МАТЕМАТИЧЕСКОЕ ПРОСВЕЩЕНИЕ

Третья серия

выпуск 21

Москва
Издательство МЦНМО
2017

УДК 51.009
ББК 22.1
М34

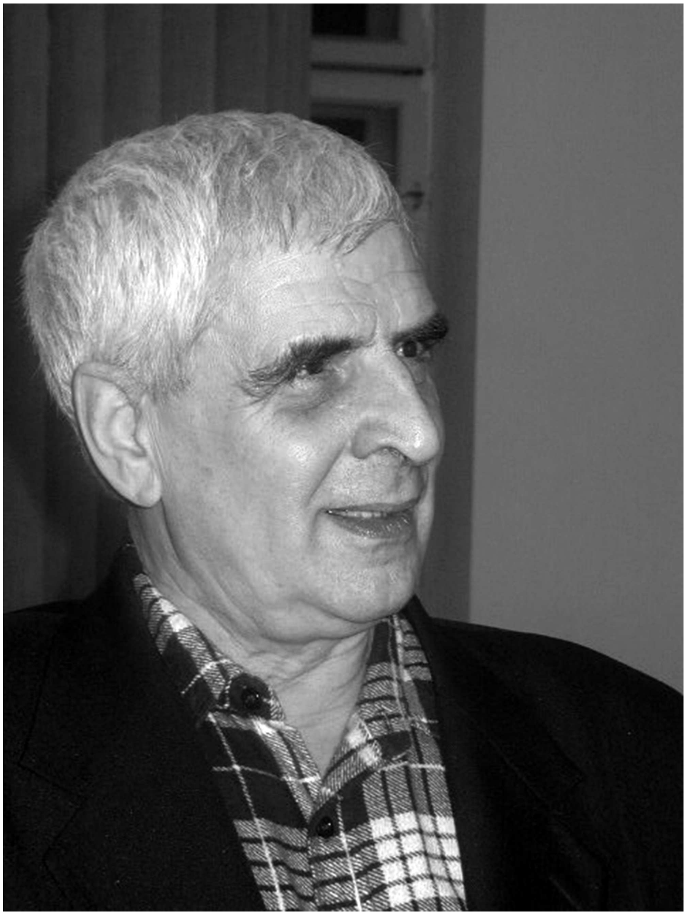
Адрес редакции:
119002, Москва, Б. Власьевский пер., д. 11, МЦНМО
(с пометкой «Математическое просвещение»)
Email: matpros@mccme.ru
Web page: www.mccme.ru/free-books/matpros.html

М34 **Математическое просвещение.** Третья серия, вып. 21. —
М.: МЦНМО, 2017. — 288 с.
ISBN 978-5-4439-1141-0

В сборниках серии «Математическое просвещение» публикуются материалы о проблемах современной математики, изложенные на доступном для широкой аудитории уровне, статьи по истории математики, обсуждаются проблемы математического образования.

УДК 51.009
ББК 22.1

ISBN 978-5-4439-1141-0



Поздравляем

Николая Николаевича Константинова

с 85-летием!

Содержание

Математический мир

Рассказ о Владимире Игоревиче Арнольде

Ю. С. Ильяшенко

На летней школе «Динамические системы» в июле 2010 г. участники попросили автора рассказать им о В. И. Арнольде. В застеклённой гостиной у подножья Высоких Татр при свете камина состоялся этот рассказ. Он был записан и расшифрован И. В. Щуровым, которому автор приносит свою глубокую благодарность. Конечно, этот рассказ далеко не полон. В нём нет ни слова ни о теории катастроф, ни о вещественной алгебраической геометрии. Это всего лишь маленький фрагмент ещё не созданного полотна [1).

Владимир Игоревич Арнольд был одним из тех людей, появление которых составляет счастье для своего поколения и вообще для их современников. Он всегда казался мне человеком гораздо более широким, чем просто математик. Он вносил дух художества и поэзии в математику. И взгляд его на математику был взглядом не только математика-профессионала, но и художника. Красота была присуща всему, что он придумывал сам или интерпретировал.

Он родился в потомственной интеллигентной семье. Был старшим из трёх детей. У него был младший брат, близкий ему по возрасту, и сестра, на 10 лет моложе. Мама его — из семейства Мандельштамов. Великий физик Леонид Исаакович Мандельштам и замечательный биолог Александр

[1) Автор благодарит А. Б. Сосинского, прочитавшего статью в рукописи и сделавшего много полезных замечаний. Автор признателен также $\boxed{\text{В. Д. Арнольду}}$, сообщившему ряд ценных сведений. Много биографической информации содержится в интервью В. И. Арнольда в книге В. Демидовича «К истории мехмата МГУ», М.: МГУ, 2013, с. 137–171.

Владимир Игоревич Арнольд

Гаврилович Гурвич — его родственники. Предположительно есть родство и с великим поэтом Осипом Эмильевичем Мандельштамом.

На Арнольда сильно повлияли люди уровня Л. И. Мандельштама, в частности физик Игорь Евгеньевич Тамм. С другим абсолютно выдающимся математиком своего поколения, Сергеем Петровичем Новиковым, он был знаком с детства. Алексей Андреевич Ляпунов, один из учеников Лузина, устроил детскую академию на даче в посёлке Ямщины близ Голицына, и подростки Новиков и Арнольд были членами этой академии[2].

В общем, Арнольд получил чрезвычайно мощный интеллектуальный импульс в детстве. По-видимому, он успел взять не очень много от своего отца, который умер, когда мальчику было 11 лет, и Владимир остался старшим мужчиной в семье. Думаю, он вполне сознавал свою ответственность. Во всяком случае, отношения с сестрой у него были очень тёплые и тесные.

Владимир Игоревич жил в одном из арбатских переулков — Спасо-Песковском. К началу войны ему было 4 года, он помнил немецкие бомбёжки и рассказывал, что, пытаясь разбомбить Бородинский мост, который идёт

[2] Ссылки на книги об А. А. Ляпунове и его деятельности см. на `http://math.ru/history/people/LyapunovAA`

к Киевскому вокзалу, немцы попали в театр Вахтангова — такая, говорит он, была в те времена точность бомбометания. В эвакуации семья была с октября 1941 по октябрь 1944 года.

Детство Арнольда и моё прошло по соседству, с 1949 по 1959 год я жил в Большом Власьевском переулке, неподалёку от Спасо-Песковского. Учились мы оба в школе № 59, которая была несомненно одной из лучших школ Москвы. Ни к нему, ни ко мне она не входила в микрорайон. Но родители — его мама и мои родители — добились того, чтобы мальчики поступили в эту прекрасную школу. В ней было много знаменитых учителей. Один из самых знаменитых, один из лучших в Москве учителей математики был Иван Васильевич Морозкин — невероятно грозный, но невероятно талантливый, способный пробудить интерес к творчеству в своих учениках. И нам он рассказывал об Арнольде. Собственно говоря, он взял нашу параллель в пятом классе, в предыдущий год выпустив параллель, где учился Арнольд. И байки, притчи о лучшем ученике параллели — Арнольде — он рассказывал нам всё время. В 1957 году он показал нам оттиск из ДАН — и сказал, что студент 3-го курса, 19-летний Дима Арнольд, решил проблему, за которую следует как минимум дать докторскую. Арнольд приходил в школу к Морозкину. Я видел такого прозрачного, худенького юношу. Шесть лет разницы — это очень много (это я сейчас с трудом отличаю 15-летнего человека от 19-летнего); тогда 19-летний казался мне невероятно взрослым. Но я помню его, такого светлого, приходящего к Ивану Васильевичу и о чём-то с ним беседующего на обширной площадке, из которой шли двери в разные кабинеты в нашей школе. Эта школа — бывшая Медведниковская[3] гимназия. В актовом зале — очень высоком — по углам гипсовые орлы с раскинутыми крыльями. Всё это видел и школьник Арнольд, и всё это я хорошо помню.

Арнольд побеждал в олимпиадах. Поколения в кружковой жизни (возрастные дистанции от учителя до ученика) были очень короткими. Арнольд, став студентом первого курса, вёл кружок, в котором я занимался. Одним из участников этого кружка был Павел Медведев, который стал студентом мехмата, аспирантом Шафаревича, кандидатом физико-математических наук, доктором экономических, а сейчас является политическим деятелем — с 1990-х годов он был членом Думы. А для меня Паша Медведев был руководителем кружка. Так что два коротеньких поколения кружковых отделяют меня от Арнольда. И хотя Арнольд формальным моим учителем был очень короткое время, но в математике он мой главный учитель. Моим учителем также был Евгений Михайлович Ландис —

[3] Её здание было построено в 1904 г. на деньги семьи Медведниковых по самым передовым технологиям. — *Прим. ред.*

у него я больше учился тому, как заботиться о своих учениках. Он был совершенно фантастически заботливый наставник.

Арнольд, будучи студентом первого курса, работал в просеминаре Витушкина. Витушкин многие годы своей жизни, поколение за поколением, учил талантливых студентов — устраивал просеминары для первокурсников.

Затем Арнольд работал у Дынкина. Евгений Борисович Дынкин был учеником сначала Гельфанда, потом Колмогорова. Дынкин, как и Арнольд, прославился чрезвычайно рано. В 20 лет студентом-четверокурсником он придумал знаменитые диаграммы Дынкина, которые сейчас являются одним из азбучных математических результатов. С Арнольдом на одном курсе учился другой выдающийся студент, Александр Александрович Кириллов. Дима Арнольд и Саша Кириллов оба работали у Дынкина какое-то время и даже сделали у него задачу, которая казалась нерешённой, но когда стали записывать, Арнольд нашёл что-то очень похожее уже опубликованное — и не стал этого писать.

На третьем курсе Арнольд сблизился с Колмогоровым. У Колмогорова был замысел атаковать 13-ю проблему Гильберта. Одна из ветвей этой проблемы — выразимость функций от большего числа переменных через функции от меньшего числа переменных. Сама проблема порождена вопросом: можно ли корни многочлена седьмой степени выразить через коэффициенты. Существенно то, что свести число коэффициентов меньше чем к трём нельзя. И вопрос: можно ли функцию от трёх переменных выразить с помощью арифметических и алгебраических действий, которые всегда вовлекают только два члена, над которыми производится операция... Этот вопрос Гильберт, в частности, свёл к вопросу, можно ли непрерывные функции большего числа переменных представить как суперпозиции функции меньшего числа переменных. Если бы ответ был отрицательный, то решилась бы и проблема про корни многочлена 7-й степени — их в принципе нельзя было бы выразить через коэффициенты. Но ответ оказался положительным, он был получен именно благодаря трудам Колмогорова и Арнольда.

Колмогоров, по-видимому, имел очень серьёзный задел, стратегические планы, как эту проблему следует атаковать. Но, когда атакуешь тяжёлую проблему, лучше об этом до времени не говорить. И Колмогоров организовал как-то очень скромно названный семинар по номографии — это такая прикладная ветвь математики. Я хотя и много общаюсь с семейством Хованских — отец Аскольда Георгиевича был одним из крупнейших специалистов по номографии, — но совсем немного могу сказать о том, что это за дисциплина. Колмогоров организовал семинар по номографии — поначалу там действительно были задачи, связанные с номографией, потом семинар всё увереннее повернул в сторону 13-й проблемы Гильберта. Сам Колмогоров доказал, что функции четырёх переменных можно представить в виде суперпозиции функций трёх переменных, и уехал, кажется, во Францию, оставив студентам список задач. Когда он вернулся, Арнольд показал ему все задачи решёнными. «Ну вот, Дима, вы и решили 13-ю проблему Гильберта», — сказал Колмогоров. Арнольд рассказывал — я думаю, что вы это слушали или читали, — что Колмогоров считал, что начинающему математику не под силу написать кондиционную научную работу. И, получив от начинающего математика, своего ученика, текст, переписывал его целиком, вместо того, чтобы объяснять: «определения пишутся не так, теоремы пишутся не так, определения не должны включаться в теоремы» и много разных других правил. Колмогоров ничего этого не говорил, а просто показывал, как это делается. У Арнольда была, по всей видимости заимствованная от Колмогорова, своя трактовка слова «интеллигентный». «Интеллигентный» ученик (надо понимать «если не дурак») после первого показа видел, как это надо делать. И второй раз Колмогоров уже не показывал. Если интеллигентный ученик — значит поймёт. Так или иначе, Арнольд написал заметку в ДАН о решении 13-й проблемы, но, как он говорил позже, «в опубликованном тексте нет ни одного моего слова — он весь переписан Колмогоровым».

Когда проблема Гильберта была решена, Колмогоров сказал Арнольду: «Дима, теперь держитесь подальше от моей тематики — вы самостоятельный человек». Я думаю, подтекст был такой: «вам больше не нужна никакая форма руководства, вы достигли высшего уровня и должны выбирать себе область сами».

Я никогда не интересовался, на какой кафедре был Арнольд — наверное, на кафедре теории вероятностей. Надо сказать, что когда Арнольд работал над 13-й проблемой Гильберта, Колмогоров был деканом. И он тогда ввёл индивидуальные планы для студентов. Это означало, что студент по решению научного руководителя и учебной части может не ходить на занятия вообще — только сдавать экзамены. И таким образом он предоставил Арнольду возможность неограниченно заниматься наукой.

Арнольд переключился на какие-то задачи, связанные с отображениями окружности. Сначала это были многозначные отображения с многими образами — так называемые соответствия. Но постепенно логика размышлений стала приводить его к тому же сюжету, о котором Колмогоров читал спецкурс, — к теории малых знаменателей. Ему было ясно, что первым приложением этой теории должна быть теорема о приведении диффеоморфизма окружности к повороту, что методы, придуманные Колмогоровым, там работают, — и его дипломная работа была первым прорывом после Данжуа.

Задача об отображениях окружности идёт от Пуанкаре. Пуанкаре первый понял, что это вообще содержательнейший предмет математических исследований, придумал число вращения и, так сказать, открыл мир диффеоморфизмов окружности. Это действительно целый мир, который и сейчас интенсивно развивается. Но начало этой теории было очень небыстрым. Пуанкаре сделал первый прорыв, затем поставил вопрос о приведении диффеоморфизма окружности к повороту. И чуть ли не через 50 лет (работа Пуанкаре — это 1880-е годы) — только в начале 1930-х годов его ученик Данжуа доказал теорему о приведении гладкого диффеоморфизма окружности к повороту — и при этом, надо сказать, придумал лемму об искажении, которая с таким успехом теперь используется.

После Данжуа был Арнольд. В 1961 году его статья была опубликована под названием «Малые знаменатели — 1». Потом были «МЗ-2», «МЗ-3». Стало ясно, что Арнольд снова тесно работает с Колмогоровым. Собственно говоря, я думаю, что вклад Колмогорова к этому времени был уже закончен. Колмогоров придумал свой совершенно гениальный подход к задачам классической механики. Опять нужно вернуться к Пуанкаре, который понял, что дифференциальные уравнения — это не только ветвь анализа, но и ветвь геометрии. В качестве основной задачи созданной им качественной теории дифференциальных уравнений Пуанкаре поставил вопрос: «Что происходит с вполне интегрируемой гамильтоновой системой при малом возмущении гамильтониана, когда она теряет интегрируемость?».

С начала двадцатого века были принадлежащие выдающимся математикам и физикам самые невероятные фантазии на тему возможного ответа. Предполагалось даже, что система будет эргодической. Колмогоров пытался угадать ответ, ему в начале 1950-х годов, когда он размышлял об этом, нужно было извлечь первые проблески света из абсолютной тьмы. Никто совершенно не представлял, на что будет похож ответ. Само наличие торов в интегрируемых системах было для Колмогорова неожиданностью, которую он нащупал, анализируя конкретные примеры. И понял, что эти торы — они сейчас называются колмогоровскими торами — выживают при малых возмущениях, и придумал, как это выживание можно было бы доказать.

Кто-то сравнительно недавно сказал мне, что Колмогоров говорил «я недостаточно сильный аналитик, чтобы провести доказательство подробно» — имея в виду доказательство теоремы Колмогорова о сохранении инвариантных торов. Но он целый год читал спецкурс об этом. И сейчас нет единого мнения, было у Колмогорова доказательство или не было. Но когда в 1962 году появилась статья Арнольда с доказательством теоремы Колмогорова, ни у кого не было сомнений в том, что Арнольд не записал, а дал впервые доказательство теоремы Колмогорова.

Сейчас эта теорема — именно та, которую доказывал Колмогоров, — имеет много опубликованных доказательств. Работу Арнольда очень тяжело читать, она очень формальная. Если Колмогоров говорил, что у него не хватает силы аналитика, то Арнольд проявил силу аналитика, написав крепко сработанный текст, длинный, прошитый связями, но трудно читаемый — с полным доказательством. Сейчас появились гораздо более простые доказательства той же самой теоремы. Но тогда это было что-то вроде первого восхождения на Эверест. Кстати, с Эверестом, я думаю, очень поучительная параллель. Существуют невероятно трудные решения научных проблем — за гранью возможностей предшественников, так же как восхождение на Эверест было в своём роде преодолением невозможности. А сейчас уже на Эвересте побывал и 70-летний восходитель, и слепец, и много женщин, и шерп Бабу Чири за 16 часов поднялся на вершину Эвереста с того места, с которого первовосходители шли вверх больше трёх дней — в общем, от Арнольда слышал я фразу Пуанкаре «Истина рождается парадоксом, а умирает тривиальностью» [4]. Вот это, по-видимому, та эволюция, благодаря которой только и можно узнавать всё больше и больше нового. Это происходит потому, что старые достижения прессуются, укладываются и становятся доступными для восприятия начинающих, а не остаются тайной для посвящённых.

Арнольд пошёл гораздо дальше Колмогорова. Он изучал и возмущения гамильтоновых систем с малым числом степеней свободы в пространстве с большим числом степеней свободы, и там устанавливал наличие торов. Он решил плоскую задачу трёх тел. И долгое время ему казалось, что он решил и пространственную задачу трёх тел. Но в 1990-е уже годы выяснилось, что в его решении был довольно существенный пробел, который потом был заполнен Эрманом и его учеником Фежосом. У меня нет ощущения, что это пробел в какой бы то ни было степени сравним по размерам с тем, что Арнольдом было достигнуто.

Иван Георгиевич Петровский, который в те годы был ректором МГУ, взял Арнольда и Кириллова профессорами на мехмат, как только они защитили докторские. С 1965 года оба они были профессорами. Надо сказать, что в то время процедура взятия на работу была непростой. Нужно было, чтобы кандидата одобрили профком и партком, и только после этого администрация могла писать приказ о его зачислении. Петровский, на мой взгляд, был человеком, который абсолютно сознательно и очень энергично противостоял системе. Если система, которая превратилась в почти бессознательно работающий механизм, старалась прихлопнуть или

[4] Арнольду повезло: весь цикл прошёл при его жизни!

даже срезать любую голову, которая высовывалась над общим уровнем, то Петровский каждого способного человека старался поставить на ноги. Петровский и Колмогоров очень сильно поддерживали друг друга, были единомышленниками. Колмогорову принадлежит фраза «надо прощать человеку его способности».

Петровский изобрёл способ, как людей, не имеющих больших общественных заслуг, и тем более с «небезупречной» национальной принадлежностью, брать работать в университет. Существовала процедура, которую Бейлинсон[5)] называл работорговлей, — я немножко при этом присутствовал, и у меня было то же ощущение, — процедура распределения. Ты — студент — получил бесплатное образование, скажи спасибо и отправляйся на два года работать туда, куда тебя пошлют. Такова была идеология этой системы. Она была не слишком жёсткой. То есть очень многие люди получали работу по своему дару или по своему вкусу. Но многим она — эта система — и попортила жизнь.

Такую же процедуру проходили выпускники аспирантуры. И партком мог легко не взять в университет и такого замечательного человека, как Арнольд. Во всяком случае, Петровский придумал обходной путь. Он прекращал дневную аспирантуру для аспиранта, переводил его в заочную аспирантуру, а самого аспиранта брал сотрудником в университет. Забавным образом, такая процедура, как нестандартная, не была обставлена стандартными препонами. Эту вещь Петровский мог сделать в обход парткома. Что он и делал. Я точно знаю, что этим трюком он воспользовался в отношении меня. Но он воспользовался им и в отношении многих совсем замечательных математиков старшего поколения — Арнольда, Синая, Кириллова, Винберга. Во всяком случае, Арнольд был взят сотрудником на факультет раньше, чем окончил аспирантуру. Петровский заведовал кафедрой дифференциальных уравнений и взял Арнольда к себе на кафедру. А очень скоро после того, как Арнольд защитил докторскую, он стал профессором.

Докторская диссертация Арнольда называлась «Малые знаменатели и проблемы устойчивости в классической и небесной механике». Вообще, вы помните фотографии в клубной части МГУ — сейчас они цветные. Тогда они висели чёрно-белые. Я очень хорошо помню фотографию, которая называлась «аспирант становится доктором». На этой фотографии был изображён Александр Александрович Кириллов, один из любимых и известнейших учеников Гельфанда, который решил одну из задач теории представлений, предложенную ему Гельфандом, и продвинулся так сильно,

[5)] А. А. Бейлинсон, один из самых знаменитых учеников Ю. И. Манина, сейчас профессор в университете Чикаго.

что ему решили дать докторскую степень. Кажется, кандидатские Арнольда и Кириллова защищались одновременно или очень близко друг к другу.

Когда Арнольд защищал свою кандидатскую — а это была 13-я проблема Гильберта — было предложение дать ему докторскую. Но решение 13-й проблемы было очень сильно поделено между Арнольдом и Колмогоровым. И Витушкин сказал, что работа, конечно, замечательная, и Колмогорову, конечно, за неё можно было бы дать докторскую степень, только непонятно, зачем она ему нужна. А вклад Арнольда не казался ему решающим. Дело осложнялось ещё тем, что после того, как Арнольд закончил решение 13-й проблемы, Колмогоров, развивая свои идеи, дал формально независимое от арнольдовского и совсем короткое решение 13-й проблемы. Действительно, это очень сильно разделённая работа между двумя исследователями. Короче, тут же был голос, что у Арнольда уже есть результаты на докторскую, и в 1963 году Арнольд докторскую уже защитил. Я на этой защите был, и на праздновании у Арнольда дома был. Был такой скромный праздник; может быть, даже на нынешних кандидатских защитах бывает не меньше народа, чем тогда было дома у Арнольда. Был, конечно, Колмогоров, и он сказал — у него был такой воркующий голос: «Я желаю, чтобы Владимир Игоревич доказывал побольше математических теорем, но не доказывал теорем о непотопляемости на море байдарок». Арнольд был всегда отчаянным человеком; физический риск доставлял ему удовольствие и был его потребностью. Я никогда не слышал от него пушкинских строк «Есть упоение в бою, и бездны мрачной на краю» — но у меня ощущение, что это были его строки.

Первый раз я увидел Арнольда на факультете, когда он принимал у меня, первокурсника, весенний экзамен во вторую сессию. У меня было ощущение, что я сдавал очень плохо. Но, по-видимому, моя цель состояла в том, чтобы давать ответы немедленно и в хорошей литературной форме, и до этой планки я не достал. Так или иначе, но совсем неожиданно для меня, довольно скоро, Арнольд сам взял со стола и принёс мне мою зачётку с пятёркой. Он был невероятно доброжелательным, и это очень ощущалось. И очень полон внутреннего света.

У Елены Николаевны[6)] на втором курсе — мы учились вместе — он вёл занятия по анализу. И она вспоминает — это мне тоже очень близко и как-то естественно, — что он приходил на занятия с отпадающей подошвой одного ботинка, а чтобы она не отпала совсем, ботинок был обвязан шнурком. Елена Николаевна рассказывала, что через год его выпустили во Францию, и вдруг он явился в вельветовом костюме. Это совсем с ним не вязалось. Вообще, этот стиль, который выражался поговоркой XIX века, а может,

[6)] Елена Николаевна Ильяшенко, жена рассказчика.

и более ранней, — «беден, да честен», он был очень присущ тому поколению. Как-то считалось само собой разумеющимся, что важно то, что внутри, а не то, что снаружи, и, в частности, проявлением этого принципа было пренебрежение к одежде.

Я помню, что в 1963 году на факультете был очень большой интерес к работе Петровского — Ландиса. Александр Михайлович Виноградов рассказывал её на семинаре у Арнольда. Он говорил, что существует такое французское понятие «feuilletage», которое можно переводить на русский как «листьяж», и рассказывал о понятиях, связанных с этими листьяжами, в работе Петровского — Ландиса. Арнольд очень живо реагировал — надо сказать, что «feuilletage», или foliation, теперь называется «слоением», но тогда термин ещё не устоялся. Послушав Виноградова раза два, Арнольд сказал: «Ну что нам слушать изложение, давайте обратимся к первоисточнику» — и позвал рассказывать Ландиса, которому тогда было 40 с небольшим. Ландис рассказывал, и в общем впечатление было, что вроде бы сюжет рассказан, но, по-видимому, никто, включая самого Арнольда, не мог бы сказать, что получено полное понимание. Это 16-я проблема Гильберта. Ну, дальше в работе Петровского — Ландиса нашлась ошибка, у меня это где-то написано.

Я на третьем курсе, страшно робея, попросил Арнольда быть моим научным руководителем — и был поражён тем, с какой лёгкостью он согласился. А на втором курсе я ходил на семинар Ландиса, где он в задачах излагал свою работу с Петровским по решению 16-й проблемы Гильберта. Я помню, как после какой-то лекции, вытирая руки, сполоснутые от мела, Арнольд шёл мне навстречу по коридору и спросил: «Юлик-Юлик, а что вы собираетесь сделать с Петровским — Ландисом?» Я ему ответил: «Ну, хочу найти доказательство попроще». Он сказал загадочную фразу: «Здесь хорошо бы применить теорию Галуа». Надо сказать, что Арнольд, по-видимому, не любил алгебраический вариант теории Галуа — и придумал свой, геометрический. Я не буду рассказывать, в чём он состоял (он был тесно связан с группой монодромии алгебраических функций и с неразрешимостью этой группы монодромии), но во всяком случае Арнольд хотел внести дух ветвления, дух монодромии в эту проблематику. Я понял, и эти слова были для меня в каком-то смысле импульсом в течение шести лет, по истечении которых я придумал, как надо применять абелевы интегралы к дифференциальным уравнениям, но это было уже позже.

Мне, наверное, не приходилось рассказывать на семинаре Арнольда до тех пор, пока я совсем не повзрослел. Я, заинтересованный работой Петровского — Ландиса, постепенно перешёл под руководство Ландиса, немножко неожиданно для себя и в общем с большим страхом взялся за абелевы интегралы, ощущая, что мимо пройти в общем-то нельзя, если следовать стратегии, которая Ландисом была намечена. И в 1969 году опубликовал две работы в «Математическом сборнике», им тогда заведовал Петровский, и статьи мои вышли чрезвычайно быстро. А в 1970 году Арнольд предложил мне рассказать на семинаре эти вещи. Надо сказать, что рассказывали тогда на семинарах страшно концентрированно, и за 90 минут я сумел изложить всё, что у меня было написано, по крайней мере из двух работ сделав выжимку. И до сих пор не забуду: когда я рассказывал короткое геометрическое рассуждение, в результате которого удавалось разбросать по плоскости примерно $n^2/2$ предельных циклов, Арнольд немного подался вперёд и сказал: «Здорово!». Я это «Здорово!» слышу до сих пор, и это одно из самых радостных моих воспоминаний.

В 1962–64 годах — я возвращаюсь сильно назад — Арнольд читал спецкурс по малым знаменателям. Я помню: в 1962 году, когда Арнольд первый раз рассказывал о результатах, по мехмату прошёл слух, что Арнольд решил задачу трёх тел, которую не мог решить Пуанкаре, — и это было очень впечатляюще. В 1964 году на заседании Московского математического общества Арнольд рассказывал про новое явление, называемое теперь диффузией Арнольда. Надо сказать, что очень долго в дифференциальных уравнениях существовал, по-видимому, один механизм устойчивости, геометрически связанный со спуском в яму, а аналитически — с функцией Ляпунова. Арнольд был первым, кто понял, что в системах классической механики есть новый вид устойчивости. Когда есть колмогоровские торы, а степеней свободы только две, то поверхность уровня энергии трёхмерна, и двумерные колмогоровские торы запирают решения — они образуют щели, из которых решения выйти не могут просто по топологическим причинам. Эта причина не работает, когда степеней свободы три, поскольку в этом случае изоэнергетическая поверхность пятимерна, а торы только трёхмерны и ничего не разделяют, — но во всяком случае Арнольд придумал этот свой любимый вид устойчивости и получил, в частности, новую теорему об устойчивости для особых точек гамильтоновых систем с двумя степенями свободы. Эти теоремы послужили гораздо позже источником совершенно неожиданных событий, о которых я расскажу.

Обычные лекции по дифференциальным уравнениям Арнольд начал читать только в 1968 году. На лекции по малым знаменателям ходили почти все сильнейшие студенты моего курса и ближайших курсов. Но понимать Арнольда было очень трудно. Он читал очень быстро. И Арнольд, и Манин читали очень быстро, и мне было трудно слушать обоих. Я из этих лекций вынес впечатление и убеждение, что читать надо по-другому. М. А. Шубин говорил мне, что каждую из еженедельных лекций Манина он прорабатывал последующие 3–4 дня, для того чтобы слушать и воспринимать следующую. Я с большим сожалением до сих пор об этом думаю — мне не хватало в студенческие годы терпения так работать над лекциями, — мне хотелось, к чему я привык в школе, понимать всё с ходу, на месте. И я решил по возможности стараться читать так, чтобы мои слушатели понимали всё на месте. Я этому учился всю жизнь, не знаю, в какой мере научился. Но во всяком случае, это вынесенная из юности такая линия. Забегая сильно вперёд скажу, что это и идея Независимого университета — там стараются читать так, чтобы было понятно на месте, — и это идёт совсем не от меня. Великих лекторов — ни Арнольда, ни Манина — не останавливал никто.

В 1965 году Арнольда неожиданно выпустили во Францию. Вообще, железный занавес был совершенно не шуткой. Сквозь него могли проникать очень немногие, а для большинства людей он был непроницаем. То, что Арнольда отпустили во Францию, это была большая удача. Его начали оформлять ещё как студента, но поехал он уже профессором. Однако бюрократическая машина неповоротлива, и во Франции его принимали по той программе, по которой его отправили. Научным руководителем его был Лере. И так вот Арнольд и был научно руководимым у Лере.

Вернёмся к виду устойчивости, который открыл Арнольд: двумерные торы перегораживают трёхмерные изоэнергетические поверхности. Трёхмерные торы пятимерных поверхностей уже не перегораживают. И возникает естественный вопрос: может ли даже для систем, близких к интегрируемым, решение, которое начинается где-то вблизи торов — уже нельзя сказать между торами, — пропутешествовать рядом с ними и уйти далеко-предалеко? Арнольд на эту тему написал единственную заметку в «Докладах» в 1964 году, но эта заметка послужила началом целой огромной новой ветви — «диффузии Арнольда», которая является сейчас, возможно, одной из самых популярных тем в классической механике. Основная проблема: «типична ли диффузия Арнольда?», и, кстати, участник этого же семинара Вадим Калошин сейчас один из ведущих в мире специалистов в этой области. У него есть масса примеров, которые движут наши знания в сторону положительного ответа на вопрос о типичности диффузии Арнольда[7].

Это был стиль Арнольда — если угодно, взгляд гения, удар молнии. Он открывает новую область, туда затем устремляются последователи, а Арнольд идёт дальше.

Статья про диффузию Арнольда — это были 4 странички. Очень содержательные, очень концентрированные, но на четырёх страничках вы

[7] В 2012 году типичность диффузии Арнольда была доказана Калошиным вместе с двумя его аспирантами.

много деталей не упишете. Мозер, который эту заметку реферировал, сказал, что если вписывать всё, пропущенное между строк, то получится страниц 20. Но для того, чтобы образовалась брешь, в которую хлынули последователи, этого было достаточно. И по диффузии Арнольда пишутся книги, и это один из знаменитых сюжетов. Арнольд предположил также, что, хотя диффузия возможна, она не может быть слишком быстрой. Он предложил эту задачу своему ученику Нехорошеву с небольшим наброском того, как это можно было делать: по его мнению, скорость диффузии должна быть — опять-таки при возмущении интегрируемой системы — обратна некоторой степени возмущающего параметра, а Нехорошев доказал, что она экспоненциально мала по возмущающему параметру. Для Арнольда это была неожиданность. Вообще, первая же серьёзная работа Нехорошева — его кандидатская диссертация — тоже породила целую теорию, которая так и называется «теория Нехорошева». К сожалению, это осталось главным достижением покойного уже теперь Николая Николаевича Нехорошева.

Надо сказать, что у Арнольда было невероятно много завистников. Тем более, что он привлекал, притягивал к себе людей со всех сторон. На него слетались математики, как бабочки на огонь. Каждый хотел его одобрения, ободрения, мнения о своих работах, и Арнольд с самой юности вынужден был поставить вокруг себя защиту, иначе бы его разорвали на части. Но в результате и завистников, и ненавистников у него было немало. Кроме того, он, конечно, абсолютно не вписывался в коммунистическую систему. Когда в 1968 году он начал читать курс дифференциальных уравнений и впервые в мехматский обиход вошли слова «диффеоморфизм», «фазовый поток», «симметрии» — в обиход во всяком случае обязательных курсов младшекурсников, — в деканате мнение было об этом курсе весьма скептическим, а студентам приходилось очень трудно. На учёном совете мехмата, кажется, секретарь парткома факультета сказал, что это не тот курс, который нам нужен.

Возвращаемся к Лере. Лере имел много замечательных работ и, в частности, работы по уравнению Навье — Стокса, по гидродинамике. Арнольд придерживался противоположного по отношению к Лере взгляда на природу турбулентности. И Арнольд является одним из авторов эвристической концепции того, что такое хаос в динамических системах вообще и турбулентность в частности. В то время он считал, что типичные динамические системы имеют гиперболические аттракторы. А на гиперболических аттракторах есть экспоненциальное разбегание траекторий и все симптомы хаоса. И эту концепцию он всячески проповедовал во Франции. Лере считал, что турбулентность происходит из-за того, что решения уравнений

Навье — Стокса с начальными условиями сколь угодно высокой гладкости в ходе эволюции теряют гладкость, становятся только непрерывными, и для них нарушается единственность. Вот это нарушение единственности является выражением турбулентности и невоспроизводимости экспериментов. Арнольд же считал, что уравнение Навье — Стокса ведёт себя как гладкая динамическая система, никакой гладкости решения не теряют, но зато выходят на гиперболический аттрактор, на котором происходит экспоненциальное разбегание траекторий, и это является моделью турбулентности. То, что типичная динамическая система хаотична, оттого что у неё достаточно сложный аттрактор, — это была пионерская идея, высказанная в середине 60-х годов Арнольдом. А кроме того, он тогда же, во Франции, понял, что решения уравнения идеальной жидкости, уравнения Эйлера — это просто геодезические на бесконечномерной группе диффеоморфизмов, и внёс ещё одну совершенно новую геометрическую точку зрения в задачу, которая раньше считалась чисто аналитической.

В 1970 году на конгрессе в Ницце друг детства Арнольда Сергей Петрович Новиков получил Филдсовскую медаль — первую Филдсовскую медаль российского математика. Филдсовскую медаль не дают человеку старше 40 лет, и 1974 год, когда Арнольду было 37, был последним годом, когда он мог получить медаль Филдса. Мы с напряжением ждали — получит или нет. Очень надеялись, что да. Но, когда конгресс прошёл и медали не дали, пронёсся слух, что глава советской математической делегации Понтрягин при обсуждении Филдсовской медали для Арнольда сказал, что «мне не известны работы такого математика». Позже говорили, что Понтрягин предупредил Филдсовский комитет, что советская делегация покинет конгресс, если Арнольду будет присуждена Филдсовская премия.

В 1968 году — я возвращаюсь на несколько лет назад — многие математики подписали письмо в защиту математика А. С. Есенина-Вольпина, который был помещён в психбольницу в качестве наказания за его правозащитную деятельность. После этого резко ухудшилось положение в университете и на мехмате в частности. У меня об этом написано[8] в тексте «„Чёрное 20-летие“ мехмата МГУ», который, наверное, многие из вас читали. Арнольд был один из тех, кто подписал это письмо, и все подписавшие попали в немилость. Вообще, конечно, можно только удивляться такой безрассудной государственной политике, когда государство предпочитает, чтобы гражданин его не имел престижной премии, если этот человек независим и неуправляем. Но с Арнольдом было именно так. Подобно

[8] `http://www.pravmir.ru/19385/`

Пушкину Арнольд был гениален и подобно Пушкину гоним. Его учеников не брали работать на мехмате. К нему шли лучшие студенты поколение за поколением. Их не брали работать на мехмат, просто потому, что они были не из той команды. У Арнольда было много замечательных учеников, некоторые достигли хорошего уровня, но многие абсолютно выдающегося. Белага, Леонтович, какое-то время был я, хотя Арнольд в список своих формальных учеников меня не включал, Хованский, Нехорошев, Пяртли, Смилка-Здравковска, Варченко, Гусейн-Заде, Закалюкин, позже В. Васильев, Казарян, Гивенталь, Ландо — всего, я думаю, человек около пятидесяти.

Только Нехорошева из тех, кого я перечислил, взяли на кафедру дифференциальных уравнений. Хованского не взяли даже в аспирантуру мехмата, просто из-за княжеского происхождения, его кандидатуру отвели на уровне парткома кафедры. Арнольд взял его в аспирантуру Стекловки, хотя сам там не работал в то время. Варченко взяли в лабораторный корпус, Гусейн-Заде взяли на географический факультет. Лучшие студенты мехмата шли к Арнольду и Ю. Манину, судьба учеников Манина была такой же: времена власти Петровского прошли, и на мехмат их не брали. Меня Петровский взял в 1968 году на мехмат, в 1969 году у него случился тяжёлый инфаркт — Тихонов настаивал на создании факультета прикладной математики, а Петровский говорил, что для обучения математиков достаточно мехмата. Как говорил Ландис, в конце концов «Тихонов получил факультет, а Петровский — инфаркт». Было непонятно, вернётся он к исполнению обязанностей ректора или нет. Он вернулся, но уже в 1968 году, как я о том писал, началось чёрное 20-летие мехмата, власть Петровского была резко подорвана. В 1973 году он умер.

Мы, на самом деле, люди очень уязвимые. Человек нашего круга может умереть после резкого разговора. Насколько я понимаю, у Петровского с его недугами это и произошло. Он, как говорили, подготовил доклад на совещание ректоров — очень, по-видимому, острый. Принёс его заведующему отделом науки и вузов ЦК КПСС С. П. Трапезникову. Доклад был отвергнут. Петровский вышел с приёма и умер у входа.

На мехмате наступили совсем другие времена. И больше никого из учеников Арнольда, кроме перечисленных, в университет не взяли — несмотря на то, что он вырастил совершенно золотую когорту математиков. И это послужило причиной того, что образовался Независимый московский университет. Потому что были люди, прекрасно обученные, были прекрасные математики, были прекрасные потенциальные преподаватели. Традиция создания научной школы шла непрерывно: Лузин, Колмогоров, Арнольд. А подавляющему большинству учеников Арнольда собственную школу создать в России не дали. Но этот заряд в них был, и как только наступили первые проблески свободы, они создали Независимый московский университет.

Арнольд говорил мне, что предвидел путч и конец перестройки, причём, предвидя путч, он вовсе не был уверен в его исходе. И, на случай несостоявшегося исхода, он заранее договорился о трёх годах подряд визитов на Запад. И 1991–1993 годы Арнольда в России не было вовсе. Вернувшись в Россию в 1994 году, он по моему предложению читал курс уравнений с частными производными в Независимом московском университете. Надо сказать — это тоже характеризует обстановку на мехмате, — что Арнольд в 1980-е годы предлагал прочесть курс уравнений с частными производными. «Ах, что Вы, Владимир Игоревич, — говорила наша начальница Ольга Арсеньевна Олейник [9], — это будет что-то совсем экзотическое?» — и не согласилась, чтобы такой курс был прочтён на мехмате.

В 1984 году против Арнольда была организована очень грамотная травля, которая привела к тяжёлому гипертоническому кризу у него. Я повторяю, что такие вещи делаются умелыми людьми и с серьёзными результатами. Это был очень сильный удар для него. И в 1986 году он ушёл с мехмата и перешёл в институт Стеклова. Он хотел остаться на мехмате на полставки, но мехматское начальство очень не торопилось это делать, и только после каких-то усилий снизу — всё-таки на мехмате были почитатели Арнольда, — поскольку всё-таки уж очень трудно было возразить против того, чтобы такого звёздного человека взять на полставки на мехмат, — его взяли. В 1994 году он ушёл с мехмата совсем.

Как говорил Гивенталь [10], приехавший из Америки на похороны Арнольда, расцвет школы Арнольда пришёлся на время, когда ему было лет 50, — тогда действительно в силу вошли те лучшие из его молодых учеников, которых я назвал. В 1987 году ему было 50.

Стиль общения Арнольда стал жёстче с возрастом. Может быть, он стал более непредсказуемым. У него, особенно в последние годы, была какая-то совершенно фантастическая производительность. Виталий Арнольд слышал от Владимира Игоревича следующий рассказ. Как-то Гельфанд предложил Арнольду написать книгу об уже обсуждавшемся между ними сюжете. Гельфанд тогда уже был в Америке, дело было, по-видимому, в 1990-е годы или в 2000-е, и Арнольд сказал: «Я послезавтра утром улетаю». Гельфанд сказал: «Ну у вас же ещё 40 часов впереди!» Арнольд сел и написал среднего размера книгу (сразу в TeX-е). Закончил Владимир

[9] О. А. Олейник — зав. кафедрой дифференциальных уравнений МГУ в 1973 — 2001 гг.

[10] А. Б. Гивенталь — один из самых ярких учеников Арнольда.

Игоревич этот рассказ со своей характерной чуть ироничной улыбкой фразой: «Не худшая из моих книг получилась».

Я помню фразу моего отца: «Гений — это прежде всего количество», — к Арнольду это имеет полное отношение. Я помню, как он попросил меня написать параграф в книгу «Дополнительные главы к теории обыкновенных дифференциальных уравнений». Это был параграф с отрывом вперёд по ходу книги — и я помню, что он приносил мне каждый день написанный новый текст, и у меня было впечатление приближающегося ко мне поезда. Мы писали с ним — как вы, может быть, знаете — совместный обзор по дифференциальным уравнениям для первого тома математической энциклопедии, это зелёная серия, и называется она «Фундаментальные направления», а на Западе — «Springer mathematical encyclopedia» — это жёлтая серия. Это было очень нелёгкое соавторство. Когда мы заканчивали работу над первым томом, вышло третье издание «Обыкновенных дифференциальных уравнений» Арнольда, и он подарил мне эту книгу с надписью «Дорогому терпеливому соавтору Юлику».

В 1965 году Арнольда выбирали в членкоры, и ему не хватило одного голоса. А затем Академия начала очень быстро набирать членов, замечательных своими общественными, а не математическими достижениями, и была пройдена отрицательная критическая масса — создался коллектив, который мог воспроизводиться только за счёт себе подобных. И было ощущение, что абсолютно безнадёжно, чтобы выбрали Арнольда в членкоры или Гельфанда в академики. Я очень горжусь, что мне пришёл в голову выход из этой ситуации. Какой выход вы бы предложили? — Разделить отделение математики на отделения чистой и прикладной математики. Это было сделано. Отрицательное равновесие, уже установившееся, нарушилось, и сразу избрали Арнольда в членкоры и Гельфанда в академики. Гельфанд, кстати сказать, был членкором почти 40 лет — с 1946 до 1984 года. Кто-то из академиков, говорят, после своего избрания сказал: «Долго же я засиделся в этом предбаннике». В 1984 году на факультете, как я уже сказал, была жестокая травля Арнольда. В то время как шло голосование на выборах в Академию, он, как это обычно делал, в одних плавках отправился бегать на лыжах. И когда он вернулся домой, ему сообщили, что голосование прошло благополучно и его избрали. Когда его избрали в членкоры, это прекратило травлю, просто одним этим фактом.

