Известия вузов. Математика
2016, № 10, с. 92–97

http://kpfu.ru/science/nauchnye-izdaniya/ivrm/
e-mail: izvuz.matem@kpfu.ru

Краткое сообщение

Ж.Н. ТЕМИРГАЛИЕВА, Н. ТЕМИРГАЛИЕВ

"ГЕОМЕТРИЯ ЧИСЕЛ" В КОНТЕКСТЕ АЛГЕБРАИЧЕСКОЙ ТЕОРИИ ЧИСЕЛ

Аннотация. Как отмечается в обстоятельной монографии "Геометрия чисел" П.М. Грубера и К.Г. Леккеркеркера, "значительного вклада в классическую теорию вычисления и оценки критических определителей в последнее время отмечено не было". В данной статье, в определенном смысле, восполняется возникшая задержка в развитии указанной темы. Предлагается новый теоретико-числовой подход с многочисленными последствиями, фактически позволяющий с других позиций пересмотреть всю эту тематику.

Ключевые слова: "геометрия чисел", теория дивизоров, теорема Эйлера–Ферма, теория делимости Куммера, решетка, допустимая решетка, критические решетки и определители, тело, упаковка, решетчатая упаковка множеств, упаковывающая решетка, лучевая функция, звездное тело, постоянная Эрмита.

УДК: 511.682

Введение. Широко известные и разработанные в многочисленных публикациях разных времен различных авторов задачи построения равномерно распределенных сеток (конечных множеств) на многомерном единичном кубе, оптимальных или близких к оптимальным квадратурных формул с равными весами на классах функций с доминирующими смешанными производными и разностями, прямых и обратных быстрых преобразований Фурье на множествах, как это показано в работах [1]–[7], сводятся к задаче построения для заданного множества из евклидового пространства R^s решетки с возможно меньшим значением модуля определителя и эффективно решаются применением теоремы Эйлера–Ферма и его распространений на многомерный случай в рамках теории делителей Куммера (например, [8] и [9]). Вместе с тем, та же задача относится к основным в "геометрии чисел"([10] и [11]). Эта работа посвящена применению теории дивизоров к задачам "геометрии чисел".

1. Оценки сверху критических определителей произвольных множеств с построением соответствующих решеток. Начнем с необходимых определений (в обозначениях в основном будем следовать ([11], сс. 19, 31)).

Всюду ниже s — целое положительное число, R^s — действительное евклидово пространство размерности s, Z^s состоит из всех точек R^s с целыми координатами.

Пусть дана невырожденная $s \times s$-матрица

$$(c_{ij})_{i,j=1}^{s}, \tag{1}$$

Поступила 28.03.2016

или, что то же самое, система линейно независимых точек (векторов) $a_1 = (c_{11}, ..., c_{s1}), ...,$ $a_s = (c_{1s}, \dots, c_{ss})$ в R^s. Определим линейное преобразование

$$u \equiv (u_1, \dots, u_s) \xrightarrow{A} \left(\sum_{j=1}^{s} c_{1j}u_j, \dots, \sum_{j=1}^{s} c_{sj}u_j \right) = u_1a_1 + \dots + u_sa_s = Au, \tag{2}$$

которое R^s переводит в R^s.

Отметим, что всегда

$$Au = u \times A; \tag{3}$$

здесь и всюду ниже знак “$\times$” будем употреблять только для умножения матриц.

Решеткой Λ_A с базисом $a_1, \dots, a_s$ называют множество

$$\Lambda_A \equiv \{a_1u_1 + \dots + a_su_s : (u_1, \dots, u_s) \in Z^s\} \equiv AZ^s \equiv Z^s \times A.$$

Данной решетке $\Lambda \equiv \Lambda_A$ отвечает бесконечное множество базисов. Их общий вид $(a_1, \dots, a_s)\times$ $\times U = (b_1, \dots, b_s)$, где U пробегает все целочисленные матрицы с определителем ± 1. Однако $b_j = (b_{1,j}, \dots, b_{s,j})$ $(j = 1, \dots, s)$, $d(\Lambda) = |\det(b_{ij})_{i,j=1}^{s}|$ — объем параллелепипеда, построенного на векторах базиса, не зависит от выбора базиса. Число $d(\Lambda)$ называется *определителем решетки* Λ.

