой несущей нарушается в момент перехода от одного к другому стационарному процессу, образующим в совокупности составную несущую. Модуляцию такой несущей предлагается осуществлять, изменяя положение момента нарушения стационарности в соответствии с передаваемым сообщением.

Приводятся результаты статистического синтеза и анализа алгоритмов оценки момента нарушения стационарности составной гауссовской шумовой несущей, наблюдаемой на фоне гауссовского белого шума. Синтез выполнялся по методу максимального правдоподобия, а для анализа использовался метод локально-марковской аппроксимации [2]. Сформулированы рекомендации по выбору параметров составной шумовой несущей, которые обеспечивают высокую скрытность передачи информации.

Литература

1.Харкевич А.А. Передача сигналов модулированным шумом.- Избранные труды. - М.: Наука. 1973, Т.2, С.524-529.

2.Трифонов А.П., Шинаков Ю.С. Совместное различение сигналов и оценка их параметров на фоне помех. - М.: Радио и связь. 1986 - 264с.

УДК.5II.

М.И.Туляганова, А.С.Файнлейб (Ташкент)

О РАЦИОНАЛЬНЫХ ТРИГОНОМЕТРИЧЕСКИХ СУММАХ

Пусть $f(x)=a_1x+\dots+a_nx^n$ – многочлен с целыми коэффициентами, q –натуральное число, $e(\alpha)=e^{2\pi i\alpha}$. Выражение $S_n(q,f)=\sum_{x=1}^{q} e\left(\frac{f(x)}{q}\right)$ называется полной рациональной тригонометрической суммой. Такие суммы изучались в работах Гаусса[I], Г.Вейля [2], Морделла[3], Давенпорта[4], Хуа Ло-Гена[5,6], А.Вейля[7], В.И.Нечаева[8,9], С.Б.Стечкина[10, II] и других авторов. В них доказывается, что

$$S_n(q)=\max_{(a_1,\dots,a_n,q)=1}|S_n(q,f)|\le A_n q^{1-\frac{1}{n}} \qquad (I)$$

где A_n зависит только от n. Для $q=p$ (p –простое) такая оценка с $A_n=n$ найдена Морделлом[3]. В случае, когда q –степень простого числа, Хуа Ло-Ген[5] доказал оценку (I) при $A_n=n^3$. В.М.Нечаев [9] доказал, что для $n\ge3$ оценка (I) справедлива при $A_n=e^{5n^2}$.

В настоящей работе оценка (I) уточняется для почти всех q.

ТЕОРЕМА I. Для любого $\varepsilon\in(0,1]$ существуют $\alpha=\alpha(\varepsilon)\in(0,1)$ и $C_1=C_1(\varepsilon)>0$, такие, что для всех $q\ge Q$, исключая не более C_1Q^{α} значений q, и для каждого $n\ge2^{1/\varepsilon}$ справедливо неравенство

$$S_n(q)<2q^{1-\frac{1}{n\varepsilon}}$$

ТЕОРЕМА 2. Для любого $\varepsilon>0$ существуют $\delta=\delta(\varepsilon)>0$ и $C_2=C_2(\varepsilon)>0$ такие, что для всех $q\ge Q$, исключая не более $C_2\frac{Q}{(\ln Q)^{\delta}}$ значений q, справедливо неравенство $S_n(q)<\sqrt{q}\,(\ln q)^{\frac{n+2}{2}\ln n}$

Л И Т Е Р А Т У Р А: I.Гаусс К.Ф.//Труды по теории чисел.- М.:Изд-во АН СССР, I959.- С.594.

2.Weyl H.Über Gleichverteilung der Zahlen mod Eins,Gesammelte Abhandlungen,1,Berlin-Heidelberg-New York,Springer-Verlag, 1968.- P.563.

3.Mordell L.J.//J.Math.- Vol 3(1932).- P.161.

4.Davenport H.//J.Reine Angew.Math.Vol.-169 (1932).-P.158.

5.Hua L.K.//J.Chinesse Math.Soc.-Vol 2(1940).- P.301.

6.Хуа Ло-Ген//Труды Матем.ин-та АН СССР.-Т.22(I948).- С.8.

7.Weil A.//Proc.Nat.Acad.Sci.USA.-Vol.34.-No.5.-P.204. I948.

8.Нечаев В.И.//Изв.АН СССР.Сер.мат.-I953.-Т.I7.- С.485.

9.Нечаев В.И.//Матем.заметки АН СССР,I975.-Т.I7.-Вып.6.-С.839.

I0.Стечкин С.Б.//Матем.заметки,I975.-Т.I7.-С.579.

II.Стечкин С.Б.//Труды Матем.ин-та АН СССР.-Т.I43(I977)-С.I88.

УДК 511.9

Тутушев Ш.Х. /Майкоп/

ОДНО ИЗ ТЕОРЕТИКО-ЧИСЛОВЫХ ТОЖДЕСТВ

Теорема. Пусть $K \geqslant 1$ - произвольное натуральное число и $l_1, \ldots, l_\lambda$ - взаимно простые с модулем K числа, $1 \leqslant \lambda \leqslant \varphi(K)$, где $\varphi(K)$ - фукция Эйлера. Обозначим через E множество всех простых чисел p, для каждого из которых выполняется одно из сравнений: $p \equiv l_i \pmod K$, $i = \overline{1.\lambda}$. Далее множество всех натуральных чисел m, все простые делители которых принадлежат E, обозначим через R.

Тогда для любого натурального $q \geqslant 1$ имеет место формула:

$$\sum_{\substack{d \mid q \\ d=(m,q),\, m \in R}} \left(\frac{1}{d} \prod_{p \mid \frac{q}{d},\, p \in E} \left(1 - \frac{1}{p}\right) \right) = 1, \quad \prod_{p \mid 1} \left(1 - \frac{1}{p}\right) = 1,$$

где суммирование проводится только по таким делителям числа q, когда $d = (m,q)$ при различных $m \in R$.

