

Окружности на решетках и матрицы Адамара

Н. А. Балонин^а, доктор техн. наук, профессор, orcid.org/0000-0001-7338-4920, korbendfs@mail.ru

М. Б. Сергеев^а, доктор техн. наук, профессор, orcid.org/0000-0002-3845-9277

Дж. Себери^б, доктор наук, профессор, orcid.org/0000-0002-9558-4293, jennifer_seberry@uow.edu.au

О. И. Сеницына^а, аспирант, orcid.org/0000-0002-2819-4682

^аСанкт-Петербургский государственный университет аэрокосмического приборостроения,
Б. Морская ул., 67, Санкт-Петербург, 190000, РФ

^бУниверситет Вуллонгонг, Вуллонгонг, Новый Южный Уэльс 2522, Австралия

Введение: гипотеза Адамара о существовании всех матриц порядков, кратных четырем, и проблема Гаусса о числе точек в круге относятся к ряду важных поворотных пунктов в развитии математики. Они стимулировали развитие научных школ по всему миру с практически необозримым количеством работ. Приводятся обоснования, что эти научные задачи глубоко связаны, число точек Гаусса (точек на решетке \mathbb{Z}^3) на сфероиде, конусе, параболоиде, параболе и их расположение диктует количество и виды матриц Адамара. **Цель:** указать верхнюю и нижнюю границы количества точек Гаусса на сфероиде с нечетными координатами в зависимости от порядка задачи с целью конкретизировать теорему Гаусса (о разрешимости квадратичных задач в треугольных числах проекциями на плоскость Лиувилля) оценками на случай, касающийся матриц Адамара. **Методы:** предложенные авторами ранее пути доказательства гипотезы Адамара на основании взаимно-однозначного соответствия между ортогональными матрицами и точками Гаусса дополнены еще одним, использующим свойства обобщенных окружностей на \mathbb{Z}^3 . **Результаты:** доказано, что нижняя граница всех точек Гаусса с нечетными координатами равна радиусу экватора R , верхняя граница точек, размещенных выше экватора, равна длине этого экватора $L = 2\pi R$ и общее число точек ограничено значением $2L$. В силу симметрии сфероида в секторе с положительными координатами (октанте) это дает значения $R/8$ и $L/4$. Таким образом, число точек Гаусса с нечетными координатами не превышает длины периметра границы и не меньше относительной доли сектора в общем объеме фигуры. **Практическая значимость:** связанные с точками решетки матрицы Адамара имеют непосредственное практическое значение для задач помехоустойчивого кодирования, сжатия и маскирования видеоинформации.

Ключевые слова — точки Гаусса, проблема Гаусса, сфероид на решетке, ортогональные матрицы, матрицы Адамара, гипотеза Адамара, массив Балонина — Себери.

Для цитирования: Балонин Н. А., Сергеев М. Б., Себери Дж., Сеницына О. И. Окружности на решетках и матрицы Адамара. *Информационно-управляющие системы*, 2019, № 3, с. 2–9. doi:10.31799/1684-8853-2019-3-2-9

For citation: Balonin N. A., Sergeev M. B., Seberry J., Sinityna O. I. Circles on lattices and Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 3, pp. 2–9 (In Russian). doi:10.31799/1684-8853-2019-3-2-9

Введение

Окружности на решетках \mathbb{Z}^2 — это классическая тема теории чисел [1], которая интересуется количеством $N(R)$ точек с целыми координатами (точек Гаусса), попадающими в область, ограниченную окружностью $x^2 + y^2 = R^2$ радиуса R . Приближенный ответ на этот вопрос очевиден (если брать во внимание взаимно-однозначное соответствие между точками Гаусса и квадратами решетки), его дает округленное значение площади соответствующего круга $S = \pi R^2$. Более точный ответ дает оценка сверху величины поправки $E(R) = N(R) - \pi R^2$.

Приведенная Гауссом грубая оценка $E(R) < \sqrt{2}L(R)$, $L(R) = 2\pi R$ — длина окружности, учитывает точки на окружности и близкие к окружности пограничные точки. Элементарные компьютерные проверки показывают, что число точек на пограничной окружности с ростом радиуса осциллирует относительно некоторого среднего значения \sqrt{R} . В 1915 г. Харди и Эдмунд Ландау [2, 3] пришли к выводу, что $E(R)$ незначитель-

но, но превышает эту величину: $E(R) < CR^{1/2+e}$, $\varepsilon = 0,1298\dots$

Точное значение количества точек Гаусса $K(R) = 4(d_3 - d_1)$ на окружности с целым значением $n = R^2$ известно из истории нахождения числа разложений целого числа на сумму двух квадратов [1]. Оно оперирует количествами d_1 и d_3 нечетных делителей числа n вида $4t + 1$ и $4t + 3$, t — целое. Числа, разлагаемые на множители вида $4t + 3$ или их нечетные степени, неразложимы на сумму двух квадратов.

Таким образом, небольшие окружности часто содержат одну точку Гаусса в квадранте (или не содержат ее). Чтобы поддерживать указанное растущее в среднем число точек для все более часто встречаемых составных значений n , точки Гаусса «переселяются» на островки в виде населенных окружностей. Точное значение числа точек не связано явно с величиной радиуса. Такие формулы существуют для выборок, в частности, для $n = 5^k$ известно, что $K(n) = 4k + 1$. К сожалению, граница этого регулярного по количе-

ствам точек Гаусса семейства окружностей не может рассматриваться как оценка сверху для $K(R) > 4(\log_5(R^2) + 1)$.