Через E^* будем обозначать множество $E \setminus \{0\}$. *Телом* называют всякое множество из R^s с непустой внутренностью, содержащееся в замыкании своей внутренности.

Говорят, что решетка $\Lambda \subset R^s$ является *допустимой* для множества $E \subset R^s$ или *E-допустимой*, если множество E^* не содержит точек решетки Λ.

Множество E, имеющее хотя бы одну допустимую решетку, называется множеством *конечного типа*; в противном случае E называется множеством *бесконечного типа*. Ясно, что всякое ограниченное множество является множеством конечного типа.

Пусть E — множество конечного типа. Наибольшая нижняя грань

$$\Delta(E) = \inf_{\Lambda\text{-}E\text{-допустима}} d(\Lambda)$$

определителей $d(\Lambda)$ всех E-допустимых решеток Λ называется *критическим определителем* множества E. Если E — множество бесконечного типа, то дополнительно определяют $\Delta(E) = +\infty$.

Всякая E-допустимая решетка Λ, для которой $d(\Lambda) = \Delta(E)$, называется *критической решеткой* множества E. Ясно, что множество бесконечного типа не имеет критических решеток. Множество E конечного типа также может не иметь критических решеток или иметь их конечное число, или иметь их бесконечное множество и счетной, и континуальной мощности [11].

Все построения в данной статье будут основаны на том, что для всякого простого $p \equiv 1 \pmod{l}$ в

$$Z^s \leftrightarrow \left\{m_1\omega_1 + \dots + m_s\omega_s : (m_1, \dots, m_s) \in Z^s,\ \theta = e^{2\pi i/l},\ \omega_j = \theta^{j-1}\ (j = 1, \dots, s)\right\}$$

можно эффективно построить целочисленную матрицу d, которой соответствует решетка (идеал) $\Lambda_p = dZ^s \equiv \rho$ с определителем (нормой идеала ρ) $d(\Lambda_p) = p$ (подробности в [2], [6]).

В условиях приведенных определений и обозначений справедлива относимая к основным

Теорема 1. *Пусть $l \geq 3$ — простое число, $s = l - 1$, $\theta = e^{2\pi i/l}$. Пусть $E \subset R^s$ — произвольное множество (не обязательно измеримое по Жордану, Лебегу и в любом другом смысле). Если существует такое простое число $p = 1 \pmod{l}$, что для всякого вектора $m = (m_1, \dots, m_s)$ с целочисленными координатами из множества E^* это число не*

является делителем целого числа $N(m) = \prod\limits_{k=1}^{s}(m_1 + m_2\theta^k + \cdots + m_s\theta^{(s-1)k})$, *то* p *оценивает сверху критический определитель,* E *имеет конечный тип, а решетка* $\Lambda_p \subset Z^s$ *с* $d(\Lambda_p) = p$, *которая эффективно строится по* p, *является* E*-допустимой.*

Прокомментируем эту теорему.

1. Теорема 1 применима для всякого ограниченного множества E, причем в этом случае проверку делимости на простое $p = 1 \pmod l$ можно проводить один раз для произведения $\prod\limits_{m\in E^*} N(m)$, сведя задачу к нахождению всех простых множителей в этом произведении.

2. Понятно, что оценка сверху критического определителя будет тем точнее, чем меньше будет найденное простое число p.

3. Аналогичные теореме 1 применения алгебраической теории чисел в задачах численного интегрирования даны в [1]–[6], в теории быстрых преобразований Фурье — в [7].

4. Теорема 1 в своих условиях и в своих методах из алгебраической теории чисел [1]–[7], по-видимому, ранее в обсуждаемой тематике не встречавшихся, дает решение общей задачи "геометрии чисел". Во всяком случае, в монографии ([10], гл. 1, п. 4) приведены различные связи между алгебраическими полями и решетками, включая нормы целых алгебраических чисел, но нет их применений в контексте теоремы 1.

5. Теорема 1 и по формулировке, и по используемому методу в геометрии чисел является новой, когда, независимо от строения множества E, единообразно устанавливается непринадлежность каждой ее ненулевой точки с целочисленными координатами будущей решетке. При этом, если к каждому конкретному случаю разрабатывался свой метод, например, метод Морделла ([11], гл. III, § 6), то теорема 1 дает общий метод для всех случаев.