Ещё одну баечку расскажу. У Арнольда был очень сильный враг на мехмате — профессор нашей же кафедры Станислав Николаевич Кружков, — и он вместе с Брюно повёл атаку на работу Арнольда по теории КАМ. Он утверждал, что у Арнольда теорема об устойчивости особых точек гамильтоновой системы с двумя степенями свободы (конечно, надо налагать условия) не доказана. Как я уже сказал, Арнольд позволял себе небрежные тексты — это была самодозволенная небрежность гения, который знал, что по его следам пройдут люди более аккуратно. Теорема эта была написана небрежно. Брюно извлёк из текста некое законченное утверждение, привёл к нему контрпример, и вокруг этого раздувался и раскручивался скандал, и в 1989 году этот скандал возобновился. Я принял в этом небольшое участие. Мой коллега Станислав Николаевич расклеивал по факультету письма, в которых он писал о «мошенничестве» Арнольда. Я помню, как мы входили на кафедру с Татьяной Дмитриевной Вентцель — с моей очень уже пожилой сослуживицей, очень симпатичной, дочкой Е. С. Вентцель [11] — мы входили на кафедру, я увидел эту записку и смял её рукой. «Вас Кружков убьёт», — сказала Татьяна Дмитриевна. Но это отдельная история.

А слухи шли, что у Арнольда что-то неладно в его работах по теории КАМ. И мне друзья и доброжелатели Арнольда, ученики Колмогорова, говорили, что «нет дыма без огня — Юлик, разберитесь». И закончив писать доказательство теоремы конечности для предельных циклов, я решил попробовать разобраться. Я, конечно, не читал подробное доказательство, но я сделал маленькое открытие, о котором сейчас расскажу.

Во время полемики по поводу доказательства Арнольда детали формулировки и доказательства навязли в зубах. Много раз переговаривалось и перелопачивалось, в том ли порядке эти детали написаны. Если в том порядке написать, то будет верно, а если не в том, то неверно, и Арнольд написал не в том, а значит, не понимал доказательства. Напомню, что у Арнольда были три части «Малых знаменателей». Первая про окружность, вторая — теорема Колмогорова, когда число степеней свободы у возмущённого и невозмущённого уравнения совпадают, а третья — когда у невозмущённого уравнения меньше степеней свободы. Критикуемая теорема была в третьей части. Я понял, что этот признак устойчивости — двумерные торы, разделяющие трёхмерную поверхность, — был Арнольду очень дорог. Новый, совершенно непохожий на всё предыдущее признак. Было понятно, что Арнольд не должен был его пропустить в любом контексте, где он возникал. И что такая теорема об устойчивости должна была возникнуть как следствие теоремы Колмогорова. И тем самым надо её искать во второй части. Я взял в руки вторую часть и как приложение теоремы Колмогорова нашёл теорему об устойчивости волчка. Она была близнецом и двойником той теоремы, которая критиковалась: те же параллельные условия надо было сформулировать, те же самые рассуждения в доказательстве надо

[11] Елена Сергеевна Вентцель — математик, известна также как писательница И. Грекова.

было применить, но только там всё было написано в идеальном порядке. После этого спорить о том, понимал ли Арнольд теорему, о которой он писал в третьей части, было уже смешно. Я рассказал об этом исследовании тем друзьям Арнольда, которые говорили «нет дыма без огня», и они были вполне удовлетворены. Но сам Арнольд не захотел, чтобы я публиковал своё исследование в «Математических заметках». Вскоре после этого я поехал во Францию и решил, что я сам себе страсбургский профессор — правда, я был им всего два месяца, — что хочу, то и публикую, — и опубликовал это исследование в препринте Страсбургского университета.

Было у Арнольда в 1999 году очень страшное падение с велосипеда. Он прекрасно ездил на велосипеде — его физическая форма была фантастической. Во Франции он упал с велосипеда, и в Москве шли какие-то очень оптимистические слухи — как будто его поставили на искусственное дыхание и на другие аппараты, для того чтобы дать ему возможность легче оправиться, — но я как-то этим слухам не верил, потому что зря человека на аппараты не поставят. На пятый день его должны были вернуть на своё дыхание, его не вернули, и мне стало совсем страшно. А по Москве ходила фраза «опасности для жизни нет». Жена его, Эля, с которой я разговаривал по телефону, просила меня: «Юлик, молитесь». Через две недели его сняли с аппаратов, и он выжил. А в предисловии к книжечке «Истории давние и недавние», которая была издана несколько лет спустя, Арнольд рассказывал о том, как он лежал в больнице, — и там не без юмора он писал, что французские врачи, когда он приходил в себя, говорили ему: «Ну, ты несколько дней протянешь». А когда он вышел из больницы, ему говорили: «Ну, ничего, умрёшь не позже чем через полгода». Арнольд в своём предисловии к этой книжечке цитирует слова из справочника об опасных и смертельных дозах алкоголя, данные там довольно подробные, и не очень большие указываются дозы. Весь этот абзац заканчивается примечанием: к людям русской национальности эти данные не относятся. По-видимому, пишет Арнольд, западные данные о выживании после черепной травмы тоже не относятся к людям русской национальности. Во всяком случае, он все французские нормы выживания тогда, в 1999 году, перекрыл.

Когда праздновалось его 50-летие, за столом шёл разговор о рекордах разного рода. Мне приходилось, хотя и не часто, пробегать с ним на лыжах 60 километров, но это было почти за пределами моих возможностей. Сам Арнольд рассказывал, что бегал 100 километров, но это занимало у него до 13 часов. Он как-то раз совершенно неожиданно для меня показал мне возможность купания в ледяной воде. В 1978 году мы бежали на лыжах, нам встретилась открытая река. Арнольд спросил: «Будем купаться?». И я вдруг обнаружил, что никаких особых возражений у меня нет, хотя ничего, кроме регулярного холодного душа, я тогда не принимал. Вообще, традиция холодных купаний идёт, по-видимому, от Павла Сергеевича Александрова, который своего младшего друга Колмогорова в это дело втянул. Александров в своих воспоминаниях пишет, как они с Колмогоровым на спор пошли и выкупались под редкими снежинками, при этом изумив всё старшее поколение Лузитании — Лузина и своих сверстников, учеников Лузина. От Колмогорова это перешло к Арнольду, а от Арнольда — к его ученикам. На 50-летии Арнольда шла речь о рекордах, и его рекорд — минимальная температура воздуха при купании зимой — был минус 27 градусов.

Юлий Сергеевич Ильяшенко, НИУ ВШЭ
yulijs@gmail.com

О работах В. И. Арнольда по теории особенностей

С. М. Гусейн-Заде

В этом году исполняется 80 лет со дня рождения одного из крупнейших математиков XX века Владимира Игоревича Арнольда. Ему принадлежат работы в разных областях математики, и дать сколько-нибудь полный обзор его математической деятельности выше моих возможностей. Моя научная деятельность, примыкающая к работам Владимира Игоревича, концентрировалась вокруг теории особенностей. Данная статья — это эссе о некоторых моментах его работы в этой области.

Теория особенностей как отдельная дисциплина возникла в конце 60-х — начале 70-х годов прошлого века. Конечно, и до этого был получен ряд результатов, которые естественно составляют её часть. Сюда можно отнести, в частности, лемму Морса, классификацию Уитни общих отображений плоскости в плоскость... Однако систематическое изучение объектов теории особенностей началось с работ Рене Тома (René Thom) и получило наиболее значительное развитие в работах Арнольда. При этом, как мне кажется, идеология Арнольда существенно отличалась от идеологии его предшественников, в том числе и Тома.

Многие из них подходили к задачам теории особенностей как к чисто классификационным. Так, Том исходил из задачи описания перестроек фазовых портретов градиентных динамических систем в общих семействах систем, зависящих от не более чем четырёх параметров. (Выбор такого количества параметров связывался с тем, что рассматриваемая система могла зависеть от точки пространства и от времени.) Поэтому он изучал семейства функций (потенциалов) общего положения, зависящие от указанного количества параметров. С точки зрения строения фазовых портретов соответствующих динамических систем (по крайней мере с «локальной» точки зрения) наибольший интерес представляют окрестности критических точек потенциалов. В окрестности некритической точки потенциала градиентная динамическая система устроена очень просто. Именно, она может быть «выпрямлена». Это означает, что в некоторых локальных координатах $x_1, \ldots, x_n$ она имеет вид $dx_1/dt = 1$, $dx_i/dt = 0$ при $2 \leqslant i \leqslant n$. В этих координатах интегральные кривые системы образуют семейство параллельных прямых. Эта картина устойчива, т. е. не меняется при небольших изменениях потенциала (или при небольших изменениях параметров, от которых он зависит).

У индивидуального потенциала, т. е. для «семейства, зависящего от нуля параметров», все критические точки невырожденны. Это означает, что, в некоторых локальных координатах $x_1, \ldots, x_n$, в которых критическая точка имеет нулевые координаты, потенциал имеет вид $c + \sum_{i=1}^{n} \pm x_i^2$. (Невырожденные критические точки, в которых в этой формуле присутствуют только плюсы, являются положениями (устойчивого) равновесия.) Интегральные кривые соответствующей градиентной динамической системы могут быть легко описаны, и их картина качественно не меняется при небольших изменениях потенциала.

Ситуация несколько другая для семейств потенциалов, зависящих от одного параметра. Для общего значения параметра (т. е. для почти всех его значений) потенциал опять-таки имеет только невырожденные критические точки. При этих исключительных (бифуркационных) значениях параметра критические точки устроены по-другому. Можно показать, что для однопараметрического семейства общего положения все критические точки потенциала, соответствующего бифуркационному значению параметра, невырожденны, за исключением одной, а эта одна в некоторых локальных координатах имеет вид $c + x_1^3 + \sum_{i=2}^{n} \pm x_i^2$. При этом с одной стороны от исключительного значения параметра потенциал имеет около этой критической точки две невырожденные критические точки, которые сливаются при исключительном значении параметра и исчезают с другой стороны от исключительного значения (можно в определённом смысле сказать, что они уходят в комплексную область). Если одна из указанных двух критических точек была минимумом потенциала (и значит, устойчивым положением равновесия) и система находилась в нём, то при прохождении параметра через бифуркационное значение этот минимум исчезает и система должна перейти в другое устойчивое состояние с меньшей потенциальной энергией. Если система достаточно быстрая, такой переход осуществляется скачком. В соответствии с законом сохранения энергии в этом случае выделяется энергия (равная разности значений потенциала в двух положениях равновесия: до перехода и после). Можно сказать, что система испытывает быструю перестройку: происходит катастрофа.

Иногда на своих лекциях я демонстрирую этот эффект с помощью некоторой игрушки, которую я получил на какой-то выставке на ВДНХ. Игрушка представляет собой немного выпуклый металлический диск с наклеенным на него пластиковым кружочком, на котором написано (довольно мелкими буквами) название фирмы. На выставке работники фирмы что-то делали с таким диском, после чего клали его на стойку. Для того чтобы увидеть, что написано на диске, посетители выставки наклонялись над ним. В этот момент диск неожиданно подпрыгивал, пугая посетителей. Описанный эффект объясняется следующим образом. Центральную часть диска можно прогибать, нажимая на неё. Потенциальная энергия диска зависит от величины прогиба. При этом она зависит ещё от одного параметра: от температуры диска. При комнатной температуре потенциальная энергия как функция от величины прогиба имеет один минимум и система (диск) находится в соответствующем положении равновесия. При несколько повышенной температуре (ближе к температуре тела человека) имеются два локальных минимума потенциальной энергии как функции от величины прогиба (и ещё один локальный максимум). Перед тем как положить диск на стойку, работник фирмы нагревал его пальцами, в результате чего появлялось второе устойчивое положение равновесия. После этого прикладывая некоторое усилие, надавливая на середину диска и тем самым совершая работу, он переводил его во вновь появившееся положение равновесия и клал на стойку. Там диск охлаждался до комнатной температуры, новый локальный минимум потенциальной энергии сливался с локальным максимумом и исчезал. Система (диск) скачком переходила в единственное положение равновесия, существующее при комнатной температуре. При этом выделялась энергия, ранее затраченная для перевода системы в новое положение равновесия, и диск подпрыгивал.

Том изучил ситуацию для семейств потенциалов общего положения, зависящих от не более чем четырёх параметров, и обнаружил, что имеются ещё шесть возможных локальных ситуаций (с точностью до некоторого естественного отношения эквивалентности: см. ниже). Тем самым он утверждал, что в общих семействах градиентных динамических систем, зависящих от четырёх или менее параметров, имеется семь возможных типов перестроек («катастроф»). Теория, начинающаяся с этого утверждения, стала называться теорией катастроф. Она получила довольно большую популярность. В её популяризации одну из ключевых ролей сыграли общедоступные статьи и книги К. Зимана (Ch. Zeeman). Утверждалось, что теория катастроф — это универсальная теория, описывающая резкие (не плавные) изменения систем. При этом делались попытки применять её повсюду. Такого рода применение можно найти в брошюре Арнольда «Теория катастроф». Сам термин «теория катастроф» Владимиру Игоревичу не очень нравился. Тот факт, что он так назвал брошюру, видимо, объясняется популярностью названия в обществе.

Надо заметить, что как математическое утверждение описанный результат Тома неверен. Дело в том, что градиентная динамическая система определяется не только своим потенциалом (как функцией от фазовых переменных), но и римановой метрикой на фазовом пространстве. Поэтому, строго говоря, речь должна идти об изучении (классификации) не просто критических точек функций в семействах, а пар, состоящих из функции и метрики. Такая классификация существенно сложнее и имеет гораздо больше семи классов. Я не знаю, какова ситуация вокруг неё в настоящее время, но некоторое время тому назад было известно, что существует как минимум 27 классов эквивалентности, и не было известно, конечно ли их общее число.

Свои исследования по теории особенностей Арнольд тоже начинал с задачи, в которой естественной была бы классификация критических точек функций, встречающихся в семействах общего положения, зависящих от малого числа параметров. Речь шла о следующей задаче. Рассматривается «быстро осциллирующий интеграл» следующего вида:

$$\int\limits_{\mathbb{R}^n} \varphi(x_1, \ldots, x_n) e^{f(x_1, \ldots, x_n)/h} dx_1 \ldots dx_n,$$

где $\varphi(\overline{x})$ — функция с компактным носителем (нужная только для того, чтобы интеграл имел смысл; от неё ничего существенного не зависит), h — малая величина (в приложениях часто — «постоянная Планка»). Можно показать, что если на области интегрирования — носителе функции $\varphi(\overline{x})$ — фаза $f(\overline{x})$ не имеет критических точек, то при h, стремящемся к нулю, значение интеграла стремится к нулю быстрее любой степени h. Таким образом, нетривиальные степенные асимптотики связаны с критическими значениями функции f. Это утверждение называется принципом стационарной фазы. Итак, задача формально сводится к классификации критических точек, которые могут встречаться в общих семействах, зависящих от фиксированного числа параметров, и вычислению соответствующих показателей для них.

До коразмерности четыре классификация была проведена Томом. (Кстати, отмечу, что в отличие от задачи, рассматриваемой Томом, в рассматриваемой Арнольдом задаче действительно нужно классифицировать только критические точки функций, а не критические точки вместе с какими-то дополнительными структурами, например с римановой метрикой. В этом смысле математический результат Арнольда соответствует естественнонаучной задаче, бывшей для него мотивировкой.) Более-менее в то же время, когда задачей классификации критических точек функций заинтересовался Арнольд, эта классификация была продвинута немного дальше.

Поэтому изначально решаемая Арнольдом задача сводилась к вычислению показателей асимптотики интеграла для уже расклассифицированных особенностей, и на этом тема была бы закрыта. Подозреваю, что такая работа привлекла бы внимание нескольких специалистов по методу стационарной фазы и не была бы известна никому, кроме них. Однако Владимир Игоревич решил сделать что-то совершенно другое.

Прежде чем описать то, что он сделал, отмечу одну особенность подхода Арнольда к математическим задачам, которая представляется мне мистической, объяснения которой у меня нет, и я никогда не мог её воспроизвести. Моё описание отражает только то, что видел и понимал я, а в действительности Владимир Игоревич видел и понимал существенно больше (в чём я не сомневаюсь), и поэтому, возможно, ничего мистического в этом не было. Однако я воспринимал и воспринимаю некоторые его подходы как совершенно необъяснимые. Именно, несколько раз на моей памяти он задавал вопрос или формулировал гипотезу, для которых, как казалось мне, да и другим участникам семинара тоже, никакого основания не было. Поэтому вопрос и/или гипотеза выглядели абсолютно ничем не мотивированными, и было неясно, откуда они взялись и что в них толку. Однако позже неожиданно оказывалось, что эти вопросы и гипотезы приводили к глубоким и интересным результатам и проблемам.

В обсуждаемой задаче также проявилась эффективность такого подхода Владимира Игоревича. Он решил, что надо классифицировать критические точки функций не по коразмерности, а по другой характеристике. Классификация Тома давала конечный список особенностей (классов эквивалентности), поскольку она заходила не слишком далеко. Начиная с некоторого места классификация перестаёт быть дискретной: классы эквивалентности особенностей могут зависеть от непрерывных параметров — модулей. Например, в семействах функций от двух переменных, зависящих от семи параметров, могут встречаться критические точки, которые в некоторых локальных координатах x, y имеют вид $xy(x+y)(x-\lambda y)$ с каким-нибудь (определённым!) значением параметра λ. При этом указанные критические точки с различными значениями параметра λ, вообще говоря, не эквивалентны, т. е. не могут быть получены друг из друга заменой координат. Это следует из того известного факта, что четыре прямые на плоскости, пересекающиеся в одной точке, имеют инвариант (модуль) — двойное отношение их коэффициентов наклона. (Эти четыре прямые — компоненты множества нулей функции.) Для функций трёх переменных подобный эффект проявляется ещё раньше: в семействах, зависящих от шести параметров.

Владимир Игоревич решил классифицировать (с точностью до замен координат) критические точки функций по количеству параметров (модулей), требуемых для их описания (более точно — для описания всех близких к ним функций). При таком подходе начинать надо с функций, описание которых модулей не требует. Такие функции Арнольд назвал простыми или 0-модальными. Сама по себе классификация таких функций не слишком сложна. (Конечно, это — апостериори. Многие математические утверждения, будучи сформулированы и доказаны, вскоре выглядят несложными. Проблема состоит в том, чтобы найти правильную формулировку и первый раз доказать.) Ответ зависит (не сильно) от того, какие функции (и, соответственно, какие замены переменных) рассматриваются: комплексно-аналитические (голоморфные) или вещественные (бесконечно) дифференцируемые. Сформулируем его в чуть более простом случае — для голоморфных функций. (Для вещественных функций некоторые из указанных классов эквивалентности расщепляются на подклассы, различающиеся знаками перед мономами. Например, голоморфная функция $x^2 + y^2$ в вещественном случае представлена функциями $x^2 + y^2$, $x^2 - y^2$ и $-x^2 - y^2$.) Для двух переменных такие функции (классы эквивалентности относительно замен координат) образуют две бесконечные серии $x^{k+1} + y^2$ $(k \geqslant 2)$ и $x^2y + y^{k-1}$ $(k \geqslant 4)$, помимо которых имеются три исключительных особенности: $x^3 + y^4$, $x^3 + xy^3$ и $x^3 + y^5$. При фиксированном количестве переменных n (не менее двух) количество классов эквивалентности такое же и они получаются из указанных функций двух переменных добавлением суммы квадратов остальных $(n - 2)$ переменных. Вообще, классификации критических точек функций разного количества переменных тесно связаны между собой. Более точно, добавление к функции квадратов дополнительных переменных определяет отображение, а именно вложение, множества классов эквивалентности функций меньшего числа переменных в множество классов эквивалентности функций большего числа переменных. Это — следствие так называемой леммы Морса с параметрами.

После того как этот список был получен, оказалось, что он встречался уже не раз в других ипостасях. Например, для функций трёх переменных из этого списка множество нулей известно как множество особенностей дю Валя, т. е. особенностей поверхностей, получаемых из комплексной плоскости факторизацией по дискретным подгруппам группы $SU(2)$ унитарных матриц с определителем 1 (соответствующих правильным многогранникам). Они же дают список так называемых рациональных двойных особых точек поверхностей. Было известно соответствие этих особенностей простым алгебрам Ли, имеющим корни одинаковой длины. Это алгебры традиционно обозначаются A_k, D_k, E_6, E_7 и E_8. Те же имена были присвоены и перечисленным выше критическим точкам функций.

Позже были найдены ещё несколько классификаций, дающих тот же список. Комплексно-аналитической функции f, определённой в окрестности начала координат в $\mathbb{C}^n$, соответствует некоторое комплексное многообразие с краем — её локальное множество уровня. Именно, для достаточно маленького $\delta > 0$ существует такое $\varepsilon_0 > 0$, что для ненулевого комплексного числа ε, по модулю меньшего ε_0, множество

$$V_f = \{\bar{z} \in \mathbb{C}^n \colon \|\bar{z}\| \leqslant \delta, f(\bar{z}) = \varepsilon\}$$

является гладким многообразием с краем. Многообразие V_f, конечно, зависит от δ и от ε, но для достаточно маленьких δ и ε_0 все эти многообразия диффеоморфны друг другу, т. е. V_f как абстрактное гладкое многообразие размерности $2(n-1)$ с краем корректно определено. (Поэтому в обозначении обычно участвует только сама функция f.) Оно называется слоем Милнора функции f. (Откуда берётся термин «слой» — другая история.) Теорема того же Дж. Милнора утверждает, что если критическая точка f в начале координат изолирована (а только такие и встречаются в случае конечной коразмерности), слой Милнора V_f гомотопически эквивалентен букету сфер размерности $n-1$, т. е. может быть стянут на такой букет. Поэтому нетривиальные гомологии у этого многообразия имеются только в размерности $n-1$. Как для всякого (ориентированного) многообразия чётной размерности, на группе гомологий средней размерности имеется билинейная форма: форма пересечения. Она симметрична при нечётных n и кососимметрична при n чётных. Поскольку V_f — многообразие с краем, эта форма не обязана быть невырожденной. Так вот, если мы зададимся вопросом, для каких функций трёх переменных эта форма (а в этом случае она симметрична) отрицательно определена, мы получим тот же список A_k, D_k, E_6, E_7, E_8. Имеются и другие критерии, определяющие этот список. Я помню, что читал статью, в которой приводилось около двадцати классификаций, приводящих к тому же списку.

Удивительно, что до сих пор непонятны априорные причины, объясняющие, почему классификация простых функций совпадает с классификацией простых алгебр Ли, имеющих корни одинаковой длины, а также с классификацией функций трёх переменных, для которых указанная выше билинейная форма отрицательно определена. Также непонятна связь с некоторыми другими классификациями, дающими тот же ответ. Их совпадение получается просто независимой классификацией тех и других с последующим сравнением полученных списков. Это совпадение классификаций получало название ADE-загадки (или даже ADE-мистики) и ждёт своего объяснения.

Классификация простых ростков функций связана с классификацией не всех простых алгебр Ли, а только тех, которые имеют корни одинаковой длины. Владимир Игоревич нашёл классификации, приводящие к другим простым алгебрам Ли. Так, оказалось, что простым алгебрам Ли B_k, C_k и F_4 с корнями двух длин (1 и $\sqrt{2}$) отвечает классификация критических точек функций на многообразиях с краем.

Следующим шагом была классификация унимодальных критических точек функций, т. е. критических точек, для описания которых требуется один параметр (модуль). Примером таких функций являются указанные выше функции $xy(x+y)(x-\lambda y)$, для которых модулем является двойное отношение прямых — компонент множества нулей. Владимир Игоревич получил такую классификацию. Оказалось, что она включает три выделенных особенности, названные им параболическими (теперь они обычно называются простыми эллиптическими: simple elliptic), одну бесконечную трёхиндексную серию и ещё 14 особенностей, названных исключительными. (Параболические особенности встречались и раньше как первые особенности, которые «окружают» простые.) Возникла естественная проблема «придать смысл этой классификации», т. е. найти соответствующие ей известные математические объекты. Это оказалось очень трудной задачей, решённой Арнольдом только частично.

Владимир Игоревич составил огромную таблицу, в которую заносил всё, что было известно и становилось известно про эти 14 исключительных особенностей, и упорно искал в ней какие-то связи или намёки на них. В какой-то момент в таблице оказались тройки чисел, соответствующие этим исключительным особенностям и имеющие совершенно различную природу. Одна тройка чисел была определена И. Долгачёвым. Он заметил, что эти особенности соответствуют некоторым треугольникам на плоскости Лобачевского с углами π/α_1, π/α_2 и π/α_3, где α_1, α_2 и α_3 — натуральные числа. (Эти 14 треугольников имеют собственное независимое описание.) Тройку чисел $(\alpha_1, \alpha_2, \alpha_3)$ называют числами Долгачёва особенности.

С другой стороны, А. Габриэлов вычислял так называемые диаграммы Дынкина особенностей. Эти диаграммы описывают форму пересечения в группе двумерных гомологий слоя Милнора функции трёх переменных (а все унимодальные особенности можно считать функциями трёх переменных) в базисах специального вида. Эти базисы определены неоднозначно, и одной из целей Габриэлова было нахождение базисов, в которых диаграммы Дынкина выглядят проще всего: они содержат минимально возможное количество рёбер. Упрощение диаграмм требовало большой рутинной вычислительной работы (при отсутствии компьютеров) с плохо предсказуемым результатом: повезёт не повезёт, т. е. получишь «хорошую» диаграмму или не получишь. Да и хорошие могут быть, вообще говоря, разными. Габриэлову повезло (впрочем, везёт сильным): для 14 исключительных особенностей он получил похожие диаграммы. Они состояли из некоторого общего ядра, от которого отходили три «хвоста» длин γ_1, γ_2 и γ_3. Тройку чисел $(\gamma_1, \gamma_2, \gamma_3)$ называют числами Габриэлова особенности.

Происхождение этих чисел не имеет ничего общего, и довольно странно было бы сравнивать их друг с другом. Владимир Игоревич попробовал сделать это. (См. выше моё описание «немотивированных» действий Арнольда.) Как и следовало ожидать, для каждой исключительной особенности числа Долгачёва и числа Габриэлова по существу не имели ничего общего. Однако Арнольд заметил, что числа Долгачёва одной исключительной особенности совпадали с числами Габриэлова другой (иногда — той же) исключительной особенности, в то время как числа Долгачёва последней совпадали с числами Габриэлова первой. Тем самым на множестве исключительных особенностей возникала некоторая инволюция, меняющая между собой числа Долгачёва и Габриэлова.

Этот эффект Владимир Игоревич назвал странной двойственностью, которая в дальнейшем получила естественное имя странной двойственности Арнольда. (Для дальнейшего стоит упомянуть, что описанные события относятся к 1973–1975 гг.) Некоторое объяснение этой двойственности было дано Г. Пинкхамом (Henry Pinkham) в 1977 г. Оказалось, что числа Габриэлова особенности являются в некотором смысле числами Долгачёва на бесконечности для некоторой так называемой K3-поверхности, содержащей эту особенность, и наоборот.

Однако по большому счёту странная двойственность Арнольда оставалась некоторым курьёзом вплоть до конца века. В начале девяностых годов математики обнаружили, что физики изучают некоторые пары алгебраических многообразий с симметричными характеристиками. Такие многообразия назвали зеркально симметричными. Вначале происхождение таких многообразий (как и «доказательства» физиков того, что они имеют симметричные характеристики) выглядело для математиков некоторой мистикой. Однако позже соответствующие объекты и конструкции получили математическое описание. Как часто бывает, обнаружилось, что некоторые из них уже встречались в математике в другом виде. В частности, оказалось, что странная двойственность Арнольда — частный случай зеркальной симметрии. Сейчас признано, что странная двойственность Арнольда была первым в математике наблюдением эффекта зеркальной симметрии.

Каждый год (а часто и каждый семестр) семинар Арнольда начинался с занятия (иногда и двух), на котором он предлагал список открытых проблем. (Собрание этих проблем можно найти в книге: *Арнольд В. И.* «Задачи Арнольда», М.: Фазис, 2000. Многие из них не решены до сих пор.) Можно сказать, что в некотором смысле это были самые важные занятия семинара. На них участники семинара часто находили задачи для своей работы (иногда на многие годы вперёд).

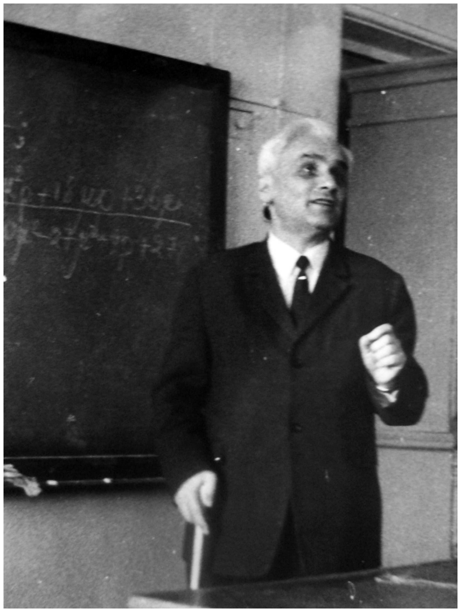
Классификация критических точек функций в большинстве случаев требует анализа мономов «младших степеней», присутствующих в разложении Тейлора. Формализацией набора мономов младших степеней функции нескольких переменных является так называемая диаграмма Ньютона функции. Для многочлена от нескольких переменных диаграмма Ньютона описывает набор «крайних» мономов, присутствующих в многочлене. В 1968 году Арнольд сформулировал задачу: «Какие топологические характеристики вещественного (комплексного) многочлена вычислимы по диаграмме Ньютона (и знакам коэффициентов)?» В тот момент на неё «решателей» не нашлось. В 1975 году Владимир Игоревич сформулировал аналогичную задачу в локальной постановке: для критических точек функций. В том же году выражение числа Милнора в терминах диаграммы Ньютона было найдено А. Г. Кушниренко и опубликовано им в журнале Inventiones Mathematicae в 1976 году. Значение этой работы трудно переоценить. Её влияние на дальнейшие исследования можно продемонстрировать тем фактом, что в «MathSciNet» (онлайн-версии американского реферативного журнала «Mathematical Reviews») на неё зарегистрировано 203 ссылки. (Далеко не все математики имеют столько ссылок на все свои работы вместе взятые.) За ней последовали работы А. Г. Хованского и Д. Н. Бернштейна, описывающие другие инварианты критических точек и многочленов. Была понята связь этих задач с торической алгебраической геометрией, в которую в этот момент вдохнули новую жизнь. Так задача Арнольда дала старт бурному развитию одной из областей математики. Подобное происходило и во многих других областях.

Уже семь лет Владимира Игоревича нет с нами. Его ученики явно ощущают нехватку его вдохновляющего и направляющего внимания.

Сабир Меджидович Гусейн-Заде, мехмат МГУ, НМУ
sabirg@list.ru

Залман Алтерович Скопец
(1917–1984)

В. М. Тихомиров



Залман Алтерович Скопец

Нам естественно здесь — в сборнике «Математическое просвещение» — вспоминать ушедших от нас преданных служителей математического просвещения (которому, собственно, и посвящён наш журнал).

Сто лет тому назад в самый первый день 1917 года родился Залман Алтерович Скопец, посвятивший математике, просвещению и обучению нашей науке всю свою жизнь.

Редакция сборника «Математическое просвещение» благодарит Е. И. Смирнова, профессора Ярославского педагогического университета им. К. Д. Ушинского, предоставившего фотографию З. А. Скопеца.

Залман Скопец родился в латвийском местечке Краслав, и первые четыре детских его года проходили в трагическую эпоху Первой мировой и Гражданской войн. Всё успокоилось в августе 1920 года, когда был подписан мирный договор между РСФСР и Латвией, по которому была признана независимость Латвийской Республики. Настал двадцатилетний период мирной жизни Латвии. В эти годы Скопец сначала учится в местной гимназии, а по окончании её он поступает в Рижский университет, который заканчивает, с присвоением магистерской степени по математике, в 1938 году. А через год начинается Вторая мировая война.

Волею судьбы в 1941 году Залман Алтерович попадает в Ярославль, где работает сначала в пригородной школе, а с 1942 года до конца своих дней в Ярославском педагогическом институте. В этом институте Скопец поднимается, преодолевая все педагогические ступени — лаборант, ассистент, доцент, профессор, заведующий кафедрой (он заведовал кафедрой элементарной математики, а потом созданной им кафедрой геометрии).

Любовью Скопеца была геометрия. Он много учится в первые свои ярославские годы. Ездит в Москву на семинары Н. Ф. Четверухина по начертательной геометрии и инженерной графике, посещает лекции П. К. Рашевского в МГУ, устанавливает тесные связи с кафедрой дифференциальной геометрии мехмата.

Все его работы посвящены геометрии. Он был убеждён в необходимости преподавания геометрии для развития логического мышления, пространственного воображения и эстетического воспитания учащихся. Геометрии посвящены и обе диссертации Залмана Алтеровича. З. А. Скопецем была проделана огромная творческая, методическая и общественная работа. Им написаны монографии «Задачи и теоремы по геометрии (планиметрия)» (с В. А. Жаровым) и «Векторные методы решения геометрических задач». Обе они были рассчитаны на школьников, студентов педвузов и учителей и пользовались большим успехом. Скопец принимает активнейшее участие во второй серии сборника «Математического просвещения» (он был предшественником нашего сборника), существовавшего краткий период в конце пятидесятых годов прошлого века. В шести вышедших сборниках им опубликовано четыре статьи.

Скопец создаёт плодотворно работающую школу в ЯГПИ, у него появляются ученики и продолжатели. Он содействует многим математикам, испытывающим затруднения с работой в семидесятые годы, ведёт большую общественную работу: создаёт «общественную» аспирантуру, в которой бесплатно учит учителей писать статьи, рассказывать на семинарах и т. п.; организует множество семинаров для студентов, аспирантов, межвузовские семинары по геометрии, знаменитые школы-семинары по алгебраической геометрии, в которых принимали участие В. И. Арнольд, А. А. Кириллов, С. П. Новиков, А. Н. Тюрин, И. Р. Шафаревич и другие.

Залман Алтерович Скопец остался в памяти знавших его людей как человек необыкновенной чуткости, заботливости и скромности, обладавший большой культурой и знаниями, которыми он щедро делился.

Более подробно о жизни и научных работах Залмана Алтеровича можно прочесть в статье Б. А. Розенфельда и Е. М. Элькиной «Памяти З. А. Скопеца» («Математическое просвещение», сер. 3, вып. 8, М.: МЦНМО, 2004).

P. S. Импульсом для написания статьи было моё многолетнее общение с дочерью Скопеца Ревеккой Залмановной Гушель. Ревекка Залмановна была замечательным человеком и бескорыстным энтузиастом просвещения. Она принимала активнейшее участие во многих мероприятиях, проводимых в Ярославле, поддерживала постоянную связь со мной, А. М. Абрамовым, А. Н. Ширяевым, С. С. Демидовым и другими по поводу разных аспектов истории математики и математического просвещения. 11 февраля она скончалась. Очень многие её замыслы, к сожалению, остались нереализованными. Хочу выразить здесь свою скорбь по поводу утраты прекрасного человека и преданного служителя нашей профессии.

Владимир Михайлович Тихомиров, мехмат МГУ
`vmtikh@googlemail.com`

Виталий Дмитриевич Арнольд (1968–2017)

А. В. Хачатурян

Виталий Дмитриевич Арнольд

Для московского математического сообщества 2017 год начался с трагедии — 4 января в автомобильной катастрофе погиб Виталий Дмитриевич Арнольд, учитель, просветитель, неутомимый организатор множества образовательных проектов, одна из самых ярких фигур в московском математическом образовании за последнюю четверть века.

«Погиб математик Виталий Арнольд» — с таким заголовком на сайте Polit.ru появилось первое сообщение о его смерти. Конечно, Виталий не был математиком в привычном понимании этого слова. Он не создал математической теории, не написал учебников или монографий, не доказал ни одной новой теоремы. Но вся его яркая и, увы, такая короткая жизнь была посвящена математике, математическому просвещению. Без него многие книги не были бы написаны, многие теоремы не были бы доказаны и многие люди не стали бы теми, кем они стали. Можно только удивляться тому, как много он успел сделать для нас.

Виталий Дмитриевич Арнольд родился в 1968 году в Москве в интеллигентной семье с интересной и богатой историей. Он впоследствии изучал историю своей семьи, собирал и бережно хранил семейный архив. Его многочисленные старшие родственники, среди которых были и представители точных наук, и гуманитарии, оказали на него большое влияние. Среди них мы, конечно, первым вспоминаем его дядю, выдающегося математика Владимира Игоревича Арнольда, но также можно назвать и деда, известного математика и педагога Игоря Владимировича Арнольда, мысли и книги которого оказали на его детей и внуков большое влияние. Ещё подростком Виталий потерял мать, и его в основном воспитывала бабушка, Марианна Михайловна, мамина мама, филолог и замечательный учитель русского языка и литературы, много лет проработавшая в известной московской школе № 710. Среди родственников Виталия Дмитриевича известные советские физики Л. И. и С. Л. Мандельштамы, писатель и путешественник Б. С. Житков и многие другие. История семьи сливалась с историей страны, и большой московский дом, где рос Виталий, был полон книг, фотографий, встреч, рассказов и воспоминаний.

Мальчику, живущему в такой семье, трудно было не увлечься физикой и математикой, и Виталий закончил в 1985 году математический класс знаменитой московской 57-й школы. По случайному совпадению его учителем математики тоже был Арнольд, но только это было его имя: научным руководителем их класса был прекрасный математик и талантливый педагог Арнольд Яковлевич Блох. В школьные годы организаторский талант Виталия уже вовсю давал о себе знать, ну а реализован он был в духе того времени — Виталий Арнольд был до самого своего выпуска бессменным комсоргом школы.

Поступить после школы в МГУ или Физтех «инвалиду пятой группы», как тогда горько шутили, было нереально, и Виталий учился в МИСиСе, закончил его по специальности «теоретическая физика». Правда, ещё два года между первым и вторым курсом Виталий провёл вдалеке от учебных аудиторий — его призвали в армию и отправили в одну из ракетных частей в Казахстане.

В 1989 году Борис Петрович Гейдман пригласил Виталия Арнольда работать в школу № 43, в один из первых созданных там математических классов. Школа со временем стала гимназией № 1543, а Виталий Дмитриевич Арнольд — ярким, харизматичным учителем информатики, создателем и хозяином одного из первых в Москве школьных компьютерных классов. В кабинете информатики проходили не только уроки — он был своеобразным клубом. Открытый до позднего вечера учителям, ученикам, выпускникам, компьютерный класс был местом душевного общения за чаем, местом, куда всегда можно было прийти за помощью, советом, критикой. Щедрость, с которой Виталий Дмитриевич делился знаниями со всеми, поражала. Поражало, как много он знал и умел — в самых разных, казалось бы далёких друг от друга областях.

Он затевал самые разные образовательные проекты. Вечерами по пятницам из упомянутого компьютерного класса слышались звуки гитар — это занимались со своими учениками известные исполнители авторской песни Виктор и Татьяна Кузнецовы. С лёгкой руки Виталия гитарная школа Кузнецовых работает в гимназии вот уже более двадцати лет. В середине 90-х годов Виталий Дмитриевич организует в городе Пущино Зимнюю школу гимназии 1543 — один из первых зимних образовательных лагерей. Его увлекает идея свободного образовательного пространства в обстановке академгородка, возможность для школьников напрямую общаться с известными учёными, например с Симоном Эльевичем Шнолем, беседа которого с ребятами была гвоздём программы каждой Зимней школы. Зимние школы в Пущино просуществовали до начала нулевых годов, были постепенно вытеснены другими подобными проектами и свёрнуты. А ещё Виталий Дмитриевич водил детей в туристические походы, ездил с ними по городам Русского Севера, и ребятам оставалось только удивляться тому, что их учитель информатики, оказывается, так хорошо знает русскую историю и так захватывающе обо всём рассказывает.

Но гимназия 1543 была только частью жизни.

В 90-е годы математическое образование в стране и в том числе в Москве начинает значительно перестраиваться. В руководство образованием приходят новые люди. Архаичные образовательные структуры «советского типа» уступают место более современным. И Виталий Дмитриевич Арнольд стал активно заниматься многими образовательными проектами и начинаниями. Его деятельность концентрируется в основном вокруг созданного в 90-е годы МЦНМО — Московского центра непрерывного математического образования, директором которого стал известный энтузиаст математического образования Иван Валериевич Ященко, а его заместителем — Виталий Дмитриевич. Заместитель — это вообще было типичным «амплуа» Виталия (замдиректора гимназии 1543, замдиректора МЦНМО, зампред оргкомитета Московской математической олимпиады...), — он любил быть формально на «второй роли», находясь при этом в самой гуще событий и активно влияя на всё происходящее.

«Под крылом» МЦНМО постепенно собирались энтузиасты математического просвещения, от учёных с мировым именем до первокурсников, туда стекались многие проекты. Существующий с начала 1990-х Независимый московский университет стал структурным подразделением МЦНМО, в уютном доме во Власьевском переулке проходили математические кружки, там обосновалось издательство математической литературы, там расположились «штабы» многих математических олимпиад — Московской олимпиады, Турнира Ломоносова, Турнира городов и других.

Школьные математические олимпиады были предметом особой заботы Виталия Дмитриевича. Математические олимпиады в нашей стране имеют богатую историю, они сами и отношение к ним общества неоднократно менялись. Для Виталия Дмитриевича было чрезвычайно важным сохранить основные традиции олимпиад — открытость, доступность каждому школьнику и их математическую ценность, которая выражалась и в качестве самих задач, и в том, что олимпиада была площадкой прямого общения ведущих математиков со школьниками, была для ребят открытой дверью в науку. Виталия раздражало как превращение олимпиадного движения в «спорт высоких достижений» и элитарный клуб избранных, так и нарастающая в последнее время бюрократизация олимпиадного движения, стремление поставить во главу угла не школьника и Математику, а строчку в каком-нибудь рейтинге или отчёте.

Много лет Виталий Арнольд был заместителем председателя оргкомитета Московской математической олимпиады, одной из старейших в стране, при нём и в значительной степени его усилиями она приняла свой современный вид. Он добился, чтобы она вышла из системы всероссийских олимпиад и осталась открытой. Много сил уделял отбору и подготовке задач, заботился о том, чтобы они были яркими, оригинальными, математически содержательными и по возможности посильными не только олимпиадным профессионалам, но и просто способным и любознательным старшеклассникам. Около двадцати лет Виталий Арнольд пестовал московскую математическую олимпиаду для самых маленьких участников — «Математический праздник». Именно из его рук получали первые в своей жизни дипломы за математические победы шестиклассники и пятиклассники. Кстати, и сборники задач Московской математической олимпиады — как ежегодные тоненькие брошюры, так и солидные сборники задач за много лет — готовились с его деятельным и непосредственным участием.

Появившиеся в последние годы многочисленные конъюнктурные, «вузовские» олимпиады отражали попытку многих вузов влиять на отбор абитуриентов в условиях господства довольно несовершенного и по форме и по содержанию Единого госэкзамена. Однако многие из этих олимпиад быстро стали довольно непрозрачными и подверженными коррупции. Виталий Дмитриевич понимал, что нужна новая олимпиада, не привязанная к конкретному вузу, но решающая задачу отбора математически грамотных абитуриентов для широкого круга институтов, прежде всего инженерно-технической направленности. И так, во многом его усилиями, под эгидой Российского союза ректоров стала проводиться ОММО — Объединённая межвузовская математическая олимпиада.