Связь точек Гаусса с матрицами Адамара

Условия существования ортогональных по столбцам матриц давно связывают с теоремами о разложении чисел (их порядков или порядков составных блоков) на суммы двух и более квадратов [4–8]. Это напрямую касается отмеченных в указанной литературе взвешенных матриц и матриц Адамара. Тем самым блочные матрицы с элементами 1 и -1 представляют собой иллюстративный материал (в виде матричных портретов), касающийся известного теорем о разложениях чисел Ферма, Эйлера, Лагранжа.

Для построения симметричных блочных матриц достаточно трех блоков, поэтому подсчет точек Гаусса на сфероиде дает информацию о количестве видов матриц Адамара заданного порядка [9, 10]. Принципиальный и самый важный вопрос всей теории ортогональных массивов, который считается до сих пор не решенным (гипотеза Адамара), это вопрос существования матриц, и мы приводим еще один аргумент в пользу его положительного решения. В данной статье нас интересуют обобщенные окружности на решетках \mathbb{Z}^3 , сфероиды, которые, в отличие от рассмотренного случая, изучены заметно хуже [10, 11].

Согласно отмеченным работам Харди и Ландау, точки на окружности в сочетании с присоединенными точками круга ведут себя более инертно, их разброс более предсказуем в том смысле, что если $K(R) < F(R)$, то $E(R) < CR^{1/2+e} < F(R)$.

Сфероид содержит на своей поверхности семейство окружностей, образованных целочисленными (по высоте) срезами трехмерных фигур. Соответственно, и количество точек Гаусса на

нем ведет себя, скорее, как среднее значение точек на окружности (напомним, пропорциональное корню квадратному из радиуса экватора). Точки Гаусса сфероида отвечают своим проекциям, точкам в круге экватора. Обратное неверно. Не все точки Гаусса в круге экватора разрешимы как целочисленные на поверхности сферы. Осцилляции количеств точек Гаусса на трехмерных поверхностях лежат в более узком коридоре, чем на окружности и в круге, не касаясь нижней границей 0.

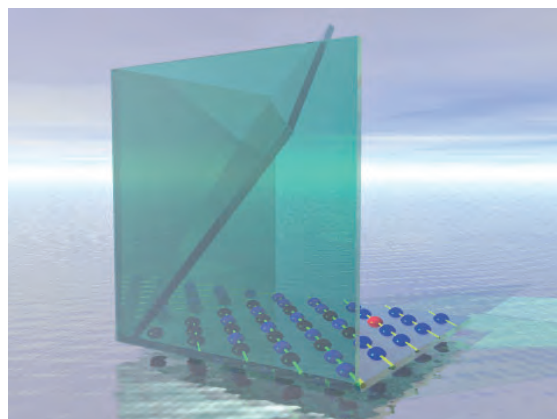
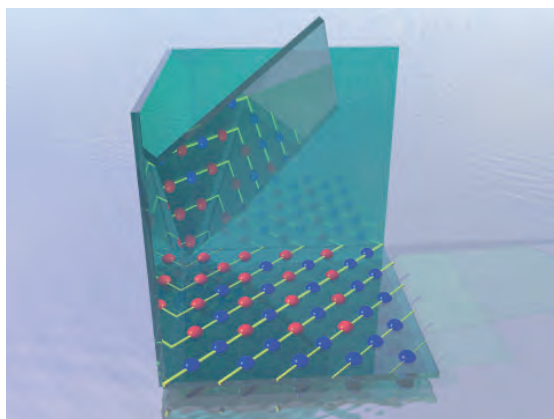
Более того, мы намерены показать, что отношение верхней и нижней границ пропорционально π по отношению к некоторой средней точке 2π .

Для удобства читателя мы даем ниже несколько исторических справок на тему точек Эйлера и Гаусса.

Задача Гольдбаха

Задача, которую Гольдбах передал товарищу по переписке, оказалась для Эйлера путеводной нитью в область теории числа. Оба они пришли к выводу, что любое четное число n состоит из суммы двух простых чисел [12]. Функция двух аргументов $n = x + y$ описывает плоскость, проходящую через начало координат, наклоненную под 45° по отношению к горизонтальной плоскости (рис. 1).

Мы даем вид на нее двумя проекциями, чтобы трехмерное построение было более понятно. Линии одинакового уровня наклонной плоскости на высотах, равных четным числам, образуют при проекции на плоскость x, y гипотенузы прямоугольных равнобедренных треугольников. Смысл наблюдения Эйлера и Гольдбаха состоит в том, что нет такой гипотенузы, на которой не встречалась бы хотя бы одна точка (отмечаемая красным цветом) с координатами, равными про-

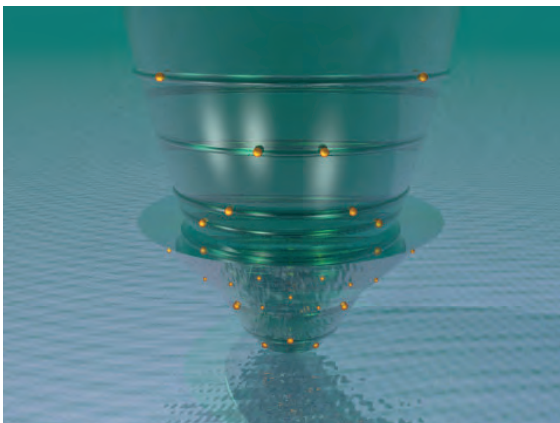


■ *Рис. 1.* Точки Эйлера — Гольдбаха
 ■ *Fig. 1.* Euler — Goldbach points

стым числам. Бинарная проблема Гольдбаха, как называют эту задачу, не решена до сих пор, хотя проверена компьютерами до очень больших значений четных чисел. Задачи, связанные с квадратичными функциями, также сводятся к точкам на плоскости, и если мы не решаем проблему селекции точек на простые и составные (по координатам), задача заметно упрощается.