6. В контексте теоремы 1 возникают специфические (типа "множества, для которых $V(E) = 2^s\Delta(E)$ в ([11], гл. IX, § 2) или же $V(E) = d(\Lambda)$) задачи классификации тел по их геометрическому строению с целью взаимного согласования с позиций критических (или близких к критическим) решеток с критическими определителями в виде простого числа $p \equiv 1 \pmod l$.

В плане практической реализации таких исследований потребуются различные известные вычислительные программы и создание новых, в частности, по той причине, что множества аналитически будут заданы как решения систем уравнений.

7. Подчеркнем, что оценки сверху критических определителей с построением конкретных решеток имеют, помимо теоретического, также и практическое значение. Оценки снизу (например, метод Блихфельдта ([10], гл. 5, § 33) используются для того, чтобы установить, насколько оценки сверху окончательны или близки к окончательным.

8. Одна из формулировок теоремы Минковского о выпуклом теле заключается в выполнении неравенства

$$\Delta(K) \geq 2^{-s}V(K), \tag{4}$$

где K — выпуклое, симметрическое относительно начала O тело из R^s объемом $V(K)$.

Условие выпуклости и симметричности множества $K \subset R^s$ для получения оценок типа (4) существенно, ибо тело K "близко" к открытому параллелепипеду

$$K = \prod_{j=1}^{s}(-b_j, b_j) \tag{5}$$

со сторонами, параллельными осям координат, и с центром в точке нуль, когда

$$V(K) = 2^s b_1 \cdots b_s \quad \text{и} \quad \Delta(K) = \det \begin{pmatrix} b_1 & 0 & \dots & 0 \\ o & b_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & b_s \end{pmatrix} = b_1 \cdots b_s.$$

Действительно, параллелепипеды (5) близки к эллипсоидам, от которых, в свою очередь, согласно теореме Джона не сильно отличаются выпуклые симметрические тела (подробности в [10], гл. I, п. 1.6).

Вместе с тем, в общем случае для всякого измеримого по Жордану (ограничимся этой самой “простой”мерой) множества E из R^s с мерой $V(E)$ и для любой решетки $\Lambda = dZ^s$ с $\det d \neq 0$ такой, что $E^* \cap \Lambda = \varnothing$, величины $V(E)$ и $|\det d|$ могут быть сколь угодно далеки друг от друга. Другое дело — сравнение $|E \cap \Lambda|$ и $|\det d|$, где для не более чем счетного множества I через $|I|$ обозначено количество его точек.

В связи с этим отметим, что для ограниченного множества $E \subset R^s$ в теореме 1 справедливо неравенство [2]

$$|E \cap \Lambda_p| \leq c(s) \sum_{m \in E^* \cap Z^s} \ln N(m).$$

9. Ограничения в размерности пространств $s = l - 1$ и значений определителей p, $p \equiv 1 \pmod{l}$, надо полагать, будут преодолены построением соответствующих алгебраических структур.

10. В теореме 1 решетки Λ_p принадлежат Z^s, что, вообще говоря, не ограничивает общности (например, [10], гл. 2, п. 16.1).

2. Случай общих допустимых решеток. Справедлива (см. также (1)–(3))

Теорема 2. *Пусть даны простое число $l \geq 3$ и множество $E \subset R^s$, где $s = l - 1$. Предположим, что найдется простое число p, $p \equiv 1 \pmod{l}$, такое, что для решетки $\Lambda_p \subset Z^s$ с базисом, записанным в виде целочисленной матрицы $d \equiv d_E$, и с определителем $\det d = d(\Lambda_p) = p$ выполнено $E^* \cap \Lambda_p \equiv E^* \cap d_E Z^s = \varnothing$. Тогда для всякой невырожденной $s \times s$-матрицы A имеет место теоретико-множественное соотношение*

$$(d_E^{-1} \times A)E^* \cap AZ^s = \varnothing.$$

Замечание 1. При заданном E и построенной по нему целочисленной матрице d_E множество всех возможных невырожденных $s \times s$-матриц A задает семейство множеств $(d_E^{-1} \times A)E$ с допустимой решеткой AZ^s.