А ещё Виталий Дмитриевич Арнольд был бессменным руководителем команды Москвы на заключительном туре Всероссийской олимпиады школьников по математике. Эту свою миссию он ценил очень высоко, пропускал ради поездки на «Всеросс» даже одну учебную неделю в школе, чего не делал никогда ни по какому иному поводу. Многие поколения финалистов олимпиады помнят его заботу, его интересные рассказы, игры и разговоры «за жизнь», его умение всегда быть рядом, понимать и помогать.

Математические олимпиады иногда непредсказуемо вмешиваются в жизнь человека. На традиционной встрече после проведения Математического праздника 1999 года Виталий обратил внимание на Наташу Кулакову, одну из студенток МГУ, помогавших проводить олимпиаду. Встреча имела далеко идущие последствия — у Наташи и Виталика завязался роман, и вскоре они поженились. Потом родилась Женечка, а следом за ней её младший брат Михаил, или Мика, как его ласково звали домашние. Семья регулярно бывала в Соединённых Штатах, где работал Наташин отец, математик, профессор НМУ А. Г. Кулаков, но жить и растить детей хотела в России, в Москве, с которой Виталия так много связывало. Их гостеприимный дом всегда был открыт для друзей. В день рождения Виталия дверь просто не закрывалась. «Звонить надо не по телефону, а в дверь», — всегда шутил он по этому поводу. Устраивались и большие детские праздники. А летом Виталий всегда находил время поехать с детьми хотя бы на одну смену в семейный лагерь. Устраивал для детей конкурсы, играл с ними в спектаклях, пел песни и читал сказки. Многие летние фотографии Виталия похожи друг на друга — улыбающийся Виталий, а на его плечах кто-нибудь из счастливых детей.

Летом проходит и самый, наверное, значительный и необычный проект Виталия Арнольда — его знаменитая «Дубна», Летняя школа «Современная математика» (ЛШСМ). Возможно, всё началось с места — живописного дома отдыха Ратмино недалеко от Дубны, в красивом сосновом бору у впадения Дубны в Волгу. Там летом 2000 года проходила организованная И. Ф. Шарыгиным и В. М. Тихомировым представительная педагогическая конференция «Математика и общество. Математическое образование на рубеже веков», в которой Виталий принимал активное участие. Под конец конференции Н. Н. Константинов предложил ежегодно проводить в этих красивых местах, недалеко от знаменитого наукограда встречу известных математиков с талантливой молодёжью. ЛШСМ впервые прошла в 2001 году, и сразу — большой успех. Уникальность этой школы была не только в «звёздном» составе преподавателей, среди которых были крупные российские и зарубежные математики, но и в необычном составе слушателей школы — ими могли стать как старшие школьники (закончившие 10 или 11 класс), так и младшекурсники (студенты первого или второго курса). Летних школ для студентов или для школьников в то время было немало, но в ЛШСМ удалось их впервые объединить, стереть границу между ними. Нередко бывало, что читавший курс академик интересовался, на каком курсе учится удививший его своими успехами юноша, и выяснял, что это десятиклассник. За шестнадцать лет школы в Дубне многие слушатели стали первоклассными математиками, стали преподавателями Школы, нередко специально приезжая в Дубну из-за границы. Ну а Виталий Арнольд руководил всей работой школы — от приглашения преподавателей и составления программ до решения самых мелких бытовых вопросов. Он был везде — на лекциях и семинарах, на посиделках за чаем и на волейбольной площадке. Он неизменно открывал работу Школы, рассказывая о её истории. Постоянно ездил на велосипеде по территории базы, всюду успевая, во всё вникая, уделяя каждому внимание. Став со временем почти полноправным хозяином «Ратмино», Виталий стал проводить там и другие мероприятия — Летнюю лингвистическую школу и финал Всероссийской олимпиады по геометрии имени И. Ф. Шарыгина.

И об ещё одной стороне его жизни не сказать нельзя — об интернет-проектах Виталия Арнольда. Их было множество, а объединяли их две основные цели: сохранить знание и сделать доступным для всех.

Виталий Арнольд создал, наполнял и поддерживал сайт `www.mccme.ru` — страницу МЦНМО, один из лучших и самых информативных русскоязычных сайтов в области математического образования. Самого беглого взгляда достаточно, чтобы понять основную идею — строгий, аскетичный дизайн, никаких украшений, максимум информативности и удобство навигации. Принципы и стиль этого сайта он поддерживал и в других сайтах схожей направленности, к которым имел отношение: сайте `math.ru`, сайте Центра педагогического мастерства, сайте `olimpiada.ru` и других. В первую очередь Виталий Дмитриевич стремился сохранить в сетевом, цифровом виде книги, журналы, публикации, аудио- и видеозаписи, которые считал важными и ценными для будущих поколений, в этом он видел свою просветительскую миссию. Он собрал библиотеку `ilib.mccme.ru`, оцифровав лучшие книги, по которым учился сам и по которым учились его учителя, книги, составляющие золотой фонд учебной математической литературы и зачастую ставшие недоступными в бумажном виде (включая «Арифметику» Магницкого, первый русский учебник математики). Арнольд переделал и расширил архив kvant.ras.ru номеров журнала «Квант», приложил руку к созданию сайта книг издательства «Mathesis», выпускавшего научно-популярную литературу в конце XIX – начале XX века, занимался оцифровкой номеров первого в России физико-математического журнала «В. О. Ф. Э. М.», сделал архив номеров журнала «Природа». Виталий Дмитриевич выкладывал на сайт МЦНМО электронную версию сборника «Математическое просвещение», а в его 19-м выпуске опубликовал статью «„Сетевая жизнь“ научно-популярных журналов». Он собирал и публиковал статьи и выступления геометра И. Ф. Шарыгина, математика и инженера А. Н. Крылова, собирал всё, что касается трудов историка В. М. Глинки, делал видеозаписи знаменитых публичных лекций лингвиста А. А. Зализняка о только что найденных берестяных грамотах, оцифровал почти все виниловые диски песен Булата Окуджавы, публиковал труды и воспоминания государственного деятеля С. Ю. Витте... Уже по этому, далеко не полному списку видны и широта интересов Виталия Дмитриевича, и та огромная просветительская работа, которая была им проделана.

Наш век короток, и, к сожалению, нас навсегда покидают замечательные люди. И конечно, Виталий Дмитриевич, хранитель и собиратель, заботился о том, чтобы память о них сохранялась надолго. Его стараниями на сайте МЦНМО была сделана страница воспоминаний об ушедших. Большинство некрологов тоже написал сам Виталик.

С бесконечной болью мы вписали на эту печальную страницу и его имя.

Александр Вячеславович Хачатурян, Московская гимназия на Юго-Западе № 1543

lupus-sapiens@yandex.ru

Геометрия: классика и современность

Теорема о семи окружностях и другие новые теоремы*

С. Дж. А. Ивлин, Г. Б. Мани-Каутс, Дж. А. Тиррелл

Вышедшая в 1974 г. книга C. J. A. Evelin, G. B. Money-Coutts, J. A. Tyrrell «The seven circles theorem and other new theorems» состоит из трёх независимых параграфов. Ниже публикуется перевод второго параграфа. Сохранены авторские обозначения.

§ 2. Обобщения теорем Паскаля и Брианшона

Теорема Паскаля утверждает, что три точки пересечения противоположных сторон шестиугольника, вписанного в конику, лежат на одной прямой (которая называется *прямой Паскаля* шестиугольника). Двойственная ей теорема Брианшона утверждает, что три главные диагонали описанного около коники шестиугольника пересекаются в одной точке (которая называется *точкой Брианшона*)[1]. Эти теоремы иллюстрируются на рис. 1 и рис. 2 (в первом случае шестиугольник, как обычно делается, изображён самопересекающимся ради компактности рисунка).

Эти теоремы не только интересны сами по себе, но и важны как отправной пункт различных путей геометрического исследования, и цель этого параграфа — проследить некоторые из них. Раздел 2.1 содержит новую

* Перевод А. А. Заславского.

[1] В дальнейшем термины «вписанный» и «описанный» означают соответственно «вписанный в конику» и «описанный около коники». Многоугольники могут быть самопересекающимися. — *Прим. перев.*

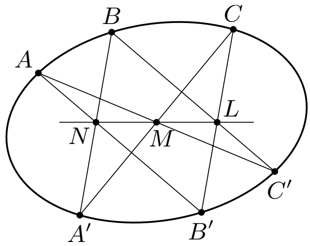


Рис. 1. *К теореме Паскаля*

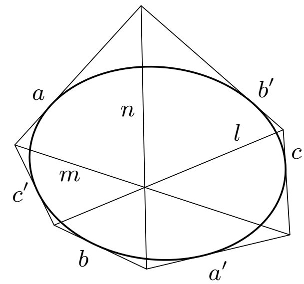


Рис. 2. *К теореме Брианшона*

(как мы полагаем) теорему о прямых Паскаля семи шестиугольников, образованных вершинами вписанного семиугольника. В разделах 2.2–2.4 доказывается ряд теорем, обобщающих теорему Паскаля (подобно тому как сама эта теорема обобщает более простую теорему Паппа). Наконец, в разделе 2.5 доказывается элегантная теорема о вписанном восьмиугольнике.

2.1. Теорема о семиугольнике

Теорема Паскаля относится к шести точкам, лежащим на конике в фиксированном циклическом порядке. В нашей первой теореме рассматриваются шестиугольники, порождённые семью точками коники с фиксированным циклическим порядком.

Теорема о семиугольнике. *Пусть H — вписанный семиугольник (циклический порядок вершин фиксирован). Тогда прямые Паскаля семи шестиугольников, получающихся удалением одной из вершин H (при сохранении циклического порядка остальных вершин), образуют описанный семиугольник I. При этом точки Брианшона семи шестиугольников, получающихся удалением одной из сторон I (с сохранением циклического порядка остальных), совпадают с вершинами исходного семиугольника H.*

Доказательство. Обозначим последовательные вершины H через 1, 2, 3, 4, 5, 6, 7 (см. рис. 3) и введём следующие точки:

$$B = (45, 71), \quad C = (56, 12), \quad D = (67, 23), \quad E = (71, 34),$$
$$F = (12, 45), \quad X = (23, 56), \quad Y = (34, 67), \quad A = (FX, BY),$$

где $B = (45, 71)$ означает, что B является точкой пересечения прямых, соединяющих 4 с 5 и 7 с 1, и т. д.

Пусть теперь $H_1, \ldots, H_7$ — шестиугольники, полученные из H удалением вершин $1, \ldots, 7$ соответственно, а $p_1, \ldots, p_7$ — их прямые Паскаля. Легко видеть, что $p_1 = XY$, $p_2 = YB$, $p_3 = BC$, $p_4 = CD$, $p_5 = DE$, $p_6 = EF$, $p_7 = FX$.

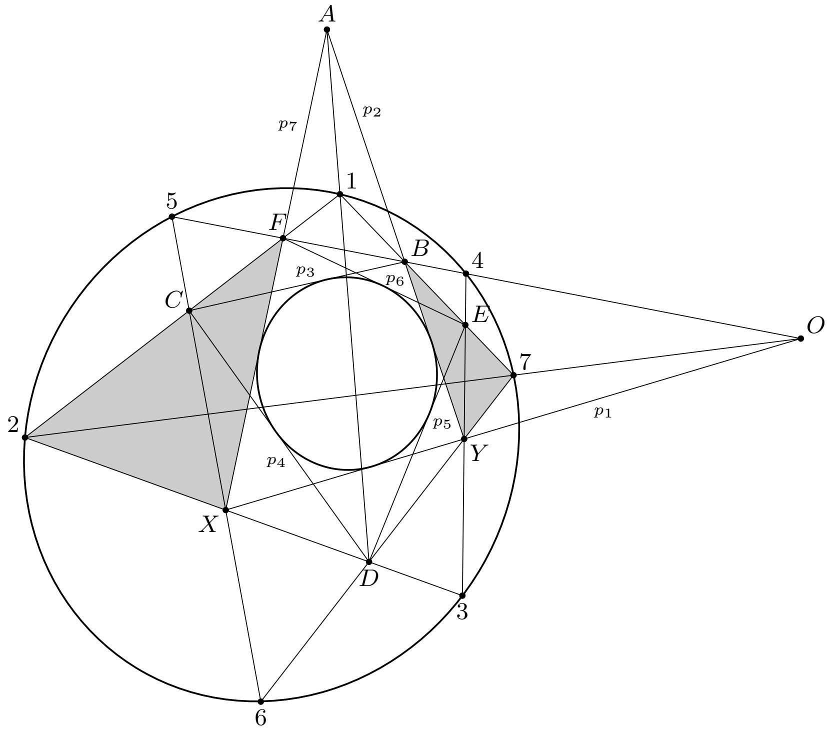


Рис. 3. К теореме о семиугольнике

Рассмотрев шестиугольник H_1, убеждаемся, что третьей точкой на его прямой Паскаля будет $O = (45, 72)$. Следовательно, прямые 45, 72 и XY пересекаются в одной точке, или, так как B и F лежат на прямой 45, треугольники $2FX$ и $7BY$ перспективны (относительно точки O на рис. 3). По теореме Дезарга точки пересечения соответственных сторон этих треугольников $A = (FX, BY)$, $D = (2X, 7Y)$ и $1 = (2F, 7B)$ лежат на одной прямой, т. е. прямая AD проходит через точку $1 = (BE, CF)$. По обратной теореме Брианшона шестиугольник $ABCDEF$, образованный прямыми $p_2, \ldots, p_7$, описан около коники, а его точка Брианшона совпадает с 1. Таким образом, прямая p_2 касается (единственной) коники k, касающейся прямых $p_3, p_4, \ldots, p_7$.

Аналогично прямые $p_1, p_3, \ldots, p_7$ образуют описанный шестиугольник, точка Брианшона которого совпадает с 2, и т. д. В частности, прямая p_1 также касается коники k, т. е. эта коника касается всех прямых $p_1, p_2, \ldots, p_7$, откуда следует теорема. $\square$

Интересно было бы исследовать фигуру, определяемую семью точками коники, рассмотренными во всех 360 возможных циклических порядках.

Эта фигура содержит 420 прямых Паскаля и 360 коник, причём каждая прямая касается шести коник, а каждая коника — семи прямых. Однако здесь мы не станем этим заниматься. (Аналогичное исследование фигуры из 60 прямых Паскаля, задаваемых шестью точками коники, содержится, например, в [1, Appendix].)

2.2. Теорема о трёх кониках

Из многих проективных теорем о кониках можно получать интересные частные случаи, заменяя конику парой прямых. Например, теорема Паппа получается таким образом из теоремы Паскаля. Здесь мы докажем теорему, для которой сама теорема Паскаля является таким частным случаем.

Теорема о трёх кониках. *Если три коники проходят через две данные точки, то три прямые, соединяющие пары остальных общих точек*[2] *каждых двух коник, пересекаются в одной точке* (рис. 4).

Отметим, что если две из трёх коник заменить парами прямых, теорема о трёх кониках переходит в теорему Паскаля[3], а если все три коники вырождены — в теорему Паппа. Если вырождена ровно одна коника, то получается ещё один частный случай, промежуточный между общей теоремой и теоремой Паскаля.

Доказательство. Пусть (см. рис. 4) коники S_1, S_2, S_3 проходят через точки I, J; S_1 и S_2 пересекаются также в точках P_3, Q_3; S_1 и S_3 — в точках P_2, Q_2; S_2 и S_3 — в точках P_1, Q_1. Докажем, что прямые P_1Q_1, P_2Q_2 и P_3Q_3 пересекаются в одной точке.

Пусть коника S_1 задана уравнением $S_1(x, y) = 0$, а прямые IJ, P_2Q_2 и P_3Q_3 — уравнениями $L = 0$, $L_2 = 0$ и $L_3 = 0$ соответственно. Тогда коника S_2 принадлежит пучку коник, содержащему S_1 и пару прямых IJ, P_3Q_3, и, значит, её уравнение имеет вид $S_1 + \lambda LL_3 = 0$, где λ — некоторая постоянная. Аналогично уравнение коники S_3 имеет вид $S_1 + \mu LL_2 = 0$.

Тогда уравнение

$$(S_1 - \lambda LL_3) - (S_1 - \mu LL_2) = L(\lambda L_3 - \mu L_2) = 0$$

задаёт конику из пучка, содержащего S_2 и S_3, т. е. проходящую через точки I, J, P_1, Q_1. Эта коника распадается на две прямые, заданные урав-

---

[2] Возможно, мнимых. — *Прим. перев.*

[3] Пусть в конику вписан шестиугольник 123456. Применим теорему о трёх кониках к данной конике, паре прямых (12, 56) и паре прямых (23, 45). Все они проходят через точки 2, 5. Получим, что в одной точке пересекаются прямые 16, 34 и прямая, соединяющая точки пересечения 12 с 34 и 23 с 56. Это и есть теорема Паскаля применительно к 123456. — *Прим. перев.*

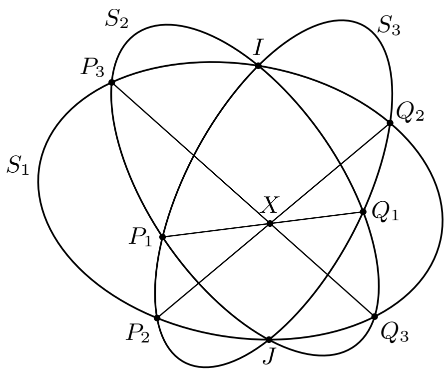


Рис. 4. К теореме о трёх кониках

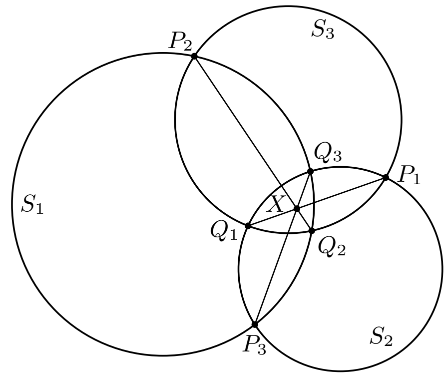


Рис. 5. Пересечение радикальных осей

нениями $L = 0$ и $\mu L_3 - \lambda L_2 = 0$. Так как первое из этих уравнений задаёт прямую IJ, второе должно задавать прямую P_1Q_1. Таким образом, уравнение прямой P_1Q_1 является линейной комбинацией уравнений прямых P_2Q_2 и P_3Q_3, т. е. эти три прямые проходят через одну точку, что и требуется. □

Менее элементарное доказательство можно получить с помощью известной *теоремы о девяти точках*, утверждающей, что *любая кубика, проходящая через восемь из девяти точек пересечения двух данных кубик, проходит и через девятую общую точку*. Действительно, применим эту теорему к двум вырожденным кубикам, одна из которых состоит из коники S_2 и прямой P_2Q_2, а другая — из S_3 и P_3Q_3. Мы видим, что кубика, состоящая из S_1 и прямой P_1Q_1, проходит через восемь их общих точек (а именно I, J, P_1, Q_1, P_2, Q_2, P_3, Q_3). Следовательно, она проходит и через точку пересечения прямых P_2Q_2 и P_3Q_3. Так как эта точка не может лежать на S_1, она лежит на прямой P_1Q_1. Таким образом, P_1Q_1, P_2Q_2 и P_3Q_3 проходят через эту точку (на рис. 4 она обозначена через X).

Нелишне отметить, что частными случаями теоремы о трёх кониках являются два известных факта евклидовой геометрии.

1) Если I, J — круговые точки (мнимые точки пересечения бесконечно удалённой прямой с некоторой окружностью), получаем известный факт (см. рис. 5): *попарные радикальные оси трёх окружностей пересекаются в одной точке*[4].

2) Если круговыми являются точки P_3, Q_3, получаем следующее утверждение.

[4] Отсюда можно получить ещё одно доказательство теоремы о трёх кониках, см. [2, с. 89]. — *Прим. перев.*

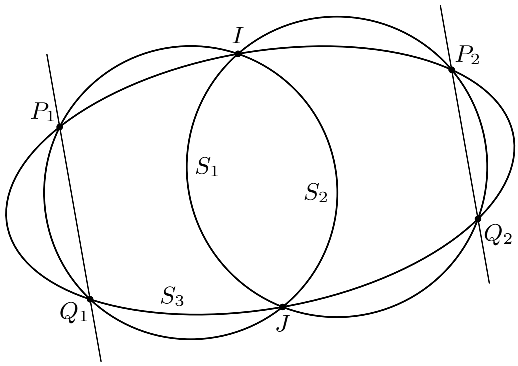


Рис. 6. Частный случай теоремы о трёх кониках

Если окружности S_1, S_2 пересекаются в точках I, J, а проходящая через эти точки коника S_3 пересекает S_1 также в точках P_2, Q_2 и S_2 — в точках P_1, Q_1, то прямые P_1Q_1 и P_2Q_2 параллельны (рис. 6).

Справедливо также следующее обращение теоремы о трёх кониках.

Пусть коники S_2, S_3 пересекаются в точках I, J, P_1, Q_1, а P_2Q_2 и P_3Q_3 — хорды коник S_3 и S_2 соответственно, пересекающиеся на прямой P_1Q_1. Тогда точки I, J, P_2, Q_2, P_3, Q_3 лежат на одной конике.

Доказательство получается стандартным рассуждением от противного. Представляет интерес также двойственная теорема.

Если три коники имеют две общие касательные, то точки пересечения пар оставшихся общих касательных лежат на одной прямой (рис. 7).

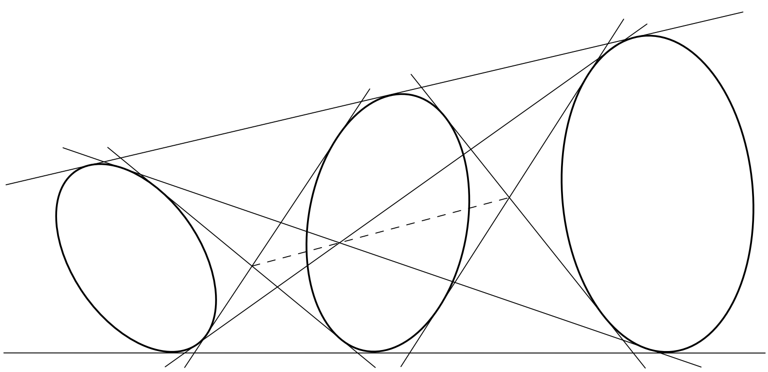


Рис. 7. К двойственной теореме о трёх кониках

Любопытное применение теоремы о трёх кониках показано на рис. 8. Пусть восемь точек $1, \ldots, 8$ лежат на конике S, а четыре коники a, b,

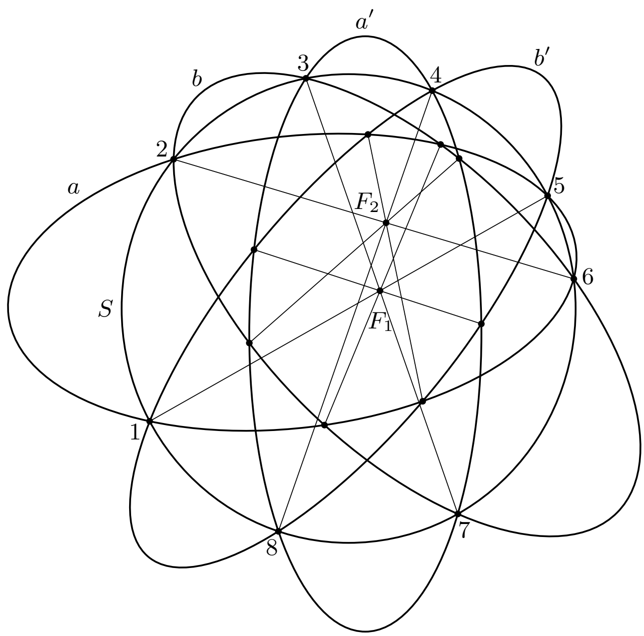


Рис. 8. Применение теоремы о трёх кониках

a', b' проходят через 1256, 2367, 3478 и 4581 соответственно. Тогда, применяя теорему к тройкам коник (S, a, b), (S, b, a'), (S, a', b') и (S, b', a), получаем две четвёрки конкурентных прямых (на рис. 8 пересекающихся в точках F_1 и F_2 соответственно).

2.3. Теорема о двойном касании

В предыдущем разделе было показано, что, если три коники проходят через две общие точки, то их «другие» общие хорды пересекаются в одной точке. Тем не менее, если у трёх коник есть три общие хорды, проходящие через одну точку, то эти коники заведомо не обязаны иметь две общие точки. Однако справедливо следующее утверждение.

Теорема о двойном касании. *Пусть коники S_1, S_2, S_3 таковы, что через некоторую точку X, не лежащую ни на одной из них, можно провести общую хорду каждой пары коник (причём эти три хорды попарно различны). Тогда существует коника ω, касающаяся каждой из данных коник в двух точках.*

Доказательство. Так как три хорды различны и пересекаются в одной точке, мы можем считать, что содержащие их прямые заданы уравнениями $L_1 = 0$, $L_2 = 0$, $L_3 = 0$, причём

$$L_1 + L_2 + L_3 = 0. \tag{1}$$

Пусть $L_1 = 0$ — уравнение прямой, содержащей общую хорду коник S_2 и S_3, и т. д. Если коника S_i задана уравнением $S_i = 0$, то $S_2 = S_3 + \lambda L_1 M_1$, где $M_1 = 0$ — уравнение общей хорды коник S_2 и S_3, противоположной хорде с уравнением $L_1 = 0$ (т. е. проходящей через две точки их пересечения, не лежащие на прямой $L_1 = 0$). Без ограничения общности можно положить $\lambda = 1$ (поскольку уравнение $M_1 = 0$ можно умножить на соответствующий коэффициент). Таким образом,

$$S_2 - S_3 = L_1 M_1. \tag{2}$$

Аналогично

$$S_3 - S_1 = L_2 M_2, \tag{3}$$

где $M_2 = 0$ — уравнение общей хорды коник S_1 и S_3, противоположной хорде с уравнением $L_1 = 0$.

Исключая S_3 из (2) и (3), получаем

$$S_1 - S_2 = -L_1 M_1 - L_2 M_2. \tag{4}$$

Так как точка X лежит на прямых $L_1 = 0$ и $L_2 = 0$, её координаты удовлетворяют уравнению $S_1 - S_2 = 0$. Но в пучке коник, содержащем S_1 и S_2, лишь одна коника проходит через X, а поскольку X лежит на общей хорде S_1 и S_2, эта коника распадается на прямую $L_3 = 0$ и противоположную общую хорду S_1 и S_2, заданную, скажем, уравнением $M_3 = 0$. Следовательно,

$$S_1 - S_2 = L_3 M_3. \tag{5}$$

Теперь из (4) и (5) получаем равенство

$$L_1 M_1 + L_2 M_2 + L_3 M_3 = 0,$$

которое с учётом (1) приводится к виду

$$L_2(M_2 - M_3) = L_1(M_3 - M_1).$$

Так как прямые $L_1 = 0$ и $L_2 = 0$ не параллельны, отсюда следует, что

$$M_2 - M_3 = kL_1 \tag{6}$$

и

$$M_3 - M_1 = kL_2 \tag{7}$$

для некоторой константы k, что вместе с (1) влечёт

$$M_1 - M_2 = kL_3. \tag{8}$$

Уравнение (6) означает, что прямые $L_1 = 0$, $M_2 = 0$ и $M_3 = 0$ пересекаются в одной точке. Заметим, что они содержат попарные общие хорды данных коник — не те три, которые предполагались конкурентными изначально. Аналогично интерпретируются равенства (7) и (8). Таким образом, мы попутно доказали следующее утверждение.

Если у каждых двух из трёх коник можно выбрать общую хорду так, что эти хорды пересекутся в одной точке, то это можно сделать четырьмя различными способами.

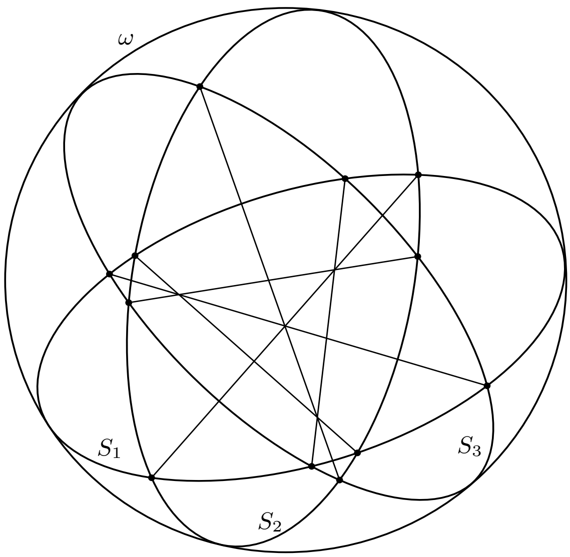


Рис. 9. *К теореме о двойном касании и обратной к ней*

Возвращаясь к доказательству теоремы о двойном касании, заметим, что верно соотношение

$$\begin{aligned}4kS_1 + (M_2 + M_3 - M_1)^2 = 4kS_2 + (M_3 + M_1 - M_2)^2 = \\ = 4kS_3 + (M_1 + M_2 - M_3)^2.\end{aligned} \tag{9}$$

Действительно, например, первое равенство можно переписать в виде

$$4k(S_1 - S_2) = 4M_3(M_1 - M_2),$$

что является очевидным следствием из (5) и (8); аналогично доказывается второе равенство. Следовательно, обозначив любое из трёх равных выражений в (9) через Ω, мы получим, что коника с уравнением $\Omega = 0$ дважды касается каждой из коник S_1, S_2, S_3 (прямые, соединяющие точки касания, заданы уравнениями $M_2 + M_3 - M_1 = 0$, $M_3 + M_1 - M_2 = 0$, $M_1 + M_2 - M_3 = 0$ соответственно). Теорема доказана. □

Обратное утверждение доказывается гораздо проще.

Если существует коника ω, дважды касающаяся каждой из коник S_1, S_2, S_3, то общие точки каждых двух из этих трёх коник можно разбить на пары так, что три пары прямых, соединяющих соответствующие точки, являются тремя парами противоположных сторон полного четырёхвершинника.

Конечно, пару противоположных общих хорд коник, скажем S_1 и S_2, можно выбрать тремя способами, и необходимо определить «правильный» способ. Как это сделать — видно из приведённого ниже доказательства.

Доказательство. Пусть коника ω задана уравнением $\Omega = 0$. Тогда уравнения коник S_1, S_2, S_3 можно задать в виде

$$\Omega + N_1^2 = 0, \quad \Omega + N_2^2 = 0, \quad \Omega + N_3^2 = 0,$$

где $N_1 = 0$, $N_2 = 0$, $N_3 = 0$ — уравнения прямых, соединяющих точки касания ω соответственно с S_1, S_2, S_3 [5]. Тогда уравнение

$$(\Omega + N_1^2) - (\Omega + N_2^2) = (N_1 + N_2)(N_1 - N_2) = 0$$

будет уравнением вырожденной коники из пучка, определяемого кониками S_1 и S_2. Эта коника распадается на пару прямых с уравнениями

$$N_1 + N_2 = 0, \quad N_1 - N_2 = 0, \tag{10}$$

содержащих две противоположные общие хорды коник S_1 и S_2. Из вида этих уравнений следует, что *эти общие хорды проходят через точку пересечения общих касательных коники ω соответственно с S_2 и S_3* (*в действительности они гармонически разделяют касательные хорды*); *это свойство определяет «правильный» способ выбора пары общих хорд.* Аналогично получаем, что общие хорды S_1 и S_3 задаются уравнениями

$$N_1 + N_3 = 0, \quad N_1 - N_3 = 0, \tag{11}$$

а общие хорды S_2 и S_3 — уравнениями

$$N_2 + N_3 = 0, \quad N_2 - N_3 = 0. \tag{12}$$

Легко видеть, что шесть прямых, заданных уравнениями (10)–(12), являются сторонами и диагоналями четырёхугольника, вершины которого заданы

[5] См. (9) и последующий абзац. — *Прим. перев.*

соотношениями $N_1 = \pm N_2 = \pm N_3$ для всех возможных выборов знаков. Это доказывает обратную теорему о двойном касании. $\square$

Рисунок 9 иллюстрирует теорему о двойном касании и обратную к ней. Отметим, что если коника ω вырождается в пару точек, обратная теорема превращается в доказанную в предыдущем параграфе теорему о трёх кониках. Нетрудно также сформулировать двойственные теоремы.

Если для каждых двух из трёх коник можно выбрать пару общих касательных так, чтобы три точки пересечения касательных из каждой пары были различны и лежали на одной прямой (*не касающейся данных коник*), *то*

(а) *это можно сделать четырьмя различными способами*;

(б) *существует четвёртая коника, дважды касающаяся каждой из данных.*

Верно и обратное: *если существует коника, дважды касающаяся трёх данных, то общие касательные каждых двух данных коник образуют две пары, точки пересечения которых являются вершинами полного четырёхсторонника.*

Рисунок 10 иллюстрирует частный случай этой теоремы, когда коника, дважды касающаяся трёх данных, вырождается в пару круговых точек;

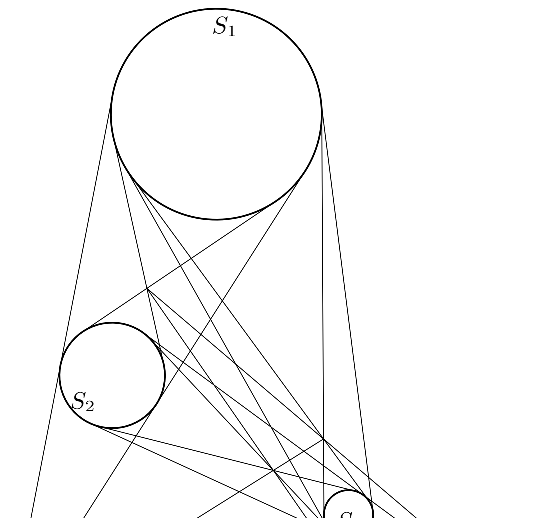


Рис. 10. Частный случай двойственной теоремы о двойном касании

при этом шесть центров гомотетии трёх окружностей являются вершинами полного четырёхсторонника.

2.4. Теорема о четырёх кониках

Полезно посмотреть на конфигурацию, описанную в предыдущем параграфе, с другой стороны. В условиях теоремы о двойном касании справедливо ещё одно тождество:

$$kS_1 + M_2M_3 = kS_2 + M_3M_1 = kS_3 + M_1M_2. \tag{1}$$

Действительно, заметим, что первое равенство эквивалентно равенству $k(S_1 - S_2) = M_3(M_1 - M_2)$, которое легко следует из уравнений (5) и (8) в разделе 2.3; второе равенство доказывается аналогично. Обозначая каждое из равных выражений в (1) через S_0, получаем из $S_0 \equiv kS_1 + M_2M_3$, что коника $S_0 = 0$ проходит через точки пересечения S_1 с прямыми $M_2 = 0$ и $M_3 = 0$. Другие два выражения для S_0 приводят к аналогичным результатам. Таким образом, доказана следующая теорема.

Теорема. *Если три коники удовлетворяют условию теоремы о двойном касании, т. е. шесть из их двенадцати точек пересечения лежат на трёх пересекающихся в одной точке прямых, то остальные шесть точек пересечения лежат на одной конике.*

Таким образом, двенадцать общих точек делятся на две шестёрки: одна образует шестиугольник Брианшона, другая — шестиугольник Паскаля. Более того, как было показано при доказательстве теоремы о двойном касании, такое деление можно осуществить четырьмя различными способами. Легко доказать и обратное утверждение.

Теорема о четырёх кониках. *Если для каждых двух из трёх коник S_1, S_2, S_3 можно выбрать две общие точки так, чтобы шесть выбранных точек лежали на конике S_0, то прямые, соединяющие оставшиеся точки пересечения каждой пары коник, проходят через одну точку.*

Доказательство. Будем использовать обозначения рис. 11. Пусть коника S_0 задана уравнением $S_0 = 0$, а прямые P_1Q_1, P_2Q_2, P_3Q_3 — уравнениями $L_1 = 0$, $L_2 = 0$, $L_3 = 0$ соответственно. Тогда S_1 принадлежит пучку, заданному коникой S_0 и парой прямых P_2Q_2, P_3Q_3, поэтому её уравнение имеет вид $S_1 \equiv \lambda_1 S_0 + L_2L_3 = 0$ где λ_1 — некоторая постоянная. Аналогично S_2 и S_3 имеют уравнения $S_2 \equiv \lambda_2 S_0 + L_3L_1 = 0$ и $S_3 \equiv \lambda_3 S_0 + L_1L_2 = 0$ с соответствующими постоянными λ_2, λ_3. Тогда

$$\lambda_2 S_3 - \lambda_3 S_2 = L_1(\lambda_2 L_2 - \lambda_3 L_3),$$

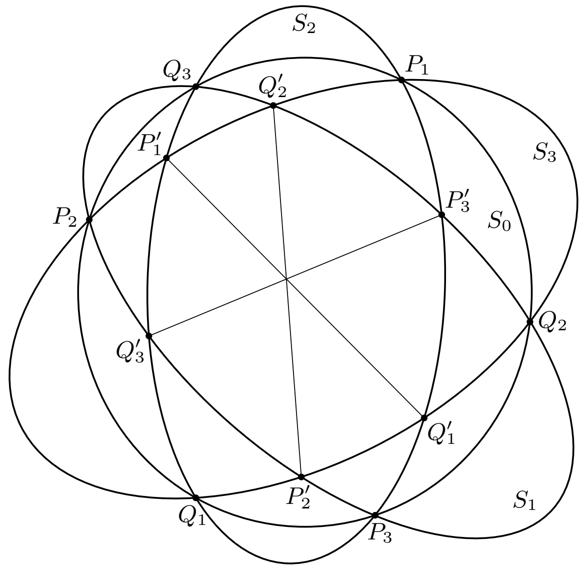


Рис. 11. *К теореме о четырёх кониках*

т. е. пара прямых $L_1 = 0$, $\lambda_2 L_2 - \lambda_3 L_3 = 0$ принадлежит пучку коник, который задают S_2 и S_3. Но такая пара единственна, а именно P_1Q_1, $P'_1Q'_1$. Следовательно, уравнением прямой $P'_1Q'_1$ будет $\lambda_2 L_2 - \lambda_3 L_3 = 0$. Аналогично прямые $P'_2Q'_2$ и $P'_3Q'_3$ задаются уравнениями $\lambda_3 L_3 - \lambda_1 L_1 = 0$ и $\lambda_1 L_1 - \lambda_2 L_2 = 0$ соответственно. Так как

$$(\lambda_2 L_2 - \lambda_3 L_3) + (\lambda_3 L_3 - \lambda_1 L_1) + (\lambda_1 L_1 - \lambda_2 L_2) = 0,$$

прямые $P'_1Q'_1$, $P'_2Q'_2$ и $P'_3Q'_3$ проходят через одну точку, ч. т. д. □

Рисунок 12 иллюстрирует двойственную теорему:

Теорема. *Если две общих касательных каждых двух из трёх коник касаются четвёртой коники, то оставшиеся общие касательные каждой пары пересекаются в трёх коллинеарных точках.*

Интересный пример применения теоремы о четырёх кониках и обращения теоремы о трёх кониках (см. раздел 2.2) показан на рис. 13. Окружность S_0 и коника S_1 пересекаются в точках A, B, C, D. Окружность S_2, проходящая через A и B, пересекает S_1 также в точках E и F, а окружность S_3, проходящая через C и D, — в точках G и H. Тогда E, F, G, H лежат на одной окружности. Для доказательства сначала применим теорему о четырёх кониках к S_1, S_2, S_3 (две точки пересечения каждой пары лежат на S_0) и получим, что EF и GH пересекаются на радикальной оси KL окружностей S_2 и S_3; а затем, применив обратную теорему о трёх

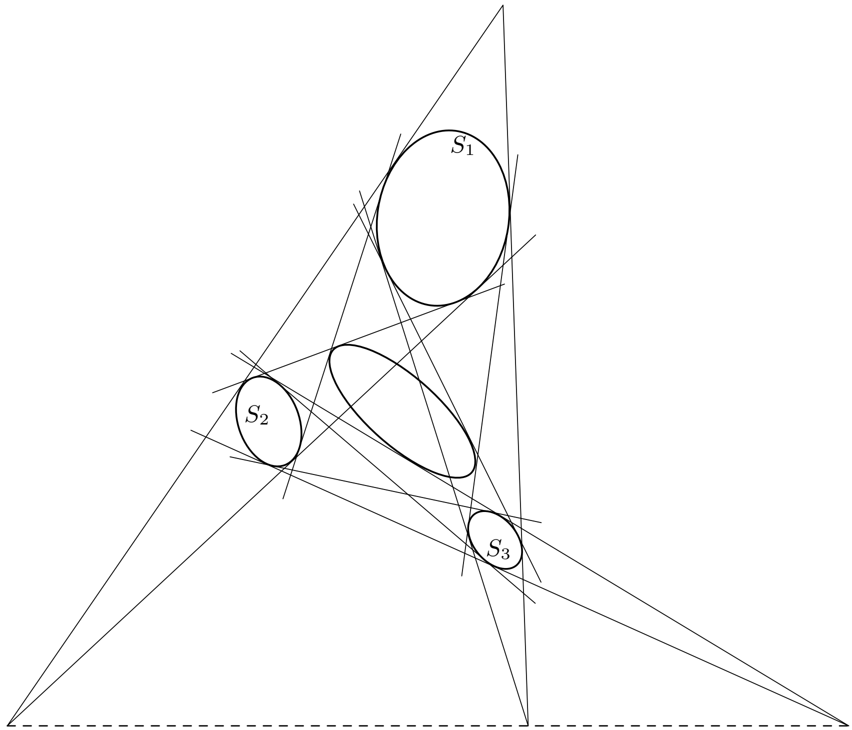


Рис. 12. К двойственной теореме о четырёх кониках

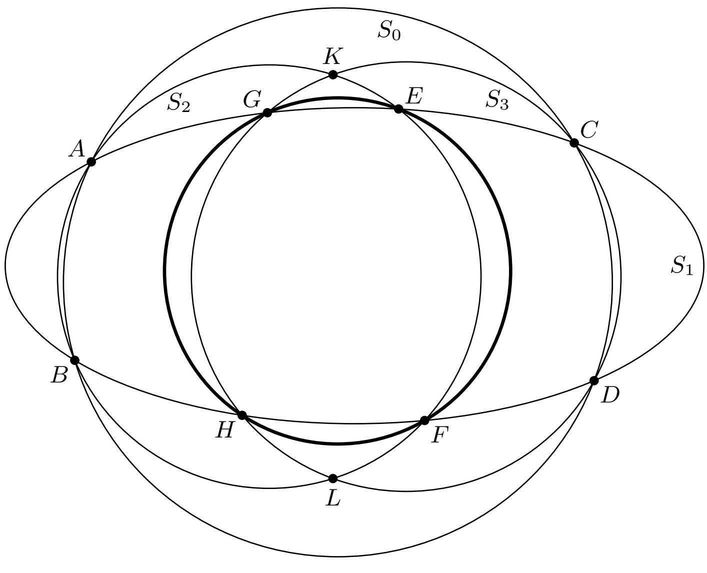


Рис. 13. Применение теорем о трёх и четырёх кониках

кониках к S_2 и S_3, получим, что E, F, G, H и две общие точки коник S_2 и S_3, отличные от K и L (круговые точки), лежат на одной конике. Значит, E, F, G, H лежат на одной окружности, что и требуется.