Задача Гаусса — Лиувилля

В отличие от Эйлера и Гольдбаха, Гаусс искал целые точки внутри сечений конуса, окружность $x^2 + y^2 = R^2$ — это сечение некоторого конуса на высоте R . Масштабированием вертикальной оси (откладывая по вертикальной оси значение квадрата вертикальной координаты конуса $n = R^2$) конус преобразуется в параболоид $n = x^2 + y^2$, окружности сечений конуса отвечают окружностям параболоида (рис. 2).



■ Рис. 2. Точки Гаусса конуса и параболоида
 ■ Fig. 2. Gauss points of a cone and paraboloid

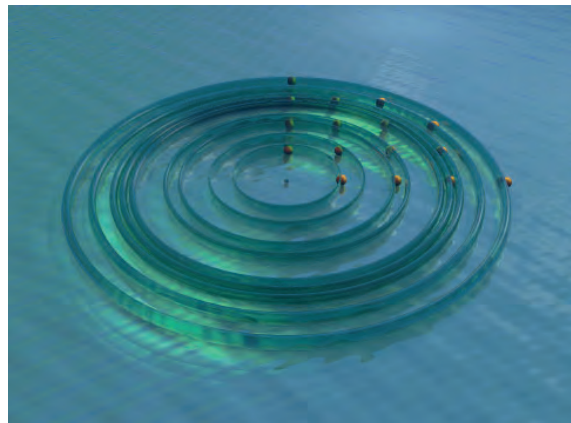
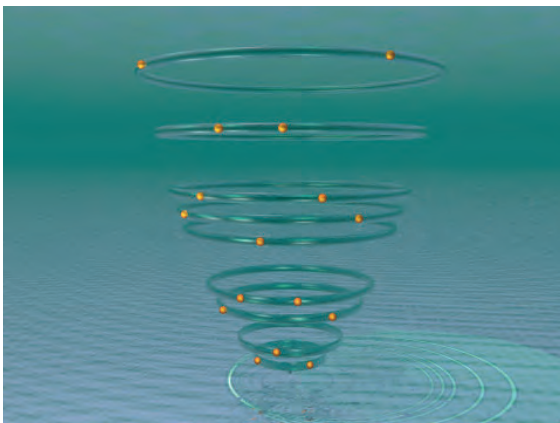
Для параболоида нет такой пары x, y , которая не нашла бы своего целочисленного разрешения. Проекция точек Гаусса на нем порождают решетку Z^2 , на рис. 3 показаны точки квадранта (фигура симметрична).

Интерес к квадратичным кривым у Гаусса обусловлен открытием, которое он сделал еще студентом. Он заметил, что равноудаленные точки, достижимые на окружности с помощью циркуля и линейки, являются корнями цепочек квадратных уравнений. Пришедшие с античных времен задачи построения вписанных в окружность правильных треугольника, пятиугольника и, как он установил, семнадцатиугольника, имеют в этом смысле одинаковую природу; построение последнего также достижимо. В настоящее время существует несколько методов построения правильного семнадцатиугольника.

Подсчеты равноотстоящих точек вывели его на задачу обобщения понятия числа. Как и Эйлер, Гаусс видел соответствие между целочисленными по значениям координат точками на плоскости (точками Гаусса) и комплексными числами. Наличие непротиворечивой арифметики комплексных чисел позволяло выделить на плоскости подобие простых чисел.

Настоящий успех пришел к Гауссу, когда он занялся сферическими поверхностями $x^2 + y^2 + z^2 = n$. Преобразование сферы в плоскость хорошо знакомо нам по видам проекций глобуса на карту мира. Само по себе это не ново, но 10 июля 1796 студент Гаусс оставил запись в своем дневнике: Эврика! $\text{num} = \Delta + \Delta + \Delta$.

Нелинейными преобразованиями координат $x^2 = 8\underline{x} + 1, y^2 = 8\underline{y} + 1, z^2 = 8\underline{z} + 1$ уравнение сферы преобразуется к уравнению плоскости вида $\underline{x} + \underline{y} + \underline{z} = r$, где $r = (n - 4)/8$ для серии порядков n дает целые числа. Гаусс доказал давнее утверждение Ферма, что для любого целого r уравне-



■ Рис. 3. Проецирование точек Гаусса с образованием решетки Z^2
 ■ Fig. 3. Gauss point projection with grid Z^2 formation

ние $x + y + z = r$ разрешимо на множестве треугольных чисел [13]. Треугольные числа, как и квадратные, принадлежат к фигурным числам, известным с древности. Они представляют собой последовательные суммы целых чисел 1, $1 + 2 = 3$, $1 + 2 + 3 = 6$ и т. д.