В частности, если $K = 1$, то для любого $q \geqslant 1$ имеем:

$$\sum_{d \mid q} \left(\frac{1}{d} \prod_{p \mid \frac{q}{d}} \left(1 - \frac{1}{p}\right) \right) = 1.$$

Для доказательства используются асимптотические формулы о количестве чисел $m \in R$, $m \leqslant x$ и о количестве этих же чисел, принадлежащих произвольно заданной арифметической прогрессии $\tau \pmod q$ в случае $(\tau, q) = 1$, доказанные автором ранее/см.: Тутушев Ш.Х. Теорема о равномерности распределения чисел с простыми делителями из фиксированных арифметических прогрессий. - Математика и ее приложения. Сб. научных трудов. Вып. 1.-Ставрополь, 1973/. Эти формулы обобщаются для любых арифметических прогрессий $\tau \pmod q$, когда $(\tau, q) = d \geqslant 1$; отсюда вытекает равномерность распределения чисел из множества R по отдельным группам классов по модулю q, соответствующих заданному наибольшему общему делителю модуля q и чисел из R. Из этих асимптотических соотношений получаются данные тождества.

УДК 511.37

Усманов Х.Х. (Душанбе)

ФУНКЦИОНАЛЬНАЯ ПРЕДЕЛЬНАЯ ТЕОРЕМА ДЛЯ АДДИТИВНЫХ ФУНКЦИЙ НА ПОСЛЕДОВАТЕЛЬНОСТИ $\{p+a\}$.

Пусть $g: \mathcal{N} \to R$ – аддитивная функция, p и q – простые числа, a – целое положительное, $\sum[a(n,q); \ldots]$ – сумма выражений $a(n,q)$ по простым q, удовлетворяющим условиям, записанным вместо многоточия. Для $t \in [0,1]$ положим

$$H_n(p,t) = \sum\left[g(q^k)/B(n); q^k \| p+a, q < y(t)\right] - \sum\left[\|g(q)/B(n)\|/(q-1); q \le y(t)\right],$$

где $B(n) > 0$, $B(n) \to \infty$ при $n \to \infty$, $\|u\| = u$ при $|u| < 1$ и $\|u\| = \operatorname{sgn} u$ при $|u| \ge 1$, $y(t) = \max\{m \le n; \sum[\|g(q)/B(n)\|^2/(q-1); q \le m] \le t \sum[\|g(q)/B(n)\|^2/(q-1); q \le n]\}$. Пусть $\mathcal{B}$ – σ – алгебра борелевских множеств A пространства $\mathcal{D}[0,1]$, $\pi(n)$ – число простых чисел $p \le n$. В $(\mathcal{D}, \mathcal{B})$ зададим последовательность мер ν_n равенством:

$$\nu_n(A) = \pi^{-1}(n) \cdot |\{p \le n; H_n(p,t) \in A\}|$$

Пусть ν – мера, соответствующая некоторому процессу $H(t)$ с реализациями из $\mathcal{D}[0,1]$ и независимыми приращениями, распределения которых неинфинитезимальны. Имеет место следующая

ТЕОРЕМА. ν_n слабо сходится к ν тогда и только тогда, когда

1) существует последовательность $\tau(n) \to \infty$ такая, что

$$\log \tau(n)/\log n \to 0, \quad \sum\left[\|g(q)/B(n)\|^2/(q-1); \tau(n) < q \le n\right] \to 0$$

при $n \to \infty$;

2) существует неубывающая ограниченная функция $L(u)$, $L(\pm\infty) = \lim\limits_{u \to \pm\infty} L(u)$, $L(+\infty) > 0$, для которой

$$\sum\left[\|g(q)/B(n)\|^2/(q-1); q < n, g(q) \le u B(n)\right] \to L(u)$$

во всех точках непрерывности функции $L(u)$.

Кроме того, если условия 1) и 2) выполнены, то характеристическая функция предельного процесса $H(t)$ однозначно определяется функцией $L(u)$.

Литература

Тимофеев Н.М., Усманов Х.Х. Об арифметическом моделировании случайных процессов с независимыми приращениями // Докл. АН Тадж.ССР. 1984. Т.27, № 10. С.556-559.

УДК 511.2

Усольцев Л.П. (Самара)

БОЛЬШИЕ УКЛОНЕНИЯ В ЗАДАЧЕ О РАСПРЕДЕЛЕНИИ ДРОБНЫХ ДОЛЕЙ ПОКАЗАТЕЛЬНОЙ ФУНКЦИИ

Пусть $q \geq 2$ – фиксированное целое число, $f(t)$ – вещественнозначная суммируемая на отрезке $[0,1]$ периодическая функция с периодом 1 и коэффициентами Фурье

$$a_m = \int_0^1 f(t)e^{-2\pi imt}dt, \quad m \in Z,$$

причем $|a_m| \leq A/m^\alpha$ $(m = 1,2,\ldots)$ с некоторыми постоянными $A > 0$ и $\alpha \geq 1$. Для $N = 1,2,\ldots$ положим

$$S_N(t) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \left(f(q^n t) - a_0 \right), \quad 0 \leq t \leq 1,$$

$$F_N(x) = mes\left\{ t \in [0,1] : \; S_N(t) < x \right\}, \quad -\infty < x < +\infty$$

Известно (теорема Форте – Каца), что существует конечный предел

$$\lim_{N\to\infty} \int_0^1 S_N^2(t)dt = \sigma^2 \quad (\sigma \geq 0)$$

Пусть $\Phi(x)$ – нормальная функция распределения с параметрами $(0,1)$.

ТЕОРЕМА. Если $\sigma = 0$, то существует постоянная $\delta > 0$, зависящая от A, α и σ, такая, что при $N \to \infty$ в области $2 \leq x \leq \delta N^{1/6}$ выполняются соотношения

$$1 - F_N(\sigma x) = \left[1 - \Phi(x) \right] \cdot \left[1 + O\left(\frac{x^3(x^2 + \ln N)}{\sqrt{N}} \right) \right], \tag{1}$$

$$F_N(-\sigma x) = \Phi(-x) \cdot \left[1 + O\left(\frac{x^3(x^2 + \ln N)}{\sqrt{N}} \right) \right] \tag{2}$$

с постоянной в знаке "O", зависящей от A, α и σ.

ЗАМЕЧАНИЕ. В работе [1] (теорема 2) показано, что в случае строгого неравенства $\alpha > 1$ (и $\sigma \neq 0$) в области $1 \leq x \leq \delta N^{1/6}$ выполняются соотношения (1) и (2) с $O\left(\frac{x^3}{\sqrt{N}} \right)$ вместо $O\left(\frac{x^3(x^2 + \ln N)}{\sqrt{N}} \right)$.