2.5. Вписанные восьмиугольники

Наконец, посмотрим на теорему Паскаля как на одну из теорем о вписанных в конику многоугольниках с чётным числом сторон.

Для начала сформулируем лемму, доказательство которой можно найти в любой достаточно полной книге по теории плоских кривых.

Лемма. *Если rn из mn общих точек двух кривых порядка m и n соответственно лежат на кривой порядка r, то оставшиеся $(m-r)n$ точек лежат на кривой порядка $m-r$.*

Взяв $m = n = 4$, $r = 2$, получаем следующий результат.

Если восемь из шестнадцати точек пересечения двух кривых четвёртого порядка лежат на одной конике, то и восемь остальных точек лежат на одной конике.

Этот результат остаётся верным и в случае, когда одна или обе кривые четвёртого порядка вырождены. Например, если каждая из кривых распадается в пару коник, мы получаем конфигурацию из 16 точек и шести коник, в которой каждая точка лежит на трёх кониках, а каждая коника проходит через восемь точек. Или, взяв в качестве кривых четвёртого порядка две четвёрки прямых, получим конфигурацию, изображённую на рис. 14.

Другая интерпретация этого же результата приводит к интересному свойству вписанного в конику восьмиугольника. А именно, предположим,

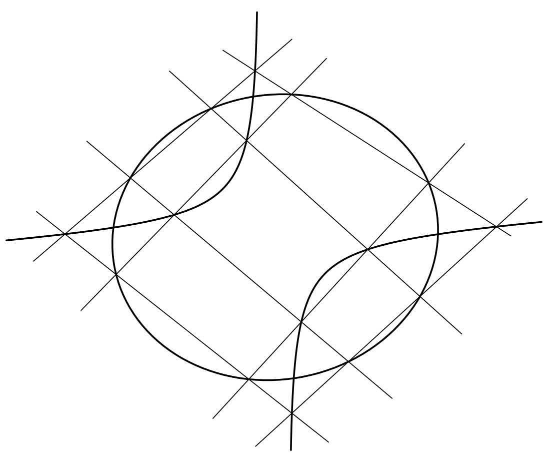


Рис. 14. К лемме

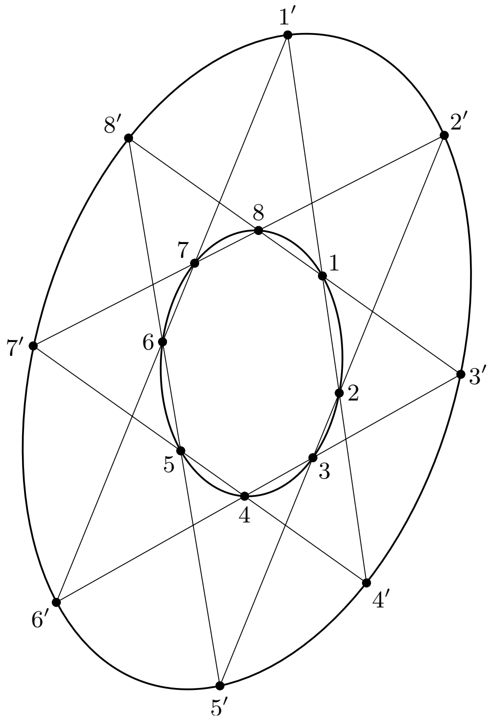


Рис. 15. *К теореме о вписанном восьмиугольнике*

что $1, 2, \ldots, 8$ — вершины такого восьмиугольника (рис. 15), и рассмотрим две вырожденные кривые четвёртого порядка, состоящие из четвёрок прямых 12, 34, 56, 78 и 23, 45, 67, 81 соответственно. Так как $1, 2, \ldots, 8$ — общие точки этих кривых, лежащие на одной конике, восемь оставшихся точек — $1', \ldots, 8'$ на рис. 15 — также лежат на одной конике. Таким образом, доказано следующее утверждение.

Теорема о вписанном восьмиугольнике. *Если восьмиугольник вписан в конику, то восемь точек пересечения каждой из его сторон с третьей от неё стороной также лежат на одной конике.*

Заметим, что конфигурации на рисунках 14 и 15 не являются проективно эквивалентными: хотя обе они описывают 16 точек пересечения двух четвёрок прямых, лишь конфигурация рис. 15 соответствует теореме о вписанном восьмиугольнике.

Интересно, что теорема о вписанном восьмиугольнике сама себе обратна. Если на рис. 15 взять вершины внешнего восьмиугольника в порядке $8'$, $3'$, $6'$, $1'$, $4'$, $7'$, $2'$, $5'$, то третьей от стороны $8'3'$ будет сторона $1'4'$, эти стороны пересекаются в вершине внутреннего восьмиугольника 1, и т. д.

Наконец, чтобы выявить связь теоремы о вписанном восьмиугольнике с теоремой Паскаля, отметим, что обе они являются частными случаями следующего факта при значениях $n = 3$ и $n = 4$.

Если $2n$-угольник вписан в конику, то $n(n-2)$ точек пересечения его «чётных» сторон (при выбранной нумерации) с несмежными «нечётными» лежат на кривой порядка $n-2$.

Доказательство. Применим сформулированную в начале параграфа лемму к двум вырожденным кривым порядка n, одна из которых содержит чётные, а другая — нечётные стороны многоугольника. Из n^2 точек их пересечения $2n$ (а именно вершины исходного многоугольника) лежат на данной конике. По лемме (при $m = n$ и $r = 2$) оставшиеся $n(n-2)$ точек (это как раз пересечения «чётных» сторон с несмежными «нечётными») лежат на кривой порядка $n-2$, что и требуется. □

Список литературы

[1] *Salmon G.* Treatise on Conic Sections (6th edition). London, 1879.

Литература, добавленная переводчиком

[2] *Акопян А. В., Заславский А. А.* Геометрические свойства кривых второго порядка. М.: МЦНМО, 2011.

Сесил Джон Алвин Ивлин (1904–1976)

Годфри Бёрдет Мани-Каутс (1905–1979)

Джон Алфред Тиррелл (1932–1992)

Анализ m-выпуклости многомерных параболоидов и гиперболоидов

Н. В. Филимоненкова, П. А. Бакусов

Работа посвящена новому понятию дифференциальной геометрии, а именно m-выпуклой гиперповерхности. Это понятие является обобщением классической выпуклости. Оно появилось в конце XX века в результате удачного применения конусов Гординга в теории полностью нелинейных дифференциальных уравнений в частных производных. Статья содержит краткое описание m-выпуклых гиперповерхностей, доступное широкой аудитории, и результаты исследования m-выпуклости многомерных квадрик: параболоидов и гиперболоидов. Полученные результаты продемонстрированы на двумерных и трёхмерных квадриках.

§ 1. Понятие m-выпуклой гиперповерхности

1.1. Элементарные симметрические функции

Для описания дифференциально-геометрических понятий нам понадобятся некоторые алгебраические структуры.

Как известно, элементарной симметрической функцией порядка p от n переменных называется сумма всевозможных произведений, где в качестве множителей выбираются p различных представителей из n переменных:

$$\sigma_p(x) = \sum_{i_1<i_2<\ldots<i_p} x_{i_1}x_{i_2}\ldots x_{i_p}, \quad x=(x_1,x_2,\ldots,x_n)\in\mathbb{R}^n, \quad 1\leqslant p\leqslant n. \tag{1.1}$$

По определению $\sigma_0(x)=1$.

Пусть $x\in\mathbb{R}^n$. Обозначим символом $x^{\langle i\rangle}$ вектор, полученный заменой i-й координаты вектора x на 0:

$$x^{\langle i\rangle} = (x_1,x_2,\ldots,x_{i-1},0,x_{i+1},\ldots,x_n), \quad 1\leqslant i\leqslant n. \tag{1.2}$$

Работа выполнена при поддержке РФФИ, проекты № 15–01–07650а, № 15–31–20600 мол_а_вед.

При вычислении $\sigma_p(x^{\langle i\rangle})$, $p < n$, можно считать, что вектор $x^{\langle i\rangle}$ получен вычёркиванием i-й координаты из вектора x. При этом $\sigma_n(x^{\langle i\rangle}) \equiv 0$.

Далее нам понадобятся два простых соотношения:

$$\sigma_p(x) = \sigma_p(x^{\langle i\rangle}) + x_i\sigma_{p-1}(x^{\langle i\rangle}), \quad 1 \leqslant p \leqslant n, \tag{1.3}$$

$$\sigma_p(x) = \frac{1}{n-p}\sum_{i=1}^{n}\sigma_p(x^{\langle i\rangle}), \quad 1 \leqslant p \leqslant n-1. \tag{1.4}$$

Рассмотрим в пространстве $\mathbb{R}^n$ множество всех точек, в которых первые m элементарных симметрических функцией принимают положительные значения:

$$K_m = \{x \in \mathbb{R}^n \colon \sigma_p(x) > 0,\ p = 1, 2, \ldots, m\}, \quad 1 \leqslant m \leqslant n. \tag{1.5}$$

По определению $K_0 = \mathbb{R}^n$.

Множество (1.5) является конусом с вершиной в нуле: если $x \in K_m$, то $\alpha x \in K_m$, $\alpha > 0$.

Элементарные симметрические функции устойчивы к перестановкам переменных, поэтому векторы из конуса K_m можно считать непронумерованными семействами чисел.

Сформулируем простую версию критерия Сильвестра для конусов (1.5):

$$\begin{aligned} x \in K_m \quad &\Rightarrow \quad x^{\langle i\rangle} \in K_{m-1},\ i = 1, 2, \ldots, n, \\ \sigma_m(x) > 0,\ \exists\, i\colon x^{\langle i\rangle} \in K_{m-1} \quad &\Rightarrow \quad x \in K_m. \end{aligned} \tag{1.6}$$

Многократно используя первую часть критерия (1.6), можно показать, что любой вектор x из конуса K_m имеет по крайней мере m положительных координат. При $m = n$ заключаем, что конус K_n состоит из тех и только из тех векторов, у которых все координаты положительны[1)].

1.2. Определение m-выпуклости

Пусть $\Gamma \subset \mathbb{R}^{n+1}$ — некоторая C^2-гладкая ориентированная гиперповерхность, т. е. двусторонняя n-мерная поверхность с выбранным направлением нормали. Обозначим символом $\varkappa(M) = (\varkappa_1, \varkappa_2, \ldots, \varkappa_n)(M)$ набор главных кривизн[2)] этой гиперповерхности в точке $M \in \Gamma$.

[1)] При $m < n$ имеется только односторонняя импликация: если $x \in K_m$, то x имеет m положительных координат, однако обратное не обязательно верно.

[2)] Заметим, что разумного способа нумерации главных кривизн на поверхности не существует, поэтому набор $\varkappa(M)$ понимается как семейство главных кривизн с произвольно выбранной нумерацией.

Определение 1.1. Пусть $1 \leqslant p \leqslant n$. Элементарная симметрическая функция порядка p от главных кривизн гиперповерхности Γ в точке M называется p-кривизной или кривизной порядка p этой поверхности в точке M. Обозначим p-кривизну символом $k_p(M) = \sigma_p(\varkappa(M))$.

В дифференциальной геометрии два случая p-кривизны являются классическими:

$$k_1 = \varkappa_1 + \varkappa_2 + \ldots + \varkappa_n \text{ — средняя кривизна,}$$

$$k_n = \varkappa_1 \varkappa_2 \ldots \varkappa_n \text{ — гауссова кривизна.}$$

Заметим, что p-кривизны, как и главные кривизны, являются геометрическими инвариантами, т. е. не зависят от способа параметризации поверхности. При этом p-кривизны, в отличие от главных кривизн, обладают естественной глобальной нумерацией на поверхности.

Определение 1.2. Пусть $1 \leqslant m \leqslant n$. Гиперповерхность Γ называется m-выпуклой в точке $M \in \Gamma$, если $\varkappa(M) \in K_m$, иначе говоря, $k_p(M) > 0$, $p = 1, 2, \ldots, m$. Областью[3)] m-выпуклости поверхности Γ называем множество всех точек $M \in \Gamma$, в которых Γ является m-выпуклой.

Все C^2-гладкие ориентированные поверхности считаются 0-выпуклыми.

Например, на рис. 1 изображена схема некоторой поверхности, где разным тоном выделены области положительной p-кривизны, $p = 1, 2, 3$. Дан-

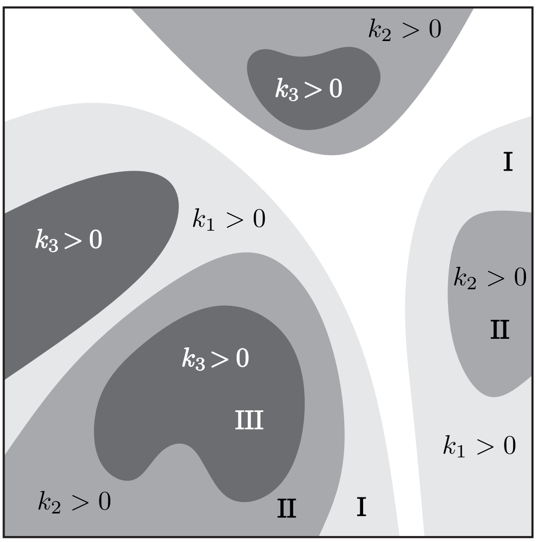


Рис. 1

3) В этой статье «область» означает открытое множество, необязательно связное; термин «поверхность» используется как синоним гиперповерхности.

ная поверхность является 1-выпуклой в светло-серой двухкомпонентной области с номером I, является 2-выпуклой в двухкомпонентной области с номером II и является 3-выпуклой в тёмно-серой связной области с номером III. В остальных тёмно-серых областях поверхность не является 3-выпуклой, так как одна из кривизн младших порядков отрицательна.

Из определения 1.2 следует, что если поверхность Γ является m-выпуклой в данной точке, то она является и $(m-1)$-выпуклой. Значит, область её m-выпуклости вложена в область $(m-1)$-выпуклости и т. д. На рис. 1 область 3-выпуклости вложена в область 2-выпуклости, а та, в свою очередь, включена в ещё более широкую область 1-выпуклости.

Замечание 1.3. Определения 1.1 и 1.2 корректны только для ориентированной гиперповерхности, поскольку при изменении направления нормали главные кривизны и p-кривизны с нечётным значением p меняют знак на противоположный.

1.3. Геометрический смысл m-выпуклости

Понятие m-выпуклости является обобщением классической строгой выпуклости и служит для более детальной стратификации поверхностей и точек на поверхности. Чтобы пояснить характер этого обобщения, обратимся к свойству конусов (1.5), описанному в конце раздела 1.1.

Конус K_n состоит из векторов с положительными координатами, следовательно, n-выпуклая гиперповерхность $\Gamma \subset \mathbb{R}^{n+1}$ — это поверхность, у которой все главные кривизны положительны, а значит, она строго выпукла в классическом смысле. Заметим, что строгая выпуклость и n-выпуклость — очень близкие, но всё же не равносильные понятия. Между ними есть небольшой зазор: строго выпуклая поверхность может иметь точки уплощения (изолированные точки нулевой гауссовой кривизны), тогда как n-выпуклость подразумевает положительность гауссовой кривизны. Для простоты изложения в этой статье мы не будем делать различия между строгой выпуклостью и n-выпуклостью.

При $m < n$ понятие m-выпуклости слабее, чем строгая выпуклость: если поверхность Γ является m-выпуклой в точке M, то в этой точке у неё имеется хотя бы m положительных главных кривизн. Это свойство, однако, не является критерием m-выпуклости, т. е. наличие m положительных главных кривизн не гарантирует m-выпуклость поверхности с $m < n$.

Геометрический смысл этого свойства заключается в следующем. Рассмотрим в точке M нормальные сечения поверхности вдоль главных направлений: каждое сечение образовано двумерной плоскостью, натянутой на вектор нормали к поверхности и одно из главных направлений. Если поверхность m-выпуклая в точке M, то хотя бы m таких сечений являются строго выпуклыми кривыми в данной точке[4)].

Проиллюстрируем понятие m-выпуклости в самом простом случае — на примере двумерной гиперповерхности $\Gamma \subset \mathbb{R}^3$. На рис. 2 изображены две такие ориентированные поверхности: стрелкой отмечено выбранное направление нормали в точке M, пунктиром выделены нормальные сечения поверхности вдоль главных направлений.

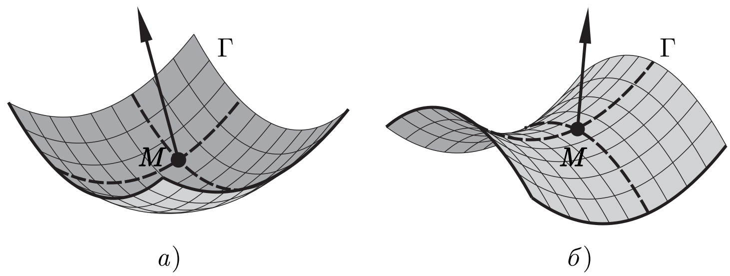


Рис. 2

Двумерная поверхность в каждой точке имеет две главные кривизны $\varkappa = (\varkappa_1, \varkappa_2)$, она может быть 1-выпуклой или 2-выпуклой. Исходя из определения 1.2 легко убедиться, что двумерная поверхность является 2-выпуклой тогда и только тогда, когда обе главные кривизны положительны, а значит, она строго выпукла в классическом смысле (рис. 2*а*):

$$\varkappa \in K_2 \subset \mathbb{R}^2 \quad \Leftrightarrow \quad k_1 = \varkappa_1 + \varkappa_2 > 0,\ k_2 = \varkappa_1 \varkappa_2 > 0 \quad \Leftrightarrow \quad \varkappa_1 > 0,\ \varkappa_2 > 0.$$

Если двумерная поверхность является 1-выпуклой, то у неё одна главная кривизна положительна (рис. 2*б*):

$$\varkappa \in K_1 \subset \mathbb{R}^2 \quad \Leftrightarrow \quad k_1 = \varkappa_1 + \varkappa_2 > 0 \quad \Rightarrow \quad \varkappa_1 > 0 \text{ или } \varkappa_2 > 0.$$

Однако ясно, что поверхность, изображённая на рис. 2*б* и имеющая одну положительную главную кривизну, может быть как 1-выпуклой, так и 0-выпуклой в точке M, поскольку её средняя кривизна k_1 необязательно положительна.

Замечание 1.4. По нашему мнению, m-выпуклые гиперповерхности наверняка обладают и другими интересными геометрическими свойствами,

[4)] Недавно выявлена более основательная связь между m-выпуклыми гиперповерхностями и их нормальными сечениями, аналогичная критерию Сильвестра (1.6). Соответствующая теорема изложена в работе [4], раздел 5.3, однако здесь мы её не приводим из-за громоздкой формулировки и малой степени наглядности.

которые пока ещё не обнаружены или не доказаны. Например, есть гипотеза, что как выпуклая, так и m-выпуклая замкнутая гиперповерхность с достаточно большим m ограничивает звёздную область и что это, возможно, является аналитическим критерием звёздности. Кроме того, хотелось бы получить модификации известных характеристик строго выпуклых гиперповерхностей, таких как расположение выше касательной плоскости, неравенство Йенсена.

1.4. Происхождение и развитие теории m-выпуклых гиперповерхностей

Конструкции p-кривизны и m-выпуклой гиперповерхности появились в конце XX века в результате развития современной теории полностью нелинейных дифференциальных уравнений второго порядка в частных производных и до сих пор тесно связаны с этой теорией.

Элементарные симметрические функции главных кривизн впервые ввели L. Caffarelly, L. Nirenberg и J. Spruck в работе 1985 г. [9], где рассматривается задача Дирихле для m-гессиановского уравнения в n-мерной ограниченной области с достаточно гладкой границей. Условие разрешимости этой задачи сводится к $(m-1)$-выпуклости граничной гиперповерхности. Этот результат обнаружил нелокальную природу полностью нелинейных задач (нелинейных по вторым производным решения): даже малейший изъян геометрических характеристик области может привести к отсутствию гладких решений, какими бы гладкими ни были данные. В этом заключается принципиальное отличие полностью нелинейных задач от линейных и квазилинейных.

Сами термины«p-кривизна» и «m-выпуклость» появились позднее — в работах Н. М. Ивочкиной [1, 12], также посвящённых теории m-гессиановских уравнений.

С появлением понятий p-кривизны и m-выпуклой гиперповерхности возникли новые задачи на стыке полностью нелинейных дифференциальных уравнений в частных производных и дифференциальной геометрии. Появились аналоги задач о построении замкнутых поверхностей по заданной средней или гауссовой кривизне. Последняя, как известно, называется классической проблемой Минковского [6]. Задача о построении замкнутой гиперповерхности по заданной p-кривизне, $1 \leqslant p < n$, сформулирована в монографии [6] и названа обобщённой проблемой Минковского. Она не имеет удовлетворительного решения до сих пор. Построение поверхности по заданной p-кривизне и краю исследовалось в работах [1, 8, 17], но также не доведено до конца. В работах [3, 11, 12, 15, 18] были получены некоторые результаты об эволюции замкнутых выпуклых гиперповерхностей с предписанным законом зависимости p-кривизны от нормальной скорости эволюции. Все эти задачи сводятся к стационарным либо эволюционным полностью нелинейным дифференциальным уравнениям в частных производных.

Систематическое изучение m-выпуклых поверхностей как самостоятельного раздела дифференциальной геометрии ещё только начинается. Есть множество открытых вопросов, которые нуждаются во внимании специалистов-геометров (см. например, замечание 1.4). Наиболее полный обзор уже накопленных фактов и методов имеется в работе [4].

Одним из пробелов теории до сих пор было построение простейших примеров m-выпуклых гиперповерхностей, их численный анализ. В данной работе восполняется именно этот пробел.

В качестве простейших гиперповерхностей мы рассмотрели квадрики (параболоиды и гиперболоиды), которые в двумерном случае называются поверхностями второго порядка.

В § 2 продемонстрирован анализ m-выпуклости для n-мерного параболоида, включая техническую реализацию.

В § 3 приведены аналогичные результаты для n-мерного гиперболоида, но уже без технических выкладок.

Полученные результаты, несмотря на незатейливость вывода, являются новыми. Главный результат работы — полное описание связи между формулой параболоида (или гиперболоида) произвольной размерности и структурой области его m-выпуклости.

Общие результаты проиллюстрированы на квадриках малой размерности. Самыми простыми и наглядными примерами служат двумерные квадрики: двумерные параболоиды подробно разобраны в разделе 2.3, двумерные гиперболоиды эпизодически рассматриваются в § 3. Но так как двумерная поверхность может быть только 1-выпуклой или 2-выпуклой, причём последнее соответствует классической строгой выпуклости и потому малоинтересно, то в двумерном случае палитра возможностей достаточно бедная. Поэтому в разделе 2.4 мы рассматриваем трёхмерные параболоиды, которые нельзя изобразить, но зато теория на их примере иллюстрируется полнее.

1.5. Связь m-выпуклых гиперповерхностей с конусами Гординга

Целесообразность определения 1.2 и некоторые свойства m-выпуклых поверхностей вытекают из алгебраической теории гиперболических многочленов и конусов Гординга [10], которая сложилась в середине XX века задолго до появления понятия m-выпуклости.

Элементарная симметрическая функция (1.1) является классическим примером гиперболических многочленов, а конус (1.5) — примером конусов Гординга.

Обзору теории Гординга посвящена наша предыдущая работа [7]. Статьи [2, 5, 13, 14, 16] освещают теорию m-выпуклых гиперповерхностей с точки зрения теории Гординга. В этом разделе мы приведём одно методологическое следствие этой теории, на котором основан наш анализ m-выпуклости квадрик.

Введём обозначение для области положительной p-кривизны гиперповерхности $\Gamma \subset \mathbb{R}^{n+1}$:

$$\Omega_p^+ = \{M \in \Gamma\colon\ k_p(M) > 0\}, \quad 1 \leqslant p \leqslant n. \tag{1.7}$$

По определению 1.2 область m-выпуклости равна пересечению $\bigcap_{p=1}^m \Omega_p^+$. В частности, область m-выпуклости содержится в Ω_m^+. Из теории Гординга вытекает, что область m-выпуклости, если она не пуста, занимает целиком одну или несколько компонент связности Ω_m^+. А именно, верна следующая лемма[5].

Лемма 1.5. *Если гиперповерхность Γ является m-выпуклой в точке M_0, то Γ является m-выпуклой во всей компоненте связности множества Ω_m^+, содержащей точку M_0.*

Лемма 1.5 неявно включает и обратное утверждение: если в точке $M_0 \in \Omega_m^+$ поверхность Γ не является m-выпуклой, то она не m-выпуклая во всей компоненте связности множества Ω_m^+, содержащей точку M_0.

Таким образом, чтобы установить m-выпуклость поверхности в какой-то компоненте Ω_m^+, достаточно проверить m-выпуклость всего в одной точке (рис. 3). Напомним, что установить m-выпуклость поверхности в какой-либо точке $M_0 \in \Omega_m^+$ — значит проверить в этой точке положительность всех p-кривизн младших порядков $p = 1, 2, \ldots, m-1$.

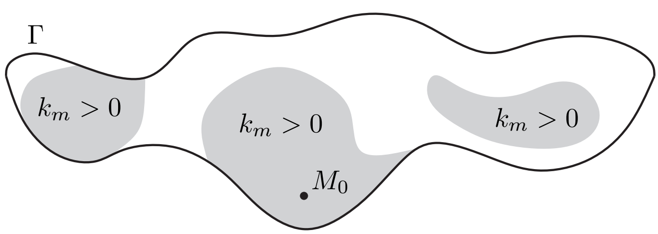


Рис. 3

[5] Лемма 1.5 является прямым следствием пункта 1 теоремы 3.2 из [7].

Благодаря лемме 1.5 можно проще определить m-выпуклость замкнутой гиперповерхности.

Определение 1.6. Замкнутая гиперповерхность $\Gamma \subset \mathbb{R}^{n+1}$, ориентированная внутренней нормалью, называется m-выпуклой, если её m-кривизна положительна.

Замечание 1.7. Для замкнутых гиперповерхностей понятие m-выпуклости однозначно, поскольку предписывается конкретное направление нормали. Выбор в пользу внутренней нормали необходим для корректности определения 1.6 при $m = n$: чтобы граница строго выпуклого компакта, например шара, оказалась n-выпуклой поверхностью (а не 0-выпуклой, как в случае выбора внешней нормали).

В определении 1.6 речь идёт о тотальной m-выпуклости — во всех точках поверхности. Согласованность определений 1.2 и 1.6 обусловлена тем, что в данном случае область $\Omega_m^+ = \Gamma$ содержит одну компоненту связности и на замкнутой гиперповерхности обязательно найдётся точка M_0 строгой выпуклости, в которой все главные кривизны положительны. В точке M_0 поверхность n-выпуклая, а значит, и m-выпуклая при $m \leqslant n$.

В подтверждение естественности определения 1.6 напомним известный факт: замкнутая поверхность с положительной гауссовой кривизной (n-кривизной) является строго выпуклой (n-выпуклой). Типичным примером служит n-мерная сфера радиуса $r > 0$, чья гауссова кривизна во всех точках равна $1/r^n$.

§ 2. Анализ m-выпуклости параболоидов

2.1. Вычисление p-кривизны параболоида

В этом разделе приведены технические рассуждения и формулы, позволяющие вычислить p-кривизну гиперповерхности, являющейся графиком функции, и, в частности, p-кривизну параболоида.

Поскольку главные кривизны трудно вычислимы и являются негладкими функциями точки на поверхности, то определение 1.1 неудобно как в теоретическом анализе, так и в вычислительной практике. Для вычисления p-кривизны используются альтернативные подходы, например такая формула:

$$k_p = \operatorname{tr}_p(g^{-1}b), \quad 1 \leqslant p \leqslant n. \tag{2.1}$$

Здесь g — матрица первой квадратичной формы, b — матрица второй квадратичной формы гиперповерхности $\Gamma \subset \mathbb{R}^{n+1}$. Матрица $g^{-1}b$ — квадратная, размерности n, в общем случае несимметричная. Символом tr_p обозначен p-след матрицы, равный сумме всех главных миноров порядка p этой матрицы. Например, 1-след матрицы равен сумме элементов на главной диагонали (обычно называется просто следом), n-след матрицы равен её определителю. Главные кривизны поверхности являются собственными числами матрицы $g^{-1}b$. С другой стороны, диагонализация матрицы не меняет значение p-следа. Поэтому формула (2.1) не противоречит определению 1.1.

Замечание 2.1. В теоретических вопросах наилучшим способом выражения p-кривизны является формула $k_p = \mathrm{tr}_p(\mathcal{K})$, где $\mathcal{K} = \tau^T b\tau$ — матрица кривизны гиперповерхности, $\tau = \sqrt{g^{-1}}$. Матрица кривизны $\mathcal{K}$ — это симметричный аналог матрицы $g^{-1}b$, аналитические преимущества которого наиболее полно изложены в статье [4]. В данной работе оказалось удобнее пользоваться несимметричной, но зато более простой в вычислительном отношении матрицей $g^{-1}b$.

В вычислении p-кривизны параболоидов (и далее гиперболоидов) по формуле (2.1) ключевую роль сыграло новое свойство p-следа, которое мы вывели из кососимметричности миноров:

$$\mathrm{tr}_p(S + t\xi \times \eta) = \mathrm{tr}_p(S) + t\sum_{i,j=1}^{n} \mathrm{tr}_p^{ij}(S)\xi_i\eta_j, \tag{2.2}$$

$$S = (s_{ij})_{i,j=1}^n, \quad \xi \times \eta = (\xi_i\eta_j)_{i,j=1}^n,\ \xi, \eta \in \mathbb{R}^n, \quad t \in \mathbb{R}, \quad \mathrm{tr}_p^{ij}(S) = \frac{\partial\,\mathrm{tr}_p(S)}{\partial s_{ij}}.$$

Допустим, гиперповерхность $\Gamma \subset \mathbb{R}^{n+1}$ является графиком C^2-гладкой функции

$$x_{n+1} = \omega(x), \quad x \in \mathbb{R}^n, \tag{2.3}$$

и Γ ориентирована нормалью, образующей острый угол с координатной осью x_{n+1}. Обозначим символом ω_x вектор градиента функции $\omega(x)$, символом ω_{xx} — матрицу вторых производных (матрицу Гессе) функции $\omega(x)$.

Замечание 2.2. Как известно, в этом случае строгая выпуклость (n-выпуклость) поверхности Γ равносильна строгой выпуклости функции $\omega(x)$ и сводится к положительной определённости матрицы ω_{xx}. К сожалению, такая редукция от поверхности к функции невозможна при анализе m-выпуклости в случае $m < n$, где не обойтись без вычисления p-кривизн.

Приведём известные расчётные формулы матриц g^{-1} и b для графика функции:

$$g^{-1}(x) = I - \frac{\omega_x \times \omega_x}{1 + \omega_x^2}, \quad b(x) = \frac{\omega_{xx}}{\sqrt{1 + \omega_x^2}}, \tag{2.4}$$

где I — единичная матрица.

В нашей работе рассматриваются n-мерные параболоиды, которые являются графиками функций следующего вида:

$$x_{n+1} = \sum_{i=1}^{n} a_i x_i^2 = a_1 x_1^2 + a_2 x_2^2 + \ldots + a_n x_n^2, \quad a_i \in \mathbb{R}. \tag{2.5}$$

Помимо стандартной записи вектора переменных $x = (x_1, x_2, \ldots, x_n)$, будем использовать следующие обозначения:

$$\begin{aligned} a &= (a_1, a_2, \ldots, a_n) \text{ — вектор коэффициентов параболоида,} \qquad (2.6)\\ A &= \operatorname{diag}(a_1, a_2, \ldots, a_n) \text{ — диагональная матрица коэффициентов.} \end{aligned}$$

После вычисления матриц (2.4), умножения и упрощения получаем для параболоида

$$g^{-1}b(x) = \frac{2}{\sqrt{1+4(Ax)^2}}\Big(A - \frac{4}{1+4(Ax)^2} Ax \times A^2 x\Big). \tag{2.7}$$

Как можно видеть, p-след этой матрицы может быть вычислен по формуле (2.2). Заметим, что если в (2.2) в качестве матрицы S взять диагональную матрицу A, то правая часть (2.2) выражается через элементарные симметрические функции от векторов a и $a^{\langle i \rangle}$ (см. обозначение (1.2)):

$$\operatorname{tr}_p(A + t\xi \times \eta) = \operatorname{tr}_p(A) + t\sum_{i=1}^{n} \operatorname{tr}_p^{ii}(A)\xi_i\eta_i = \sigma_p(a) + t\sum_{i=1}^{n} \sigma_{p-1}(a^{\langle i \rangle})\xi_i\eta_i.$$

Для выражения p-кривизны параболоида осталось применить последнюю формулу к (2.7), используя однородность p-следа:

$$\begin{aligned} k_p(x) &= \operatorname{tr}_p(g^{-1}b(x)) = \\ &= \left(\frac{2}{\sqrt{1+4(Ax)^2}}\right)^p \left(\sigma_p(a) - \frac{4}{1+4(Ax)^2}\sum_{i=1}^{n} \sigma_{p-1}(a^{\langle i \rangle}) a_i^3 x_i^2\right) = \\ &= \frac{1}{4}\left(\frac{2}{\sqrt{1+4(Ax)^2}}\right)^{p+2} \left(\sigma_p(a) + 4\sum_{i=1}^{n} a_i^2 x_i^2 \big(\sigma_p(a) - a_i\sigma_{p-1}(a^{\langle i \rangle})\big)\right) = \\ &= c \cdot \left(\sigma_p(a) + 4\sum_{i=1}^{n} a_i^2 x_i^2 \sigma_p(a^{\langle i \rangle})\right), \quad c > 0. \qquad (2.8) \end{aligned}$$

Для преобразования p-кривизны к виду (2.8) пригодилось соотношение (1.3).

2.2. Область m-выпуклости параболоида

В этом разделе приведены результаты исследования m-выпуклости параболоида (2.5), ориентированного нормалью, образующей острый угол с координатной осью x_{n+1}. Будем использовать обозначения (2.6) и (1.2).

Под областью m-выпуклости параболоида удобнее понимать не только часть самого параболоида (см. определение 1.2), но и множество точек $x \in \mathbb{R}^n$ (аргументов функции (2.5)), в которых параболоид m-выпуклый.

Формула (2.8) при $p = m$ задаёт в пространстве $\mathbb{R}^n$ область положительной m-кривизны параболоида (2.5). Используем для этой области обозначение (1.7) и запишем её в явном виде:

$$\Omega_m^+ = \left\{ x \in \mathbb{R}^n \colon \sigma_m(a) + 4 \sum_{i=1}^{n} a_i^2 x_i^2 \sigma_m(a^{\langle i \rangle}) > 0 \right\}, \quad 1 \leqslant m \leqslant n. \tag{2.9}$$

Выявление топологической структуры Ω_m^+ составляет несложное упражнение. Область Ω_m^+ может быть

- связной, если $\sigma_m(a) > 0$;
- связной или двухкомпонентной, если $\sigma_m(a) \leqslant 0$ и $\exists\, i \colon \sigma_m(a^{\langle i \rangle}) > 0$;
- пустой в остальных случаях.

В общей ситуации (см. раздел 1.5) можно утверждать, что если гиперповерхность имеет непустую область m-выпуклости, то она совпадает с некоторыми компонентами связности Ω_m^+. Поскольку у параболоида область Ω_m^+ содержит не более двух компонент, да и те симметричны (геометрические характеристики параболоида на них одинаковы), то имеется альтернатива, отражённая в следующей теореме.

Теорема 2.3. *Пусть $1 \leqslant m < n$. Область m-выпуклости параболоида (2.5) либо пуста, либо совпадает с непустой областью Ω_m^+. Последнее верно тогда и только тогда, когда*

$$\exists\, i \colon a^{\langle i \rangle} \in K_m, \tag{2.10}$$

причём достаточно выполнения условия

$$a \in K_m. \tag{2.11}$$

(*В случае* (2.11) *область* Ω_m^+ *связна, в случае* (2.10) *область* Ω_m^+ *может быть как связной, так и двухкомпонентной.*)

Область n-выпуклости параболоида (2.5) *либо пуста, либо совпадает со всем пространством $\mathbb{R}^n$. Последнее верно тогда и только тогда, когда*

$$a \in K_n. \tag{2.12}$$

Доказательство. Условие (2.12) равносильно положительности всех коэффициентов a_i. Ясно, что в этом и только в этом случае параболоид (2.5) является n-выпуклым, причём в каждой точке $x \in \mathbb{R}^n$. В рамках нашей методологии это подтверждается тем, что $\sigma_n(a^{\langle i \rangle}) \equiv 0$ и в силу (2.9) либо $\Omega_n^+ = \varnothing$, либо $\Omega_n^+ = \mathbb{R}^n$.

Для проверки m-выпуклости параболоида в области Ω_m^+, $1 \leqslant m < n$, используем подход, описанный в разделе 1.5 и основанный на лемме 1.5.

I. Докажем достаточность условия (2.10). Пусть существует такой номер i, $1 \leqslant i \leqslant n$, что $a^{\langle i \rangle} \in K_m$, т. е. $\sigma_p(a^{\langle i \rangle}) > 0$, $p = 1, 2, \ldots, m$. Следовательно, область Ω_m^+ непуста. Проверим m-выпуклость параболоида в отдельных точках области Ω_m^+. Рассмотрим два случая.

1. Если $a_i = 0$, то $\sigma_p(a) = \sigma_p(a^{\langle i \rangle}) > 0$, $p = 1, 2, \ldots, m$. Область Ω_m^+ связна и в силу (2.9) содержит точку $\mathbf{0} = (0, 0, \ldots, 0)$. В этой точке все p-кривизны (2.8) положительны, $p = 1, 2, \ldots, m$. Следовательно, параболоид является m-выпуклым в точке $\mathbf{0}$, а значит, по лемме 1.5 он является m-выпуклым во всей области Ω_m^+.
2. Если $a_i \neq 0$, то в силу (2.9) область Ω_m^+ содержит пару точек

$$x = (0, 0, \ldots, \pm x_i, \ldots, 0), \quad |x_i| \gg 1. \tag{2.13}$$

Если область Ω_m^+ двухкомпонентная, то эти точки попадают в разные компоненты связности. В точках (2.13) все p-кривизны (2.8) положительны, $p = 1, 2, \ldots, m$. Следовательно, параболоид является m-выпуклым в этих точках, а по лемме 1.5 и во всей области Ω_m^+.

Достаточность условия (2.11) вытекает из свойств (1.6), (1.4).

II. Докажем необходимость условия (2.10). Пусть $a^{\langle i \rangle} \notin K_m$, $i = 1, 2, \ldots, n$. Покажем, что тогда для параболоида возможны две ситуации: $\Omega_m^+ = \varnothing$ или $\Omega_m^+ \cap \Omega_p^+ = \varnothing$ для некоторого $p < m$. В обеих ситуациях область m-выпуклости пуста.

1. Если $\sigma_m(a^{\langle i \rangle}) \leqslant 0$, $i = 1, 2, \ldots, n$, то по формуле (1.4) получаем $\sigma_m(a) \leqslant 0$ и область Ω_m^+ пуста.
2. Если существует такой номер i, что $\sigma_m(a^{\langle i \rangle}) > 0$, то область Ω_m^+ содержит точки x вида (2.13). Но поскольку $a^{\langle i \rangle} \notin K_m$, можно показать, что найдётся такое $p < m$, что $\sigma_p(a^{\langle i \rangle}) < 0$. Из (2.8) следует, что $k_p(x) < 0$ и параболоид не является m-выпуклым в точках (2.13). Тогда по лемме 1.5 параболоид не является m-выпуклым ни в одной точке области Ω_m^+. $\square$

Из теоремы 2.3 вытекает критерий тотальной m-выпуклости параболоида.

Следствие 2.4. *Пусть $1 \leqslant m \leqslant n$. Параболоид* (2.5) *является m-выпуклым в любой точке $x \in \mathbb{R}^n$ тогда и только тогда, когда*[6)]

$$a \in K_m, \quad \sigma_m(a^{\langle i \rangle}) \geqslant 0, \quad i = 1, 2, \ldots, n. \tag{2.14}$$

Доказательство. Из (2.9) понятно, что $\Omega_m^+ = \mathbb{R}^n$ только при $\sigma_m(a) > 0$ (возьмём $x = \mathbf{0}$), $\sigma_m(a^{\langle i \rangle}) \geqslant 0$, $i = 1, 2, \ldots, n$ (возьмём x из (2.13)). Достаточность условия (2.14) очевидна из (2.11). Необходимость следует из (2.10) и критерия Сильвестра (1.6). □

Таким образом, теорема 2.3 и следствие 2.4 дают полное описание области m-выпуклости параболоида (2.5). Показательно, что условия m-выпуклости параболоида записываются в терминах принадлежности вектора коэффициентов a или $a^{\langle i \rangle}$ конусу K_m.

Общие результаты этого раздела проиллюстрированы в следующих разделах на примерах двумерных и трёхмерных параболоидов.

Замечание 2.5. Обратим внимание на связь между m-выпуклостью параболоида (2.5) и количеством его положительных коэффициентов. Поскольку любой вектор из конуса K_m имеет хотя бы m положительных координат (см. раздел 1.1), из критерия (2.10) следует вывод: если параболоид имеет непустую область m-выпуклости, то у него есть не менее m положительных коэффициентов. Однако параболоид, имеющий m положительных коэффициентов, необязательно является m-выпуклым хотя бы в одной точке. Это верно только при $m = n$ и $m = n - 1$.

Случай $m = n$ очевиден. Случай $m = n - 1$ вытекает из теоремы 2.3. Допустим, параболоид (2.5) имеет ровно $(n-1)$ положительных коэффициентов и один неположительный коэффициент: $a_j \leqslant 0$. Тогда $a^{\langle j \rangle} \in K_{n-1}$, и параболоид является $(n-1)$-выпуклым в непустой области Ω_{n-1}^+, причём эта область устроена следующим образом. Согласно следствию 2.4 в случае вырождения параболоида в цилиндрическую поверхность имеет место его тотальная $(n-1)$-выпуклость:

$$a_j = 0 \quad \Rightarrow \quad \Omega_{n-1}^+ = \mathbb{R}^n.$$

В невырожденном случае $(n-1)$-выпуклой является только часть параболоида, расположенная ниже определённого уровня:

$$a_j < 0 \quad \Rightarrow \quad \Omega_{n-1}^+ = \left\{ x \in \mathbb{R}^n \colon \sum_{i=1}^{n} a_i x_i^2 < -\frac{\sigma_{n-1}(a)}{4\sigma_n(a)} \right\}.$$

[6)] Условие (2.14) при $m = n$ не противоречит условию (2.12), так как $\sigma_n(a^{\langle i \rangle}) \equiv 0$.

2.3. Двумерный параболоид

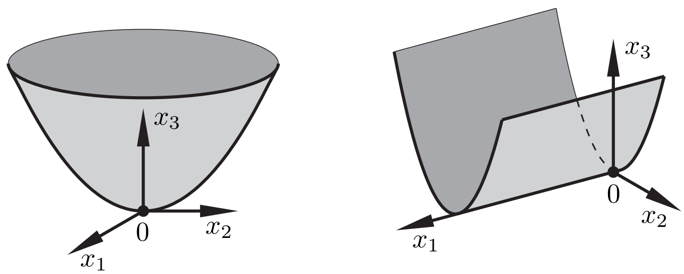
Рассмотрим в пространстве $\mathbb{R}^3$ двумерный параболоид

$$x_3 = a_1 x_1^2 + a_2 x_2^2, \tag{2.15}$$

ориентированный нормалью, образующей острый угол с координатной осью x_3.