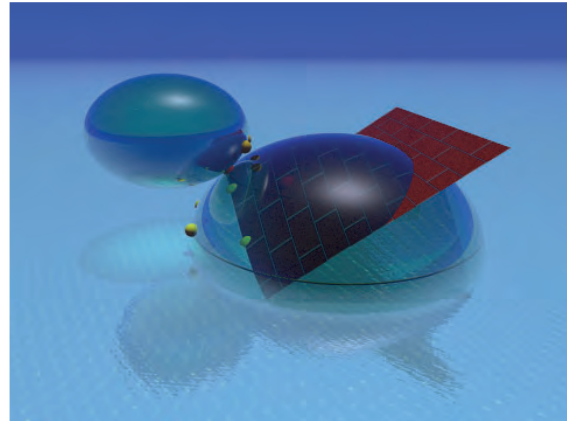
Лиувилль сделал следующий важный для нас шаг, он распространил теорему Гаусса на взвешенные суммы трех квадратов вида $x^2 + 2y^2 + z^2 = n$ [14]. Таким образом, так же, как круг, выделенные задачей сфера и сфероид разрешимы как минимум одной ненулевой точкой, в остальном их поведение различно. Нас интересует в первую очередь сфероид, потому что он обобщает разложение чисел на сумму четырех квадратов. С обобщениями окружностей на решетках \mathbf{Z}^4 нам не хотелось бы иметь дело, а при равенстве между собой любой пары координат четырехмерного пространства мы переходим к сфероиду Лиувилля.

Изучение сфероида Лиувилля

Как это водится при решениях уравнений Диофанта, часть точек являются эфемерными (нам не годится решение типа «полтора землекопа»). Точек Гаусса с четными координатами нет на порядках n , кратных $8(4k + 7)$. Они являются дополнением (как присоединенные к окружности точки круга) и исчезают при сжатии сфероида вдвое со смещением его в точку $v/2$ (по всем трем координатам). Так как задачи на поиски матриц Адамара приводят к уравнению малого сфероида, то, работая с большим, мы будем иметь в виду точки с нечетными координатами. Эту ситуацию с большим и малым (сжатым и смещенным) сфероидом и плоскостью Лиувилля для $n = 36$ отражает рис. 4.

У сфероида $x^2 + 2y^2 + z^2 = n$, помимо большого радиуса экватора $R = \sqrt{n}$, есть вторая (вертикальная) полуось размера $R/\sqrt{2}$. На рисунке приведено три точки Гаусса с нечетными координатами в одном из октантов и плоскость $x + 2y + z = r$, проектирование на которую гарантированно дает точки с треугольными координатами. Сфероид, сжатый вдоль одной из осей, имеет двойственную природу, представляя собой совокупность сложенных стопкой окружностей или, это как посмотреть, совокупность эллипсов в иной нарезке.

Правило 1. При $n = 4v$, v — нечетное, верхняя граница для точек с нечетными координатами, размещенными выше экватора, равна длине этого экватора $L = 2\pi R$ (т. е. общее число точек ограничено значением $2L$). Нижняя граница всех точек с нечетными координатами равна радиусу экватора R .



■ *Рис. 4.* Большой и малый сфероиды Лиувилля
 ■ *Fig. 4.* Large and small Liouville spheroids

В силу симметрии сфероида это замечательное правило ограничивает верхнее и нижнее значения возможного числа точек в секторе с положительными координатами (октанте) значениями $L/4$ и $R/8$. Таким образом, число точек Гаусса с нечетными координатами не превышает длины периметра границы и оно не меньше относительной доли октанта в общем объеме фигуры.

Доказательство первого утверждения состоит в том, что на границе действительно не уместить большее число целых точек, чем ее длина, тем более с нечетными координатами, а возможности, которые дают сечения сверху, столь быстро убывают, что длина границы экватора лимитирует число точек сверху. Что касается минимального числа точек, то радиус является осью для нарезанных на нем эллипсоидов; если каждый из них разрешим как минимум одной точкой, число точек ограничено размером фигуры. Учитывая, что нам нужны точки с нечетными координатами, в рассмотрение попадает радиус экватора, а не диаметр полной нарезки. Пропуски точек не влияют на оценку ввиду возможностей объемной фигуры так или иначе их компенсировать.

Мы привели, разумеется, простейшее обоснование установленных нами границ. Так как теоремы Гаусса и Лиувилля достаточны для принципиальной разрешимости задачи о точках на сфероиде, дополнительная компьютерная проверка правила для порядков матриц Адамара до миллиона дает нам в руки проверенный, практичный и надежный инструмент оценивания числа решений.

У сфероида есть два характеризующих его размера, эта двойственность проявляется в двойных оценках верхней и нижней границы на число точек Гаусса.

Правило 2. Для порядков $n < 10^5/2$ верхняя граница для точек с нечетными координатами,

размещенными выше экватора, равна $4\sqrt{2}R$ (в октанте в 4 раза меньше: $\sqrt{2}R$). Нижняя граница всех точек с нечетными координатами равна $4R/\pi$, в октанте в 8 раз меньше.

Доказательство второго положения более чем элементарно и заключается в компьютерной проверке числа решений уравнений сфероида Лиувилля.

Отношения верхней и нижней границ в обоих случаях пропорционально π . Жесткое отношение составляет величину 4π , для малых порядков координатор в $\sqrt{2}$ уже.

Правило 3. Отношение верхней и нижней границ пропорционально π , по отношению к средней точке оно равно 2π , что легко запомнить. Эти правила связывают число точек Гаусса для сжатого сверху сфероида, их нет в доступной нам научной литературе. Тем самым это существенно новые, неизвестные ранее (по крайней мере, широко) оценки для обобщенной задачи Гаусса. Ее значение усиливается рассматриваемым далее приложением к теории симметричных матриц Адамара.