Литература

1. Усольцев Л.П. Центральная предельная теорема и большие уклонения для одной суммы с показательной функцией.//Марковские случайные процессы и их применение. Межвуз. научн. сб. Изд–во Сарат. ун–та, 1980. С.105–114.

УДК 511.2

Усольцев Л.П. (Самара)

МОДИФИКАЦИЯ ТЕОРЕМЫ ЭРДЕША–ТУРАНА В ТЕОРИИ РАВНОМЕРНОГО РАСПРЕДЕЛЕНИЯ ПО МОДУЛЮ 1

Пусть $x_1, x_2, \ldots, x_n, \ldots$ – заданная последовательность действительных чисел. Для любого натурального числа N и любого подмножества $\Delta \subset [0;1)$ мы обозначим через $Q_\Delta(N)$ количество чисел x_n, $1 \le n \le N$, для которых $\{x_n\} \in \Delta$. Величина

$$D(N) = \sup_{0 \le \alpha < \beta \le 1} \left| \frac{Q_{[\alpha;\beta)}(N)}{N} - (\beta - \alpha) \right|$$

обычно называемая отклонением последовательности (x_n), характеризует степень отклонения распределения этой последовательности от "идеального" равномерного распределения. Однако, далеко не всегда нас могут интересовать значения величины $Q_{[\alpha;\beta)}(N)$ для сколь угодно малых промежутков $[\alpha;\beta)$. В этих случаях является уместной следующая модификация понятия отклонения последовательности. Для любого числа $\gamma \in (0;1)$ мы полагаем

$$\Delta_\gamma(\lambda) = \begin{cases} [\lambda,\ \lambda+\gamma), & \text{если} \quad 0 \le \lambda \le 1-\gamma, \\ [\lambda, 1) \cup [0; \lambda+\gamma-1), & \text{если} \quad 1-\gamma < \lambda < 1. \end{cases}$$

$$D_\gamma(N) = \sup_{0 \le \lambda < 1} \left| \frac{Q_{\Delta_\gamma(\lambda)}(N)}{N} - \gamma \right|$$

Справедливо следующее утверждение, представляющее собой модификацию классической теоремы Эрдеша–Турана (см., например, [1], стр. 125).

ТЕОРЕМА. Пусть натуральное число N и действительные числа ν, τ и l таковы, что $0 < \nu < \tau < 1$ и $1 \le l \le N$. Если действительные числа $x_1, x_2, \ldots, x_N$ таковы, что $\sup\limits_{0 \le \lambda < 1} Q_{\Delta_\nu(\lambda)}(N) \le l$, то выполняется неравенство

$$D_\tau(N) \le 9 \left(\frac{l}{N} + \sum_{m=1}^{[2/\nu]+1} \min\left(\tau, \frac{1}{\pi m}\right) \cdot \left| \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i m x_n} \right| \right).$$

Легко видеть, что последнее неравенство содержит больше информации, нежели классическое неравенство Эрдеша–Турана и позволяет более дифференцированно подразделять числовые последовательности на последовательности с "более хорошим" и "менее хорошим" равномерным распределением.

Литература

1. Кейперс Л., Нидеррейтер Г. Равномерное распределение последовательностей. М.: Наука, 1985.

УДК 511.19

Федоровский С.В., Синявский О.В. (Одесса)

О НЕКОТОРЫХ АНАЛОГАХ ФУНКЦИИ ДЕЛИТЕЛЕЙ НА АРИФМЕТИЧЕСКИХ ПРОГРЕССИЯХ

На множестве натуральных чисел рассмотрим три функции

$$\tau_{1,2}(n)=\sum_{n=n_1 n_2^2} 1 \quad , \quad R_{1,2}(n)=\sum_{\substack{n=w(u^2+v^2)\\ w\in\mathbb{N},\ u,v\in\mathbb{Z}}} 1 \quad , \quad P_{1,2}(n)=\sum_{\substack{n=p(u^2+v^2)\\ p-\text{простое}\\ u,v\in\mathbb{Z}}} 1 \ ,$$

которые являются аналогами функции делителей $\tau(n)$. Используя оценки тригонометрических сумм на алгебраических многообразиях над конечным полем, мы доказываем теоремы:

ТЕОРЕМА 1. Пусть $a, q\in\mathbb{N}$. $(a,q)=1$. Тогда равномерно для $q\ll x^{1/3}$ имеем

$$\sum_{\substack{n\le x\\ n\equiv a(q)}} \tau_{1,2}(n) = c(a,q)\cdot\frac{x}{q}+O\left(x^{\frac{1}{3}}\log x\right),$$

где $1\ll c(a,q)\ll 1$ – вычислимая постоянная.

ТЕОРЕМА 2. Для $q\ll x^{\frac{1}{2}}$ имеем

$$\sum_{\substack{n\le x\\ n\equiv a(q)}} R_{1,2}(n) = \frac{\pi x\log x+Cx}{\varphi(q)}+O\left(q^{\frac{1}{2}}\tau(q)\right)+O\left(x^{\frac{5}{6}}q^{-\frac{2}{3}}\tau(q)\right)$$

ТЕОРЕМА 3. Существуют абсолютные постоянные $C_1, C_2>0$ такие, что для $q\ll \exp\left(c_1\sqrt{\log x}\right)$

$$\sum_{\substack{n\le x\\ n\equiv a(q)}} P_{1,2}(n) = B(a,q)\frac{x}{q\log x}+O\left(x\exp\left(-c_2\sqrt{\log x}\right)\right).$$

Эти теоремы применяются для построения асимптотических формул для некоторых аддитивных задач.

УДК 511.9

К. К. ФРОЛОВ (НИИЦСУ "Экор")

ИСПОЛЬЗОВАНИЕ ТЕОРЕТИКО-ЧИСЛОВЫХ СЕТОК В ЗАДАЧАХ ВОССТАНОВЛЕНИЯ ПЕРИОДИЧЕСКИХ ФУНКЦИЙ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ, ЗАДАННЫХ КОНЕЧНЫМ ПОЛИНОМОМ ФУРЬЕ.

В работе предлагается конструктивный метод построения узлов теоретико-числовых сеток для точного восстановления периодических функций нескольких переменных, заданных конечным полиномом Фурье.