Двумерная поверхность может иметь точки 1-выпуклости и точки 2-выпуклости (точки строгой выпуклости). Это случаи $m = n$ и $m = n - 1$, которые разобраны в замечании 2.5.

- При $a_1 > 0$, $a_2 > 0$ имеем эллиптический параболоид (рис. 4*а*). Только такой параболоид является 2-выпуклым, причём сразу во всех точках.
- При $a_1 = 0$, $a_2 > 0$ происходит вырождение эллиптического параболоида в параболический цилиндр (рис. 4*б*). Эта поверхность является 1-выпуклой во всех точках.



а) *б*)

Рис. 4

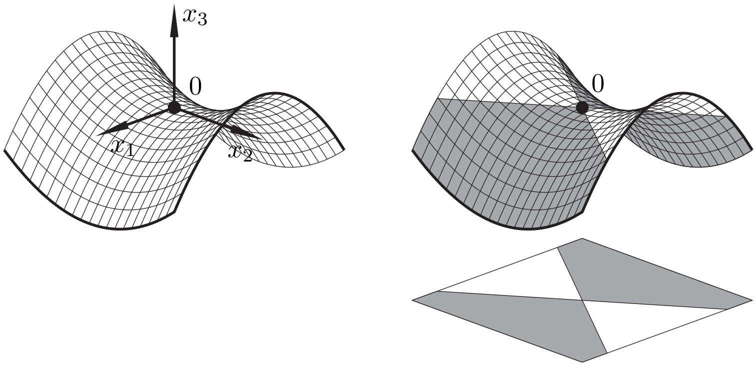
- При $a_1 < 0$, $a_2 > 0$ поверхность (2.15) называется гиперболическим параболоидом или «седлом» (рис. 5*а*).

Только часть этой поверхности является 1-выпуклой, а именно та часть, которая расположена ниже плоскости

$$x_3 = -\frac{a_1 + a_2}{4a_1 a_2}.$$

В зависимости от знака суммы $a_1 + a_2$ это может быть плоскость нулевого уровня (рис. 5*б*), отрицательного или положительного уровня (рис. 6). Соответственно, область 1-выпуклости гиперболического параболоида может быть связной или двухкомпонентной. На рисунках она выделена серым цветом: как на самом параболоиде, так и в пространстве аргументов $\mathbb{R}^2$.

- При $a_1 < 0$, $a_2 < 0$ параболоид (2.15) с указанной ориентацией является 0-выпуклым. Понятно, что с противоположной ориентацией этот параболоид является всюду 2-выпуклым.



а) *б*)

Рис. 5

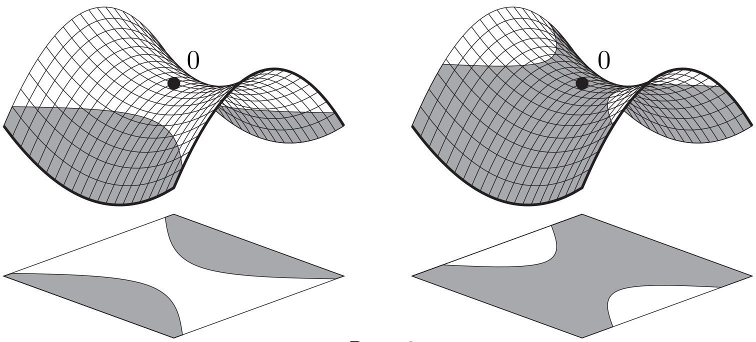


Рис. 6

2.4. Трёхмерный параболоид

Рассмотрим в пространстве $\mathbb{R}^4$ трёхмерный параболоид

$$x_4 = a_1x_1^2 + a_2x_2^2 + a_3x_3^2, \tag{2.16}$$

ориентированный нормалью, образующей острый угол с координатной осью x_4. Трёхмерная гиперповерхность может иметь точки 1-выпуклости, 2-выпуклости и 3-выпуклости.

- Параболоид (2.16) может быть 3-выпуклым (строго выпуклым) только при условии $a_1 > 0$, $a_2 > 0$, $a_3 > 0$, причём в этом случае он является тотально 3-выпуклым.
- При $a_1 > 0$, $a_2 > 0$, $a_3 \leqslant 0$ параболоид имеет непустые области 2-выпуклости и 1-выпуклости.
- При $a_1 > 0$, $a_2 \leqslant 0$, $a_3 \leqslant 0$ параболоид может иметь только непустую область 1-выпуклости, однако может быть даже 0-выпуклым (см. замечание 2.5).

- При $a_1 < 0$, $a_2 < 0$, $a_3 < 0$ параболоид является всюду 0-выпуклым (однако является 3-выпуклым с противоположной ориентацией).

В таблице приведены некоторые примеры трёхмерных параболоидов с одним или двумя отрицательными коэффициентами и с различными областями m-выпуклости, $m = 1, 2$.

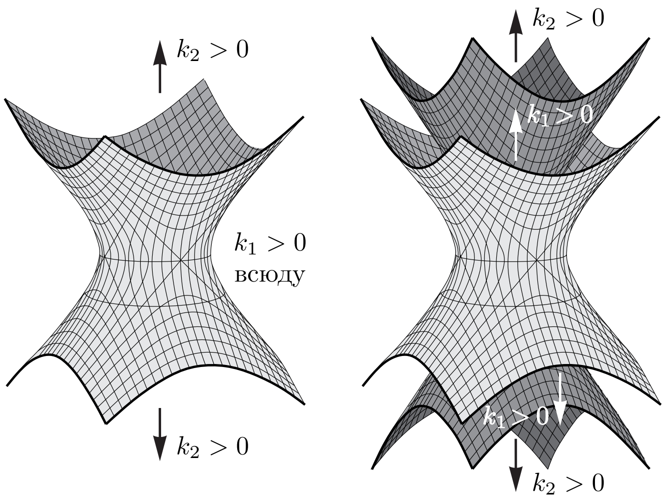
параболоид	**область 1-выпуклости**	**область 2-выпуклости**
$x_4 = 3x_1^2 + 2x_2^2 - x_3^2$ (рис. 7*а*)	$\mathbb{R}^3$	связная область: $-72x_1^2 - 48x_2^2 + 24x_3^2 > -1$
$a = (3, 2, -1)$	$a \in K_1$, $\sigma_1(a^{\langle i \rangle}) \geqslant 0 \ \forall i$	$a \in K_2$
$x_4 = 2x_1^2 + 2x_2^2 - 3x_3^2$ (рис. 7*б*)	связная область: $-16x_1^2 - 16x_2^2 + 144x_3^2 > -1$	двухкомпонентная область: $-12x_1^2 - 12x_2^2 + 18x_3^2 > 1$
$a = (2, 2, -3)$	$a \in K_1$	$\exists i \colon a^{\langle i \rangle} \in K_2 \ (i = 3)$
$x_4 = x_1^2 + x_2^2 - 3x_3^2$ (рис. 8*а*)	двухкомпонентная область: $-8x_1^2 - 8x_2^2 + 72x_3^2 > 1$	двухкомпонентная область: $-12x_1^2 - 12x_2^2 + 36x_3^2 > 5$
$a = (1, 1, -3)$	$\exists i \colon a^{\langle i \rangle} \in K_1 \ (i = 3)$	$\exists i \colon a^{\langle i \rangle} \in K_2 \ (i = 3)$
$x_4 = 2x_1^2 - x_2^2 - x_3^2$ (рис. 8*б*)	связная область: $-8x_1^2 + x_2^2 + x_3^2 > 0$	$\varnothing$
$a = (2, -1, -1)$	$\exists i \colon a^{\langle i \rangle} \in K_1 \ (i = 2, 3)$	$\nexists i \colon a^{\langle i \rangle} \in K_2$
$x_4 = 2x_1^2 - 3x_2^2 - x_3^2$ (рис. 9*а*)	двухкомпонентная область: $-32x_1^2 + 18x_2^2 - 2x_3^2 > 1$	$\varnothing$
$a = (2, -3, -1)$	$\exists i \colon a^{\langle i \rangle} \in K_1 \ (i = 2)$	$\nexists i \colon a^{\langle i \rangle} \in K_2$
$x_4 = x_1^2 - x_2^2 - x_3^2$ (рис. 9*б*)	$\varnothing$	$\varnothing$
$a = (1, -1, -1)$	$\nexists i \colon a^{\langle i \rangle} \in K_1$	$\nexists i \colon a^{\langle i \rangle} \in K_2$

Каждый пример мы сопровождаем анализом вектора коэффициентов параболоида: проверяем, выполняются ли условия теоремы 2.3 и следствия 2.4.

Каждому примеру соответствует один из рис. 7–9. Поскольку трёхмерную поверхность в четырёхмерном пространстве изобразить здесь невозможно, рисунок даёт представление только об областях 1-выпуклости и 2-выпуклости параболоида, мы изображаем их как области подходящих аргументов $x \in \mathbb{R}^3$. Точнее говоря, для каждого параболоида, включённого в таблицу, изображены границы областей

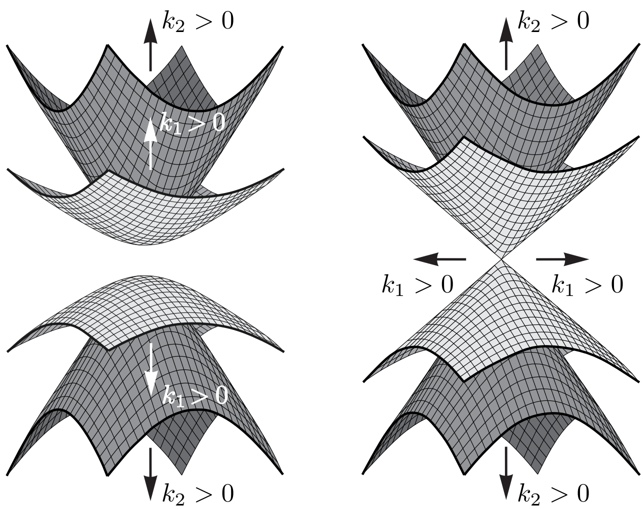
$$\Omega_1^+ = \{x \in \mathbb{R}^3 \colon k_1 > 0\}, \quad \Omega_2^+ = \{x \in \mathbb{R}^3 \colon k_2 > 0\},$$

полученные из формулы (2.8), и стрелками указаны эти области. Область Ω_1^+ является также областью 1-выпуклости параболоида, пересечение $\Omega_1^+ \cap \Omega_2^+$ является областью 2-выпуклости. Так как $\Omega_1^+ \cap \Omega_2^+ = \varnothing$ на рис. 8*б*, 9*а*, *б*,



а) *б*)

Рис. 7



а) *б*)

Рис. 8

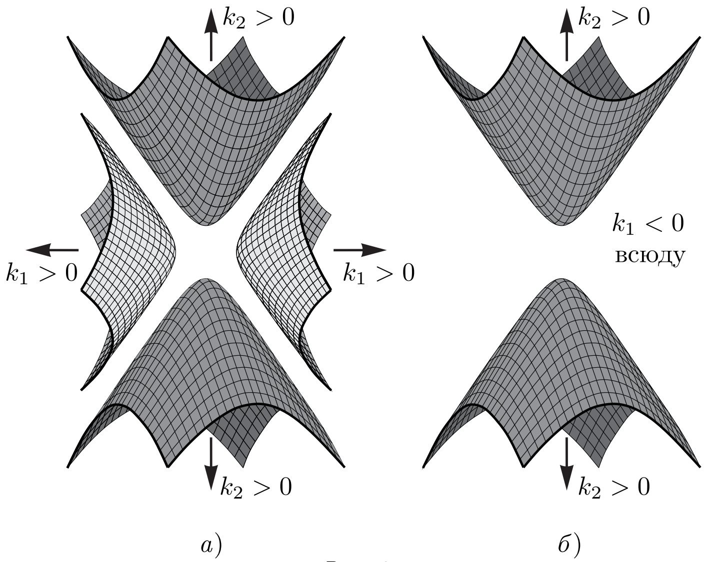


Рис. 9

то соответствующие параболоиды в таблице не имеют точек 2-выпуклости. Последний параболоид в таблице не имеет также точек 1-выпуклости, поскольку для него $\Omega_1^+ = \varnothing$ (рис. 9*б*).

§ 3. Анализ m-выпуклости гиперболоидов

Анализ m-выпуклости гиперболоидов во всём аналогичен анализу параболоидов, но технически более трудоёмок. Поэтому здесь мы ограничимся описанием полученных результатов.

Напомним, что n-мерным гиперболоидом называется квадрика

$$\frac{x_1^2}{c_1^2} + \ldots + \frac{x_k^2}{c_k^2} - \frac{x_{k+1}^2}{c_{k+1}^2} - \ldots - \frac{x_{n+1}^2}{c_{n+1}^2} = 1.$$

Поскольку наша техника вычисления p-кривизны приспособлена для графиков функций (см. раздел 2.1), рассмотрим функцию вида

$$x_{n+1} = \sqrt{\sum_{i=1}^{n} a_i x_i^2 + b}, \quad a_i, b \in \mathbb{R}. \tag{3.1}$$

В зависимости от знаков a_i, b графиком этой функции может быть пустое множество, точка, полусфера, конус, но в большинстве случаев — верхняя половина гиперболоида. Для краткости будем называть поверхность (3.1) гиперболоидом.

Считаем, что поверхность (3.1) ориентирована нормалью, образующей острый угол с координатной осью x_{n+1}. Для вектора коэффициентов a_i используем обозначения (2.6), (1.2).

Область положительной m-кривизны гиперболоида (3.1) устроена следующим образом:

$$\Omega_m^+ = \left\{ x \in \mathbb{R}^n \colon b\,\sigma_m(a) + \sum_{i=1}^n a_i(a_i+1)x_i^2\sigma_m(a^{\langle i\rangle}) > 0 \right\}, \quad 1 \leqslant m \leqslant n.$$

Способ проверки m-выпуклости в этой области описан в разделе 1.5 и продемонстрирован при доказательстве критерия m-выпуклости параболоида (§ 2, теорема 2.3). Для гиперболоида таким же рассуждением удалось получить только достаточные условия m-выпуклости в области Ω_m^+.

Теорема 3.1. *Пусть $\Omega \subset \mathbb{R}^n$ — область определения и C^2-гладкости функции* (3.1), $1 \leqslant m \leqslant n$.

Для того чтобы гиперболоид (3.1) *с $b > 0$ являлся m-выпуклым в непустой области $\Omega_m^+ \cap \Omega$, достаточно выполнения условия*

$$a \in K_m. \tag{3.2}$$

Для того чтобы гиперболоид (3.1) *с $b \leqslant 0$ являлся m-выпуклым в непустой области $\Omega_m^+ \cap \Omega$, достаточно выполнения условия*

$$\exists\, i \colon a_i > 0, \quad a^{\langle i\rangle} \in K_m. \tag{3.3}$$

При $m = n$ условия (3.2), (3.3) *являются также необходимыми.*

Таким образом, условие m-выпуклости гиперболоида, как и параболоида, выражается в терминах принадлежности векторов a, $a^{\langle i\rangle}$ конусу K_m. Заметим, что требование (3.3) сильнее, чем (3.2).

Проанализируем требование (3.2) при $m = n$. Для гиперболоидов (3.1) с $b > 0$ условие $a \in K_n$ равносильно положительности всех коэффициентов a_i. Очевидно, что в этом и только в этом случае гиперболоид является n-выпуклым (строго выпуклым), причём всюду. Двумерная версия такого гиперболоида изображена на рис. 10*а*.

Требование (3.3) при $m = n$ не может быть выполнено, поскольку $\sigma_n(a^{\langle i\rangle}) \equiv 0$. Это соответствует тому, что гиперболоиды (3.1) с $b < 0$ и конусы ($b = 0$) не могут иметь точек n-выпуклости (строгой выпуклости), даже если все их коэффициенты a_i положительны.

Рассмотрим подробнее свойства поверхностей (3.1) с параметрами вида

$$b \leqslant 0, \quad a_i > 0, \quad i = 1, 2, \ldots, n. \tag{3.4}$$

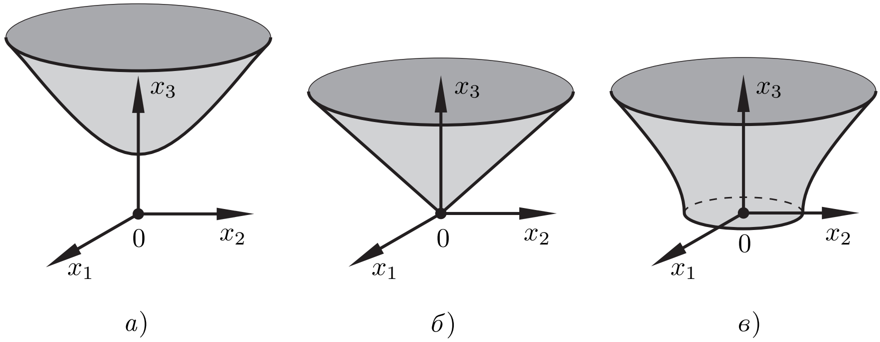


Рис. 10

Двумерные версии соответствующего конуса ($b = 0$) и гиперболоида ($b < 0$) изображены на рис. 10*б*, *в*. Согласно теореме 3.1 в этом случае гарантированно имеется m-выпуклость в области $\Omega_m^+ \cap \Omega$ при всех $m = 1, 2, \ldots, n-1$. Для конусов это означает $(n-1)$-выпуклость во всех точках, кроме вершины. Поясним, какова ситуация для гиперболоидов, на конкретном их представителе

$$x_{n+1} = \sqrt{\sum_{i=1}^{n} x_i^2 - 1}. \tag{3.5}$$

В этом случае $a = (1, 1, \ldots, 1)$ и прямые вычисления приводят к формуле

$$\Omega_m^+ = \left\{ x \in \mathbb{R}^n \colon 2 \sum_{i=1}^{n} C_{n-1}^m x_i^2 > C_n^m \right\}.$$

Для данного гиперболоида (3.5) области Ω_m^+ и Ω занимают части пространства, расположенные вне некоторых сфер. Сравнивая радиусы этих сфер, приходим к следующим выводам. Если $n/2 < m < n$, то m-выпуклой является только часть гиперболоида (3.5), расположенная выше плоскости

$$x_{n+1} = \sqrt{\frac{2m-n}{2n-2m}}.$$

При $m \leqslant n/2$ гиперболоид (3.5) является m-выпуклым во всех своих внутренних точках. В частности, двумерная версия гиперболоида (3.5), изображённая на рис. 10*в*, — 1-выпуклая поверхность во всех своих внутренних точках. Аналогичным образом можно получить условия тотальной m-выпуклости для остальных гиперболоидов с параметрами вида (3.4).

Замечание 3.2. При $b > 0$, $a_i < 0$, $i = 1, 2, \dots, n$, график функции (3.1) является верхней половиной сферы, которая ориентирована внешней (по отношению к сфере) нормалью. Нет ничего странного в том, что согласно теореме 3.1 такая поверхность не является n-выпуклой. Сферу, как и любую замкнутую поверхность, нужно ориентировать внутренней нормалью, чтобы она оказалась n-выпуклой (см. определение 1.6, замечание 1.7).

Список литературы

[1] *Ивочкина Н. М.* Задача Дирихле для уравнения кривизны порядка m // Алгебра и анализ. 1990. Т. 2, № 3. С. 192–217.

[2] *Ивочкина Н. М.* От конусов Гординга к p-выпуклым гиперповерхностям // Современная математика. Фундаментальные направления. 2012. Т. 45. С. 94–104.

[3] *Ивочкина Н. М., Ладыженская О. А.* Оценка вторых производных на границе для поверхностей, эволюционирующих под действием их главных кривизн // Алгебра и анализ. 1997. Т. 9, № 2. С. 30–50.

[4] *Ивочкина Н. М., Филимоненкова Н. В.* Геометрическиме модели в теории полностью нелинейных уравнений. Препринты Санкт-Петербургского математического общества. 2016. № 6.

[5] *Ивочкина Н. М., Филимоненкова Н. В.* О новых структурах в теории полностью нелинейных уравнений // Современная математика. Фундаментальные направления. 2015. Т. 58. С. 82–95.

[6] *Погорелов А. В.* Многомерная проблема Минковского. М.: Наука, 1975.

[7] *Филимоненкова Н. В., Бакусов П. А.* Гиперболические многочлены и конусы Гординга // Математическое просвещение. Сер. 3. Вып. 20. М.: МЦНМО, 2016. С. 143–166.

[8] *Caffarelli L., Nirenberg L., Spruck J.* Nonlinear second-order elliptic equations V. The Dirichlet problem for Weingarten hypersurfaces // Comm. Pure Appl. Math. 1988. V. 41, № 1. P. 47–70.

[9] *Caffarelly L., Nirenberg L., Spruck J.* The Dirichlet problem for nonlinear second order elliptic equations III. Functions of the eigenvalues of the Hessian // Acta Math. 1985. V. 155. P. 261–301.

[10] *Gårding L.* An inequality for hyperbolic polynomials // J. Math. Mech. 1959. V. 8. P. 957–965.

[11] *Ivochkina N. M.* Geometric evolution equations preserving convexity // AMS Transl. Ser. 2. Adv. Math. Sci. 2007. V. 220. P. 191–121.

[12] *Ivochkina N. M.* Symmetry and geometric evolution equations // Записки науч. сем. ПОМИ. 2004. Т. 318. С. 135–146.

[13] *Ivochkina N. M., Filimonenkova N. V.* On algebraic and geometric conditions in the theory of Hessian equations // J. Fixed Point Theory Appl. 2015. V. 16, № 1. P. 11–25.

[14] *Ivochkina N. M., Filimonenkova N. V.* On the backgrounds of the theory of m-Hessian equations // Comm. Pure Appl. Math. 2013. V. 12, № 4. P. 1687–1703.

[15] *Ivochkina N. M., Nehring Th., Tomi F.* Evolution of starshaped hypersurfaces by nonhomogeneous curvature functions // Алгебра и анализ. 2000. Т. 12, вып. 1. С. 185–203.

[16] *Ivochkina N. M., Prokof'eva S. I, Yakunina G. V.* The Gårding cones in the modern theory of fully nonlinear second order differential equations // J. Math. Sci. 2012. V. 184, № 3. P. 295–315.

[17] *Trudinger N. S.* The Dirichlet problem for the prescribed curvature equations // Arch. Rat. Mech. Anal. 1990. V. 111. P. 153–179.

[18] *Urbas J.* On the expansion of starshaped hypersurfaces by symmetric functions of their principal curvatures // Math. Z. 1990. V. 205, № 3. P. 355–372.

Надежда Викторовна Филимоненкова, Санкт-Петербургский политехнический университет Петра Великого

nf33@yandex.ru

Павел Анатольевич Бакусов, Санкт-Петербургский государственный архитектурно-строительный университет

bakusovpavel@gmail.com

Наш семинар: математические сюжеты

Неравенства С. Н. Бернштейна для тригонометрических многочленов

С. Б. Гашков, С. В. Кравцев

§ 1. Введение

Сначала сформулируем несколько задач.

Первая из них предлагалась на LXXVII Московской математической олимпиаде (2014 г., 11 класс, 2-й день, задача 2).

Задача 1. Найдите все такие a и b, что $|a|+|b| \geqslant 2/\sqrt{3}$ и при всех x выполнено неравенство $|a\sin x + b\sin 2x| \leqslant 1$.

Первоначальная формулировка была такова:

Задача 2. Доказать, что если при всех x выполнено неравенство

$$|b_1 \sin x + b_2 \sin 2x| \leqslant 1,$$

где b_i — постоянные коэффициенты, то $|b_1|+|b_2| \leqslant 2/\sqrt{3}$, причём равенство возможно, лишь когда $|b_1| = 4/\sqrt{27}$, $|b_2| = 2/\sqrt{27}$.

Задача 3. Если для многочлена $t(x) = b_1\sin x + b_2\sin 2x + b_3\sin 3x$ выполняются неравенства

$$\left|t\left(\tfrac{2\pi}{7}\right)\right| = \left|b_1\sin\frac{2\pi}{7} + b_2\sin\frac{4\pi}{7} + b_3\sin\frac{6\pi}{7}\right| \leqslant 1,$$
$$\left|t\left(\tfrac{4\pi}{7}\right)\right| = \left|b_1\sin\frac{4\pi}{7} - b_2\sin\frac{\pi}{7} - b_3\sin\frac{5\pi}{7}\right| \leqslant 1,$$
$$\left|t\left(\tfrac{6\pi}{7}\right)\right| = \left|b_1\sin\frac{6\pi}{7} - b_2\sin\frac{5\pi}{7} + b_3\sin\frac{4\pi}{7}\right| \leqslant 1,$$

то выполняется неравенство

$$|b_1| + |b_2| + |b_3| \leqslant \frac{6}{\sqrt{7}}.$$

Задача 4. Проверить, что многочлен

$$\frac{2\sqrt{7}}{7}\sin x + \frac{2\sqrt{7}}{7}\sin 2x - \frac{2\sqrt{7}}{7}\sin 3x$$

удовлетворяет неравенствам из предыдущей задачи и тем самым неравенство $|b_1| + |b_2| + |b_3| \leqslant 6/\sqrt{7}$ нельзя улучшить.

Можно добавить ещё несколько подобных задач, но ограничимся этими. Рекомендуем вам, прежде чем читать дальше, попробовать решить хотя бы одну из них.

Пусть n — простое число. Напомним следующее определение (и обозначение):

$\left(\dfrac{k}{n}\right) = 1$, если k равно остатку от деления квадрата некоторого целого числа на n;

$\left(\dfrac{k}{n}\right) = 0$, если k делится на n;

$\left(\dfrac{k}{n}\right) = -1$ в оставшихся случаях.

Так определённая величина $\left(\dfrac{k}{n}\right)$ называется *символом Лежандра*; числа k, для которых он равен 1, называются *квадратичными вычетами по модулю n*, а числа, для которых он равен -1, — *квадратичными невычетами по модулю n*.

Далее будут доказаны следующие замечательные (и незаслуженно мало известные) неравенства для суммы модулей коэффициентов тригонометрических многочленов, частные случаи которых были сформулированы выше.

Академик АН СССР
Сергей Натанович Бернштейн
(1880–1968)

Теорема 1 (С. Н. Бернштейн). *Пусть нечётный действительный тригонометрический многочлен*

$$t_n(x) = \sum_{k=1}^{n} b_k \sin kx$$

удовлетворяет неравенствам

$$\left|t_n\left(\frac{2\pi k}{2n+1}\right)\right| \leqslant 1, \quad k = 1, \ldots, n. \qquad (*)$$

Тогда

$$\sum_{k=1}^{n} |b_k| \leqslant \sqrt{2n+1} - \frac{1}{\sqrt{2n+1}}.$$

Неравенство обращается в равенство при нечётных n, *для которых* $p = 2n+1$ *— простое, и*

$$b_k = \frac{2}{\sqrt{2n+1}}\left(\frac{k}{2n+1}\right), \quad k = 1, \ldots, n.$$

Пусть чётный действительный тригонометрический многочлен

$$t_n(x) = \sum_{k=1}^{n} a_k \cos kx$$

удовлетворяет условию $t_n(0) = 0$ *и неравенствам* $(*)$. *Тогда*

$$\sum_{k=1}^{n} |a_k| \leqslant \sqrt{2n+1} - \frac{1}{\sqrt{2n+1}}.$$

Неравенство обращается в равенство при чётных n, *для которых* $p = 2n+1$ *— простое, и*

$$a_k = \frac{2}{\sqrt{2n+1}}\left(\frac{k}{2n+1}\right), \quad k = 1, \ldots, n.$$

Эти неравенства (а также ряд других) были найдены С. Н. Бернштейном чуть больше ста лет назад (см. [1]), причём в их доказательстве неожиданно оказались задействованы не самые тривиальные теоретико-числовые факты.

§ 2. Квадратичный закон взаимности

Напомним некоторые понятия. Если m — целое и $n > 1$ — натуральное число, то существуют единственные целые числа k и $0 \leqslant l < n$, для которых выполняется равенство $m = k \cdot n + l$. Число l в этом равенстве называется *остатком от деления* m на n.

Два целых числа a, b называются *сравнимыми по модулю натурального числа* $n > 1$ (что обозначается как $a \equiv b \pmod{n}$), если при делении на n они дают одинаковые остатки. Если все сравнимые между собой целые числа объединить в одно подмножество множества целых чисел, то получится n таких подмножеств, соответствующих остаткам $0, 1, 2, \ldots, n-1$. Перечислим несколько свойств *сравнений*.

Задача 5. Докажите, что если $a \equiv b \pmod{n}$ и $c \equiv d \pmod{n}$, то $a + c \equiv b + d \pmod{n}$, $a - c \equiv b - d \pmod{n}$, $ac \equiv bd \pmod{n}$.

Указание. Эти свойства вытекают из равенств

$$\begin{aligned} (b+d)-(a+c) &= (b-a)+(d-c),\\ (b-d)-(a-c) &= (b-a)-(d-c),\\ b\cdot d-a\cdot c &= (b-a)d+(d-c)a. \end{aligned}$$

Тем самым сравнимость чисел не нарушится, если к одному из них прибавить число, сравнимое с 0 по заданному модулю, а также если оба сравнимых числа умножить на одно и то же целое число или возвести их в одинаковую натуральную степень.

Из перечисленных свойств следует, что сравнение остаётся верным, если какое-либо его слагаемое перенести из одной части сравнения в другую с изменением знака на противоположный или если возвести обе части сравнения в одинаковую степень.

Задача 6. Докажите, что если $a_i \equiv b_i \pmod n$, $i = 0, 1, \ldots, m$, и $x \equiv y \pmod n$, то

$$a_m x^m + a_{m-1}x^{m-1} + \ldots + a_0 \equiv b_m y^m + b_{m-1}y^{m-1} + \ldots + b_0 \pmod n.$$

Указание. Применить предыдущую задачу.

Справедлива

Теорема 2 (квадратичный закон взаимности Эйлера — Гаусса). *Для простых чисел $p, q > 2$ справедливо тождество*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Иными словами, если хотя бы одно из чисел p, q при делении на 4 даёт остаток 1, то число p является квадратом по модулю числа q в точности тогда, когда число q является квадратом по модулю числа p. Если же оба числа p, q при делении на 4 дают остаток 3, то число p является квадратом по модулю числа q в точности тогда, когда число q не является квадратом по модулю числа p. В ходе доказательства понадобится несколько лемм, в которых везде a обозначает целое число, а p — простое число.

Лемма 1 (малая теорема Ферма). $a^p \equiv a \pmod p$.

Доказательство. Заметим, что[1] биномиальные коэффициенты

$$\binom{p}{k} = \frac{p(p-1)(p-2)\cdot\ldots\cdot(p-k+1)}{1\cdot 2\cdot 3\cdot\ldots\cdot k}, \quad k = 1, 2, \ldots, p-1,$$

[1] Биномиальные коэффициенты обозначаются также C_n^k.

делятся на p, поскольку множитель p в числителе дроби не может сократиться со знаменателем. Если теперь m, n — целые числа, то из предыдущего наблюдения и формулы бинома следует, что каждое слагаемое в правой части разложения

$$(m+n)^p - m^p - n^p = \binom{p}{1} m^{p-1} n^1 + \binom{p}{2} m^{p-2} n^2 + \ldots + \binom{p}{p-1} m^1 n^{p-1}$$

делится на p, поэтому и левая часть равенства делится на p. Точно так же делится на p число $(l+m+n)^p - l^p - m^p - n^p$, если l, m, n — целые числа. Чтобы убедиться в этом, достаточно применить предыдущее наблюдение к правой части записи

$$(l+m+n)^p - l^p - m^p - n^p = \\ = \big(((l+m)+n)^p - (l+m)^p - n^p\big) + ((l+m)^p - l^p - m^p).$$

Рассуждая аналогично, приходим к выводу, что выражение

$$\left(\sum_{i=1}^{n} a_i\right)^p - \sum_{i=1}^{n} a_i^p$$

всегда делится на p.

Утверждение леммы получается теперь, если взять в последнем сравнении все слагаемые равными 1, а n — равным a. $\square$

Следствие 1. *Если p не делит a, то после деления сравнения $a^p \equiv a \pmod p$ на a получится верное сравнение $a^{p-1} \equiv 1 \pmod p$, поскольку из условия $a \cdot (a^{p-1} - 1) = k \cdot p$ вытекает, что простое число p делит именно $a^{p-1} - 1$.*

Часто малую теорему Ферма формулируют так, как в этом следствии.

Сравнения вида

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \equiv 0 \pmod p, \quad a_n \neq 0,$$

называют *сравнениями степени n*.

Лемма 2. *Любое сравнение $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \equiv 0 \pmod p$ равносильно некоторому сравнению степени не выше $p-1$.*

Доказательство. Разделим многочлен $q(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ на двучлен $x^p - x$, в результате получим $q(x) = (x^p - x) f(x) + r(x)$, причём степень остатка $r(x)$ не превосходит $p-1$. По малой теореме Ферма верно сравнение $x^p - x \equiv 0 \pmod p$, поэтому исходное сравнение равносильно сравнению $r(x) \equiv 0 \pmod p$. $\square$

Лемма 3. *Если сравнение $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \equiv 0 \pmod p$ степени n имеет более n различных решений, то все коэффициенты $a_n, a_{n-1}, \ldots, a_0$ кратны p (и тогда сравнение тривиально, т. е. все целые числа являются его решениями).*

Доказательство. Если рассматриваемое сравнение имеет по меньшей мере $n+1$ различное решение $x_1, x_2, \ldots, x_{n+1}$, $0 \leqslant x_i < p$, то многочлен

$$q(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

можно записать в виде

$$\begin{aligned} q(x) = b_n(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1})(x-x_n) + \\ + b_{n-1}(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1}) + \\ + b_{n-2}(x-x_1)(x-x_2)\ldots(x-x_{n-2}) + \ldots + b_1(x-x_1) + b_0. \end{aligned}$$

В самом деле, достаточно положить $b_n = a_n$, затем взять коэффициент b_{n-1} равным коэффициенту при x^{n-1} в разности

$$q(x) - a_n(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1})(x-x_n),$$

после чего взять коэффициент b_{n-2} равным коэффициенту при x^{n-2} в разности

$$\begin{aligned} q(x) - a_n(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1})(x-x_n) - \\ - b_{n-1}(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1}) \end{aligned}$$

и т. д. Но тогда $0 \equiv q(x_1) = b_0 \pmod p$, т. е. p делит b_0,

$$0 \equiv q(x_2) = b_0 + b_1(x_2 - x_1) \equiv b_1(x_2 - x_1) \pmod p,$$

и тогда p делит b_1, поскольку $0 < |x_2 - x_1| < p$. Последовательно подставляя далее $x = x_3, x_4, \ldots, x_{n-1}$, убеждаемся, что все коэффициенты b_i, $i = 1, 2, \ldots, n$, делятся на p, но тогда и все коэффициенты многочлена $q(x)$ делятся на p, поскольку они являются суммами произведений чисел b_i, $i = 1, 2, \ldots, n$, и целых чисел. □

Следствие 2. *Всякое нетривиальное*[2)] *сравнение по модулю простого числа p равносильно сравнению степени не выше $p-1$ и имеет не более чем $p-1$ решение.*

Доказательство. Это непосредственно вытекает из лемм 2 и 3. □

[2)] То есть сравнение, для которого не все целые числа являются решениями.

Лемма 4 (критерий Эйлера). *Если $p>2$ — простое и a не кратно p, то*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p.$$

Доказательство. Согласно малой теореме Ферма $a^{p-1} \equiv 1 \pmod p$, что можно также переписать в виде

$$(a^{\frac{p-1}{2}} - 1) \cdot (a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod p.$$

Разность сомножителей в левой части последнего сравнения равна 2, поэтому только один из них делится на $p > 2$. Рассмотрим первый из двух возможных случаев: число a является квадратичным вычетом по модулю p, т. е. сравнение $a \equiv x^2 \pmod p$ имеет решение. Тогда то же самое решение имеет и сравнение $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$, которое получается из предыдущего сравнения почленным возведением в степень $\dfrac{p-1}{2}$ и применением малой теоремы Ферма. Осталось заметить, что сравнение $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ согласно следствию 10 не может иметь более $\dfrac{p-1}{2}$ решений, т. е. множество решений этого сравнения исчерпывается квадратичными вычетами. Тем самым все квадратичные невычеты удовлетворяют сравнению $a^{\frac{p-1}{2}} \equiv -1 \pmod p$. $\square$

Следующие две задачи пригодятся в дальнейшем.

Задача 7 (Эйлер — Лежандр). Доказать для простого числа n тождества

$$\left(\frac{k}{n}\right)\left(\frac{m}{n}\right) = \left(\frac{km}{n}\right), \quad \left(\frac{k}{n}\right)^2 = 1, \quad \left(\frac{k}{n}\right)\left(\frac{n-k}{n}\right) = \left(\frac{n-1}{n}\right).$$

Указание. Применить критерий Эйлера.

Задача 8 (Эйлер — Лежандр). Доказать для простого числа n вида $4l+3$ тождество

$$\left(\frac{k}{n}\right) = -\left(\frac{n-k}{n}\right),$$

а для простого числа n вида $4l+1$ доказать тождество

$$\left(\frac{k}{n}\right) = \left(\frac{n-k}{n}\right).$$

Указание. Применить критерий Эйлера.

Прежде чем сформулировать следующую лемму, введём необходимые дополнительные обозначения. Ранее уже говорилось, что если все целые числа, сравнимые между собой по модулю фиксированного числа n, объединить в одно подмножество множества целых чисел, то получится n таких подмножеств, соответствующих остаткам $0, 1, 2, \ldots, n-1$. Заметим, что эти остатки мы считали обозначениями получающихся подмножеств. Понятно, что можно ввести и иные обозначения для подмножеств чисел, сравнимых между собой по фиксированному модулю. Достаточно просто выбрать по одному числу из каждого такого подмножества и назначить выбранные числа обозначениями подмножеств. Выбранные числа образуют набор, который называется *полной системой вычетов по модулю* n.

Например, для сравнения по простому модулю $p > 2$ удобно выбрать в качестве набора обозначений классов сравнимых чисел набор

$$\left\{-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-3}{2}, \frac{p-1}{2}\right\}.$$

Такой выбор интересен тем, что из каждого подмножества был выбран его элемент, имеющий наименьшую абсолютную величину в этом подмножестве. Набор вычетов с указанным свойством называют набором *абсолютно наименьших вычетов*.

Обозначим символом Ω положительную часть этого набора:

$$\Omega = \left\{1, 2, \ldots, \frac{p-3}{2}, \frac{p-1}{2}\right\}.$$

Для произведения целого числа a и каждого $s \in \Omega$ найдём его абсолютно наименьший вычет по модулю p: $a \cdot s \equiv t_s \pmod p$, после чего положим $\varepsilon_s = 1$, если $t_s > 0$, и $\varepsilon_s = -1$, если $t_s < 0$. Будем также считать, что $t_s = \varepsilon_s \cdot r_s$, $r_s > 0$.

Если из полной системы вычетов по некоторому модулю n удалить все вычеты, которые имеют общий делитель, больший 1, с модулем сравнения, то оставшийся набор взаимно простых с модулем вычетов называется *приведённой системой вычетов*.

Число элементов в приведённой системе вычетов по модулю n равно количеству тех натуральных чисел из набора $1, 2, \ldots, n-1$, которые взаимно просты с n. Это число обозначается символом $\varphi(n)$, а φ называется *функцией Эйлера*. Из определения приведённой системы вычетов следует, что любые $\varphi(n)$ попарно не сравнимых по модулю n и взаимно простых с этим модулем целых чисел образуют приведённую систему вычетов по модулю n.

Лемма 5. *Если целое число a взаимно просто с модулем n и переменная x пробегает приведённую систему вычетов по модулю n, то произведение $a \cdot x$ также пробегает приведённую систему вычетов по этому модулю.*

Доказательство. Поскольку различные значения переменной x попарно несравнимы и взаимно просты, как и число a, с модулем, то и числа

ax будут попарно несравнимы и взаимно просты с модулем. Осталось заметить, что таких чисел ровно $\varphi(n)$. $\square$

Лемма 6 (лемма Гаусса). *Если $p > 2$ — простое, то* $\left(\frac{a}{p}\right) = \prod_{s\in\Omega} \varepsilon_s$.

Доказательство. Согласно лемме 5 множество чисел $\{\pm a\cdot s \mid s\in\Omega\}$ является приведённой системой вычетов по модулю p. Соответствующие абсолютно наименьшие вычеты составляют набор

$$\{\pm\varepsilon_s r_s \mid s\in\Omega\} = \Bigl\{-\varepsilon_1 r_1, \varepsilon_1 r_1, -\varepsilon_2 r_2, \varepsilon_2 r_2, -\varepsilon_3 r_3, \ldots, -\varepsilon_{\frac{p-1}{2}} r_{\frac{p-1}{2}}, \varepsilon_{\frac{p-1}{2}} r_{\frac{p-1}{2}}\Bigr\}.$$

Подмножество положительных вычетов из последнего набора, т. е. множество $\{r_1, r_2, \ldots, r_{\frac{p-1}{2}}\}$, совпадает с множеством чисел $1, 2, \ldots, \dfrac{p-1}{2}$, т. е. со множеством Ω. Перемножим теперь сравнения

$$a\cdot 1 \equiv \varepsilon_1 r_1 \pmod p,\quad a\cdot 2\equiv \varepsilon_2 r_2 \pmod p,\quad \ldots,$$
$$a\cdot\frac{p-1}{2} \equiv \varepsilon_{\frac{p-1}{2}} r_{\frac{p-1}{2}} \pmod p$$

и разделим обе части сравнения-произведения на число

$$1\cdot 2\cdot\ldots\cdot\frac{p-1}{2} = r_1 r_2\cdot\ldots\cdot r_{\frac{p-1}{2}}.$$

Получаем сравнение $a^{\frac{p-1}{2}} \equiv \varepsilon_1\varepsilon_2\ldots\varepsilon_{\frac{p-1}{2}} \pmod p$. Остаётся применить критерий Эйлера. $\square$

Лемма 7 (лемма Эйзенштейна). *Для каждого нечётного натурального числа $2n+1$ справедливо тождество*

$$\frac{\sin((2n+1)x)}{\sin x} = (-4)^n \prod_{1\leqslant k\leqslant n} \Bigl(\sin^2 x - \sin^2\frac{2\pi k}{2n+1}\Bigr).$$

Доказательство. Заметим, что

$$\sin((2n+1)x) = \operatorname{Im}((e^{ix})^{2n+1}) = \operatorname{Im}((\cos x + i\sin x)^{2n+1}).$$

Если в правой части этого равенства воспользоваться формулой бинома Ньютона, то мнимая единица появится только в тех слагаемых, которые будут содержать множитель $i\sin x$ в нечётной степени, и тогда множитель $\cos x$ будет присутствовать в таких слагаемых непременно в чётной степени, поскольку сумма степеней этих двух множителей всегда равна нечётному числу $2n+1$. Используя тождество $\cos^2 x = 1-\sin^2 x$, получаем, что левая часть доказываемого тождества — это многочлен степени n от функции $\sin^2 x$. Числа $\dfrac{2\pi k}{2n+1}$, $k = 1, 2, \ldots, n$, обращают левую часть тождества в 0, и их количество совпадает со степенью левой части как многочлена от $\sin^2 x$. Поэтому нулями многочлена в левой части доказываемого тождества являются числа $\sin^2 \dfrac{2\pi k}{2n+1}$, $k = 1, 2, \ldots, n$, и только они. Осталось проверить, что множитель перед произведением в правой части тождества выбран правильно. Для этого достаточно найти старший коэффициент многочлена относительно $\sin^2 x$ в левой его части. Старший коэффициент в правой части доказываемого тождества, очевидно, равен $(-4)^n$.