Результаты компьютерного исследования задачи о числе точек Гаусса с нечетными координатами для $n < 2 \times 10^5$ приведены на рис. 5 в виде двух качественных диаграмм: рисунок справа повторяет зависимость слева, но вдоль горизонтальной оси взят корень квадратный аргумента n .

Масштабирование приводит к характерному для квадратичных задач спрямлению границ. Возможные решения все лежат в секторе, для малых сфероидов более узком. Переключение одного типа возрастания числа точек на другой происходит примерно после первой четверти значений порядков. Всего было проверено значение аргумента до миллиона, тенденция сохранилась.

Приложение к теории симметричных матриц Адамара

Матрицы Адамара — квадратные матрицы \mathbf{H} порядка n выше 1, 2, кратного 4, с элементами -1 и 1 такие, что выполняется

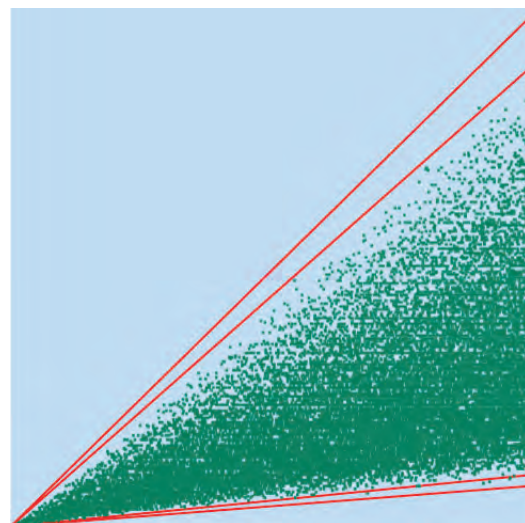
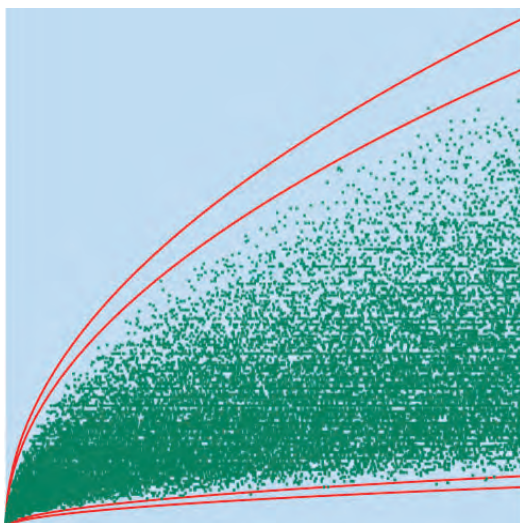
$$\mathbf{H}^T \mathbf{H} = n\mathbf{I}, \quad (1)$$

где $\mathbf{I} = \text{diag}(1, 1, \dots, 1)$ — единичная матрица [5, 6]. Эти матрицы появились благодаря работам основоположника матричной математики Дж. Сильвестра, который задал их рекурсивной и наиболее известной в теории матриц Адамара последовательностью $\mathbf{H} = \begin{pmatrix} \mathbf{A} & \mathbf{A} \\ \mathbf{A} & -\mathbf{A} \end{pmatrix}$, где \mathbf{A} — матрица Адамара на предыдущем шаге рекурсии. Начинать можно от $\mathbf{A} = 1$, как это делал Сильвестр, Адамар нашел еще две стартовые несимметричные матрицы 12-го и 20-го порядков [4].

Позднее в обиход вошли конструкции на двух не обязательно ортогональных основаниях \mathbf{A}, \mathbf{B} , например: $\mathbf{H} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^T & -\mathbf{A}^T \end{pmatrix}$, для симметричных матриц $\mathbf{A} = \mathbf{A}^T$. Дополним ее более универсальной конструкцией

$$\mathbf{H} = \begin{pmatrix} \mathbf{A} & -\mathbf{B}\mathbf{R} & -\mathbf{C}\mathbf{R} & -\mathbf{D}\mathbf{R} \\ -\mathbf{C}\mathbf{R} & \mathbf{R}\mathbf{D} & -\mathbf{A} & -\mathbf{R}\mathbf{B} \\ -\mathbf{B}\mathbf{R} & -\mathbf{A} & -\mathbf{R}\mathbf{D} & \mathbf{R}\mathbf{C} \\ -\mathbf{D}\mathbf{R} & -\mathbf{R}\mathbf{C} & \mathbf{R}\mathbf{B} & -\mathbf{A} \end{pmatrix}, \quad (2)$$

где \mathbf{A}^T — симметричный блок, условие (1) сводится к $\mathbf{A}^T \mathbf{A} + \mathbf{B}^T \mathbf{B} + \mathbf{C}^T \mathbf{C} + \mathbf{D}^T \mathbf{D} = n\mathbf{I}$. Симметрия второй



■ **Рис. 5.** Качественный график числа точек Гаусса на сфероиде Лиувилля
 ■ **Fig. 5.** Qualitative graph of the Gauss point numbers on the Liouville spheroid

конструкции обеспечивается условием $B = C$, приводящим к (2). Итерационное расширение по правилу Сильвестра закрывает симметричными матрицами порядка s четным значением v . Поэтому более первичны конструкции с нечетным размером блоков v , когда $r = (v - 1)/2$ — номер конструкции.