Для оценки числа узлов сетки получены оценки сверху.
Так для s-мерного "гиперболического креста" задаваемого соотношениями $\max(0,|m_1|)\cdot(\max(0,|m_2|)\cdot\ldots\cdot\max(0,|m_s|)<N$, $N\ge s+2$,
число узлов решетки не превосходит $N\cdot(\ln N)^{s^2}$

Л И Т Е Р А Т У Р А

1. Темляков В.И. О восстановлении периодических функций нескольких переменных по значениям в узлах теоретико-числовых сеток//An.Math. 1986, v.12, No.4, p.287-305.

2. Коробов Н.М. Теоретико-числовые методы в приближенном анализе. М.,Наука, 1974.

3. Воронин С.М., Скалыга В.И. О квадратурных формулах // Доклады АН СССР, 1984, т.276, No.5, с.1038-1041.

4. Фролов К.К. Оценки сверху погрешности квадратурных формул на классах функций// Докл. АН СССР, 1976, т.231, No.4, с.818-821.

5. Chen W.W.L. On irregularities of distribution// Mathematica, 1980, v.27, No.2, p.329-354.

6. Roth K.F. On irregularities of distribution.1// Mathematica, 1954, v.1, p.73-79.

7. Roth K.F. On irregularities of distribution.4// Acta Arith. 1980, v.37, p.65-76.

8. Shmidt W.W. Irregularities of distribution. X// Number Theory and Algebra. Academic Press, 1977

Работа выполнена при финансовой поддержке Российского Фонда Фундаментальных Исследований, грант No. 93-011-16021

УДК 511.364.

Холявка Я.М. (Львов)

ОБ АРИФМЕТИЧЕСКИХ СВОЙСТВАХ $\mathrm{sn}z$

Пусть $\wp(z)$ – эллиптическая функция Вейерштрасса, g_2, g_3 – ее инварианты, 2ω, $2\omega_1$ – произвольная фиксированная пара ее основных периодов; $\mathrm{sn}z$ – эллиптическая функция Якоби, $4K = 4\omega$, $2iK' = 2\omega_1$ – ее основные периоды. Обозначим через $\varkappa$ модуль $\mathrm{sn}z$, $\xi_0, \ldots, \xi_4$ – приближающие алгебраические числа, n_i и L_i – их степени и длины, $n = \deg \mathbb{Q}(\xi_0, \ldots, \xi_4)$.

Теорема. Пусть

$$P = n\left(\ln n + \frac{\ln n_0}{n_0} + \frac{\ln L_1}{n_1} + \frac{\ln L_4}{n_4} + \min(n_2, n_3)\left(1 + \frac{\ln L_2}{n_2} + \frac{\ln L_3}{n_3}\right)\right).$$

Тогда

$$|\omega - \xi_0| + |\omega_1 - \xi_1| + |g_2 - \xi_2| + |g_3 - \xi_3| + |\varkappa - \xi_4| > \exp(-\Lambda P^3),$$

где Λ – некоторая эффективная постоянная.

Доказательство теоремы проводится вторым методом Гельфонда.

Эта работа была частично поддержана Международной Соросовской программой поддержки образования в области точных наук, грант № АРЦ 051106.

I. Фельдман Н.И. Седьмая проблема Гильберта. – М.: Изд-во при МГУ, 1982. – 311 с.

УДК 511

Хрипунова М.Б. (Владимир)

АДДИТИВНЫЕ ЗАДАЧИ С ЧИСЛАМИ ИМЕЮЩИМИ ЗАДАННОЕ ЧИСЛО ПРОСТЫХ ДЕЛИТЕЛЕЙ.

Пусть $\omega(n)$-число простых делителей n, $\Omega(n)$-число простых делителей n с учетом их кратности.

В работе [1] была доказана теорема типа А.И.Виноградова-Бомбьери для чисел с $\Omega(n) = k$ или $\omega(n) = k$, что позволило найти асимптотику для числа решений уравнения $n - 1 = md$, при $n \le x$, $m, d \in N$, $\Omega(n) = k$, $k \le (2-\varepsilon)\ln\ln x$.

В дальнейшем была исследована задача о нахождении асимптотики при $N \to \infty$ числа решений уравнения $N = n+md$, $\Omega(n) = k$, при $k \le (2-\varepsilon)\ln_2 N$ и $(2+\varepsilon)\ln_2 N \le k \le b\ln_2 N$.

Целью настоящей работы является исследование сумм

$$\sum_{n\le N} \tau(|bn - a|),$$

где сумма берется по n таким, что либо $\Omega(n) = k$, либо $\omega(n) = k$, $bn - a \ne 0$, равномерно по $k \le b\ln_2 N$, $N \to \infty$, $|a| \le cN$, $|b| \le \ln^{\alpha} N$, $c, \alpha - const > 0$. Эта задача при конкретных a и b содержит, в частности, предыдущие результаты.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (93-01-00260).

Литература

[1] Тимофеев Н.М., Хрипунова М.Б. Распределение чисел с заданным числом простых делителей в прогрессиях// Математические заметки. 1994, т. 55, вып. 2, с. 144-156

Об одном арифметическом свойстве чисел перестановок с заданной сигнатурой, связанном с последовательностью Морса, и свойстве "12" чисел Бернулли

В.С.Шевелев
(Россия, Ростов-на-Дону)

Пусть $e(n)$ число единиц в двоичном представлении числа $n \in N$. (0,1) последовательность вычетов по $mod\,2$ для последовательности $\{e(n-1)\}$ называется последовательностью Морса $\{m(n)\}_{n=1}^{\infty}$.

Пусть $a = (a_1, a_2, \ldots, a_n)$ перестановка из элементов $1,2,\ldots, n$. Число $K = K(a)$ называется сигнатурой перестановки a, если i-я цифра в $(n-1)$- значном двоичном представлении числа $K-1$ ($i = 1,2,\ldots, n-1$) равна 1 или 0 в зависимости от того, какое неравенство имеет место: $a_i < a_{i+1}$ или $a_i > a_{i+1}$. через $S_n^{(k)}$ обозначим множество перестановок a с фиксированной сигнатурой K.

Доказаны следующие утверждения.