В связи с этим возникает вопрос описания множеств вида $(d_E^{-1} \times A)E$ при невырожденных матрицах A в разных постановках. Одной из них является построение по наперед заданному множеству $J \subset R^s$ множества E и невырожденной матрицы A таких, что имеет место равенство или вложение $J \subset (d_E^{-1} \times A)E$ (аналогичные задачи в своих конкретизациях обсуждаются в [10], [11] (например, в [10], гл. 5, § 34, метод Блихфельдта–Морделла)).

Замечание 2. При критических Λ_E и $\Delta(E)$ для E будет ли критической для $K = (d_E^{-1} \times A)E$ решетка AZ^s.

Разумеется, это представленное выше направление исследований требует детализации, сравнений с известными результатами (библиографический список только в [10] составляет 100 страниц текста), что будет продолжено в последующих публикациях. Тем самым заложен потенциал для будущих исследований, основу которых составляют теоремы 1, 2.

Здесь ограничимся некоторыми следствиями из теорем 1, 2.

3. Алгоритмы построения упаковок. Потребуются известные определения ([10], с. 216–275). Набор множеств пространства R^s называется упаковкой (также применяется термин "*укладка*"), если внутренности любых двух из них не пересекаются.

Если в упаковке вида $\{E;\Lambda\} \equiv \{E+x : x \in \Lambda\}$ множество Λ является решеткой, то упаковка называется *решетчатой упаковкой множества E с упаковывающей решеткой Λ*, а само это семейство множеств — *расположением* множества E по решетке Λ.

Если решетка Λ имеет базис $a_1,\dots,a_s$, то полуоткрытый параллелепипед

$$E = \{v_1a_1 + \dots + v_sa_s : 0 \le v_j < 1 \ (j = 1,\dots,s)\}$$

и Λ образуют решетчатую упаковку множества E, причем $R^s = \bigcup\limits_{x\in\Lambda}\{E+x\}$.

Из теоремы Биркгофа–Блихфельдта [10], [11] и теоремы 1 вытекает

Теорема 3. *Пусть $l = s+1 > 2$ — простое число и E — такое множество из R^s, что для всех $m \in (E-E)^* \cap Z^s$ простое число $p \equiv 1 \pmod l$ не является делителем $N(m)$. Тогда*

$$\{E;\Lambda_p\} \equiv \{E+x : x \in \Lambda_p\}$$

составляет решетчатую упаковку множества E с упаковывающей решеткой Λ_p.

Из теорем 3 и 2 следует

Теорема 4. *Пусть $s+1 = l > 2$ — простое число и для простого $p \equiv 1 \pmod l$ множество E из R^s образует $\{E;\Lambda_p \equiv d_EZ^s\}$-упаковку. Тогда для любой невырожденной $s\times s$-матрицы A множество $K = (d_E^{-1}\times A)E$ образует $\{(d_E^{-1}\times A)E; AZ^s\}$-упаковку.*

4. Об одном практическом приеме построения упаковок заданной конфигурации. Из теорем 2 и 4 следует такой способ вычисления упаковок.

Для заданных простых $l = s+1$ и $p \equiv 1 \pmod l$ вычислением $m \in Z^s$ таких, что $p \nmid N(m)$ формируется множество $K = (d_E^{-1}\times A)E$ заданной конфигурации, образующее $\{(d_E^{-1}\times A)E; AZ^s\}$-упаковку.

5. Оценки постоянной Эрмита. Пусть $F(x) = F(x_1,\dots,x_s)$ — лучевая, т. е. неотрицательная, непрерывная, однородная функция, полностью описывающая *звездные* тела E, $E = \{x \in R^s : F(x) < 1\}$. Определяется постоянная Эрмита:

$$\gamma(F) = \sup_{\Lambda} \frac{m(F,\Lambda)}{\{d(\Lambda)\}^{1/s}},$$

где $m(F,\Lambda) = \inf\limits_{n\in\Lambda,\, n\ne 0} F(n)$, с которой связана

Теорема 5. *В условиях теоремы 1 для всякой лучевой функции $F(x)$ справедливы неравенства*

$$m(F,\Lambda_p) \le \gamma(F)p^{1/s} \quad и \quad \gamma(F) \ge p^{-1/s}.$$

Отметим, что значения $\gamma(F)$ для случая экстремальных положительно определенных форм $F(x_1,\dots,x_s)$ при $s = 2,\dots,8$ вычислены в ([10], с. 404–405).