В научной литературе она получила наименование массива Балонина — Себерри, или, для простоты, Пропус: Эта Близнецов (η Gem / η Geminorum) — тройная звезда в созвездии Близнецов — имеет традиционное название Procyon. Учитывая сложившуюся практику наименований блоков матриц Адамара, так кратко называют иногда не весь массив, а блоки; будучи все симметричными, они совпадают с матрицами Вильямсона. Противоположный случай именуется массивом семейства Пропусов (Propus-type array) [8, 9].

Связь симметричных матриц Адамара с задачей Гаусса — Лиувилля становится очевидной, если мы учтем, что количество -1 в каждой строке блоков (орнаментальные коэффициенты [10, 11]) описывается формулами

$$k_1 = (v - x)/2, k_2 = (v - y)/2, k_3 = (v - z)/2, \quad (3)$$

данными над уравнением связи

$$x^2 + 2y^2 + z^2 = n. \quad (4)$$

Параметр ортогонального баланса $\lambda = (k_1 + 2k_2 + k_3) - n/4$ задает число соседних -1 в каждой паре строк матрицы H (в делителе n фигурирует количество блоков матрицы без учета их возможного тождества). Таким образом, доказательство теоремы Адамара о существовании всех матриц порядков, кратных 4, сводится к доказанным в теории чисел теоремам о разрешимости точек плоскости Гаусса — Лиувилля $\underline{x} + 2\underline{y} + \underline{z} = r$ треугольными числами [1, 12].

Бициклические матрицы и моноблоки

Для двублочной конструкции H необходимое условие существования несимметричной, в общем, матрицы Адамара заключается в разложимости ее порядка на сумму двух квадратов. Аналог сфероида в данном случае — окружность Лиувилля (срез ранее обсуждаемого параболоида) (рис. 6).

Роль малого сфероида Лиувилля играет вдвое более узкий параболоид с точками $k_1 = (v - x)/2$, $k_2 = (v - y)/2$, с центром, смещаемым в точку $v/2$ по обеим координатам. Положения его срезов показаны на рис. 7.

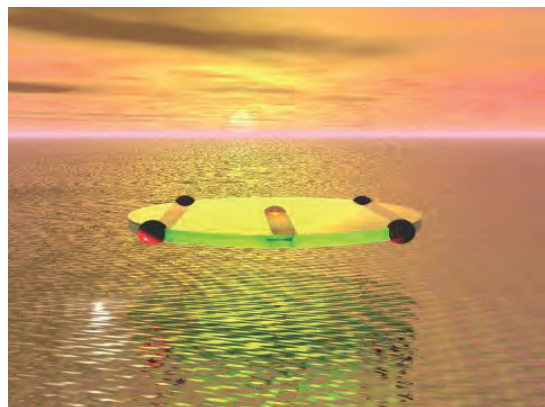
Компьютерные портреты матриц Адамара являются превосходным и мало известным иллюстративным материалом к древним числовым тео-

ремам Ферма, Эйлера, Лагранжа и Гаусса о разложениях чисел на суммы квадратов. Каждое такое разложение сопровождается своей матрицей, орнаментальные особенности которой тесно связаны с сортом поверхности, на котором точка расположена, и особенностями самих чисел (рис. 8).

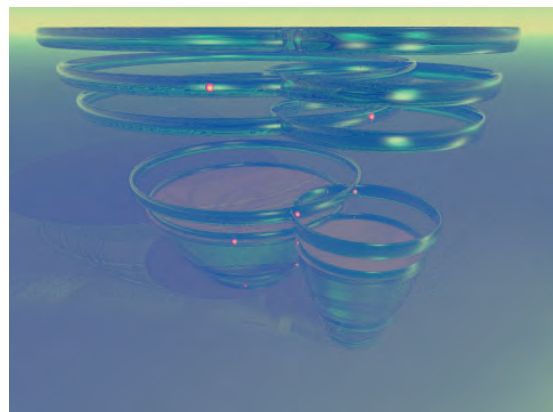
Например, порядок $n = 4 \times 3^2 = 36$ разлагается на сумму двух квадратов, поскольку содержит критический делитель 3 в четной степени. Соответствующая матрица Адамара существует, однако на ее орнамент наложено более серьезное, чем в других таких случаях, ограничение: ее не реализовать при помощи двух циклических блоков A, B . Необходимо более сложная конструкция, например в виде Пропуса.

Вместе с тем порядок n является квадратом, так что Пропус, в свою очередь, может рассматриваться как моноблок A с $k_1 = (n - x)/2$.

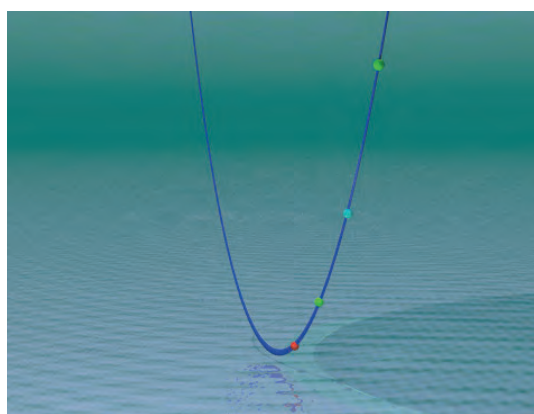
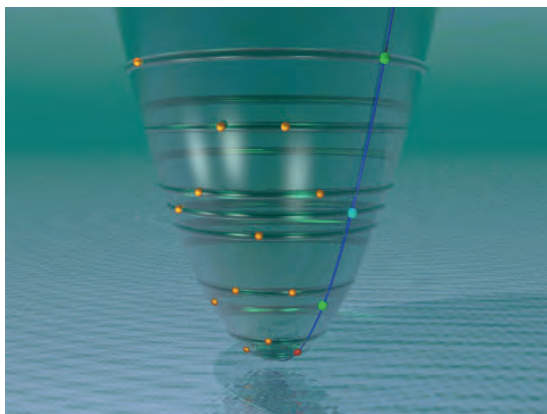
Точки Гаусса $\{n, x\}$ размещены на параболе $n = x^2$, $x = 2u$ — четное число. Такого сорта перевертыши порождают так называемые регулярные матрицы Адамара со свойствами магических