1) $|S_n^{(k)}|$ является многочленом относительно n степени $\lceil \log_2 K \rceil$, где $\lceil x \rceil$ означает ближайшее к x целое число $\geq x$;

2) если все делители n, отличные от 1, больше $\lceil \log_2 K \rceil$, то

$$|S_n^{(K)}| \equiv (-1)^{m(K)} \pmod{n};$$

3) (следствие для альтернирующих перестановок: "свойство "12" чисел Бернулли). Если B_n - n- ное число Бернулли, $|B_n| = \alpha_n / \beta_n$ - несократимая дробь и $n-1 \geq 3$ - простое число, то

$$12\alpha_n + (-1)^{n/2}\beta_n \equiv 0 \pmod{(n-1)}.$$

В дополнение получено следующее свойство последовательности Морса $\{m(n)\}$. Пусть $\{Z_i\}$ и $\{U_i\}$ номера членов последовательности Морса, равных соответственно 0 и 1:

$$\{Z_i\} = \{1,4,6,7,10,11,\ldots\}, \quad \{U_i\} = \{2,3,5,8,9,12,\ldots\}.$$

Пусть, далее, $0 \leq S < t$ и $0 \leq z \leq t - S$ - целые числа. Разделим отрезок $[1, 2^t] \cap N$ на 2^s равных частей и в каждой части выберем первые 2^z чисел. Множество выбранных чисел обозначим $A(z, s, t)$. Тогда для любого $x \in C$ справедливо равенство

$$\sum_{i \in A(z,s,t)} (x + Z_i)^{z+s} = \sum_{i \in A(z,s,t)} (x + U_i)^{z+s}.$$

УДК 511

Широков Б.М. (Петрозаводск)

РАСПРЕДЕЛЕНИЕ ЗНАЧЕНИЙ ОБОБЩЕННОЙ СУММЫ ДЕЛИТЕЛЕЙ В КЛАССАХ ВЫЧЕТОВ

Целочисленная арифметическая функция $f(n)$ называется *слабо равномерно распределенной по модулю целого числа* N, если для любых целых чисел a и b, взаимно простых с N, при $x \to \infty$

$$\#\{n \le x \mid f(n) \equiv a \pmod N\} \sim \#\{n \le x \mid f(n) \equiv b \pmod N\}$$

при условии, что множество $\{n \mid (f(n), N) = 1\}$, бесконечно (см. [1]).

Обозначения: p, q — простые числа, χ — неглавный вещественный характер модуля q^k,

$$\sigma(n, \chi) = \sum_{d \mid n} \chi(d) d$$

$X(n)$ — произвольный характер Дирихле модуля n, если $q^s \| N$, то $N' = N/q^s$,

$$\lambda = \begin{cases} \prod_{p \mid N} \frac{p-2}{p-1}, & \text{если либо } (N, q) = 1, \text{ либо } q \mid N \text{ и } q \equiv 1 \pmod 4, \\ \prod_{p \mid N'} \frac{p-2}{p-1}, & \text{если } q \mid N \text{ и } q \equiv 3 \pmod N. \end{cases}$$

и, наконец, если X_0 — главный характер модуля N, а $K = [N, q^k]$, то

$$\mu = \max_{X \ne X_0} \Re \frac{1}{\varphi(K)} \sum_{(a, K)=1} X(1 + \chi(a) a).$$

Теорема. *Для того, чтобы $\sigma(n, \chi)$ была слабо равномерно распределена по модулю N, необходимо и достаточно, чтобы N не делилось на 6. При этом, если N нечетно, то для любого a, $(a, N) = 1$ при $x \to \infty$ справедлива асимптотика*

$$\#\{n \le x \mid f(n) \equiv a \pmod N\} = C \frac{x}{\ln^{1-\lambda} x} + O\left(\frac{x}{\ln^{1-\mu} x}\right).$$

Получена формула и для четного N, не кратного 3.

Литература

1. Narkiewicz W. On distribution of values of multiplicative functions in residue classes.// Acta Arithm. 1967. v. XII. P. 269–279.

УДК 5II.9

Шокуев В.Н. (Нальчик)

О ПРОСТЫХ ДЕЛИТЕЛЯХ ЧИСЛА $(a^p+b^p)(a+b)^{-1}$.

Пусть p – нечетное простое число, a и b – целые взаимно простые числа, q – любой простой делитель числа

$$(a^p+b^p)(a+b)^{-1},$$

отличный от p. Тогда $(-1)^{\frac{p-1}{2}}p$ является квадратичным вычетом по модулю q. В частности, если 2^p-1 – простое число Мерсенна, то

$$\left(\frac{(-1)^{\frac{p-1}{2}}p}{2^p-1}\right)=1.$$

Литература

1. Серр Ж. Алгебраические группы и поля классов.- Мир.,1968,278с.
2. Эдвардс Г. Последняя теорема Ферма. Генетическое введение в алгебраическую теорию чисел.- Мир,М., 1980, 288с.

УДК 511:513.82

ШУШБАЕВ С.Ш. (Ташкент)

ОБ ОДНОЙ СОВЕРШЕННОЙ ФОРМЕ ВОРОНОГО, НЕ ЯВЛЯЮЩЕЙСЯ ФИНАЛЬНО ЭКСТРЕМАЛЬНОЙ ФОРМОЙ ДЕЛОНЕ-РЫШКОВА.

Пусть задана положительная квадратичная (п.к.ф.) от n переменных $f = f(x) = f(x_1, \dots, x_n) = \sum_{1 \le i,j \le n} a_{ij} x_i x_j$ с вещественными коэффициентами $a_{ij} = a_{ji}$ и m – ее арифметический минимум. Пусть этот минимум достигается в s целых точках $\pm m_k = \pm(m_{1k}, \dots, m_{nk})$ $(k = 1, \dots, s)$.

П.к.ф. f называется совершенной, если по значению ее арифметического минимума m и по его представлениям $\pm m_k$ однозначно находятся коэффициенты a_{ij} формы f.

П.к.ф. f называется финально экстремальной, если существует такое число $s_0 \ge 1$, что форма f есть точка локального минимума дзета-функции Эпштейна $Z(f;s) = \sum_{x \ne 0} \{f(x)\}^{-ns/2}$ в пространстве коэффициентов формы f для всех $s > s_0$.

Т е о р е м а. Совершенная форма $\varphi_3^n = x_1^2 + \dots + x_n^2 + x_1x_2 + \dots + x_{n-1}x_n - \frac{1}{2}\{x_1x_2 + x_3x_4 + x_5x_6\}$ не является финально экстремальной для всех $n \ge 6$.

Аналогичный результат ранее был известен для φ_3^6 и φ_3^7.