Чтобы не смешивать обозначения, положим $\sin x = t$. Многочлен в левой части перепишется в виде

$$\sum_{k=0}^{n}(-1)^k\binom{2n+1}{2k+1}t^{2k}(1-t^2)^{n-k}.$$

Его коэффициент при t^{2n} будет равен

$$(-1)^n\sum_{k=0}^{n}\binom{2n+1}{2k+1} = (-1)^n 2^{2n} = (-4)^n,$$

потому что в силу формулы бинома

$$\sum_{k=0}^{n}\binom{2n+1}{2k+1} - \sum_{k=0}^{n}\binom{2n+1}{2k} = (1-1)^{2n+1} = 0,$$

$$\sum_{k=0}^{2n+1}\binom{2n+1}{k} = (1+1)^{2n+1} = 2^{2n+1}. \qquad \square$$

Изложенное ниже доказательство[3)] закона взаимности содержится, например, в [2, с. 20–21].

По лемме 6 для двух простых чисел $p, q > 2$ справедливо тождество

$$\left(\frac{q}{p}\right) = \prod_{s\in\Omega}\varepsilon_s.$$

Используя обозначения из доказательства этой леммы, имеем $q\cdot s = \varepsilon_s r_s$, поэтому, используя нечётность синуса, получаем

$$\sin\frac{2\pi qs}{p} = \varepsilon_s\sin\frac{2\pi r_s}{p}.$$

Перемножая эти равенства для всех индексов s, имеем (с учётом биективности отображения $s\to r_s$)

$$\left(\frac{q}{p}\right) = \prod_{s\in\Omega}\varepsilon_s = \prod_{s\in\Omega}\left(\frac{\sin(2\pi qs/p)}{\sin(2\pi s/p)}\right).$$

3) Оно принадлежит ученику Гаусса Эйзенштейну.

Применяя лемму 7 к сомножителям правой части последнего тождества (для $2n+1=q$), получаем

$$\left(\frac{q}{p}\right)=\prod_{s\in\Omega}(-4)^{\frac{q-1}{2}}\prod_{1\leqslant k\leqslant\frac{q-1}{2}}\left(\sin^2\frac{2\pi s}{p}-\sin^2\frac{2\pi k}{q}\right)=$$

$$=(-4)^{\frac{(q-1)(p-1)}{4}}\prod_{1\leqslant k\leqslant\frac{q-1}{2},\, s\in\Omega}\left(\sin^2\frac{2\pi s}{p}-\sin^2\frac{2\pi k}{q}\right).$$

Меняя числа q и p ролями, точно так же получаем

$$\left(\frac{q}{p}\right)=(-4)^{\frac{(q-1)(p-1)}{4}}\prod_{1\leqslant k\leqslant\frac{q-1}{2},\, s\in\Omega}\left(\sin^2\frac{2\pi k}{q}-\sin^2\frac{2\pi s}{p}\right).$$

Осталось заметить, что соответствующие множители в правых частях двух последних тождеств противоположны по знаку, причём число этих множителей равно $\dfrac{(q-1)(p-1)}{4}$, поэтому

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)(-1)^{\frac{(q-1)(p-1)}{4}},$$

что и завершает доказательство. □

Для доказательства неравенств С. Н. Бернштейна понадобится несколько тригонометрических тождеств.

Задача 9. Докажите, что при $l<m$ справедливы тождества

$$\sum_{k=1}^{m}\sin\left(x+\frac{2\pi kl}{m}\right)=0=\sum_{k=1}^{m}\cos\left(x+\frac{2\pi kl}{m}\right).$$

Указание. Сумма векторов, выходящих из начала координат в точки на единичной окружности, образующие правильный n-угольник, равна нулю. Чтобы доказать этот факт, достаточно повернуть плоскость с изображёнными на ней векторами против часовой стрелки на угол $2\pi/m$. Если сумма рассматриваемых векторов ненулевая, то она тоже должна была бы повернуться на этот угол. С другой стороны, при таком повороте каждый вектор превратился в соседний вектор, т. е. набор векторов не изменился и сумма измениться не должна. Осталось заметить, что

$$\sum_{k=1}^{m}\cos\left(x+\frac{2\pi kl}{m}\right)+\sum_{k=1}^{m}i\sin\left(x+\frac{2\pi kl}{m}\right)=\sum_{k=1}^{m}e^{i(x+2\pi kl/m)},$$

а последняя сумма геометрически изображается как раз как сумма векторов, выходящих из начала координат в точки на единичной окружности, образующие правильный n-угольник.

Задача 10. Докажите, что при $l < m/2$ выполняются тождества

$$\sum_{k=1}^{m} \sin\Bigl(x + 2\frac{\pi kl}{m}\Bigr) \cos\Bigl(y + \frac{2\pi ks}{m}\Bigr) = 0 = \sum_{k=1}^{m} \sin\Bigl(x + \frac{2\pi kl}{m}\Bigr) \sin\Bigl(y + \frac{2\pi ks}{m}\Bigr),$$

$$\sum_{k=1}^{m} \cos\Bigl(x + \frac{2\pi kl}{m}\Bigr) \cos\Bigl(y + \frac{2\pi ks}{m}\Bigr) = 0,$$

$$\sum_{k=1}^{m} \cos^2\Bigl(x + \frac{2\pi kl}{m}\Bigr) = \frac{m}{2} = \sum_{k=1}^{m} \sin^2\Bigl(x + \frac{2\pi kl}{m}\Bigr).$$

Указание. Достаточно выразить каждое слагаемое вида

$$\cos(x + la)\sin(y + sa), \quad \cos(x + la)\cos(y + sa), \quad \sin(x + la)\sin(y + sa)$$

в виде линейной комбинации синусов или косинусов от $x + y + (l + s)a$ и $x - y + (l - s)a$, а каждый квадрат — через косинус двойного угла, и применить тождества задачи 9.

Задача 11. Докажите, что для каждого действительного тригонометрического многочлена

$$t_n(x) = \frac{a_0}{2} + \sum_{k=1}^{n} (a_k \cos kx + b_k \sin kx)$$

при $m > 2n$, $l \leqslant n$ справедливы тождества

$$\frac{1}{m} \sum_{k=1}^{m} t_n^2\Bigl(x + \frac{2\pi k}{m}\Bigr) = \frac{a_0^2}{4} + \sum_{k=1}^{n} \frac{a_k^2 + b_k^2}{2},$$

$$a_l = \frac{2}{m} \sum_{k=1}^{m} t_n\Bigl(\frac{2k\pi}{m}\Bigr) \cos\frac{2kl\pi}{m}, \quad b_l = \frac{2}{m} \sum_{k=1}^{m} t_n\Bigl(\frac{2k\pi}{m}\Bigr) \sin\frac{2kl\pi}{m}.$$

Указание. Применить тождества задачи 10.

Задача 12. Докажите, что при каждом натуральном $m \leqslant 2n$ справедливы тождества

$$\sum_{k=1}^{n} \cos\frac{2mk\pi}{2n+1} = -\frac{1}{2},$$

$$\sum_{k=1}^{n} \sin^2\frac{mk\pi}{2n+1} = \frac{2n+1}{4}, \quad \sum_{k=1}^{n} \cos^2\frac{mk\pi}{2n+1} = \frac{2n-1}{4}.$$

Указание. Первое из этих тождеств следует из второй строки тождеств в задаче 10 при $x = y = s = 0$, остальные два тождества следуют из первого, если применить формулы двойного угла.

Далее понадобится замечательное тригонометрическое тождество:

Теорема 3 (Гаусс). *При простом $n = 4m + 1$ и $l = 1, \ldots, n-1$*

$$\sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \cos \frac{2kl\pi}{n} = \pm\sqrt{n}, \quad \sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \sin \frac{2kl\pi}{n} = 0.$$

При простом $n = 4m + 3$ и $l = 1, \ldots, n-1$

$$\sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \sin \frac{2kl\pi}{n} = \pm\sqrt{n}, \quad \sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \cos \frac{2kl\pi}{n} = 0.$$

На самом деле Гаусс доказал более сильное утверждение: в правой части левых равенств можно заменить $\pm\sqrt{n}$ на $\sqrt{n}\left(\frac{l}{n}\right)$. Но доказательство сложно, а нас устроит более слабое утверждение.

Сначала докажем вспомогательные тождества, тоже найденные Гауссом.

Задача 13. При простом n и $l = 1, \ldots, n$

$$\sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \cos \frac{2kl\pi}{n} = \left(\frac{l}{n}\right) \sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \cos \frac{2k\pi}{n},$$

$$\sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \sin \frac{2kl\pi}{n} = \left(\frac{l}{n}\right) \sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \sin \frac{2k\pi}{n}.$$

Указание. При l, кратном n, обе части формул нулевые, так как $\left(\frac{l}{n}\right) = 0$ и $\sum_{k=1}^{n-1}\left(\frac{k}{n}\right) = 0$. Если l не кратно n, то

$$\left(\frac{l}{n}\right) \sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \cos \frac{2kl\pi}{n} = \sum_{k=1}^{n-1} \left(\frac{kl}{n}\right) \cos \frac{2kl\pi}{n} = \sum_{k=1}^{n-1} \left(\frac{k}{n}\right) \cos \frac{2k\pi}{n},$$

потому что остатки от деления kl на n при $k = 1, \ldots, n-1$ пробегают все числа от 1 до $n-1$ по одному разу. Для синуса доказательство аналогично.

Теперь всё готово для доказательства теоремы Гаусса. Удобно использовать комплексное обозначение $e^{i\varphi} = \cos\varphi + i\sin\varphi$ и тождества доказывать одновременно (равенство нулю в них легко проверить непосредственно). Эти тождества можно записать в компактном виде:

$$\sum_{k=1}^{n-1} \left(\frac{k}{n}\right) e^{2kl\pi i/n} = \pm\sqrt{n} \quad \text{при } n = 4m + 1$$

и

$$\sum_{k=1}^{n-1}\left(\frac{k}{n}\right)e^{2kl\pi i/n} = \pm i\sqrt{n} \quad \text{при } n = 4m+3,$$

или, в общем случае,

$$\left(\sum_{k=1}^{n-1}\left(\frac{k}{n}\right)e^{2kl\pi i/n}\right)^2 = n(-1)^{(n-1)/2}.$$

Далее будем использовать обозначение

$$g_l = \sum_{k=1}^{n-1}\left(\frac{k}{n}\right)e^{2kl\pi i/n}.$$

Из доказанных тригонометрических тождеств следует, что $g_0 = g_n = 0$ и при $0 < l < n$

$$g_l^2 = \left(\sum_{k=1}^{n-1}\left(\frac{k}{n}\right)e^{2kl\pi i/n}\right)^2 =: g^2 = \left(\sum_{k=1}^{n-1}\left(\frac{k}{n}\right)e^{2k\pi i/n}\right)^2.$$

Вычислим двумя способами сумму $\sum_{l=1}^{n} g_l g_{n-l}$. С одной стороны, согласно задаче 7,

$$g_l g_{n-l} = \left(\frac{l}{n}\right)\left(\frac{n-l}{n}\right)g^2 = \left(\frac{n-1}{n}\right)g^2, \quad g_0 = g_n = 0,$$

поэтому сумма равна $(n-1)(-1/n)g^2$. С другой стороны, непосредственно после раскрытия скобок имеем

$$g_l g_{n-l} = \sum_{k=1}^{n-1}\left(\frac{k}{n}\right)e^{2kl\pi i/n}\sum_{m=1}^{n-1}\left(\frac{m}{n}\right)e^{2m(n-l)\pi i/n} = \sum_{k,m=1}^{n-1}\left(\frac{k}{n}\right)\left(\frac{m}{n}\right)e^{2(k-m)l\pi i/n},$$

откуда

$$(n-1)\left(\frac{n-1}{n}\right)g^2 = \sum_{l=1}^{n} g_l g_{n-l} = \sum_{k,m=1}^{n-1}\left(\frac{k}{n}\right)\left(\frac{m}{n}\right) =$$

$$= \sum_{l=1}^{n} e^{2(k-m)l\pi i/n} = \sum_{k=1}^{n-1}\left(\frac{k}{n}\right)^2 n = \sum_{k=1}^{n-1} n = n(n-1),$$

и теорема Гаусса доказана. □

Задача 14. Докажите, что для любого набора действительных чисел $(b_1, b_2, \ldots, b_n)$ справедливо неравенство Коши:

$$|b_1| + |b_2| + \ldots + |b_n| \leqslant \sqrt{n(b_1^2 + b_2^2 + \ldots + b_n^2)}.$$

Это неравенство обращается в равенство тогда и только тогда, когда все числа $|b_i|$ равны.

Наконец мы можем доказать теорему С. Н. Бернштейна (см. с. 88). Напомним её формулировку.

Теорема. *Пусть нечётный действительный тригонометрический многочлен*

$$t_n(x) = \sum_{k=1}^{n} b_k \sin kx$$

удовлетворяет неравенствам

$$\left|t_n\Big(\frac{2\pi k}{2n+1}\Big)\right| \leqslant 1, \quad k = 1, \ldots, n. \tag{$*$}$$

Тогда

$$\sum_{k=1}^{n} |b_k| \leqslant \sqrt{2n+1} - \frac{1}{\sqrt{2n+1}}.$$

Неравенство обращается в равенство при нечётных n, для которых $p = 2n+1$ — простое, и

$$b_k = \frac{2}{\sqrt{2n+1}}\Big(\frac{k}{2n+1}\Big), \quad k = 1, \ldots, n.$$

Пусть чётный действительный тригонометрический многочлен

$$t_n(x) = \sum_{k=1}^{n} a_k \cos kx$$

удовлетворяет условию $t_n(0) = 0$ и неравенствам $(*)$. Тогда

$$\sum_{k=1}^{n} |a_k| \leqslant \sqrt{2n+1} - \frac{1}{\sqrt{2n+1}}.$$

Неравенство обращается в равенство при чётных n, для которых $p = 2n+1$ — простое, и

$$a_k = \frac{2}{\sqrt{2n+1}}\Big(\frac{k}{2n+1}\Big), \quad k = 1, \ldots, n.$$

Доказательство теоремы 1. Рассмотрим случай нечётного многочлена. Воспользуемся тождеством из задачи 11, в котором выберем $x = 0$, $m = 2n+1 > 2n$, и тогда

$$\sum_{k=1}^{2n+1} t_n^2\Big(\frac{2k\pi}{2n+1}\Big) = \frac{2n+1}{2} \sum_{k=1}^{n} b_k^2.$$

Заметим, что середина отрезка $\left[\dfrac{2k\pi}{2n+1}, \dfrac{2(2n+1-k)\pi}{2n+1}\right]$ находится в точке π, поэтому

$$t_n\Big(\frac{2k\pi}{2n+1}\Big) = -t_n\Big(\frac{2(2n+1-k)\pi}{2n+1}\Big)$$

в силу тождества $t_n(x)=-t_n(2\pi-x)$, справедливого для всех нечётных тригонометрических многочленов. Таким образом, верхнюю границу индекса суммирования в левой части написанного выше равенства можно понизить до n, если одновременно вдвое уменьшить его правую часть (слагаемое при $k = 2n+1$ равно нулю). Следовательно, имеем

$$\sum_{k=1}^{n} t_n\Big(\frac{2k\pi}{2n+1}\Big)^2 = \frac{2n+1}{4}\sum_{k=1}^{n} b_k^2.$$

С другой стороны, из условия теоремы следует, что все слагаемые левой части последнего равенства не превосходят единицы, поэтому их сумма не превосходит числа слагаемых. Тем самым доказано неравенство

$$\sum_{k=1}^{n} b_k^2 \leqslant \frac{4n}{2n+1}.$$

Чтобы получить выписанную в условии теоремы оценку для суммы модулей коэффициентов, воспользуемся неравенством Коши:

$$\sum_{k=1}^{n}|b_k| \leqslant \sqrt{n\sum_{k=1}^{n} b_k^2} \leqslant \sqrt{\frac{4n}{2n+1}}\sqrt{n} = \sqrt{2n+1} - \frac{1}{\sqrt{2n+1}},$$

и неравенство теоремы в случае нечётного тригонометрического многочлена доказано. Конечно, всё изящество этого результата проявится лишь тогда, когда мы докажем, что полученная оценка — точная, т. е. её уже не удастся улучшить, если рассматривать всё множество нечётных тригонометрических многочленов, удовлетворяющих условиям теоремы. Для этого понадобятся тождества Гаусса.

Сначала заметим, что для коэффициентов, удовлетворяющих условию

$$|b_k| = \frac{2}{\sqrt{2n+1}}, \quad k = 1, \ldots, n,$$

неравенство теоремы превращается в равенство. Остаётся для каждого числа n из множества, указанного в теореме, предъявить нечётный тригонометрический многочлен порядка n, коэффициенты которого удовлетворяют этому условию, а его значения — условию

$$\Big|t_n\Big(\frac{2\pi k}{2n+1}\Big)\Big| \leqslant 1, \quad k = 1, \ldots, n,$$

что и доказывает неулучшаемость полученных неравенств. И действительно, при простом $p = 2n + 1 = 4m + 3$ и

$$b_k = \frac{2}{\sqrt{2n+1}}\left(\frac{k}{2n+1}\right), \quad k = 1, \ldots, n,$$

из теоремы Гаусса получаем:

$$\sum_{k=1}^{n}\left(\frac{k}{2n+1}\right)\sin\left(\frac{2kl\pi}{2n+1}\right) = \pm\sqrt{\frac{2n+1}{4}};$$

отсюда для любого $l = 1, \ldots, n$

$$t_n\left(\frac{2l\pi}{n}\right) = \sum_{k=1}^{n} b_k \sin\left(\frac{2kl\pi}{2n+1}\right) = \frac{2}{\sqrt{2n+1}}\sum_{k=1}^{n}\left(\frac{k}{2n+1}\right)\sin\left(\frac{2kl\pi}{2n+1}\right) = \pm 1,$$

что и требовалось доказать. $\square$

Чётный случай аналогичен, и мы предлагаем читателю разобрать его самостоятельно, по аналогии с доказательством для нечётного тригонометрического многочлена.

Список литературы

[1] *Bernstein Serge.* Sur certaines fonctions périodiques qui s'écartent le moins possible de zéro // Сообщ. Харьковского математ. об-ва. Сер. 2. Т. 14. 1914. С. 145–152.

[2] *Серр Ж.-П.* Курс арифметики. М.: Мир, 1972.

Сергей Борисович Гашков, мехмат МГУ

`sbgashkov@gmail.com`

Сергей Владимирович Кравцев, мехмат МГУ

`svkrav@gmail.com`

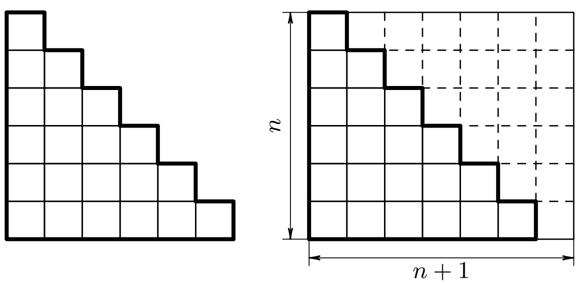
Алгебра, геометрия и анализ сумм степеней последовательных чисел

Г. А. Мерзон

Речь в этой статье пойдёт о вычислении суммы $1^k + 2^k + \ldots + n^k$. Обсудив, как найти формулу для любого конкретного k, мы попробуем по нескольким первым формулам угадать, какого рода должен быть общий ответ. После этого мы увидим, как различные точки зрения на нашу задачу — аналитическая, геометрическая, алгебраическая — объясняют различные замеченные закономерности. Будет получен и явный общий ответ в терминах чисел Бернулли (вместе с рецептом вычисления этих чисел). Частично текст основан на лекциях автора в летнем лагере московской 57-й школы в 2016 году.

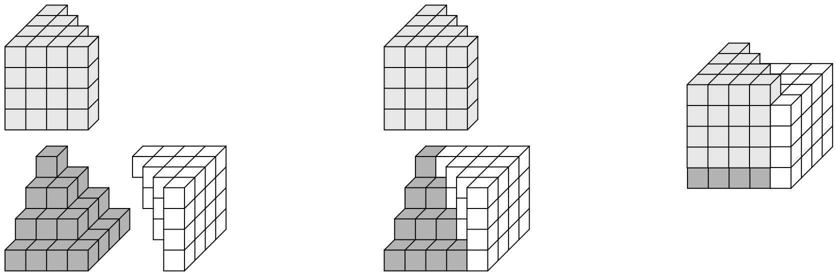
§ 1. Начало

При $k = 1$ речь идёт просто о сумме $1 + 2 + \ldots + n$. Наиболее наглядный, видимо, способ её вычислить — геометрический: об этой сумме можно думать как о *треугольном числе*, т. е. площади «пиксельного» (составленного из единичных квадратиков) равнобедренного прямоугольного «треугольника» со стороной n. Но из двух таких треугольников легко составить прямоугольник размера $n \times (n + 1)$, поэтому площадь «треугольника» равна $n(n + 1)/2$ (вдвое меньше площади прямоугольника).



Подобным образом можно вычислить и сумму $1^2 + 2^2 + \ldots + n^2$: её можно проинтерпретировать как площадь пирамиды, основание которой —

квадрат $n \times n$, а высота имеет длину n и попадает в вершину основания. Из шести таких пирамид можно сложить параллелепипед $n \times (n+1) \times (2n+1)$ (на рисунке ниже показано, как сложить половину этого параллелепипеда из трёх пирамид), поэтому искомая сумма равна $n(n+1)(2n+1)/6$.



Как работать с (многомерными) пирамидами в многомерном пространстве — не очень понятно (хотя мы ещё немного поговорим об этом в § 4), поэтому обратимся к алгебре.

Хорошо известно, что формулы типа

$$\begin{aligned} 1\ \ +2\ \ +\ldots+n\ \ &= \frac{n(n+1)}{2}; \\ 1^2+2^2+\ldots+n^2 &= \frac{n(n+1)(2n+1)}{6}; \\ 1^3+2^3+\ldots+n^3 &= \frac{n^2(n+1)^2}{4} \end{aligned}$$

несложно доказать по индукции, — но не очень понятно, как подобные формулы искать.

Самое общее, что можно сказать об ответе, глядя на случаи $k=1, 2, 3,$ — что это многочлен от n. В действительности так будет и дальше.

Теорема 1. $S_k(n) := 1^k+2^k+\ldots+n^k$ *— многочлен от n степени $k+1$. Вообще, если p — многочлен степени k, то $p(1)+p(2)+\ldots+p(n)$ — многочлен от n степени $k+1$.*

Каким должен быть многочлен P, чтобы можно было доказать индукцией по n, что $1^k+\ldots+n^k = P(n)$? База индукции — равенство $P(0)=0$. А утверждение шага индукции состоит в том, что

$$n^k = P(n) - P(n-1) =: \Delta P(n).$$

Доказать, что такой многочлен существует, можно двумя способами.

Доказательство 1. Любой многочлен является суммой мономов, поэтому достаточно доказать первую часть теоремы.

Условие $\Delta P(n) = n^k$ представляет собой систему уравнений на коэффициенты многочлена

$$P(n) = a_0 n^{k+1} + a_1 n^k + \ldots + a_k n.$$

А именно, в выражении $P(n) - P(n-1)$ после раскрытия скобок и приведения подобных коэффициент при n^k должен получиться равным 1, а коэффициенты при всех остальных степенях n — равными 0.

Так как

$$n^i - (n-1)^i = in^{i-1} + \ldots,$$

возникающие уравнения имеют вид (в квадратных скобках указано, коэффициенты при каких степенях n сравниваются):

$$\begin{array}{ll} [n^{k+1}]: & 0 = 0; \\ [n^{k}\quad]: & 1 = (k+1)a_0; \\ [n^{k-1}]: & 0 = ka_1 + (\ldots)\cdot a_0; \\ [n^{k-2}]: & 0 = (k-1)a_2 + (\ldots)\cdot a_1 + (\ldots)\cdot a_0; \\ \ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

Эта система имеет решение: последовательно находим коэффициенты a_0, a_1 и т. д. (из уравнения с правой частью $(k-i)a_{i+1} + \ldots$ видно, как выразить a_{i+1} через уже найденные коэффициенты с меньшими номерами). $\square$

Доказательство 2. Определённое выше Δ — линейное отображение из $(k+2)$-мерного пространства многочленов степени не выше $k+1$ в пространство многочленов степени не выше k. Его ядро одномерно ($\Delta P = 0 \Leftrightarrow P$ — константа). Поэтому его образ имеет размерность $(k+2)-1 = k+1$, а значит, совпадает со всем пространством многочленов степени не выше k. $\square$

Упражнение 1. Пользуясь теоремой 1, найдите формулу для суммы $1^4 + 2^4 + \ldots + n^4$.

Решить это упражнение можно даже двумя способами: можно воспользоваться *утверждением* теоремы и записать, что

$$S_4(n) = an^5 + bn^4 + cn^3 + dn^2 + en,$$

а неизвестные коэффициенты найти, подставляя небольшие n; но проще найти коэффициенты, посмотрев на первое *доказательство* теоремы.

Отметим, что хотя ответ можно записать в форме, напоминающей формулу для $S_2(n)$, он уже *не раскладывается на линейные множители*! Возможно поэтому формула для $S_4(n)$ была найдена примерно на 1000 лет позже, чем формула для $S_3(n)$, известная уже в античности.

§ 2. Эксперименты и гипотезы

Теперь в принципе понятно, как получить ответ для любого фиксированного k. Но хотелось бы понять, как связаны ответы для разных k (а в идеале — иметь и общую формулу, работающую для произвольного k).

Начнём с эксперимента. Выпишем уже известные нам формулы, но слегка в другой форме: так как ответ не раскладывается, вообще говоря, на линейные множители, будем записывать его просто как многочлен:

$$\begin{aligned}
S_1(n) &= \frac{1}{2}n^2 + \frac{1}{2}n;\\
S_2(n) &= \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n;\\
S_3(n) &= \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}n^2 + 0;\\
S_4(n) &= \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 + 0 - \frac{1}{30}n.
\end{aligned}$$

Некоторые закономерности сразу бросаются в глаза.

Гипотеза 1. *Старший член многочлена $S_k(n)$ равен $\frac{1}{k+1}n^{k+1}$, следующий равен $\frac{1}{2}n^k$.*

Кроме того, появились нулевые коэффициенты. Добавим в таблицу ещё несколько первых k.

$$\begin{aligned}
S_2(n) &= \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n;\\
S_3(n) &= \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}n^2 \ + 0;\\
S_4(n) &= \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 \ + 0 - \frac{1}{30}n;\\
S_5(n) &= \frac{1}{6}n^6 + \frac{1}{2}n^5 + \frac{5}{12}n^4 + 0 - \frac{1}{12}n^2 + 0;\\
S_6(n) &= \frac{1}{7}n^7 + \frac{1}{2}n^6 + \frac{1}{2}n^5 \ + 0 - \frac{1}{6}n^3 \ + 0 + \frac{1}{42}n;\\
S_7(n) &= \frac{1}{8}n^8 + \frac{1}{2}n^7 + \frac{7}{12}n^6 + 0 - \frac{7}{24}n^4 + 0 + \frac{1}{12}n^2 + 0.
\end{aligned}$$

Гипотеза 2. *После $\frac{1}{2}n^k$ каждый второй коэффициент (при n^{k-2}, n^{k-4}, …) равен нулю.*

Остальные коэффициенты выглядят довольно загадочно. Попробуем, тем не менее, разобраться. Как ведут себя коэффициенты при n^{k-1} ($1/6$, $1/4$, $1/3$, $5/12$) — сразу не видно, потому что все они записаны в виде несократимых дробей. Приведём их к общему знаменателю: $2/12$, $3/12$, $4/12$, $5/12$ — теперь закономерность очевидна, коэффициент равен $k/12$.

Дальше идёт коэффициент при n^{k-3}. После приведения к общему знаменателю получается последовательность $-4/120$, $-10/120$, $-20/120$, $-35/120$.

Упражнение 2. а) Угадайте формулу для коэффициента при n^{k-3} (если не получается, попробуйте найти числители $4, 10, 20, 35 \ldots$ в треугольнике Паскаля).

б) Придумайте формулу для коэффициента при n^{k-5}.

Если решить это упражнение, то станет ясно, какого рода должен быть ответ: коэффициент при n^{k-i} является, видимо, многочленом от k, и даже понятно, каким именно — но... только с точностью до мультипликативной константы. Эти константы ($1/12$, $-1/120$, $1/252$, $\ldots$) непосредственно связаны с *числами Бернулли* — но о них мы поговорим чуть позже.

Упражнение 3. Докажите, что

$$S_k(n) = \frac{1}{k+1}n^{k+1} + \frac{1}{2}n^k + \frac{k}{12}n^{k-1} + \ldots$$

(где многоточие заменяет члены меньшей степени по n).

Читатель, желающий как можно быстрее узнать доказательства гипотез и общий ответ, может пропустить следующие два параграфа (дальше их материал не используется).

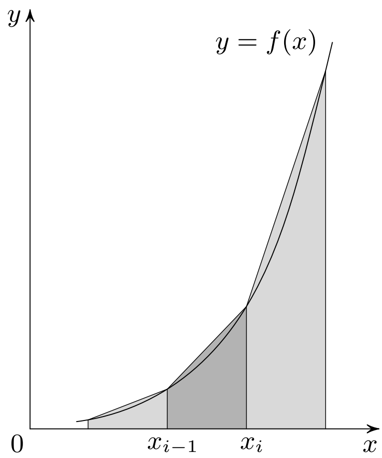
§ 3. Суммы и интегралы

Старший член многочлена $S_k(x)$, $\frac{1}{k+1}x^{k+1}$, должен вызывать немедленную ассоциацию: это как раз первообразная (интеграл) функции x^k, которую мы суммируем по целым точкам. Эту связь с интегрированием нетрудно и объяснить: коэффициент при старшем члене в многочлене $S_k(n)$ — это предел выражения

$$\frac{S_k(n)}{n^{k+1}} = \frac{1^k + 2^k + \ldots + n^k}{n^{k+1}} = \frac{1}{n}\cdot\left(\left(\frac{1}{n}\right)^k + \left(\frac{2}{n}\right)^k + \ldots + \left(\frac{n}{n}\right)^k\right),$$

т. е. предел интегральных сумм для интеграла $\int_0^1 x^k\,dx$.

На самом деле, используя подобные соображения, можно найти и следующий член, $\frac{1}{2}x^k$. Обычная интегральная сумма возникает, если приблизить площадь под графиком функции $f(x)$ суммой площадей прямоугольников со сторонами $1/n$ и $f(i/n)$. Но ясно, что точность приближения повысится, если заменить прямоугольники прямоугольными трапециями (как на рисунке ниже).



Для функции x^n это соответствует переходу от оценки

$$\int_0^1 x^k\,dx \approx \frac{1}{n}\cdot\left(\left(\frac{1}{n}\right)^k + \left(\frac{2}{n}\right)^k + \ldots + \left(\frac{n}{n}\right)^k\right)$$

к оценке

$$\int_0^1 x^k\,dx \approx \frac{1}{n}\cdot\left(\frac{(0/n)^k+(1/n)^k}{2} + \frac{(1/n)^k+(2/n)^k}{2} + \ldots + \frac{((n-1)/n)^k+(n/n)^k}{2}\right) =$$

$$= \frac{1}{n}\cdot\left(\left(\frac{1}{n}\right)^k + \left(\frac{2}{n}\right)^k + \ldots + \left(\frac{n}{n}\right)^k - \frac{1}{2}\left(\frac{n}{n}\right)^k\right),$$

откуда

$$\frac{1}{k+1} \approx \frac{S_k(n)}{n^{k+1}} - \frac{1}{2}\cdot\frac{1}{n}.$$

Величину ошибки, которая возникает при таком приближении, можно оценить.

Упражнение 4. а) Докажите *формулу трапеций*: если функция f бесконечно дифференцируема на отрезке $[a;b]$, то

$$\int_a^b f(x)\,dx = (b-a)\frac{f(a)+f(b)}{2} - \frac{1}{12}f''(\xi)(b-a)^3$$

для некоторой точки $\xi \in [a;b]$.

б) При помощи формулы трапеций и соображений, приведённых выше, докажите, что

$$S_k(n) = \frac{1}{k+1}n^{k+1} + \frac{1}{2}n^k + o(n^k).$$

На самом деле существует последовательность *квадратурных формул*, приближающих интегралы, которые дают всё более точные приближения для $S_k(n)$, — причём возникающие утверждения верны и для нецелых k.

Проиллюстрируем полезность формулы трапеций (и других квадратурных формул) ещё на одном примере.

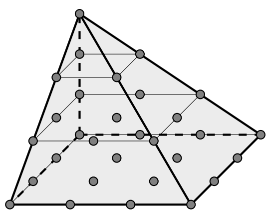
Упражнение 5. Докажите слабую форму *формулы Стирлинга*:

$$n! \sim C\sqrt{n}\left(\frac{n}{e}\right)^n.$$

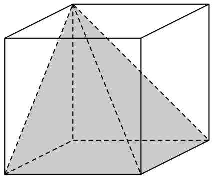
Её надо понимать в том смысле, что отношение левой и правой частей стремится к 1 для некоторой константы C. (*Указание*: примените формулу трапеций к интегралу функции $\ln x$.)

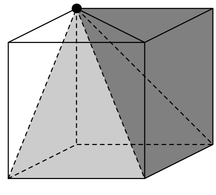
§ 4. Целые точки в многомерных многогранниках

Сказанное выше можно изложить и без интегралов, на геометрическом языке. Посмотрим, например, на сумму $S_2(n+1)$. Она выражает число целых точек в пирамиде с вершиной в точке $(0,0,n)$ и квадратным основанием с вершинами в точках $(0,0,0)$, $(n,0,0)$, $(0,n,0)$, $(n,n,0)$. Действительно, в плоскости $z=n-i$ лежит как раз $(i+1)^2$ целых точек этой пирамиды.



При больших n количество целых точек примерно равно объёму этой пирамиды. Но из трёх таких пирамид нетрудно сложить куб с ребром n: выберем одну вершину куба и соединим её с каждой из трёх не содержащих её граней. Поэтому объём одной пирамиды равен $\frac{1}{3}n^3$, а значит, $S_2(n+1) \approx \frac{1}{3}n^3$.





Аналогично $S_k(n+1)$ есть количество целых точек в $(k+1)$-мерной пирамиде высоты n с основанием в виде k-мерного куба со стороной n

(и высотой, попадающей в одну из вершин основания). Куб с ребром n разбивается на $k+1$ такую пирамиду: весь куб задаётся неравенствами $0 \leqslant x_i \leqslant n$, а j-я часть состоит из точек, для которых $\max\{x_1, \ldots, x_n\} = x_j$. Поэтому объём одной пирамиды (являющийся первым приближением для $S_k(n+1)$) равен $\frac{1}{k+1} n^{k+1}$.

(Разумеется, объём нашей пирамиды можно записать как интеграл функции x^k. А предыдущее рассуждение позволяет вычислить этот интеграл геометрически, не используя формулу Ньютона — Лейбница.)

Для данного k при всех n интересующие нас пирамиды получаются растяжением эталонной пирамиды с ребром 1 в n раз по всем измерениям. О том, как при гомотетии меняется количество целых точек внутри многогранника, говорит *теория Эрхарта.*

Теорема 2. (1) *Пусть P — некоторый k-мерный многогранник с вершинами в целых точках. Тогда количество $N(nP)$ целых точек внутри многогранника P, растянутого в n раз, зависит от n как многочлен степени k («многочлен Эрхарта»), причём старший коэффициент многочлена $N(nP)$ равен объёму многогранника P.*

(2) *Кроме того, имеет место* взаимность Эрхарта — Макдональда:

$$N(-nP) = (-1)^k I(nP),$$

где $I(\ldots)$ — количество целых точек строго внутри многогранника.

Вероятно, вторая половина теоремы требует комментария. Мы определяем $N(nP)$ как количество целых точек в некотором многограннике *только для целых положительных n*. Но раз это многочлен от n, можно формально подставлять в него и отрицательные аргументы. Смысл получающихся значений и объясняет вторая часть теоремы.

Упражнение 6. Выведите из теоремы *формулу Пика*: площадь многоугольника на клетчатой бумаге с вершинами в узлах сетки равна $i + \frac{b}{2} - 1$, где i — число вершин строго внутри многоугольника, а b — на его границе.

Теорему 2 можно рассматривать как многомерный аналог формулы Пика. О формуле Пика можно прочитать в популярной статье [3]; из неё же можно узнать, как доказать первую часть теоремы 2 для многоугольников и трёхмерных многогранников. Здесь доказывать эту теорему мы не будем. Вместо этого применим её к нашей $(k+1)$-мерной пирамиде.

Целые точки внутри этой пирамиды суть целые точки в пирамиде такого же вида, но меньшего размера: действительно, целые точки строго внутри квадрата со стороной n суть целые точки в квадрате со стороной $n-2$, а кроме того, основание внутренней пирамиды находится «на этаж выше» основания внешней пирамиды. Следовательно, $I((n+1)P) = N((n-2)P)$. Напомним ещё, что $S_k(m) = N((m-1)P)$. Поэтому взаимность Эрхарта — Макдональда даёт связь между значениями многочлена S_k в отрицательных и неотрицательных целых числах:

$$S_k(-n) = N((-n-1)P) = (-1)^{k+1} I((n+1)P) = \\ = (-1)^{k+1} N((n-2)P) = (-1)^{k+1} S_k(n-1).$$

На самом деле получившееся равенство $S_k(-n) = (-1)^{k+1} S_k(n-1)$ несложно доказать чисто алгебраически. Об этом пойдёт речь в следующем параграфе.

Упражнение 7. Из соотношения $S_k(-n) = (-1)^{k+1} S_k(n-1)$ выведите, что в многочлене $S_k(n)$ после коэффициента $1/2$ при n^k каждый второй коэффициент равен 0.

В качестве последней иллюстрации теории Эрхарта (уже не связанной непосредственно с суммированием степеней) рассмотрим k-мерный *симплекс* $0 \leqslant x_1 \leqslant x_2 \leqslant \ldots \leqslant x_k \leqslant 1$ (для $k = 2$ это треугольник, для $k = 3$ — тетраэдр).

По теореме 2 функция $I((n+1)P)$ является многочленом от n. Этот многочлен читателю отлично известен: целые точки строго внутри многогранника суть наборы целых чисел, удовлетворяющие условию $0 < x_1 < x_2 < \ldots < x_k < n+1$, т. е. k-элементные подмножества n-элементного множества. Таким образом,

$$I((n+1)P) = \binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{k!}.$$

Посмотрим теперь на многочлен $N((n-1)P)$. Его значение даёт количество наборов целых чисел с условием $0 \leqslant x_1 \leqslant x_2 \leqslant \ldots \leqslant x_k \leqslant n-1$, т. е. количество k-элементных подмножеств *с повторениями* в n-элементном множестве. А в силу взаимности Эрхарта

$$N((n-1)P) = (-1)^k I((1-n)P) = \\ = (-1)^k \binom{-n}{k} = \frac{n(n+1)\ldots(n+k-1)}{k!} = \binom{n+k-1}{k}.$$

Разумеется, количество подмножеств с повторениями можно найти и при помощи несложных комбинаторных соображений, но теория Эрхарта даёт общий взгляд на разные утверждения такого рода.

Тем, кого эта теория заинтересовала, рекомендуем книгу [5] (в частности, в ней можно найти доказательство теоремы 2).

§ 5. Коммутирующие операторы

Вернёмся на шаг назад. Мы выяснили, что если продифференцировать старший член многочлена $S_k(x)$, то получится функция, которую мы суммируем, т. е. x^k. А что будет, если продифференцировать остальные члены?

Посмотрим на два следующих члена:

$$\left(\frac{1}{2}x^k\right)' = k\frac{1}{2}x^{k-1}, \quad \left(k\frac{1}{12}x^{k-1}\right)' = k(k-1)\frac{1}{12}x^{k-2}.$$

В обоих случаях получается соответствующий член для многочлена $S_{k-1}(x)$, только умноженный на k. То же, кстати, можно сказать и про старший член.

Гипотеза 3. *Производная многочлена S_k равна многочлену kS_{k-1}.*

Внимательный читатель заметил уже, вероятно, что буквально такая гипотеза верна быть не может: $S_k(0)=0$, но ненулевой свободный член регулярно возникает при дифференцировании многочленов S_k (при $k=2, 4, \ldots$). Однако *с точностью до свободного члена* гипотеза, как нетрудно проверить, для всех найденных многочленов выполняется.

Гипотеза 3′. $S_k' = kS_{k-1} + \mathrm{const}$.

На самом деле, это утверждение становится почти очевидным, если говорить не об отдельных многочленах, а об операторах, действующих на множестве многочленов.

Обозначим символом Σ «оператор суммирования», переводящий многочлен P в такой многочлен $\Sigma[P]$, что

$$(\Sigma[P])(n) = P(1) + P(2) + \ldots + P(n).$$

Напомним (см. § 1), что он определяется двумя условиями[1]:

$$(\Sigma[P])(0) = 0; \qquad (*)$$

$$\Delta\Sigma[P] = P. \qquad (**)$$

Таким образом, оператор суммирования Σ соотносится с оператором разностной производной Δ примерно так же, как (определённый) интеграл соотносится с дифференцированием.

Наша гипотеза состояла в том, что $D\Sigma[x^k] = \Sigma D[x^k] + \mathrm{const}$, где D — оператор дифференцирования.

Лемма 1. *Операторы D и Σ «коммутируют с точностью до констант»: $D\Sigma[P] - \Sigma D[P] = \mathrm{const}$ (где константа своя для каждого многочлена P).*

[1] Напомним также, что $(\Delta[P])(n) = P(n) - P(n-1)$.

Доказательство. Как отмечено выше, Σ — это почти обратная к Δ операция. Но уже ясно, что оператор Δ коммутирует с D. Действительно,

$$D\Delta[f] = [f(x) - f(x-1)]' = f'(x) - f'(x-1) = \Delta D[f].$$

Отсюда $\Delta D\Sigma = D\Delta\Sigma = D$, и из уравнения $(**)$ для P' получаем $\Delta D\Sigma = \Delta\Sigma D$, откуда следует утверждение леммы. □

В частности, взяв $P(x) = x^k$, мы получаем, что гипотеза $3'$ верна.

Предложение 1. *$S_k(x)' = kS_{k-1}(x) + B_k^*$ для некоторой константы B_k^*.*

С помощью этого предложения можно, зная многочлен S_{k-1}, найти многочлен S_k: взять первообразную многочлена S_{k-1} с нулевым свободным членом, умножить на k, а потом прибавить $B_k^* x$, где константу B_k^* нужно выбрать из условия $S_k(1) = 1$.

Отсюда немедленно следует доказательство возникавшей в упражнении 2 гипотезы о том, как меняются коэффициенты многочленов S_k при изменении k.

Предложение 2. *Коэффициент при n^{k+1-i} в многочлене $S_k(n)$ имеет вид*

$$B_i^* \cdot \frac{k(k-1)\dots(k+2-i)}{i!}.$$

Осталось объяснить, почему примерно половина этих коэффициентов обращается в нуль, другими словами, почему функция $S_k(x) = \Sigma x^k$ является почти чётной/нечётной (в зависимости от чётности k). Конечно, это связано просто с чётностью/нечётностью функции x^k.

Обозначим символом T оператор, переводящий функцию $f(x)$ в функцию $f(-x)$. Функция f чётна, если $Tf = f$, и нечётна, если $Tf = -f$. Поэтому, чтобы выяснить, что происходит с чётной/нечётной функцией при применении оператора Σ, нужно выяснить, как связаны операторы ΣT и $T\Sigma$.