■ Рис. 6. Точки Гаусса на окружностях Лиувилля
 ■ Fig. 6. Gauss points on Liouville circles



■ Рис. 7. Окружности Лиувилля для начальных порядков
 ■ Fig. 7. Liouville circles for initial orders



■ Рис. 8. Точки Лиувилля на параболе (срезе параболоида)

■ Fig. 8. Liouville points on a parabola (cut of a paraboloid)

квадратов: суммы строк и столбцов одинаковы между собой.

Хорошо известно, что четные сомножители не оказывают влияния на сам факт разложения порядка. Тем не менее одним лишь умножением порядка 36 на 4 мы переходим в расширенное пространство с $n = 16 \times 3^2 = 144$, в котором циклические парные блоки **A**, **B**, оказывается, существуют.

Заключение

В работе исследована мало изученная связь задач об окружностях на решетках с темой ортогональных матриц. Эта связь дает нам в руки очень важные инструменты для установления внешнего вида матриц, регламентируемого орнаментальными коэффициентами (количествами -1 в строках). Тщательное исследование сфероидов Лиувилля привело нас к выводу о том, что количество точек Гаусса на них отвечает известной теореме о наличии решений.

Установлено, что число решений растет с порядком и подчиняется секторным ограничениям, описанным нами.

Формулы для подсчетов минимального, среднего и максимального количества точек Гаусса на

сфероиде новы и ранее в научной литературе не встречались. Они важны, поскольку иллюстрируют не только качественно, но и количественно число различных между собой симметричных матриц Адамара — Пропусов, т. е. отвечают подробно на задачу, поставленную Жаком Адамаром более ста лет тому назад: существуют ли матрицы Адамара на порядках, кратных 4, каковы они, и сколько таких матриц существует.

Финансовая поддержка

Работа выполнена при поддержке Минобрнауки РФ при проведении научно-исследовательской работы в рамках проектной части государственного задания в сфере научной деятельности по заданию № 2.2200.2017/4.6.

Благодарности

Мы приносим благодарность за многолетнее сотрудничество и поддержку профессору Драгомиру Джоковичу. Большую помощь в технической работе с рукописью статьи оказала Т. В. Балонина.

Литература

1. Вавилов В. В., Устинов А. В. Окружности на решетках. *Квант*, 2006, № 6, с. 34–40.
2. Hardy G. H. On the expression of a number as the sum of two squares. *Quart. J. Math.*, 1915, vol. 46, pp. 263–283.
3. Landau E. Über die Gitterpunkte in einem Kreise. *Nachr. Ges. Wiss. Göttingen*, 1915, pp. 148–160 (In German).
4. Hadamard J. Résolution d'une Question Relative aux Déterminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246 (In French).
5. Seberry J., Yamada M. Hadamard matrices, sequences, and block designs. In: *Contemporary design theory: A collection of surveys*/ J. H. Dinitz and D. R. Stinson, eds. John Wiley and Sons, 1992. Pp. 431–560.
6. *Handbook of combinatorial designs*. 2nd ed./ Charles J. Colbourn, Jeffrey H. Dinitz, eds. Chapman and Hall/CRC, 2006. 1000 p.
7. Yamada M., Seberry J. *Hadamard matrices constructed using number theory and algebra*. John Wiley (to appear).

8. Balonin N. A., Seberry J. Two infinite families of symmetric Hadamard matrices. *Australian Journal of Combinatorics*, 2017, vol. 69(3), pp. 349–357.
9. Balonin N. A., Balonin Y. N., Djokovic D. Z., Karbovskiy D. A., Sergeev M. B. Construction of symmetric Hadamard matrices. *Информационно-управляющие системы*, 2017, № 5, с. 2–11. doi.org/10.15217/issn1684-8853.2017.5.2 (16 Aug 2017; arXiv:1708.05098).
10. Балонин Н. А., Сергеев М. Б. Как гипотезе Адама-ра помочь стать теоремой. Ч. 1. *Информационно-управляющие системы*, 2018, № 6, с. 2–13. doi:10.31799/1684-8853-2018-6-2-13
11. Балонин Н. А., Сергеев М. Б. Как гипотезе Адама-ра помочь стать теоремой. Ч. 2. *Информационно-управляющие системы*, 2019, № 1, с. 2–10. doi:10.31799/1684-8853-2019-1-2-10
12. Стюарт И. *Величайшие математические задачи*. М., Альпина нон-фикшн, 2016. 460 с.
13. Гаусс К. Ф. *Труды по теории чисел*/ пер. Б. Б. Демьянова; под ред. И. М. Виноградова; комментарии Б. Н. Делоне. М., Изд-во АН СССР, 1959. 978 с.
14. Liouville J. Nouveaux théorèmes concernant les nombres triangulaires. *Journal de Mathématiques Pures et Appliquées*, 1863, no. 8, pp. 73–84 (In French).