УДК 5II

Чекин А.Л. /Москва/

НОВЫЙ ТИП ВЕСОВОГО РЕШЕТА БУХШТАБА
/К 90-летию со дня рождения А.А.Бухштаба/

В I985г. на Всесоюзной конференции "Теория чисел и ее приложения" /г.Тбилиси/ автором этих строк был анонсирован новый тип весового решета, который явился последней разработкой А.А.Бухштаба в этой области. С помощью этого нового типа решета А.А.Бухштаб предполагал улучшить результаты по ряду актуальных задач с почти простыми числами. К сожалению, в дальнейшем эта тема не получила своего развития: ожидаемые арифметические приложения автором не только не были опубликованы, но и, насколько мне известно, не были получены в завершенном виде. Более того, так и не было в какой-либо форме предъявлено доказательство основной теоремы по данному типу весового решета. В настоящем докладе предполагается, по-возможности, устранить этот пробел.

ЛИТЕРАТУРА.

I. Бухштаб А.А. Комбинаторное усиление метода эратосфенова решета, УМН, I967, т.22, вып.3/I35/, с.I99-226.

2. Бухштаб А.А. Новый тип весового решета, в сб.:Тезисы докладов Всесоюзной конференции "Теория чисел и ее приложения", ТГУ, Тбилиси, I985.

3. Laborde M. Buchstab's sifting weights, Mathematika, 26 (1979), N°2, pp. 250-257.

УДК 511.36

Чирский В.Г. (Москва)

ОБ АРИФМЕТИЧЕСКИХ СВОЙСТВАХ НЕКОТОРЫХ РЯДОВ

В 1990-1992 автор установил необходимое и достаточное условие отсутствия глобальных соотношений для рядов из класса

$$F(K, c_1, c_2, c_3, q_0)$$

к которому можно естественным образом перейти от известных E - и G -функций и в который, например, входят обобщённые гипергеометрические ряды вида

$$\sum_{n=0}^{\infty} \frac{(\mu_1)_n \dots (\mu_p)_n}{(\lambda_1)_n \dots (\lambda_q)_n} \left(\frac{z}{p-q}\right)^{(p-q)n}, \quad p > q,$$

с рациональными параметрами μ_i, $i = 1, \dots, p$, λ_j, $j = 1, \dots, q$.

Используя методы, развитые в работах Ю.В. Нестеренко, доказывается отсутствие линейных глобальных соотношений для обобщённых гипергеометрических рядов с алгебраическими иррациональными параметрами.

В 1994 году автор опубликовал статью, в которой приведены примеры рядов с рациональными членами, сходящихся во всех локальных полях, причём к алгебраически независимым элементам этих полей.

Установлен критерий трансцендентности рядов определённого вида в неархимедовски нормированных полях.

УДК 511

Юдин А.А. (Владимир)

ОБРАТНЫЕ ЗАДАЧИ АДДИТИВНОЙ ТЕОРИИ ЧИСЕЛ И РАСПРЕДЕЛЕНИЕ ЗНАЧЕНИЙ ГАРМОНИЧЕСКИХ МНОГОЧЛЕНОВ.

Пусть G-абелева группа с операцией записываемой аддитивно, мерой Хаара μ, $\hat{G}$-ее группа характеров и $f : \mathbf{G} \to \mathbf{C}$, $f(0) = 1$.

Пусть

$$f(x) = \sum_{\chi \in \hat{G}} c(\chi)\chi(x), \forall \chi \in \hat{\mathbf{G}}, c(\chi) \geq 0,$$

разложение $f(x)$ в ряд Фурье на G.

Функция $f(x)$-характеристическая функция случайной величины ξ со значениями в G. В работах [1], [2] изучается распределение значений $f(x)$, а именно оценка сверху меры множества

$$E_\varepsilon = \{x \in \mathbf{G} : \mid f(x) \mid \geq 1 - \varepsilon\}, 0 < \varepsilon < 1,$$

в терминах распределения случайной величины ξ.

Используя методы обратных задач аддитивной теории чисел [3], можно изучить не только меру, но и структуру множества E_ε.

Обозначим $A + B = \{z = x + y \mid x \in A, y \in B\}, A, B \subset \mathbf{G}$.

$$(s + 1)A = sA + A.$$

Имеет место отношение двойственности.

Теорема. Пусть

$$E_u = \{\chi \in \hat{\mathbf{G}} : c(\chi) \geq (1 - u)\mu(E_\varepsilon)\}, 0 < u < 1,$$

тогда

$$\mu(E_\varepsilon)\mu(sE_m) \leq (1 - s^2u)^{-2},$$

при $0 < s^2u < 1$.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований,грант 93-01-00260.

Литература

[1] T.V.Arak and A.Yu.Zaitsev.Uniform limit theorems for sums of independent random variables.Proceedings of the Steklov Institute of Mathematics(1988), issue 1,41-61.

[2] J-M.Deshouillers,G.A.Freiman and A.A.Yudin.On Bounds for the Concentration Function, I.Preprint, IHES, 1995, Paris.

[3] G.Freiman."What is the structure of K if K+K is small?"Lecture Notes in Mathematics, 1240(1987), Springer-Verlag, New York, 109-134.

Кухарев В.Н.
Лебедев Ю.И.
Махинов Ю.Н.
Толстых Н.Н.

Один из путей построения систем обеспечения безопасности каналов передачи данных и связи

Криптография как средство, используемое для "закрытия" канала связи от несанкционированного доступа, прослушивания и приема информации имеет важное значение для построения различных систем связи специального назначения. Однако, повсеместному распространению скремблеров, кодеков, шифраторов и маскираторов в сетях передачи данных и речи препятствует высокая стоимость оборудования, а при использовании простых методов "закрытия" канала, не высокая степень стойкости применяемых кодов. Для оперативной сети связи военного, банковского и комерческого назначения необходимо разработать такую технику шифрования, которая могла бы быть приемлема с экономической точки зрения ее использования, отличалась бы простотой ввода и достаточной надежностью дешифрования. При создании криптографических систем в комерческой области, а также в оперативных системах связи военного назначения одним из главных направлений является автоматизация процессов их работы. Анализ современного состояния техники шифрования и скремблирования в России и за рубежом показал, что основные пути развития таких систем в настоящее время связаны в основном с проблемами:

- обеспечения достаточной степени криптостойкости, при приемлемой стоимости и технологичности этих изделий;
- стандартизации основных технических параметров систем шифрования, способствующей оценке различных устройств по одним критериям;
- микроминиатюризации шифровальной техники.