Как показывает доказательство леммы 1, для этого полезно выяснить, как связаны операторы $T\Delta$ и ΔT, т. е. сравнить выражения

$$T\Delta[P] = P(-x) - P(-x-1);$$
$$\Delta T[P] = P(-x) - P(-(x-1)) = -(P(-x+1) - P(-x)).$$

Предложение 3. *Если $T[P] = \pm P$, то соответственно*

$$(\Sigma[P])(-x) = \mp(\Sigma[P])(x-1).$$

Доказательство (в духе доказательства леммы 1) оставляется читателю. Одно следствие полученного утверждения мы видели в упражнении 7: $B^*_{2k+1} = 0$ при $k \neq 0$. Ещё одним следствием является следующая *теорема Фаульхабера.*

Упражнение 8. Выведите из предложения 3, что

- $S_{2k-1}(n)$ является многочленом степени k от $u := n(n+1)/2$;
- $S_{2k}(n)$ имеет вид $(2n+1) \cdot$ (многочлен степени k от u).

(Например, $S_3(n) = u^2$, $S_2(n) = (2n+1)u/6$.)

§ 6. Числа Бернулли и символические манипуляции

Итак, мы получили формулу для сумм степеней:

$$S_k(n) = \frac{1}{k+1}n^{k+1} + \frac{1}{2}n^k + \ldots + B^*_i \cdot \frac{k(k-1)\ldots(k+2-i)}{i!} \cdot n^{k+1-i} + \ldots + B^*_k n,$$

а коэффициенты B^*_k можно вычислять последовательно из соотношения $S_k(1) = 1$.

Эти коэффициенты — почти числа Бернулли B_k, а конкретнее $B_1 = -B^*_1$, $B_k = B^*_k$ при $k > 1$. Другими словами, числа Бернулли B_k играют роль, аналогичную числам B^*_k при суммировании степеней не до n^k, а до $(n-1)^k$:

$$S_k(n-1) = \frac{1}{k+1}n^{k+1} - \frac{1}{2}n^k + \ldots + B_i \cdot \frac{k(k-1)\ldots(k+2-i)}{i!} \cdot n^{k+1-i} + \ldots + B_k n.$$

В таблице приведены несколько первых чисел Бернулли. Отметим, что дальше числа $|B_{2n}|$ быстро растут (примерно как факториалы).

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
B_n	1	$-\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$	0	$\frac{5}{66}$	0	$-\frac{691}{2730}$	0	$\frac{7}{6}$

Компактно записать (и запомнить) получающиеся формулы можно следующим образом. Заметим, во-первых, что

$$\frac{k(k-1)\ldots(k+2-i)}{i!} = \frac{1}{k+1}\binom{k+1}{i},$$

поэтому

$$S_k(n-1) = \frac{1}{k+1}\Big(n^{k+1} + (k+1)B_1 n^k + \ldots + \\ + \binom{n+1-i}{i} B_i n^{k+1-i} + \ldots + (k+1)B_k n\Big)$$

и получается выражение, напоминающее бином Ньютона. Чтобы сделать сходство более явным, будем писать у чисел Бернулли индекс не снизу, а сверху:

$$S_k(n-1) = \frac{1}{k+1}\Big(n^{k+1} + (k+1)B^1 n^k + \ldots + \\ + \binom{n+1-i}{i} B^i n^{k+1-i} + \ldots + (k+1)B^k n\Big).$$

Наконец, проигнорируем то, что в записи B^i число i является индексом, а не показателем степени, и запишем полученный нами ответ в следующем виде.

Теорема 3. $S_k(n-1) = \dfrac{(B+n)^{k+1} - B^{k+1}}{k+1}$.

Можно считать эту запись в духе *теневого исчисления*[2)] просто способом запомнить правильную формулу — получающуюся, если раскрыть скобки, а затем заменить i-ю степень формального символа B на i-е число Бернулли.

При $n=1$ получается компактная форма записи рекурренты для чисел Бернулли.

Предложение 4. $(B+1)^{k+1} - B^{k+1} = 0$ (*при* $k > 0$).

Если в этой формуле раскрыть скобки, то B_{k+1} сократится и останется равенство, выражающее B_k через числа Бернулли с меньшими номерами:

$$B_k = -\sum_{i<k} \binom{k+1}{i} \frac{B_i}{k+1}.$$

Упражнение 9. Докажите *формулу Эйлера — Маклорена* для многочленов: если многочлен F — первообразная многочлена f, то

$$f(0) + \ldots + f(n-1) = F(B+n) - F(B) =: \int\limits_0^n f(x+B)\,dx.$$

В заключение приведём ещё одну совсем уж загадочную манипуляцию с символом B. Подставим формально в последнее равенство $f(n) = q^n$ (игнорируя тот факт, что это не многочлен). Получим ещё одно выражение для суммы геометрической прогрессии:

$$\frac{q^n-1}{q-1} = 1 + \ldots + q^{n-1} = \frac{q^{B+n} - q^B}{\ln q} = \frac{q^n-1}{\ln q} q^B,$$

откуда $q^B = \dfrac{\ln q}{q-1}$. Чтобы избавиться от логарифма, сделаем замену $q = e^s$. Получим следующее равенство.

---

2) Кое-что о теневом исчислении можно узнать из гл. 5 книги [4].

Предложение 5. $e^{sB} = \dfrac{s}{e^s - 1}$.

Понимать это следует как равенство формальных степенных рядов. А именно, экспонента e^t — это ряд

$$1 + t + \frac{t^2}{2!} + \frac{t^3}{3!} + \ldots,$$

в правой части стоит результат деления (если угодно, «в столбик») двух рядов,

$$\frac{s}{s + \frac{1}{2}s^2 + \frac{1}{6}s^3 + \frac{1}{24}s^4 + \ldots} = 1 - \frac{1}{2}s + \frac{1}{12}s^2 + 0 \cdot s^3 + \ldots,$$

а в левой части — ряд

$$1 + B_1 s + \frac{B_2}{2!}s^2 + \frac{B_3}{3!}s^3 + \ldots,$$

и утверждается, что коэффициенты при всех степенях s в обеих частях равны.

Упражнение 10. Докажите предложение 5: выведите из рекурренты для чисел Бернулли равенство формальных рядов

$$\Big(\sum \frac{B_i}{i!} s^i\Big)(e^s - 1) = s.$$

Обычно равенство из предложения 5, наоборот, считается *определением* чисел Бернулли, и в более стандартном (и, в определённом смысле, концептуально более правильном) способе получения формулы для $S_k(n)$ и формулы Эйлера — Маклорена числа Бернулли сразу возникают именно как коэффициенты такого ряда (см., например, книгу [2]).

§ 7. Значения дзета-функции

Числа Бернулли возникают в разных задачах теории чисел, комбинаторики, алгебраической топологии... Здесь мы приведём (без доказательства) ещё только один пример — тоже связанный с вычислением некоторой суммы k-х степеней.

Напомним, что для $s > 1$ *дзета-функция Римана* $\zeta(s)$ определяется как сумма ряда

$$1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots$$

Например, хорошо известно, что

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \ldots = \frac{\pi^2}{6}.$$

На самом деле, это частный случай следующего утверждения (элементарное доказательство можно найти в гл. 7 книги [1]).

Теорема 4. *$\zeta(2k) = (-1)^{k+1}\dfrac{(2\pi)^{2k}}{2(2k)!}B_{2k}$ для целых положительных k.*

Кроме того, хотя бесконечные суммы $1^k + 2^k + \ldots$ очевидным образом расходятся, существует некоторый канонический способ аналитически продолжить функцию $\zeta(s)$ на $s < 1$, и для $s = -k$ получается совсем простая формула (ср. с формулой $\dfrac{(B+n)^{k+1} - B_{k+1}}{k+1}$ для конечной суммы k-х степеней).

Теорема 5. *$\zeta(-k) = -\dfrac{B^*_{k+1}}{k+1}$ для целых неотрицательных k.*

Благодарности

Автор благодарит А. И. Сгибнева за обсуждение различных тем, близких к задаче о сумме степеней, и за многочисленные замечания к предыдущим версиям текста, а также Г. Б. Шабата — и за полезные обсуждения, и за возможность поучаствовать в работе Клуба экспериментальной математики (всё это, несомненно, повлияло на данный текст).

Список литературы

[1] *Айгнер М., Циглер Г.* Доказательства из Книги. Лучшие доказательства со времён Евклида до наших дней. М.: Бином, 2015.

[2] *Грэхем Р., Кнут Д., Паташник О.* Конкретная математика. Основание информатики. М.: Мир, 1998.

[3] *Кушниренко А.* Целые точки в многоугольниках и многогранниках // Квант. 1977. № 4. С. 13–20.

[4] *Ландо С. К.* Введение в дискретную математику. М.: МЦНМО, 2014.

[5] *Beck M., Robins S.* Computing the Continuous Discretely: Integer-point Enumeration in Polyhedra. New York: Springer, 2007.

Григорий Александрович Мерзон, МЦНМО

merzon@mccme.ru

Теорема Абъянкара — Моха — Судзуки

Л. Г. Макар-Лиманов

Эта заметка содержит полное доказательство Теоремы Абъянкара — Моха — Судзуки (АМС-теоремы, см. «Математическое просвещение», вып. 12, задача 11). Доказательство основано на новом алгоритме для нахождения алгебраической зависимости двух многочленов от одной переменной. Для понимания заметки не требуется знаний, выходящих за рамки школьной программы.

§ 1. Введение

АМС-теорема характеризует пары многочленов от одной переменной, через которые можно выразить саму переменную.

Вот её точная формулировка (для рациональных коэффициентов).

Теорема АМС. *Пусть f и g — два многочлена с рациональными коэффициентами степеней n и m от переменной z, и пусть существует такой многочлен Q от двух переменных, что $Q(f, g) = z$. Тогда бо́льшая степень делится на меньшую степень без остатка.*

Многочлены с рациональными коэффициентами мы рассматриваем для простоты. Более опытный читатель заметит, что коэффициенты могут быть взяты из любого поля характеристики нуль и даже из поля конечной характеристики.

Интересна история доказательства этой теоремы. Первое доказательство опубликовал в 1956 году известный итальянский математик Беньямино Сегре [1]. Затем в 1970 году появилась работа двух мексиканских математиков Игнасио Канальса и Эмилио Льюиса Риеры [2], указывающая на ошибки в работе Сегре и предлагающая новое доказательство. Наконец, в 1975 году была опубликована статья двух американских математиков Шрирама Шанкара Абъянкара и Тцуонг-Тсиенга Моха [3], в которой и доказательство Сегре, и доказательство Канальса и Льюиса Риеры характеризовались как совершенно ошибочные.

Доказательство Абъянкара и Моха состояло из объёмистой подготовительной статьи, написанной в 1971 году и опубликованной в двух частях в 1973 году [4], и уже упомянутой основной статьи [3], окончательный вариант которой был написан в 1973 году.

Тем временем молодой японский математик Масакадзу Судзуки, узнав о работе Абъянкара и Моха, написал в 1972 году статью [5], содержащую доказательство. (Это его первая опубликованная статья, появившаяся в печати в 1974 году.) В сноске к статье он упоминает, что ему известно о результате Абъянкара (видимо, он не слышал, что Мох является соавтором), и, оправдывая свою работу, справедливо замечает, что подходы к доказательству совершенно различны. Действительно, его подход — это подход геометра, а подход Абъянкара и Моха чисто алгебраический.

Любопытно, что, упоминая AMC-теорему в своих статьях и выступлениях, Абъянкар зачастую называл её леммой для старшеклассников (high school lemma). После доказательств Абъянкара, Моха и Судзуки появилось не меньше дюжины доказательств AMC-теоремы. Некоторые из них занимают пять-шесть страниц. Правда, чтобы их понять, читатель должен знать намного больше, чем старшеклассник. Автор надеется, что доказательство в этой заметке будет доступно старшеклассникам, интересующимся математикой.

§ 2. Неприводимая зависимость двух многочленов

Возьмём два многочлена f и g от одной переменной z степеней n и m соответственно. Мы хотим проверить, зависимы ли они, т. е. существует ли такой ненулевой многочлен $P(x, y)$ от двух переменных, что $P(f, g) = 0$.

Для натурального числа l рассмотрим все многочлены вида $y^l + R_l$, где $\deg_y(R_l) < l$. Может случиться, что среди них есть многочлен $P(x, y)$, для которого $P(f, g) = 0$, и тогда f и g зависимы. Если $g^l + R_l(f, g)$ не равно нулю для любого R_l, то $\deg_z(g^l + R_l(f, g))$ — натуральное число. (Если $\deg_z(g^l + R_l(f, g)) = 0$ для какого-то $R_l(f, g)$, то $g^l + R_l(f, g)$ — рациональное число и, вычитая его, мы получим многочлен с нулевым значением.) В этом случае выберем тот многочлен Q_l, у которого $\deg_z(Q_l(f, g))$ минимальна. Многочлен Q_l существует, поскольку любое непустое множество натуральных чисел содержит наименьшее число. Обозначим степень этого многочлена через e_l.

Допустим, что $e_a - e_b$ делится на n для некоторых положительных целых чисел a и b и что $a > b$. Тогда $e_a < e_b$. Действительно, если $e_a \geqslant e_b$, то, поскольку $n = \deg(f)$, можно подобрать неотрицательное целое число j и рациональный коэффициент c так, что

$$\deg_y\bigl(Q_a(f, g) - cf^j Q_b(f, g)\bigr) < \deg_z(Q_a(f, g))$$

вопреки определению Q_a.

Теперь мы можем получить противоречие, если для всех l многочлен Q_l определён, т. е. если зависимость вида $y^l + R_l$ не существует. Если поделить целое число на n с остатком, то остаток должен быть одним из чисел $0, 1, \ldots, n-1$. Поэтому все e_l можно распределить по n классам, в каждом из которых остатки e_l при делении на n одинаковы. Поскольку в каждом из этих классов числа убывают с ростом l, каждый класс может содержать лишь конечное число элементов. Поэтому Q_l может существовать только для конечного числа l. Следовательно, для всякого достаточно большого l зависимость вида $y^l + R_l(x, y)$, где $g^l + R_l(f, g) = 0$, существует.

Найдём зависимость Q такого вида с минимальным l. Можно найти, конечно, и зависимость

$$P = p_0(x)y^k + p_1(x)y^{k-1} + \ldots + p_k(x)$$

с минимальной степенью по y, но она может задаваться многочленом, у которого ведущий коэффициент p_0 не равен единице, а является многочленом от x ненулевой степени. Кроме минимальности k мы можем предположить, что коэффициенты p_i не имеют общего делителя, иначе на него можно было бы сократить. На самом деле после сокращения получаем $P = Q$, и мы в этом сейчас убедимся.

Разумеется, k не может быть больше l. Если $k = l$, то $P = p_0 Q$, поскольку $P - p_0 Q$ — тоже зависимость и $\deg_y(P - p_0 Q) < k$. В этом случае $P = Q$, поскольку коэффициенты многочлена P не имеют общего делителя.

Если $l > k$, заменим многочлен Q на $Q_1 = p_0 Q - y^{l-k} P$. Многочлен Q_1 — тоже зависимость между f и g, если $Q_1 \neq 0$. В этом случае степень Q_1 по y не меньше k, поскольку зависимостей меньшей степени не существует. Заменим Q_1 на $Q_2 = p_0 Q_1 - r_1 y^{l_1 - k} P$, где $l_1 = \deg_y(Q_1)$, а многочлен $r_1(x)$ подобран так, чтобы ведущие коэффициенты $p_0 Q_1$ и $r_1 y^{l_1-k} P$ совпадали. Если результат не нуль, проделаем ещё один шаг, и т. д. По построению $\deg_y(Q_{i+1}) < \deg_y(Q_i)$. Поскольку все Q_i являются зависимостями, через несколько шагов будет получено $Q_j = 0$.

Многочлены Q_i можно выразить через P и Q: $Q_i = s_i(x)Q - S_i(x, y)P$. Следовательно, $0 = Q_j = s_j(x)Q - S_j(x, y)P$ и $s_j(x)Q = S_j(x, y)P$. Если коэффициенты S_j как многочлена от y имеют общий делитель $d(x)$, то, поскольку ведущий коэффициент многочлена Q равен единице, s_j делится на $d(x)$ и на него можно сократить. В результате мы получим $s(x)Q = S(x, y)P$, где общие делители коэффициентов многочленов P, Q и S равны 1.

Многочлен s является произведением ведущих коэффициентов S и P как многочленов от y и поэтому делится на p_0. Если $p_0 = q_1 q_2$, где степени многочленов q_1, q_2 положительны, то мы проверим, разлагаются ли многочлены q_1 и q_2 подобным образом, и продолжим разложение p_0 на множители с положительными степенями, пока это возможно. Поскольку сумма степеней всех множителей равна степени p_0, процесс разложения остановится и мы получим разложение p_0 в произведение неразложимых далее многочленов. Такие многочлены называются неприводимыми. Это разложение подобно разложению целого числа на простые множители.

Возьмём один из сомножителей этого разложения — многочлен q. Он делит p_0 и может делить и другие коэффициенты p_i. Однако он не может делить все коэффициенты, поскольку их общий делитель — единица. Среди не делящихся коэффициентов выберем коэффициент p_j при наибольшей степени y и поступим аналогично с

$$S = \sum_{i=0}^{r} s_i(x)y^{r-i}$$

— выберем коэффициент s_l, не делящийся на q, при наибольшей возможной степени y.

В произведении P и S рассмотрим коэффициент $\sum_{a+b=j+l} p_a s_b$ при $y^{k+r-j-l}$. Все слагаемые $p_a s_b$, кроме $p_j s_l$, делятся на q, так как либо $j < a$, либо $l < b$ и либо p_a, либо s_b делится на q. Поскольку $SP = sQ$, многочлен $\sum_{a+b=j+l} p_a s_b$ делится на s и тоже должен делиться на q. (Как вы помните, s делится на p_0.) Поэтому $p_j s_l$ тоже делится на q.

Таким образом, произведение двух многочленов от x, не делящихся на неприводимый многочлен q, делится на q. Осталось привести это к противоречию.

Допустим, что такая ситуация возможна, и найдём неприводимый многочлен ρ минимальной степени, для которого это происходит. Для него, в свою очередь, найдём два многочлена τ_1 и τ_2, не делящиеся на него, с делящимся произведением: $\tau_1\tau_2 = \rho\sigma$ и с минимальной возможной суммой степеней. Степени многочленов τ_1, τ_2 меньше $\deg_x(\rho)$, поскольку иначе можно, скажем, τ_1 поделить с остатком на ρ и представить в виде $\tau_1 = \alpha\rho + \tau_3$, где $\deg_x(\tau_3) < \deg_x(\rho)$. Но тогда ρ делит $\tau_3\tau_2$, поскольку

$$\rho\sigma = \tau_1\tau_2 = (\alpha\rho + \tau_3)\tau_2 = \alpha\rho\tau_2 + \tau_3\tau_2.$$

Многочлен σ имеет положительную степень, так как иначе $\rho = (\sigma^{-1}\tau_1)\tau_2$, а ρ — неприводимый многочлен, и

$$\deg_x(\sigma) = \deg_x(\tau_1\tau_2) - \deg_x(\rho) < \deg_x(\rho).$$

Разложим многочлен σ на неприводимые множители так же, как мы разложили многочлен p_0. Возьмём один из этих множителей σ_1. Поскольку

$\deg_x(\sigma_1) < \deg_x(\rho)$, либо τ_1, либо τ_2 делится на многочлен σ_1 и его можно сократить в равенстве $\rho\sigma = \tau_1\tau_2$. Это и приводит нас к противоречию: сумма степеней многочленов τ_1, τ_2 не была минимальной.

Итак, мы убедились, что многочлен p_0 должен иметь нулевую степень и потому существует минимальная зависимость

$$P = y^k + p_1(x)y^{k-1} + \ldots + p_k(x)$$

многочленов f и g с ведущим коэффициентом 1. Понятно, что любая зависимость получается из минимальной умножением на многочлен от x и y.

В следующем параграфе мы научимся её находить.

§ 3. Алгоритм для нахождения зависимости

Вначале неформально опишем процедуру получения многочлена P.

Найдём минимальное a, для которого степень g^a делится на степень f, а затем многочлен $g^a - cf^b$, где рациональное число c и неотрицательное целое число b подобраны так, что $\deg_z(g^a - cf^b) < \deg_z(g^a)$. Затем, если существует такой моном $f^i g^j$, что $\deg_z(f^i g^j) = \deg_z(g^a - cf^b)$, возьмём $g^a - cf^b - c_1 f^i g^j$, где рациональное число c_1 подобрано так, что

$$\deg_z(g^a - cf^b - c_1 f^i g^j) < \deg_z(g^a - cf^b).$$

Уменьшим степень результата, если найдётся подходящий моном, и так до тех пор, пока не получим многочлен h, степень которого не может быть уменьшена.

Если $h = 0$, мы получили зависимость. Если $h \neq 0$, найдём минимальное a', при котором для $h^{a'}$ существует моном $f^i g^j$ с такой же степенью, как у $h^{a'}$. Затем уменьшим эту степень, вычтя $cf^i g^j$ из $h^{a'}$. Продолжим уменьшение степени, вычитая мономы от f, g и h, пока не получим многочлен h', степень которого не может быть уменьшена, и т. д. После нескольких таких шагов мы получим зависимость.

Посмотрим, как это работает, на примере $f = z^4$, $g = z^6 - z$. Нужно начать с $g^2 - f^3 = -2z^7 + z^2$, так что $h = -2z^7 + z^2$. Далее получаем $h^2 - 4f^2 g = z^4$, $h^2 - 4f^2 g - f = 0$, так что $h^2 - 4f^2 g - f = (g^2 - f^3)^2 - 4f^2 g - f$ — это зависимость, которую мы ищем.

Дадим теперь формальное описание алгоритма.

Формальное описание

Первый шаг. Положим $g_0 = g$, $m_0 = \deg_z(g_0)$, $n = \deg_z(f)$. Найдём наибольший общий делитель d_0 чисел n и m_0. Затем найдём $a_0 = n/d_0$, $b_0 = m_0/d_0$.

Тогда $\deg_z(g_0^{a_0}) = \deg_z(f^{b_0})$ и a_0 — минимальное положительное число, для которого $\deg_z(g_0^{a_0})$ делится на n. Найдём $k_0 \in \mathbb{Q}$, для которого $m_{0,1} = \deg_z(g_0^{a_0} - k_0 f^{b_0}) < \deg_z(g_0^{a_0})$. Если $m_{0,1}$ делится на d_0, найдём моном $f^i g_0^{j_0}$ (где $i, j_0 \in \mathbb{Z}$, $0 \leqslant j_0 < a_0$), для которого $\deg_z(f^i g_0^{j_0}) = m_{0,1}$, а также $k_1 \in \mathbb{Q}$, для которого $m_{0,2} = \deg_z(g_0^{a_0} - k_0 f^{b_0} - k_1 f^i g_0^{j_0}) < m_{0,1}$, и т. д.

Если после конечного числа уменьшений степени мы получим нуль, зависимость получена и мы останавливаем алгоритм.

Если после конечного числа уменьшений степени мы получим $m_{0,i}$, не делящееся на d_0, обозначим соответствующий многочлен g_1 и перейдём к следующему шагу.

Как показано ниже, алгоритм всегда останавливается после конечного числа шагов.

Общий шаг. Допустим, что после s шагов мы получили $g_0, \ldots, g_s$. Положим $m_i = \deg_z(g_i)$. Найдём наибольший общий делитель d_i чисел $n, m_0, \ldots, m_i$. Число d_i положительно, хотя про числа m_i это не ясно. Положим $d_{-1} = n$ и $a_i = d_{i-1}/d_i$ для $0 \leqslant i \leqslant s$. (Легко видеть, что $a_s m_s$ делится на d_{s-1} и что a_s — наименьшее положительное число, обладающее этим свойством.) Моном $\mathbf{m} = f^i g_0^{j_0} \ldots g_s^{j_s}$, где $i, j_0, \ldots, j_s \in \mathbb{Z}$ и $0 \leqslant j_k < a_k$ при $k = 0, \ldots, s$, назовём *s-стандартным.* Найдём $(s-1)$-стандартный моном $\mathbf{m}_{s,0}$, у которого $\deg_z(\mathbf{m}_{s,0}) = a_s m_s$, а также найдём $c_0 \in \mathbb{Q}$, для которого $m_{s,1} = \deg_z(g_s^{a_s} - c_0 \mathbf{m}_{s,0}) < a_s m_s$. Если $m_{s,1}$ делится на d_s, найдём s-стандартный моном $\mathbf{m}_{s,1}$, у которого $\deg_z(\mathbf{m}_{s,1}) = m_{s,1}$, а также найдём $c_1 \in \mathbb{Q}$, для которого $m_{s,2} = \deg_z(g_s^{a_s} - c_0 \mathbf{m}_{s,0} - c_1 \mathbf{m}_{s,1}) < m_{s,1}$, и т. д. (Мы проверим в лемме 1, что любое число, делящееся на d_s, является степенью s-стандартного монома.)

Если после конечного числа уменьшений степени мы получим нуль, зависимость получена и мы останавливаем алгоритм.

Если после конечного числа уменьшений степени мы получим $m_{s,i}$, не делящееся на d_s, обозначим соответствующий многочлен g_{s+1} и перейдём к следующему шагу.

Как показано ниже, алгоритм всегда останавливается после конечного числа шагов.

Замечание. Если g_{i+1} найдено, то $d_{i+1} = (d_i, m_{i+1}) < d_i$, поскольку m_{i+1} не делится на d_i; следовательно, $d_0 > d_1 > \ldots > d_s$.

Если алгоритм нашёл g_i, то g_i — это многочлен от f, g и, возможно, от f^{-1}, поскольку мы пока не знаем, что стандартные мономы не содержат отрицательных степеней f. (В случае поля рациональных чисел и любого поля характеристики нуль отрицательные степени не появляются и мы это докажем.)

Для выражений вида $h = \sum_{i=0}^{k} g_i g^i$, $k \geqslant 0$, где $g_i = \sum_{j=-a}^{b} f^j$, $a \geqslant 0$, $b \geqslant 0$, мы будем использовать следующие четыре функции. Во-первых, степени $\deg_f(h)$, $\deg_g(h)$ относительно f и g, причём $\deg_f(h)$ может оказаться отрицательной, и степень $\deg_z(h)$ относительно z (выражение $h(f(z), g(z))$ можно записать как $\dfrac{h_0(f(z), g(z))}{h_1(f(z), g(z))}$, где h_0 и h_1 являются многочленами,

$$\deg_z(h) = \deg_z(h_0(f(z), g(z)) - \deg_z(h_1(f(z), g(z))).$$

Эти три функции обладают обычными свойствами степени. Четвёртая функция, pow_f, определена только для стандартных мономов:

$$\mathrm{pow}_f(f^i g_0^{j_0} \dots g_s^{j_s}) = i.$$

Эта функция не является степенной, поскольку произведение двух стандартных мономов может не быть стандартным мономом: например, степень g_0 может стать слишком большой в произведении.

Выражения вида $\sum_{j=-a}^{b} f_j f^j$, $a \geqslant 0$, $b \geqslant 0$, $f_j \in \mathbb{Q}$, называются многочленами Лорана. Таким образом, h — это многочлен от g с коэффициентами — многочленами Лорана от f.

Лемма 1. *Если элементы $g_0, g_1, \dots, g_s$ определены, то*:

(а) *для любого $a \in \mathbb{Z}$, делящегося на $d_s = (n, m_0, \dots, m_s)$, существует единственный s-стандартный моном $\mathbf{m}$, у которого $\deg_z(\mathbf{m}) = a$*;

(б) *для $t \leqslant s$ имеем $\deg_g(g_t) = \prod_{i=0}^{t-1} a_i$ и g_t является многочленом от g с ведущим коэффициентом единица*;

(в) *для любого целого неотрицательного числа $d < a_s \deg_g(g_s)$ существует единственный s-стандартный моном $\mathbf{m}$, у которого $\deg_g(\mathbf{m}) = d$, $\mathrm{pow}_f(\mathbf{m}) = 0$.*

Доказательство. В этом доказательстве мы дважды используем так называемый принцип Дирихле: если есть два конечных множества A и B с одинаковым количеством элементов ($|A| = |B|$) и функция из A в B (определённая на всём A), отображающая разные элементы A в разные элементы B, то в каждый элемент B отображён какой-то элемент A.

(а) Если $\deg_z(\mu) - \deg_z(\nu)$ делится на n и $\mathrm{pow}_f(\mu) = \mathrm{pow}_f(\nu) = 0$ для s-стандартных мономов $\mu = g_0^{j_0} \dots g_s^{j_s}$ и $\nu = g_0^{i_0} \dots g_s^{i_s}$, то $\mu = \nu$. Действительно, если $\sum_{k=0}^{s} j_k m_k - \sum_{k=0}^{s} i_k m_k$ делится на n, то $j_s m_s - i_s m_s$ делится на d_{s-1} (поскольку $n = \deg_z(f)$, а d_{s-1} — наибольший общий делитель $n, m_0, \dots, m_{s-1}$). Таким образом, $(j_s - i_s)m_s$ делится на d_{s-1}, в то время как $-a_s < j_s - i_s < a_s$, поскольку $0 \leqslant i_s, j_s < a_s$. Поэтому $j_s - i_s = 0$, так как по определению a_s — наименьшее целое положительное число, для которого

$a_s m_s$ делится на d_{s-1}. Значит, $j_s = i_s$, и мы можем аналогично проверить, что $j_{s-1} = i_{s-1}$, $j_{s-2} = i_{s-2}$, ..., $j_0 = i_0$.

Имеется в точности

$$\prod_{k=0}^{s} a_k = \frac{d_{-1}}{d_s} = \frac{n}{d_s}$$

различных s-стандартных мономов μ_i, у которых $\operatorname{pow}_f(\mu_i) = 0$. Их степени по z дают, как только что доказано, разные остатки при делении на n и делятся на d_s. Поскольку таких остатков тоже n/d_s, по принципу Дирихле для любого такого остатка найдётся соответствующий моном. Поэтому для любого целого числа l, делящегося на d_s, найдётся ровно один такой s-стандартный моном μ, $\operatorname{pow}_f(\mu) = 0$, что n делит $l - \deg_z(\mu)$. Домножив его на f в подходящей степени, найдём единственный s-стандартный моном ν, для которого $\deg_z(\nu) = l$.

(б) Проверим по индукции, что $\deg_g(g_t) = \prod_{i=0}^{t-1} a_i$ и что g_t — многочлен от g с ведущим коэффициентом единица. База индукции очевидна, поскольку $g_0 = g$. Предположим, что $\deg_g(g_k) = \prod_{i=0}^{k-1} a_i$ для всех $k < t+1$. Тогда у t-стандартного монома $\mathbf{m} = g_0^{j_0} \ldots g_t^{j_t}$ степень равна

$$\begin{aligned}
\deg_g(\mathbf{m}) &= \sum_{l=0}^{t} j_l \deg_g(g_l) \leqslant \sum_{l=0}^{t} (a_l - 1) \deg_g(g_l) = \\
&= \sum_{l=0}^{t-1} (\deg_g(g_{l+1}) - \deg_g(g_l)) + (a_t - 1) \deg_g(g_t) = \\
&= \deg_g(g_t) - 1 + (a_t - 1) \deg_g(g_t) = a_t \deg_g(g_t) - 1.
\end{aligned}$$

Следовательно, $\deg_g(\mathbf{m}) \leqslant a_t \deg_g(g_t) - 1$. По определению

$$g_{t+1} = g_t^{a_t} - r_t(f, g_0, \ldots, g_t).$$

Поскольку все мономы из r_t являются t-стандартными,

$$\deg_g(r_t) \leqslant a_t \deg_g(g_t) - 1$$

и g_{t+1} — многочлен степени

$$\deg_g(g_{t+1}) = \deg_g(g_t^{a_t}) = a_t \prod_{i=0}^{t-1} a_i = \prod_{i=0}^{t} a_i$$

с ведущим коэффициентом единица.

(в) Если $\deg_g(\mu) = \deg_g(\nu)$ и $\mathrm{pow}_f(\mu) = \mathrm{pow}_f(\nu)$ для s-стандартных мономов μ и ν, то $\mu = \nu$. Действительно,

$$\deg_g(\mu) = \sum_{k=0}^{s} j_k \deg_g(g_k), \quad \deg_g(\nu) = \sum_{k=0}^{s} i_k \deg_g(g_k).$$

В каждой сумме все слагаемые, кроме i_0 и j_0, заведомо делятся на a_0. Из $\deg_g(\mu) = \deg_g(\nu)$ следует, что $j_0 - i_0$ делится на a_0, откуда $j_0 = i_0$, поскольку $0 \leqslant j_0 < a_0$ и $0 \leqslant i_0 < a_0$. После этого мы можем доказать, что $j_1 = i_1$, поскольку $j_0 = i_0$ влечёт делимость $j_1 - i_1$ на a_1, и т. д.

Есть в точности $\prod_{k=0}^{s} a_k = a_s \deg_g(g_s)$ различных s-стандартных мономов μ_i, у которых $\mathrm{pow}_f(\mu_i) = 0$. Как мы убедились в п. (б), ровно столько же есть возможностей для степеней s-стандартных мономов по g, поскольку для s-стандартного монома $\deg_g(\mu) < a_s \deg_g(g_s)$. Поэтому по принципу Дирихле для любого d, удовлетворяющего условию $0 \leqslant d < a_s \deg_g(g_s)$, существует единственный s-стандартный моном $\mathbf{m}$, у которого $\deg_g(\mathbf{m}) = d$, $\mathrm{pow}_f(\mathbf{m}) = 0$. $\square$

Замечание. Таким образом, стандартный моном $\mathbf{m} = f^i g_0^{j_0} \ldots g_s^{j_s}$ полностью определяется величинами $i = \mathrm{pow}_f(\mathbf{m})$ и $\deg_g(\mathbf{m})$.

Лемма 2. *На каждом шаге алгоритм останавливается после конечного числа уменьшений степени.*

Доказательство. Во втором параграфе мы убедились в том, что существует неприводимая зависимость между f и g, заданная многочленом P степени k по g, у которого ведущий коэффициент — единица. Допустим, что $k < a_s \deg_g(g_s)$. Тогда P можно выразить суммой стандартных s-мономов, у которых $\mathrm{pow}_f = 0$, с коэффициентами — многочленами Лорана. Действительно, согласно лемме 1 для любого целого неотрицательного числа $d < a_s \deg_g(g_s)$ существует единственный s-стандартный моном $\mathbf{m}$, у которого $\deg_g(\mathbf{m}) = d$, $\mathrm{pow}_f(\mathbf{m}) = 0$ (пункт (в)), а согласно пункту (б) его ведущий коэффициент — единица. Найдём стандартный моном $\mathbf{m_1}$, $\mathrm{pow}_f(\mathbf{m_1}) = 0$, имеющий степень k по g. Тогда $\deg_g(P(f,g) - \mathbf{m_1}) < k$ и $P(f,g) - \mathbf{m_1}$ — многочлен от g с коэффициентами — многочленами Лорана от f. Найдём теперь стандартный моном $\mathbf{m_2}$, $\mathrm{pow}_f(\mathbf{m_2}) = 0$, для которого $\deg_g(\mathbf{m_2}) = \deg_g(P(f,g) - \mathbf{m_1})$, и такой многочлен Лорана c_2 от f, что $\deg_g(P(f,g) - \mathbf{m_1} - c_2\mathbf{m_2}) < \deg_g(P(f,g) - \mathbf{m_1})$. Продолжим понижение степени, вычитая соответствующие стандартные мономы, имеющие $\mathrm{pow}_f = 0$, с коэффициентами — многочленами Лорана от f. В конце мы получим многочлен нулевой степени, являющийся многочленом Лорана. Поскольку 1 — тоже стандартный моном, мы получим обещанное представление $P=\sum_i c_i\mathbf{m_i}$. Но тогда $P(f,g)\neq 0$, поскольку по лемме 1(a) величины $\deg_z(\mathbf{m_i})$ дают различные остатки при делении на $n=\deg_z(f)$. Поэтому различные слагаемые $c_i\mathbf{m_i}$ имеют разные степени по z и их сумма не может быть нулём. Следовательно, $k\geqslant a_s\deg_g(g_s)$.

Если $k=a_s\deg_g(g_s)$, то $\deg_g(P-g_s^{a_s})<k$ и $P-g_s^{a_s}=\sum_i(c_i\mathbf{m_i})$. В этом случае алгоритм выдаст нуль.

Если $k>a_s\deg_g(g_s)$, рассмотрим выражения вида $c_0g_s^{a_s}-\sum_i c_i\mathbf{m_i}$, где c_i — многочлены от f, подобранные так, что $c_0g_s^{a_s}-\sum_i c_i\mathbf{m_i}$ принадлежат $\mathbb{Q}[f,g]$, т. е. не содержат отрицательных степеней f. Назовём такие выражения допустимыми. Поскольку k — это степень минимальной зависимости, $\deg_z(c_0g_s^{a_s}-\sum_i c_i\mathbf{m_i})\neq 0$, если хотя бы один из многочленов c_i ненулевой.

Предположим, что $\deg_z(c_0g_s^{a_s}-\sum_i c_i\mathbf{m_i})$ делится на d_s для всех допустимых выражений. Тогда рассуждение, похожее на рассуждение во втором параграфе, показывает, что некоторое допустимое выражение является зависимостью между f и g, что невозможно, поскольку $k>a_s\deg_g(g_s)$.

Действительно, все допустимые выражения можно распределить по n/d_s классам в соответствии с остатком при делении степени на n. При доказательстве леммы 1(a) мы убедились, что для каждого такого остатка найдётся соответствующий s-стандартный моном μ_i с $\mathrm{pow}_f(\mu_i)=0$. Значит, в каждом классе найдётся s-стандартный моном ν_i, являющийся допустимым выражением. Для определённости мы можем считать, что величина $\mathrm{pow}_f(\nu_i)$ минимальная из возможных.

Обозначим через Md_s максимальную степень элементов ν_i по z. Пусть Q — произвольное допустимое выражение. Вычитая из Q элементы вида $qf^j\nu_i$, $q\in\mathbb{Q}$, $j\in\mathbb{N}$, мы получим элемент $\delta(Q)=Q-r_l$ (где r_l — сумма s-стандартных мономов) со степенью по z, меньшей чем Md_s.

Степени многочленов $\delta(Q)$ распределены по M классам: $\{\deg_z(\delta(Q))=d_s, 2d_s, \ldots, Md_s\}$ (некоторые из них могут оказаться пустыми). В каждом непустом классе выберем некоторый элемент $\delta(Q_i)$. Тогда любой $\delta(Q)$ имеет вид $\delta(Q)=\sum_i q_i\delta(Q_i)$ для некоторых рациональных чисел $q_0,\ldots,q_{M-1}$. Действительно, $\deg_z(\delta(Q))=\deg_z(\delta(Q_i))$ для одного из выбранных представителей, и можно подобрать $q_i\in\mathbb{Q}$ так, что

$$\deg_z(\delta(Q)-q_i\delta(Q_i))<\deg_z(\delta(Q)).$$

Поскольку $\deg_z(\delta(Q)-q_i\delta(Q_i))<Md_s$, это число тоже принадлежит одному из классов и процесс можно продолжить, пока степень не станет нулём. Это означает, что $\delta(Q)-q_i\delta(Q_i)=q_0\in\mathbb{Q}$ и $\delta(Q)=\sum_{i=0}^{M-1}q_i\delta(Q_i)$, где $\delta(Q_0)=1$.

Рассмотрим теперь допустимое выражение $f^lg_s^{a_s}$, где l больше максимума $\deg_f(\delta(Q_i))$. Поскольку слагаемые в r_l являются s-стандартными мономами, их степени по g меньше, чем $a_s\deg_g(g_s)$. Поэтому в $\delta(f^lg_s^{a_s})$ как многочлене от f, g сохранится моном $f^l g^{a_s \deg_g(g_s)}$, содержавшийся в $f^l g_s^{a_s}$, и степень $\delta(f^l g_s^{a_s})$ по f не может быть меньше l. Как мы видели выше, $\delta(f^l g_s^{a_s}) = \sum_{i=0}^{M-1} q_i \delta(Q_i)$ для некоторых $q_0, \ldots, q_{M-1} \in \mathbb{Q}$ (хотя степень левой части по f больше степени правой части по f, они имеют одинаковую степень как многочлены от z). Но тогда многочлен $\delta(f^l g_s^{a_s}) - \sum_{i=0}^{M-1} q_i \delta(Q_i)$ является зависимостью между f и g, у которой степень по g меньше k, что невозможно.

Полученное противоречие показывает, что $\deg(c_0 g_s^{a_s} - \sum_i c_i \mathbf{m_i})$ не делится на d_s при некотором выборе $c_i \in \mathbb{Q}[f]$. Как мы увидим, в этом случае алгоритм даёт g_{s+1}.

Найдём $\delta = c_0 g_s^{a_s} - \sum_i c_i \mathbf{m_i}$, для которого $\deg_z(\delta)$ не делится на d_s. Если $c_0 = q_0 f^l$, то, поделив на c_0, мы получим

$$g_s^{a_s} - \sum_i \frac{c_i}{q_0 f^l} \mathbf{m_i} = \frac{\delta}{q_0 f^l},$$

где все $\dfrac{c_i}{q_0 f^l}$ — многочлены Лорана. Запишем каждое слагаемое $\dfrac{c_i}{q_0 f^l}\mathbf{m_i}$ в виде $\alpha_{i,1} + \alpha_{i,2}$, где степень по z стандартных мономов в $\alpha_{i,1}$ больше $\deg_z\left(\dfrac{\delta}{q_0 f^l}\right)$, а в $\alpha_{i,2}$ меньше. (Равенство невозможно, поскольку $\deg_z(\delta)$ не делится на d_s.) Тогда

$$g_s^{a_s} - \sum_i \alpha_{i,1} = \frac{\delta}{q_0 f^l} + \sum_i \alpha_{i,2} \quad \text{и} \quad g_{s+1} = g_s^{a_s} - \sum_i \alpha_{i,1},$$

где $\deg_z(g_{s+1}) = \deg_z\left(\dfrac{\delta}{q_0 f^l}\right)$ не делится на d_s. Действительно, степени по z стандартных мономов попарно различны (лемма 1(а)). Поэтому $\sum_i \alpha_{i,1}$ содержит именно те стандартные мономы, которые будут использованы в алгоритме для уменьшения степени $g_s^{a_s}$.

Если $c_0 = q_0 f^l - r$, где $\deg_f(r) < l$, рассмотрим

$$\frac{c_0}{q_0 f^l} g_s^{a_s} - \sum_{i=1} \frac{c_i}{q_0 f^l} \mathbf{m_i} = \frac{\delta}{q_0 f^l}.$$

В левой части коэффициенты являются многочленами Лорана, а

$$\frac{c_0}{q_0 f^l} = 1 - w,$$

где $\deg_f(w) \leqslant -1$. Воспользовавшись формулой

$$\frac{1}{1-w} = 1 + w + \ldots + w^a + \frac{w^{a+1}}{1-w},$$

мы получим

$$g_s^{a_s} - \Big(1 + w + \ldots + w^a + \frac{w^{a+1}}{1-w}\Big) \sum_i \frac{c_i}{q_0 f^l} \mathbf{m_i} = \frac{\delta}{q_0 f^l (1-w)}$$

и

$$g_s^{a_s} - (1 + w + \ldots + w^a) \sum_i \frac{c_i}{q_0 f^l} \mathbf{m_i} = \frac{\delta}{q_0 f^l (1-w)} + \frac{w^{a+1}}{1-w} \sum_i \frac{c_i}{q_0 f^l} \mathbf{m_i}.$$

Поскольку $\deg_z(w) \leqslant -n$, при достаточно большом a получим

$$\deg_z\Big(\frac{w^{a+1}}{1-w} \sum_i \frac{c_i}{q_0 f^l} \mathbf{m_i}\Big) < \deg_z\Big(\frac{\delta}{q_0 f^l}\Big).$$

Как и в случае $c_0 = q_0 f^l$, положим

$$(1 + w + \ldots + w^a) \frac{c_i}{q_0 f^l} \mathbf{m_i} = \alpha_{i,1} + \alpha_{i,2},$$

где степень по z стандартных мономов в $\alpha_{i,1}$ больше $\deg_z\Big(\dfrac{\delta}{q_0 f^l}\Big)$, а в $\alpha_{i,2}$ меньше. Тогда

$$g_{s+1} = g_s^{a_s} - \sum_i \alpha_{i,1},$$

где $\deg_z(g_{s+1}) = \deg_z\Big(\dfrac{\delta}{q_0 f^l}\Big)$ не делится на d_s. □

Мы доказали, что алгоритм работает. Осталось проверить, что после конечного числа шагов он выдаст неприводимую зависимость.