UDC 519.614

doi:10.31799/1684-8853-2019-3-2-9

Circles on lattices and Hadamard matricesN. A. Balonin^a, Dr. Sc., Tech., Professor, orcid.org/0000-0001-7338-4920, korbendfs@mail.ruM. B. Sergeev^a, Dr. Sc., Tech., Professor, orcid.org/0000-0002-3845-9277J. Seberry^b, Dr. Sc., Tech., Honorary Professor, orcid.org/0000-0002-9558-4293, jennifer_seberry@uow.edu.auO. I. Sinityna^a, Post-Graduate Student, orcid.org/0000-0002-2819-4682^aSaint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaya St., 190000, Saint-Petersburg, Russian Federation^bDepartment of Computing and Information Technology, University of Wollongong, NSW 2522, Australia

Introduction: The Hadamard conjecture about the existence of Hadamard matrices in all orders multiple of 4, and the Gauss problem about the number of points in a circle are among the most important turning points in the development of mathematics. They both stimulated the development of scientific schools around the world with an immense amount of works. There are substantiations that these scientific problems are deeply connected. The number of Gaussian points (Z^3 lattice points) on a spheroid, cone, paraboloid or parabola, along with their location, determines the number and types of Hadamard matrices. **Purpose:** Specification of the upper and lower bounds for the number of Gaussian points (with odd coordinates) on a spheroid depending on the problem size, in order to specify the Gauss theorem (about the solvability of quadratic problems in triangular numbers by projections onto the Liouville plane) with estimates for the case of Hadamard matrices. **Methods:** The authors, in addition to their previous ideas about proving the Hadamard conjecture on the base of a one-to-one correspondence between orthogonal matrices and Gaussian points, propose one more way, using the properties of generalized circles on Z^3 . **Results:** It is proved that for a spheroid, the lower bound of all Gaussian points with odd coordinates is equal to the equator radius R , the upper limit of the points located above the equator is equal to the length of this equator $L = 2\pi R$, and the total number of points is limited to $2L$. Due to the spheroid symmetry in the sector with positive coordinates (octant), this gives the values of $R/8$ and $L/4$. Thus, the number of Gaussian points with odd coordinates does not exceed the border perimeter and is no less than the relative share of the sector in the total volume of the figure. **Practical significance:** Hadamard matrices associated with lattice points have a direct practical significance for noise-resistant coding, compression and masking of video information.

Keywords — Gaussian points, Gauss problem, spheroid on a lattice, orthogonal matrices, Hadamard matrices, Hadamard conjecture, Balonin — Seberry array.

For citation: Balonin N. A., Sergeev M. B., Seberry J., Sinityna O. I. Circles on lattices and Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 3, pp. 2–9 (In Russian). doi:10.31799/1684-8853-2019-3-2-9

References

1. Vavilov V. V., Ustinov A. V. Circles on lattices. *Kvant*, 2006, no. 6, pp. 34–40 (In Russian).
2. Hardy G. H. On the expression of a number as the sum of two squares. *Quart. J. Math.*, 1915, vol. 46, pp. 263–283.
3. Landau E. Über die Gitterpunkte in einem Kreise. *Nachr. Ges. Wiss. Göttingen*, 1915, pp. 148–160 (In German).
4. Hadamard J. Résolution d’une Question Relative aux Déterminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246 (In French).
5. Seberry J., Yamada M. *Hadamard matrices, sequences, and block designs*. In: *Contemporary design theory: A collection of surveys*. J. H. Dinitz and D. R. Stinson, eds. John Wiley and Sons, 1992. Pp. 431–560.
6. *Handbook of combinatorial designs*. 2nd ed. Charles J. Colbourn, Jeffrey H. Dinitz eds. Chapman and Hall/CRC, 2006. 1000 p.
7. Yamada M., Seberry J. *Hadamard matrices constructed using number theory and algebra*. John Wiley (to appear).
8. Balonin N. A., Seberry J. Two infinite families of symmetric Hadamard matrices. *Australian Journal of Combinatorics*, 2017, vol. 69(3), pp. 349–357.
9. Balonin N. A., Balonin Y. N., Djokovic D. Z., Karbovskiy D. A., Sergeev M. B. Construction of symmetric Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2017, no. 5, pp. 2–11. doi:10.15217/issn1684-8853.2017.5.2 (16 Aug 2017; arXiv:1708.05098).
10. Balonin N. A., Sergeev M. B. Helping Hadamard conjecture to become a theorem. Part 1. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 6, pp. 2–13 (In Russian). doi:10.31799/1684-8853-2018-6-2-13
11. Balonin N. A., Sergeev M. B. Helping Hadamard conjecture to become a theorem. Part 2. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 1, pp. 2–10 (In Russian). doi:10.31799/1684-8853-2019-1-2-10
12. Stewart Ian. *The Great Mathematical Problems*. Profile Books, 2013. 320 p.
13. Gauss K. F. *Trudy po teorii chisel* [Works by number theory]. Moscow, AN SSSR Publ., 1959. 978 p.
14. Liouville J. Nouveaux théorèmes concernant les nombres triangulaires. *Journal de Mathématiques Pures et Appliquées*, 1863, no. 8, pp. 73–84 (In French).