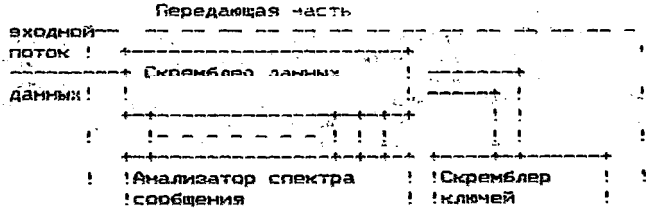
В настоящее время наиболее эффективным алгоритмом шифрования данных является алгоритм DES (Data Encryption Standart). Основная идея, заложенная в алгоритм DES - это применение обычных перестановок информационных символов и использование двух скремблеров (скремблера данных и скремблера ключей). Скремблирование данных и ключей производится перестановками информационных символов по заданной программе или же по заданным таблицам. Высокая степень закрытия обеспечивается при минимальной длине информационного блока равной 64 битам.

До настоящего времени при создании средств информационного обмена по телефонному и радиоканалу господствует концепция обособленного решения проблем, связанных с поиском наиболее рациональных для конкретных условий методов модуляции сигналов, повышением достоверности обмена за счет коррекции ошибок, появляющихся в канале связи, а также отдельно решается

проблема кодирования канала от несанкционированного доступа к нему. В соответствии с этой концепцией совершенствуются существующие модемы передачи данных, в которых повышение помехозащищенности достигается применением устройств защиты от ошибок, работающих по принципу многократного повторения команд управления; тем самым резко сокращается пропускная способность канала связи, а следовательно и ее эффективность. С теоретической точки зрения такой путь вполне оправдан при создании систем передачи данных, расчитанных на работу в канале с априорно неизвестными характеристиками.

Однако, такую концепцию нельзя считать перспективной и приемлемой для современных каналов связи, для которых высокая помехоустойчивость информационного обмена, криптостойкость к несанкционированному доступу и незначительные аппаратные затраты, обеспечиваются за счет комплексного подхода к решению этих проблем. Целесообразность комплексного подхода очевидна. Развитие в последнее время теории сигналов, кодирования, помехоустойчивого приема и модуляции позволяет говорить о "слиянии" процессов преобразования информационного сигнала не только на приемной, но и на передающей стороне. Именно на таких позициях базируется предлагаемый подход к построению высоко помехозащищенных и криптостойких систем информационного обмена, основанный на формировании и обработке сложных многопозиционных систем сигналов с марковскими дискретными информационными параметрами (марковские системы сигналов), предусматривающие тесную взаимосвязь помехоустойчивого - криптостойкого кодирования и модуляции, демодуляции и декодирования. Суть подхода состоит в том, чтобы интегралы воздействием помехоустойчивого - криптостойкого кодирования и модуляций преобразовать передаваемые сообщения в многопозиционный - марковский сигнал, посылаемый в канал связи, и совместным выполнением демодуляции и декодирования произвести непосредственное преобразование искаженных шумами сложных кодированных сигналов в сообщения с учетом марковских свойств информационных параметров. При этом, с точки зрения теории информации, марковские свойства сигнала можно рассматривать, с одной стороны, как результат введения информационной избыточности в передаваемое сообщение, а с другой, - как дополнительные свойства информационных параметров сложного кодированного сигнала.

Один из множества вариантов построения таких устройств преобразования сигнала показан на рис.1.



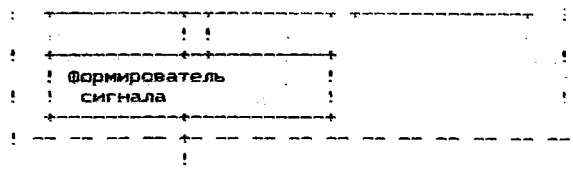


Рис. 1

Входной информационный поток, поступает на скремблер данных, а затем полученный кодированный пакет поступает на анализатор спектра сообщения. Анализатор спектра кодированного сообщения формирует спектральный " образ" кодограммы, спектральные составляющие которого в свою очередь являются параллельными составными сигналами, поступающими затем на модулятор. В большинстве современных систем с ключами шифрования применяются алгоритмы, которые затрудняют многократное изменение ключей, а использование одного и того же ключа на протяжении продолжительного времени увеличивает вероятность рассекречивания системы. Автоматизируя процессы смешивания ключей, можно существенно уменьшить этот риск. Диффи и Хелльман в 1976 году предложили способ формирования ключей автоматически, используя обычную линию связи. Такой принцип установки и коррекции ключей между абонентами называется ДН - методом. Данная система установки ключей используется в предложенном способе маскирования информации. У каждого из абонентов (A и B) имеются индивидуальные ключи и ключи общего пользования определяемые по формулам:

$$Y_a = M^a \pmod n, \qquad Y_b = M^b \pmod n$$

где M и n - параметры используемых параллельно составных сигналов. Для установления ключей маскирования достаточно пользователю A послать свой ключ Y_a, а пользователю B послать свой ключ Y_b. Каждый из пользователей формирует общий ключ Z, что соответствует криптографической системе, использующей следующие значения ключей:

$$Z = (Y_b)^a = M^{ab} \pmod n$$

$$Z = (Y_a)^b = M^{ab} \pmod n.$$

Если постороннему абоненту удастся определить значения величин M и n и ключей Y_a и Y_b, он не сможет демаскировать сообщение не восстановив ключа Z. Когда n составляет несколько сотен бит или больше, не возможно с помощью компьютерных вычислений оперативно определить величины a и b, а следовательно раскрыть передаваемое сообщение. В тоже время опознавание и восстановление

ключей состоящих из нескольких сотен информационных бит достаточно просто решаемая задача. В DH - алгоритме используется целое число для вычисления степени модуля другого числа, что обеспечивает больший уровень секретности, чем полиномиальный метод.

Экспериментальные проверки показали, что для ключа длиной 200 бит время восстановления ключа доступа Z на основании ключа общего пользования Y, сигнальным микропроцессором TMS320C25 не превышает 0.76 сек. в худшем случае. Это время может быть учтено при организации соединения и синхронизации абонентов.