Заметим, что эти результаты нашли применения в спектральном тестировании Ковэю–Макферсона генераторов случайных чисел Лехмера с максимальным периодом ([12], с. 109), числовые значения в которых уточнены (в сторону уменьшения) в [13].

Литература

[1] Воронин С.М., Темиргалиев Н. *О квадратурных формулах, связанных с дивизорами поля гауссовых чисел*, Матем. заметки **46** (2), 34–41 (1989).

[2] Темиргалиев Н. *Применение теории дивизоров к численному интегрированию периодических функций многих переменных*, Матем. сб. **181** (4), 490–505 (1990).

[3] Воронин С.М. *О построении квадратурных формул*, Изв. РАН. Сер. матем. **59** (4), 3–8 (1995).
[4] Темиргалиев Н., Баилов Е.А., Жубанышева А.Ж. *Об общем алгоритме численного интегрирования периодических функций многих переменных*, Докл. РАН **416** (2), 169–173 (2007).
[5] Жубанышева А.Ж., Темиргалиева Ж.Н., Темиргалиев Н. *Применение теории дивизоров к построению таблиц оптимальных коэффициентов квадратурных формул*, Журн. вычисл. матем. и матем. физ. **49** (1), 14–25 (2009).
[6] Баилов Е.А., Сихов М.Б., Темиргалиев Н. *Об общем алгоритме численного интегрирования функций многих переменных*, Журн. вычисл. матем. и матем. физ. **54** (7), 1059-1077 (2014).
[7] Темиргалиева Ж.Н., Темиргалиев Н. *Быстрые “алгебраические”преобразования Фурье на равномерно распределенных сетках*, Изв. вузов. Матем., № 5, 93–98 (2016).
[8] Эдвардс Г. *Последняя теорема Ферма. Генетическое введение в алгебраическую теорию чисел* (Мир, М., 1980).
[9] Гекке Э. *Лекции по теории алгебраических чисел* (ГИТТЛ., М.–Л., 1940).
[10] Грубер П.М., Леккеркеркер К.Г. *Геометрия чисел*, Пер. с англ. (Наука, М., 2008).
[11] Касселс Дж. *Введение в геометрию чисел* (Мир, М., 1965).
[12] Кнут В.Э. *Искусство программирования*. Т. 2. *Полученные алгоритмы* (Изд. дом “Вильямс” М., 2001).
[13] Темиргалиев Н., Темиргалиева Ж.Н. *Полное спектральное тестирование по методу Ковэю–Макферсона генераторов случайных чисел Лехмера с максимальным периодом*, Вестн. Евразийск. нац. ун-та им. Л.Н. Гумилева, № 2, 61–83 (2016).

Ж.Н. Темиргалиева

Университет Южной Калифорнии, Лос-Анджелес, США,

e-mail: temirgal@usc.edu

Н. Темиргалиев

Институт теоретической математики и научных вычислений,
Евразийский национальный университет им. Л.Н. Гумилева,
ул. Сатпаева, д. 2, г. Астана, 010008, Республика Казахстан,

e-mail: ntmath 10@mail.ru

Zh.N. Temirgaliyeva and N. Temirgaliyev

“Geometry of numbers” in a context of algebraic theory of numbers

Abstract. As noted in circumstantial monograph “Geometry of Numbers” by P.M. Gruber and C.G. Lekkerkerker, lately there is no considerable contribution to classical theory of calculation and estimates of critical determinants. In this article, in a certain sense, we fill a gap in occurred retardation in developing this theme. We propose a new theoretical-numerical approach with numerous consequences which, in fact, allows to revise all these subjects from another position.

Keywords: “geometry of numbers”, divisors theory, Euler–Fermat theorem, Kummer’s theory of divisibility, lattice, permissible lattice, critical determinants and lattice, body, packing, lattice packing set, packing lattice, ray function, star body, Hermite’s constant.

Zh.N. Temirgaliyeva

University of Southern California, Los Angeles, CA, USA,

e-mail: temirgal@usc.edu

N. Temirgaliyev

Institute of Theoretical Mathematics and Scientific Computing,
L.N. Gumilyov Eurasian National University,
2 Satpayev str., Astana, 010008 Republic of Kazakhstan,

e-mail: ntmath10@mail.ru