Кроме того, предложенная методика преобразования сигнала позволяет полностью автоматизировать процессы опознования и контроля абонентов при работе в закрытом режиме. Полученная степень криптостойкости превышает степень DES алгоритмов, так как за счет преобразования информационное сообщение получает дополнительно несколько степеней свободы.

Таким образом, подводя итоги всему выше сказанному, можно сделать следующие выводы:

1. Применение нового метода кодирования и модуляции сигнала обеспечивает надежную защиту сообщений.

2. Предлагаемый алгоритм маскирования аналогичен или превосходит по своим свойствам алгоритмы маскирования стандартных систем Западной Европы, Японии, США (стандарт - DES

3. Реализация предложенного метода маскирования в данной работе позволяет автоматически производить для всех абонентов или выборочно установку ключей маскирования и их смену в канале связи.

SOME PROBLEMS ON EULER'S PHI-FUNCTION

BY J. WALID

In this paper we look at some problems related to Euler's ϕ function ($\phi(x)$ denotes the number of integers a, such that $1 \leq a < x$, where $gcd(a, x) = 1$. Thus if $x = p$, and p is a prime, then $\phi(p) = p - 1$, and $\phi(p^k) = p^{k-1}(p-1)$ for any $k \geq 1$).

First we call $F_A = \{x : |\phi(x) = A\}$ the set of all solutions of the equation $\phi(x) = A$, and we improve the work done on Carmicheal's conjecture by proving that the cardinal of F_A is never one (when the set $F_A \neq \emptyset$) in many different cases. The paper also contains some other properties related to the question of Cardinality.

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

УДК 62.529

Завгородний М.Г., Скрыль С.В.

СПОСОБ ФОРМИРОВАНИЯ АНАЛИТИЧЕСКИХ ВЫРАЖЕНИЙ ДЛЯ ОЦЕНКИ СВОЕВРЕМЕННОСТИ РЕАКЦИИ СИСТЕМ ОХРАНЫ

Анализ условий использования современных и перспективных систем охраны позволил установить, что процессы их функционирования крайне критичны к временным показателям, наиболее обобщенным из которых является своевременность.

С целью определения данного показателя введем необходимые обозначения. Под временем реакции системы охраны $t_р$ понимается интервал времени от несанкционированного проникновения на охраняемый объект до идентификации проникновения и принятия мер по устранению его последствий. Принятые меры считаются своевременными, если время реакции системы охраны окажется не больше некоторой максимально допустимой величины $t_м$. Формально это условие представляется неравенством: $t_р < t_м$, а так как входящие в него величины являются случайными, его выполнение является случайным событием, которое оценивается соответствующей вероятностью $P(t_р < t_м)$.

С целью получения выражения для $P(t_р < t_м)$ воспользуемся тем обстоятельством, что время $t_р$ можно представить в виде комбинации времени $t_о$, затрачиваемого на обнаружение несанкционированного проникновения на охраняемый объект и времени $t_п$, затрачиваемого на принятие мер по устранению последствий проникновения.

При произвольных плотностях распределения $f_о$, $f_п$, $f_м$ случайных величин $t_о$, $t_п$, $t_м$, соответственно, выражение для своевременности реакции системы охраны можно представить в виде:

$$P(t_р < t_м) = 1 - P(t_м < t_р) = 1 - \int_0^{t_р} f_м(x)dx, \qquad (1)$$

где $t_р = \int_0^\infty y \int_0^\infty f_о(y-z) \cdot f_п(z)dzdy.$

Из общей интегральной формулы (1), задавая конкретные законы случайных величин $t_о$, $t_п$, $t_м$, можно получить соответствующие аналитические зависимости своевременности реакции системы охраны.

УДК 681.324:519.6

Меньших В.В. (Воронеж)

ВЫБОР МЕТОДОВ ОПТИМИЗАЦИИ ПОСЛЕДОВАТЕЛЬНОСТИ ВЫПОЛНЕНИЯ ДЕЙСТВИЙ В ВЫЧИСЛИТЕЛЬНЫХ ПОДСИСТЕМАХ СИСТЕМ ОХРАНЫ

Для решения задачи оптимизации последовательности выполнения действий в вычислительных подсистемах систем охраны, целесообразно использовать алгоритмы получения этих последовательностей на основе задания приоритетов одних действий перед другими [1-4]. Если в алгоритмах используется информация об оптимальном для априорно оцененных длительностей действий расписании, то алгоритмы называются жесткими диспетчерами. В противном случае, т.е. если приоритеты действий задаются по эвристическим правилам, алгоритмы называются адаптивными диспетчерами. Оптимизация последовательности выполнения действий осуществляется, как правило, при некотором рассогласовании априорных и апостериорных оценок длительностей отдельных действий, что ставит под сомнение обоснованность оптимальности выбранной последовательности. Поэтому важным представляется вопрос об описании условий предпочтительности тех или иных методов. Получено конкретное описание условий предпочтительности использования жестких и адаптивных диспетчеров в зависимости от значений r - неопределенности длительности действий, и s - средней загруженности исполнителей. Определено, что условия предпочтительности жестких диспетчеров перед адаптивными определяют связную область на (r,s)-плоскости.

Заметим, что вопрос об условиях предпочтительности использования жестких и адаптивных диспетчеров для оптимизации последовательности выполнения действий - это фактически вопрос об условиях, при которых оптимизацию необходимо производить с помощью трудоемких точных методов "глобальной" оптимизации, и при которых достаточно использовать эвристические методы "локальной" оптимизации, осуществляемой алгоритмами, имеющими небольшую вычислительную сложность.

1. Бублик Н.Г., Литвиненко Д.Э., Меньших В.В. Сравнение алгоритмов диспетчеризации в условиях неопределенности длительностей операций. Управляющие системы и машины, 1990, N3, с. 69-72.

2. Агафонова Н.А., Бублик Н.Г., Кипрушев А.А., Меньших В.В. Поведение жестких диспетчеров в условиях неопределенности длительностей операций. Автоматика и вычислительная техника, 1991, N2, с. 56-58.

3. Агафонова Н.А., Меньших В.В. Сравнение алгоритмов диспетчеризации для двухпроцессорной вычислительной системы. Автоматика и вычислительная техника, 1992, N1, с. 3-5.

4. Меньших В.В. Использование жестких диспетчеров в двухпроцессорной вычислительной системе. Автоматика и вычислительная техника, 1993, N3, с. 76-78.

ИМЕННОЙ УКАЗАТЕЛЬ