Лемма 3. *После конечного числа шагов алгоритм выдаст нуль и неприводимую зависимость между $f(z)$ и $g(z)$.*

Доказательство. Как было замечено выше, $d_0 > d_1 > \ldots > d_i$. Поскольку $d_i \in \mathbb{N}$, через конечное число шагов мы получим минимальное d_s, и после этого алгоритм выдаст $0 = g_s^{a_s}(f,g) - r_s(f,g)$. В доказательстве леммы 2 было показано, что $\deg_y(P) = a_s \deg_g(g_s)$. Следовательно, $P = g_s^{a_s}(x,y) - r_s(x,y)$. □

§ 4. Доказательство теоремы АМС

Ещё одна лемма — и мы сможем доказать теорему АМС.

Лемма 4. *Все g_i являются многочленами от f и g.*

Доказательство. Упорядочим мономы $f^i g^j$, $i, j \in \mathbb{Z}$, лексикографически по степеням $\deg_g$, $\deg_f$, т. е. будем говорить, что $f^{i_1} g^{j_1} > f^{i_2} g^{j_2}$, если $j_1 > j_2$ или $j_1 = j_2$, $i_1 > i_2$.

Назовём моном *отрицательным*, если его степень по f отрицательна, в противном случае назовём его *положительным*.

Обозначим через L множество многочленов от g с коэффициентами — многочленами Лорана от f, т. е. $L=\mathbb{Q}[g, f, f^{-1}]$. Введём для элемента $h \in L$ функцию gap следующим образом. Если $h \notin \mathbb{Q}[f, g]$, то $\mathrm{gap}(h)$ — это моном $\overline{h} \div \widetilde{h}$ (здесь $a \div b = a/b$), где $\overline{h}$ — самый большой моном в h, а $\widetilde{h}$ — самый большой отрицательный моном в h; если $h \in \mathbb{Q}[f, g]$, то $\mathrm{gap}(h) = \infty$, где ∞ больше любого монома по определению.

Будем пользоваться следующими легко проверяемыми свойствами функции gap:

(а) $\mathrm{gap}(h_1 h_2) \geqslant \min(\mathrm{gap}(h_1), \mathrm{gap}(h_2))$;

(б) $\mathrm{gap}(h^d) = \mathrm{gap}(h)$, $d \in \mathbb{N}$, если у h как многочлена от g ведущий коэффициент — единица.

Так как g_{s+1} — это элемент, полученный на последнем шаге алгоритма, т. е. g_{s+1} — неприводимая зависимость между $f(z)$ и $g(z)$, мы знаем, что $\mathrm{gap}(g_{s+1}) = \infty$, поскольку g_{s+1} — многочлен от f и g. Мы собираемся проверить, что $\mathrm{gap}(g_{j+1}) \leqslant \mathrm{gap}(g_j)$, где g_j, $j=0, 1, \ldots, s+1$, рассматриваются как элементы L. Из этого будет следовать, что $\mathrm{gap}(g_j) = \infty$ для $j = 0, 1, \ldots, s$. Поскольку $\mathrm{gap}(h) = \infty$ означает, что $h \in K[f, g]$, лемма будет доказана.

Воспользуемся индукцией. Поскольку $\mathrm{gap}(g_1) \leqslant \mathrm{gap}(g_0) = \infty$, база индукции очевидна.

Предположим, что $\mathrm{gap}(g_{j+1}) \leqslant \mathrm{gap}(g_j)$, если $j<k$. Имеем $g_{k+1} = g_k^{a_k} - r_k$ и $\mathrm{gap}(g_k^{a_k}) = \mathrm{gap}(g_k)$ по свойству (б) (по лемме 1(б) у всех g_i ведущий коэффициент — единица). Чтобы доказать, что $\mathrm{gap}(g_{k+1}) \leqslant \mathrm{gap}(g_k)$, достаточно проверить, что самые большие отрицательные мономы у r_k и $g_k^{a_k}$ различны. Действительно, пусть ϱ — самый большой отрицательный моном r_k, а γ — самый большой отрицательный моном $g_k^{a_k}$ и они не равны. Если $\gamma > \varrho$, то $\mathrm{gap}(g_{k+1}) = g^{a_0 \ldots a_k} \div \gamma = \mathrm{gap}(g_k^{a_k}) = \mathrm{gap}(g_k)$, а если $\varrho > \gamma$, то $\mathrm{gap}(g_{k+1}) = g^{a_0 \ldots a_k} \div \varrho < \mathrm{gap}(g_k^{a_k}) = \mathrm{gap}(g_k)$.

Если $g_k^{a_k}$ не содержит отрицательных мономов, то g_k — многочлен и $\mathrm{gap}(g_{k+1}) \leqslant \mathrm{gap}(g_k) = \infty$, а если r_k не содержит отрицательных мономов, то $\mathrm{gap}(g_{k+1}) = \mathrm{gap}(g_k)$.

Вспомним, что r_k является суммой k-стандартных мономов с рациональными коэффициентами. Эти мономы тоже можно лексикографически упорядочить по $\deg_g$, pow_f (а именно, $\mathbf{m_i} > \mathbf{m_j}$, если $\deg_g(\mathbf{m_i}) > \deg_g(\mathbf{m_j})$ или если $\deg_g(\mathbf{m_i}) = \deg_g(\mathbf{m_j})$ и $\mathrm{pow}_f(\mathbf{m_i}) > \mathrm{pow}_f(\mathbf{m_j})$). Стандартный моном $\mathbf{m}$ является элементом в L. Легко видеть, что самый большой его моном — это $\overline{\mathbf{m}} = f^i g^j$, где $i = \mathrm{pow}_f(\mathbf{m})$, а $j = \deg_g(\mathbf{m})$. Таким образом, $\mathbf{m_i} < \mathbf{m_j}$, если $\overline{\mathbf{m_i}} < \overline{\mathbf{m_j}}$. Два различных стандартных монома не могут оказаться равными относительно введённого порядка, поскольку $i = \mathrm{pow}_f(\mathbf{m})$ и $j = \deg_g(\mathbf{m})$

определяют стандартный моном однозначно (см. замечание к лемме 1). Назовём k-стандартный моном $\mathbf{m}$ *отрицательным*, если $\mathrm{pow}_f(\mathbf{m}) < 0$, а при $\mathrm{pow}_f(\mathbf{m}) \geqslant 0$ — *положительным*.

Если k-стандартный моном $\mathbf{m}$ отрицателен, то $\mathrm{gap}(\mathbf{m}) = 1$, поскольку его наибольший моном отрицателен. Если $\mathbf{m} = f^i g_0^{j_0} \dots g_k^{j_k}$ положителен, т. е. если $i \geqslant 0$, то

$$\mathrm{gap}(\mathbf{m}) \geqslant \min\bigl(\mathrm{gap}(f^i), \mathrm{gap}(g_0^{j_0}), \dots, \mathrm{gap}(g_k^{j_k})\bigr)$$

по свойству (а),

$$\min\bigl(\mathrm{gap}(f^i), \mathrm{gap}(g_0^{j_0}), \dots, \mathrm{gap}(g_k^{j_k})\bigr) = \min\bigl(\infty, \mathrm{gap}(g_0), \dots, \mathrm{gap}(g_k)\bigr)$$

по свойству (б),

$$\min\bigl(\infty, \mathrm{gap}(g_0), \dots, \mathrm{gap}(g_k)\bigr) = \mathrm{gap}(g_k)$$

по предположению индукции.

Следовательно,

$$\mathrm{gap}(\mathbf{m}) \geqslant \mathrm{gap}(g_k) = \mathrm{gap}(g_k^{a_k}).$$

Поскольку $\deg_g(\mathbf{m}) < \deg_g(g_k^{a_k})$ по лемме 1(б), а $\mathrm{gap}(\mathbf{m}) \geqslant \mathrm{gap}(g_k^{a_k})$, даже если положительный k-стандартный моном $\mathbf{m} \in L$ не является многочленом, его отрицательные мономы меньше, чем наибольший отрицательный моном γ элемента $g_k^{a_k}$. Поэтому только один из отрицательных k-стандартных мономов r_k может иметь наибольший моном равным γ.

Чтобы облегчить понимание доказательства, рассмотрим два случая: (i) $\mathrm{gap}(g_k) < \mathrm{gap}(g_{k-1})$ и (ii) $\mathrm{gap}(g_k) = \mathrm{gap}(g_{k-1})$.

(i) $\mathrm{gap}(g_k) < \mathrm{gap}(g_{k-1})$. Поскольку $g_k = g_{k-1}^{a_{k-1}} - r_{k-1}$ и

$$\mathrm{gap}(g_{k-1}^{a_{k-1}}) = \mathrm{gap}(g_{k-1}) > \mathrm{gap}(g_k),$$

наибольший отрицательный моном ν_{k-1} в r_{k-1} больше, чем наибольший отрицательный моном в $g_{k-1}^{a_{k-1}}$. Отсюда $\mathrm{gap}(g_k) = \overline{g_{k-1}^{a_{k-1}}} \div \overline{\nu_{k-1}}$.

Далее,

$$g_k^{a_k} = (g_{k-1}^{a_{k-1}} - r_{k-1})^{a_k} = g_{k-1}^{a_{k-1}a_k} - R.$$

Поскольку $\deg_g(R) < a_k \deg_g(g_k)$, мы знаем, что R можно представить суммой k-стандартных мономов (лемма 1(в)). Наибольший отрицательный k-стандартный моном μ, являющийся слагаемым в $g_k^{a_k}$, — это наибольший отрицательный k-стандартный моном в R, и он равен $\nu_{k-1} g_k^{a_k - 1}$. Действительно,

$$\mathrm{gap}(g_k^{a_k}) = \mathrm{gap}(g_{k-1}^{a_{k-1}a_k} - R) = \mathrm{gap}(g_k) < \mathrm{gap}(g_{k-1}^{a_{k-1}a_k}) = \mathrm{gap}(g_{k-1});$$

следовательно, наибольший отрицательный моном в $g_{k-1}^{a_{k-1}a_k}$ меньше, чем μ. Более того,

$$\operatorname{gap}(g_k) = \overline{g_{k-1}^{a_{k-1}}} \div \overline{\nu_{k-1}} = \operatorname{gap}(g_k^{a_k}) = \operatorname{gap}(g_{k-1}^{a_{k-1}a_k} - R) = \overline{g_{k-1}^{a_{k-1}a_k}} \div \bar{\mu}.$$

Поскольку $\overline{g_{k-1}^{a_{k-1}}} = \overline{g_k}$, мы получаем, что $\bar{\mu} = \overline{\nu_{k-1}}\overline{g_k^{a_k-1}}$ и k-стандартный моном μ равен $\nu_{k-1}g_k^{a_k-1}$.

Согласно процедуре алгоритма $g_k = g_{k-1}^{a_{k-1}} - r_{k-1}$ и степень по z любого $(k-1)$-стандартного монома в r_{k-1} больше, чем $\deg_z(g_k) = m_k$. Следовательно,

$$\deg_z(\mu) = \deg_z(\nu_{k-1}g_k^{a_k-1}) = \deg_z(\nu_{k-1}) + (a_k-1)m_k > a_k m_k.$$

Аналогично $g_{k+1} = g_k^{a_k} - r_k$, где степень по z любого k-стандартного монома в r_k не превосходит $a_k m_k$. Следовательно, μ не может быть слагаемым в r_k и наибольшие отрицательные мономы в r_k и $g_k^{a_k}$ различны. Как отмечено перед п. (i), отсюда следует утверждение леммы.

(ii) $\operatorname{gap}(g_k) = \operatorname{gap}(g_{k-1})$. Если $\operatorname{gap}(g_k) = \infty$, то $\operatorname{gap}(g_{k+1}) \leqslant \operatorname{gap}(g_k)$. Поэтому предположим, что $\operatorname{gap}(g_k) < \infty$. Так как $\operatorname{gap}(g_0) = \infty$ и $\operatorname{gap}(g_k) < \infty$, мы можем найти такое p, что

$$\operatorname{gap}(g_k) = \operatorname{gap}(g_{k-1}) = \ldots = \operatorname{gap}(g_p) < \operatorname{gap}(g_{p-1}).$$

Аналогично предыдущему случаю $g_k^{a_k} = g_{p-1}^{a_{p-1}\ldots a_k} - R$, где R можно представить суммой k-стандартных мономов и $g_{k+1} = g_{p-1}^{a_{p-1}\ldots a_k} - R - r_k$. Поскольку

$$\operatorname{gap}(g_{p-1}^{a_{p-1}\ldots a_k}) = \operatorname{gap}(g_{p-1}) > \operatorname{gap}(g_k) = \operatorname{gap}(g_{p-1}^{a_{p-1}\ldots a_k} - R) = \operatorname{gap}(g_p),$$

мы можем заключить, что наибольшим отрицательным k-стандартным мономом в представлении R суммой k-стандартных мономов является $\nu_{p-1}g_p^{a_p-1}\ldots g_k^{a_k-1}$, где ν_{p-1} — наибольший отрицательный $(p-1)$-стандартный моном в r_{p-1}. Следовательно,

$$\begin{aligned}\deg_z(\nu_{p-1}g_p^{a_p-1}\ldots g_{k-1}^{a_k-1}) &= \\ &= \deg_z(\nu_{p-1}) + (a_p-1)m_p + \ldots + (a_k-1)m_k > a_k m_k,\end{aligned}$$

потому что $\deg_z(\nu_{p-1}) > m_p$ и $a_j m_j > m_{j+1}$ при любом j. Но $\deg_z(r_k) < a_k m_k$, и рассматриваемый моном не может быть слагаемым в r_k. Как и в предыдущем случае, наибольшие отрицательные мономы r_k и $g_k^{a_k}$ различны. Лемма доказана. □

Замечание для читателя, знакомого с полями конечной характеристики

В процессе работы алгоритма отрицательные степени f действительно появляются, если характеристика конечна и делит m и n. (Проверьте пример перед формальным описанием алгоритма для характеристики, равной двум.) Наше доказательство не работает в этом случае, поскольку функция gap перестаёт удовлетворять условию (б).

Итак, мы доказали, что все g_i являются многочленами от f и g, а значит, и все стандартные мономы $g_0^{j_0} \dots g_s^{j_s}$ тоже многочлены от f и g. Мы заметили при доказательстве леммы 2, что любой многочлен Q от f и g, у которого $\deg_g(Q) < a_s \deg_g(g_s)$, является суммой положительных и отрицательных s-стандартных мономов. Теперь мы можем заметить, что отрицательных s-стандартных мономов в этой сумме нет. Действительно, если $Q = q_0(f)g^l + \ldots + q_l$, где $q_i \in \mathbb{Q}[f]$, то найдём s-стандартный моном $\mathbf{m}$ степени l по g, у которого $\operatorname{pow}_f(\mathbf{m}) = 0$. Тогда $Q - q_0\mathbf{m}$ — многочлен, степень которого меньше l, и мы можем применить индукцию по степени.

Для любого многочлена $H(x, y)$ от двух переменных найдётся многочлен $Q(x, y)$, для которого $\deg_y(Q(x, y)) < a_s \deg_g(g_s)$ и $Q(f(z), g(z)) = H(f(z), g(z))$. Достаточно поделить $H(x, y)$ на $P(x, y)$ с остатком, рассматривая их как многочлены от y с коэффициентами — многочленами от x. Тогда $H(x, y) = a(x, y)P(x, y) + Q(x, y)$.

Таким образом, любой многочлен $H(f(z), g(z))$ может быть записан двумя способами: с помощью обычных мономов,

$$H(f(z), g(z)) = \sum_{i,j} h_{i,j} f(z)^i g(z)^j,$$

и с помощью положительных s-стандартных мономов. Более того, если s-стандартные мономы найдены, то можно сказать, какой многочлен $h(z)$ от одной переменной может быть записан как многочлен от $f(z)$ и $g(z)$. По лемме 1(а), степени по z у всех s-стандартных мономов различны. Поэтому, чтобы узнать, является ли $h(z)$ многочленом от $f(z)$ и $g(z)$, нужно проверить, существует ли s-стандартный моном степени $\deg_z(h)$. Если нет, то $h \notin \mathbb{Q}[f(z), g(z)]$, где $\mathbb{Q}[f(z), g(z)]$ — множество всех многочленов от $f(z)$ и $g(z)$. Если же такой s-стандартный моном $\mathbf{m}_1$ нашёлся, то нужно заменить $h(z)$ на $h_1(z) = h(z) - q_1\mathbf{m}_1$, где рациональное число q_1 выбрано так, что $\deg_z(h(z) - q_1\mathbf{m}_1) < \deg_z(h(z)$. Понятно, что h_1 — многочлен от $f(z)$ и $g(z)$ тогда и только тогда, когда h — многочлен от $f(z)$ и $g(z)$. Повторяя проверку для h_1, мы либо узнаем, что h и h_1 не многочлены от $f(z)$ и $g(z)$, либо получим многочлен h_2, причём $\deg_z(h_2) < \deg_z(h_1)$.

Таким образом, не больше чем за $\deg_z(h)$ шагов мы узнаем, является ли h многочленом от $f(z)$ и $g(z)$, и, если является, найдём такой многочлен H от двух переменных, что $h(z) = H(f(z), g(z))$.

Если f и g удовлетворяют условиям теоремы AMC, то $\mathbb{Q}[f(z), g(z)] = \mathbb{Q}[z]$. Следовательно, любой многочлен от z является суммой положительных s-стандартных мономов и для произвольного натурального числа d существует положительный s-стандартный моном, имеющий степень d по z. Существует такой моном и для d_0. Поскольку d_0 делится на себя, по лемме 1(a) этот моном равен $f^i g_0^j$, где $in + jm = d_0$ и $0 \leqslant j < a_0$, а поскольку он положительный, $i \geqslant 0$. Так как d_0 — это наибольший общий делитель n и m, такое равенство возможно, только если $n = d_0$ или $m = d_0$.

Список литературы

[1] *Segre B.* Corrispondenze di Möbius e trasformazioni cremoniane intere // Atti Accademia Sci. Torino. 1956–1957. V. 91. P. 3–19.

[2] *Canals I., Lluis E.* Acerca de un resultado de Segre // Anales del Instituto de Matemáticas. Universidad Nacional Autónoma de México. 1970. V. 10. P. 1–15.

[3] *Abhyankar S. S., Moh T. T.* Embeddings of the line in the plane // J. Reine Angew. Math. 1975. V. 276. P. 148–166.

[4] *Abhyankar S. S., Moh T. T.* Newton — Puiseux expansion and generalized Tschirnhausen transformation. I, II // J. Reine Angew. Math. 1973. V. 260. P. 47–83; 1973. V. 261, P. 29–54.

[5] *Suzuki M.* Propriétés topologiques des polynômes de deux variables complexes, et automorphismes algébriques de l'espace $\mathbb{C}^2$ // J. Math. Soc. Japan. 1974. V. 26. P. 241–257.

Леонид Григорьевич Макар-Лиманов, Университет Уэйна,
Мичиган, США

lml@wayne.edu

Уравновешенные разложения на множители в некоторых алгебрах

А. А. Клячко, А. М. Мажуга, А. Н. Понфиленко

Мы доказываем, что во всяком поле характеристики не два и не три, кроме $\mathbb{F}_5$, каждый элемент раскладывается в произведение четырёх множителей, сумма которых равна нулю. Мы также находим все такие k, n, q, что каждая матрица размера $n \times n$ над полем из q элементов раскладывается в произведение k коммутирующих матриц с нулевой суммой.

§ 0. Введение

> Покажите, что всякое рациональное число можно разложить в произведение нескольких рациональных чисел, сумма которых равна нулю.

Эта задача предлагалась на Казахстанской республиканской олимпиаде для школьников в 2013 году [1]. Аналогичный вопрос для произвольного поля характеристики не два предлагался на студенческой олимпиаде по алгебре в МГУ в 2014 году [2]. Задача рассматривалась и раньше [3] (также в контексте работы со способными школьниками).

Вопрос о наличии таких *уравновешенных* или *сбалансированных* разложений (то есть разложений в произведение нескольких множителей, сумма которых равна нулю) решается легко в любом поле характеристики не два. Гораздо труднее выяснить, сколько множителей могут содержать такие уравновешенные разложения. На самом деле (см. [4]),

> в любом поле характеристики не два каждый элемент допускает уравновешенное разложение в произведение k сомножителей для каждого $k \geqslant 5$. (А для каждого $k < 5$ найдётся поле, в котором это утверждение перестаёт быть верным.)

При $k < 5$ вопрос становится более тонким, например, в поле рациональных чисел не всякий элемент допускает уравновешенное разложение

Первые два автора поддержаны РФФИ, грант № 15–01–05823.

в произведение трёх множителей [3], а вопрос о четырёх множителях оставался открытым. В [3] приводится следующее электронное письмо М. А. Цфасмана А. В. Иванищуку:

$$3 = (363/70) \cdot (20/77) \cdot (-49/110) \cdot (-5). \quad \text{Уф...} \qquad \text{Ваш М. А.}$$

Это письмо содержит (первое открытое) уравновешенное разложение тройки в произведение четырёх множителей в поле рациональных чисел. Аналогичные разложения для единицы и двойки выглядят не так впечатляюще: $1=1\cdot1\cdot(-1)\cdot(-1)$ и $2=(1/6)\cdot(9/2)\cdot(-2/3)\cdot(-4)$. Статья [3] содержит полученные с помощью компьютера уравновешенные разложения первых пятидесяти натуральных чисел в произведение четырёх рациональных множителей.

Мы доказываем, что любое рациональное число допускает уравновешенное разложение в произведение четырёх рациональных сомножителей. Более того, имеет место следующая теорема, отвечающая на два вопроса из [4] (один из них был поставлен раньше [3]).

Теорема 1. *Во всяком поле характеристики не два и не три, кроме пятиэлементного поля* $\mathbb{F}_5$, *каждый элемент допускает уравновешенное разложение в произведение четырёх множителей*; *если это поле бесконечно*, *то каждый элемент допускает бесконечно много таких разложений.*

По поводу этого результата мы не уверены в своём приоритете, поскольку

— школьный учитель второго автора, Дмитрий Витальевич Андреев, много лет назад (в 2003 году) предлагал такую задачу на уроке (для случая поля рациональных чисел); задача не была решена, но из данных учителем подсказок второй автор (теперь, уже зная решение) склонен делать вывод, что Дмитрий Витальевич умел решать эту задачу;

— в 2016 году, уже зная решение, второй автор задал такой вопрос (для случая рациональных чисел) на форуме `http://math.stackexchange.com/` и вскоре кто-то из посетителей этого форума предоставил решение, отличающееся от нашего, но, вероятно, тоже правильное; сейчас этот вопрос, к сожалению, удалён, и мы не можем дать никакой более точной ссылки.

Следующая теорема из [4] описывает для каждого k все конечные поля, в которых каждый элемент допускает уравновешенное разложение в произведение k множителей.

Теорема об уравновешенных разложениях в конечных полях [4]. *Пусть* $k \geqslant 2$ — *целое число и* F — *конечное поле. В поле* F *всякий элемент можно разложить в произведение* k *сомножителей*, *сумма которых равна нулю*, *тогда и только тогда*, *когда* (см. табл. 1) *либо* $|F| = 2$ *и* k *чётно*, *либо* $|F| = 4$ *и* $k \neq 3$, *либо* $|F|$ — *степень двойки*, *но не двойка и не четвёрка* *(и k любое), либо $|F| \in \{3, 5\}$ и $k \notin \{2, 4\}$, либо $|F| = 7$ и $k \notin \{2, 3\}$, либо $|F|$ не степень двойки, не три, не пять и не семь и $k \neq 2$.*

Таблица 1

Наличие уравновешенного разложения в конечных полях

	$k=2$	$k=3$	$k=4$	$k=5,7,9,\ldots$	$k=6,8,10,\ldots$
$\mathbb{F}_2$	да	нет	да	нет	да
$\mathbb{F}_3$	нет	да	нет	да	да
$\mathbb{F}_4$	да	нет	да	да	да
$\mathbb{F}_5$	нет	да	нет	да	да
$\mathbb{F}_7$	нет	нет	да	да	да
$\mathbb{F}_8, \mathbb{F}_{16}, \mathbb{F}_{32}, \mathbb{F}_{64}, \ldots$	да	да	да	да	да
$\mathbb{F}_9, \mathbb{F}_{11}, \mathbb{F}_{13}, \mathbb{F}_{17}, \ldots$	нет	да	да	да	да

Следующая теорема дополняет этот результат из [4], см. табл. 2.

Теорема 2. *Пусть $k, n \geqslant 2$ — целые числа и F — конечное поле. Каждая матрица $n \times n$ над полем F раскладывается в произведение k коммутирующих матриц, сумма которых равна нулю, тогда и только тогда, когда либо $k = 3$ и $|F| = 5$, либо $k = 3$ и $|F| \geqslant 8$, либо $k = 4$ и $|F| = 4$, либо $k = 4$ и $|F| \geqslant 7$, либо $k \geqslant 5$ и $|F| \geqslant 3$.*

Другими словами, ситуация в матричных алгебрах над конечными полями такая (на верхние индексы пока не нужно обращать внимание):

Таблица 2

Наличие уравновешенного разложения
в матричных алгебрах над конечным полем

	$k=2$	$k=3$	$k=4$	$k=5,6,7,8,\ldots$
$\mathbb{F}_2$	нет^1	нет^0	нет^2	нет^2
$\mathbb{F}_3$	нет^1	нет^8	нет^0	да^{3,4}
$\mathbb{F}_4, \mathbb{F}_7$	нет^1	нет^0	да^{5,7}	да^{3,4,5,7}
$\mathbb{F}_5$	нет^1	да^5	нет^0	да^{3,4}
$\mathbb{F}_8, \mathbb{F}_9, \mathbb{F}_{11}, \mathbb{F}_{13}, \mathbb{F}_{16}, \ldots$	нет^1	да^{5,6}	да^{5,7}	да^{3,4,5,7}

Обратите внимание, что от размера матриц ответ не зависит, если этот размер по крайней мере 2.

В первом параграфе мы доказываем теорему 1 и ещё одну теорему о конечных полях (теорема 3), которая играет ключевую роль в доказательстве теоремы 2. Все рассуждения первого параграфа вполне элементарны, за исключением того, что доказательство теоремы 3 существенно опирается на результаты работы [4] (которые, в свою очередь, опираются на теорию эллиптических кривых). Во втором параграфе мы доказываем теорему 2.

Обозначения, которые мы используем, в целом стандартны. Отметим только, что символ $\mathbb{F}_q$ обозначает поле из q элементов, а буква E обозначает единичную матрицу.

§ 1. Поля

Доказательство теоремы 1. Имеет место тождество

$$x = \frac{2(1-4x)^2}{3(1+8x)} \cdot \frac{-(1+8x)}{6} \cdot \frac{-(1+8x)}{2(1-4x)} \cdot \frac{18x}{(1-4x)(1+8x)}.$$

Мы можем только предложить читателю проверить непосредственно это тождество и тот факт, что сумма множителей равна нулю. В исключительных случаях, когда знаменатели обращаются в нуль, т. е. при $x \in \{1/4, -1/8\}$, следует умножить x на y^4, подобрав y так, что $xy^4 \notin \{1/4, -1/8, 0\}$ (в любом поле характеристики не два и не три, кроме $\mathbb{F}_5$, это заведомо возможно), написать аналогичное разложение для xy^4 и потом разделить каждый сомножитель на y:

$$x = \frac{2(1-4xy^4)^2}{3y(1+8xy^4)} \cdot \frac{-(1+8xy^4)}{6y} \cdot \frac{-(1+8xy^4)}{2y(1-4xy^4)} \cdot \frac{18xy^4}{y(1-4xy^4)(1+8xy^4)}.$$

Таким образом, мы получаем уравновешенное разложение любого элемента в произведение четырёх множителей. Бесконечность числа таких разложений в случае бесконечного поля вытекает из последнего тождества и следующего элементарного факта, доказательство которого мы оставляем читателям в качестве упражнения:

> не равная константе рациональная дробь над бесконечным полем принимает бесконечное число значений.

(Отметим, что, например, второй сомножитель в последнем тождестве при каждом x представляет собой не равную константе рациональную дробь $f(y)$.) Это завершает доказательство теоремы. Поле из пяти элементов действительно является исключением, как видно из табл. 1. □

Аналогично можно получить бесконечно много уравновешенных разложений в произведение любого большего числа сомножителей, то есть

> в любом бесконечном поле характеристики не два каждый элемент допускает бесконечно много уравновешенных разложений в произведение k сомножителей для каждого $k \geqslant 5$.

Например, следующее тождество получается лёгкой модификацией из тождества, приведённого в [4], и даёт бесконечно много уравновешенных разложений произвольного ненулевого элемента бесконечного поля характеристики не два в произведение 2017 сомножителей:

$$x = \frac{xy^{2016}}{2} \cdot \frac{xy^{2016}}{2} \cdot (-xy^{2016}) \cdot \frac{2}{xy^{2018}} \cdot \left(-\frac{2}{xy^{2018}}\right) \cdot \left(\frac{1}{y}\right)^{1006} \cdot \left(-\frac{1}{y}\right)^{1006}.$$

Разложение на множители $x = x_1 x_2 \ldots x_k$ называется *степенны́м*, если все сомножители равны друг другу: $x_1 = \ldots = x_k$ [4].

Теорема 3. *Пусть $k \geqslant 2$ — целое число и F — конечное поле. В поле F всякий элемент допускает нестепенное уравновешенное разложение в произведение k множителей тогда и только тогда, когда либо $k = 3$ и $|F| = 5$, либо $k = 3$ и $|F| \geqslant 8$, либо $k = 4$ и $|F| = 4$, либо $k = 4$ и $|F| \geqslant 7$, либо $k \geqslant 5$ и $|F| \geqslant 3$.*

Другими словами, ответ здесь такой же, как в теореме 2 (табл. 2).

Доказательство. Верхние индексы у частиц *да* и *нет* в табл. 2 соответствуют случаям из доказательства ниже.

Случай 0: нет, так как тогда у некоторых элементов нет никаких сбалансированных разложений (по теореме об уравновешенных разложениях в конечных полях).

Случай 1: $k = 2$ — нет. Для любого элемента a рассмотрим его уравновешенное разложение $a = xy$, $x + y = 0$. Если у поля характеристика 2, то наше разложение $a = (-x)x$ является степенным; если же характеристика конечного поля не два, то не всякий элемент является квадратом и, следовательно, не всякий элемент допускает уравновешенное разложение в произведение двух множителей.

Случай 2: $|F| = 2$ — нет. В разложении единицы могут участвовать только единицы, поэтому оно будет степенным.

Случай 3: $k = 5 + 2n$, где $n \geqslant 0$ и $\operatorname{char} F \neq 2$ — да. Здесь можно использовать универсальную формулу для уравновешенных разложений в произведение $5 + 2n$ сомножителей из [4]:

$$\pm a = (-a) \cdot \frac{a}{2} \cdot \frac{a}{2} \cdot \frac{2}{a} \cdot \frac{-2}{a} \cdot 1^n \cdot (-1)^n \quad (\text{при } a \neq 0).$$

При этом $\operatorname{char} F \neq 2$, поэтому $\frac{2}{a} \neq -\frac{2}{a}$ и, значит, это разложение нестепенное. А нулевой элемент очевидно имеет уравновешенное нестепенное разложение: $0 = (-1) \cdot 1 \cdot 0^{k-2}$.

Случай 4: $k = 6 + 2n$, где $n \geqslant 0$ и $\operatorname{char} F \neq 2$ — да. Воспользуемся общей формулой для уравновешенных разложений в произведение $6 + 2n$ множителей из [4]. Рассмотрим такое ненулевое $c \in F$, что $c^2 \neq a$ (такое c всегда найдётся, кроме случая, когда $F = \mathbb{F}_3$ и $a = 1$; но тогда всё очевидно).

Положим $b = (c^2 - a)/c$. Тогда
$$\pm a = (-c)\cdot(c-b)\cdot\frac{b}{2}\cdot\frac{b}{2}\cdot\frac{2}{b}\cdot\frac{-2}{b}\cdot 1^n\cdot(-1)^n.$$
Так как $\operatorname{char} F \neq 2$, мы имеем $\frac{2}{b} \neq -\frac{2}{b}$, поэтому разложение нестепенное.

Случай 5: $|F| = 5, 8$ и $k = 3$; $|F| = 7, 9, \ldots$ и $k = 4$; $|F| = 4, 8$ и $k = 5 + 2n$, где $n \geqslant 0$. В этом случае уравновешенное разложение существует по теореме об уравновешенных разложениях в конечных полях и не может быть степенным, поскольку число сомножителей не делится на характеристику поля, а их сумма равна нулю.

Случай 6: $|F| \geqslant 9$, $\operatorname{char} F \neq 2$ и $k = 3$ — да.

Здесь нужно рассмотреть два случая. Если $\operatorname{char} F \neq 3$, то по теореме об уравновешенных разложениях в конечных полях уравновешенное разложение у любого элемента существует, а так как $\operatorname{char} F \neq 3$, то оно заведомо нестепенное.

Для доказательства в случае характеристики три нам понадобится вспомогательное утверждение.

Лемма. *В поле $\mathbb{F}_{3^n}$, где $n \geqslant 2$, существует такой ненулевой квадрат u, что $u+1$ — тоже ненулевой квадрат.*

Доказательство. Если 2 — квадрат, то $u = 1$ — искомый элемент. Иначе предположим, что для любого $u \notin \{0, 1, 2\}$ верно следующее утверждение: если u — квадрат, то $u + 1$ — не квадрат. Тогда в любом множестве вида $\{u, u+1, u+2\}$ не более одного квадрата. Значит, всего квадратов не больше $3^{n-1} + 1$. С другой стороны, в поле характеристики 3 квадратов ровно $(3^n + 1)/2$. Отсюда получаем неравенство $(3^n + 1)/2 \leqslant 3^{n-1} + 1$, которое выполняется только при $n = 1$. Лемма доказана. □

Вернёмся к доказательству теоремы 3. Итак, мы хотим показать, что в конечном поле характеристики три и порядка по крайней мере девять каждый элемент имеет уравновешенное нестепенное разложение в произведение трёх множителей.

Отметим, что в таком поле любой элемент является кубом ровно одного элемента. Будем искать сбалансированное разложение элемента $a = 2b^3 \neq 0$: $a = xyz$, $x + y + z = 0$. Избавляясь от z, получаем
$$yx^2 + y^2x + a = 0. \tag{$*$}$$
Будем решать это уравнение относительно x. По лемме существует такой $\tau^2 \neq 0$, что $\tau^2 + 1 = \pi^2 \neq 0$ тоже квадрат. Возьмём $y = b + b\pi$. Значит, дискриминант квадратного уравнения $(*)$ является квадратом:
$$D = y^4 - 4ay = y(y^3 - 8b^3) = y(y-2b)^3 = (b\pi + b)\cdot(b\pi - b)^3 = \\ = b^2(\pi^2 - 1)(b\pi - b)^2 = b^2\tau^2(b\pi - b)^2$$

и у уравнения $(*)$ есть решение. Полученное разложение не будет степенным, так как $y^3 \neq a$. Действительно, иначе $2b^3 = b^3(1+\pi)^3 = b^3(1+\pi^3)$, откуда $\pi^3 = 1$, $\pi = 1$ и $\tau = 0$, что неверно.

Осталось найти нестепенное уравновешенное разложение нуля, но это легко: $0 = (-1) \cdot 1 \cdot 0$.

Случай 7: $|F| = 2^n$ и $k = 4 + 2m$, где $m \geqslant 0$, $n > 1$. Так как $\operatorname{char} F = 2$, любой элемент поля является квадратом: $a = b \cdot b$. Если $a \neq 1$, то $b \neq 1$ и $a = b^2 \cdot 1^{2m+2}$ — искомое разложение. Если $a = 1$, то $a = 1 = c^2 \cdot (1/c)^2 \cdot 1^{2m}$ — искомое разложение, где c — любой элемент, отличный от нуля и единицы.

Случай 8: $|F| = 3$ и $k = 3$ — нет. В разложении единицы не может участвовать нуль, а 1 и -1 обязаны участвовать, чтобы разложение было нестепенным. Тогда третий множитель — нуль, так как разложение уравновешенное. Это противоречие завершает доказательство теоремы 3. $\square$

§ 2. Матрицы

Доказательство теоремы 2. Сперва заметим, что при $k = 2$ теорема верна по простой причине:

> жорданова клетка J размера $n \times n$ с собственным значением нуль не является квадратом в кольце матриц $n \times n$ при $n \geqslant 2$

(доказательство этого утверждения мы оставляем читателям в качестве простого упражнения) и, следовательно, матрица $-J$ не обладает сбалансированным разложением в произведение двух сомножителей.

В случае $k \geqslant 3$ по теореме 3 нам достаточно доказать следующее утверждение.

Теорема 2′. *Пусть $n \geqslant 2$ и $k \geqslant 3$ — целые числа и F — поле (необязательно конечное). Тогда следующие условия равносильны*:

а) *каждая матрица $n \times n$ над F обладает уравновешенным разложением в произведение k коммутирующих множителей*;

б) *каждый элемент поля F обладает нестепенным уравновешенным разложением в произведение k множителей.*

Доказательство. Импликация б) $\Rightarrow$ а) сразу вытекает из следующего факта, доказанного в [4].

> Пусть F — поле и k — натуральное число, большее двух. Если во всех конечных расширениях поля F каждый элемент обладает нестепенным сбалансированным разложением в произведение k элементов, то это же верно для каждого элемента каждой конечномерной ассоциативной алгебры с единицей над F.

Импликация а) $\Rightarrow$ б). Заметим, что $0 \in F$ имеет нестепенное уравновешенное разложение в произведение k множителей для любого $k \geqslant 3$: $0 = 0^{k-2} \cdot 1 \cdot (-1)$. Чтобы разложить ненулевой элемент $a \in F$, нам понадобится следующий простой факт из линейной алгебры, доказательство которого мы тоже оставляем читателям в качестве упражнения:

> централизатор нильпотентной жордановой клетки J размера $n \times n$ в алгебре матриц $n \times n$ состоит из многочленов от J, т. е. $C(J) = \{a_0E + a_1J + \ldots + a_{n-1}J^{n-1} \mid a_i \in F\}$.

Теперь если жорданова клетка $aE + J$ обладает сбалансированным разложением $aE + J = X_1 \ldots X_k$ в произведение коммутирующих матриц, то все эти матрицы X_i лежат в централизаторе матрицы J и, в силу упомянутого выше факта, мы получаем уравновешенное разложение элемента a в поле F: $a = x_1 \ldots x_k$, где x_i — единственное собственное значение матрицы X_i. Остаётся заметить, что это разложение не может быть степенным при $a \neq 0$. Действительно, предположив противное, мы бы получили такое уравновешенное разложение в кольце матриц: $aE + J = (xE + J_1) \ldots (xE + J_k)$, где J_i — некоторые нильпотентные коммутирующие матрицы. Уравновешенность этого разложения означает, что k делится на $\operatorname{char} F$ и $\sum J_i = 0$. Но тогда, раскрывая скобки, мы получаем

$$aE + J = (xE + J_1) \ldots (xE + J_k) = aE + f(J_1, \ldots, J_k),$$

где многочлен f не имеет членов первой степени, т. е. в правой части равенства стоит матрица $aE + J'$, где $(J')^{n-1} = 0$ и, значит, $J' \neq J$. Полученное противоречие завершает доказательство теорем $2'$ и 2. □

Без условий коммутативности вопрос об уравновешенных разложениях в алгебрах матриц над конечными полями остаётся открытым.

Вопрос. При каких q, k и n верно, что всякая матрица размера $n \times n$ над полем из q элементов имеет уравновешенное разложение в произведение k матриц того же размера?

Мы можем сказать лишь следующее.

1. В некоторых случаях разложение существует по теореме 2.

2. При $k = 2 \leqslant n$ разложения нет по теореме 2 (поскольку сомножители такого уравновешенного разложения обязательно коммутируют).

Кроме того, компьютерные эксперименты показывают следующее.

3. Над полем из двух элементов все матрицы 2×2, кроме $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ и (подобной ей матрицы) $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, допускают уравновешенное разложение в произведение трёх сомножителей, а эти две матрицы не имеют таких разложений.

4. Матрица $\begin{pmatrix}1&0\\1&1\end{pmatrix}$ и две подобные ей матрицы над полем из двух элементов не имеют уравновешенных разложений в произведение четырёх множителей, а остальные матрицы 2×2 над $\mathbb{F}_2$ имеют такие разложения.

5. Матрица $\begin{pmatrix}1&0&0\\1&1&0\\0&0&1\end{pmatrix}$ и подобные ей матрицы над полем из двух элементов не имеют уравновешенных разложений в произведение трёх множителей, а остальные матрицы 3×3 над $\mathbb{F}_2$ имеют такие разложения.

6. Все матрицы 3×3 над $\mathbb{F}_2$ имеют уравновешенные разложения в произведение четырёх множителей.

7. Все матрицы 2×2 над полями $\mathbb{F}_3$, $\mathbb{F}_4$, $\mathbb{F}_5$ и $\mathbb{F}_7$ имеют уравновешенные разложения в произведение трёх и четырёх множителей. Отсюда вытекает, что и для любого большего числа множителей это верно, поскольку мы можем увеличивать количество множителей на два, умножая имеющееся разложение на E и $-E$.

Список литературы

[1] *Васильев А. Н.* Казахстанская республиканская олимпиада по математике. 2013. Заключительный этап. 9 класс. Задача 4. http://matol.kz/olympiads/151

[2] *Васильев А. Н.* Девятая студенческая олимпиада по алгебре в МГУ. 2014. Задача 3. http://halgebra.math.msu.su/Olympiad/

[3] *Иванищук А. В.* Из опыта учебно-исследовательской деятельности учащихся в лицее 1511 при МИФИ // *Сгибнев А. И.* Исследовательские задачи для начинающих. М.: МЦНМО, 2015. С. 21–25. http://www.mccme.ru/free-books/sgibnev-issl.pdf

[4] *Klyachko A. A., Vassiliyev A. N.* Balanced factorizations // American Mathematical Monthly. 2016. V. 123, № 10. P. 989–1000. См. также https://arxiv.org/abs/1506.01571

Антон Александрович Клячко, мехмат МГУ
klyachko@mech.math.msu.su

Андрей Михайлович Мажуга, мехмат МГУ
mazhuga.andrew@yandex.ru

Анастасия Николаевна Понфиленко, мехмат МГУ
stponfilenko@gmail.com

Разностные множества, конечные геометрии, матрицы Царанкевича и экстремальные графы

С. Б. Гашков

§ 1. Введение

В статье будет рассказано о некоторых интересных понятиях и результатах современной комбинаторики. Надеемся, что они будут интересны читателю хотя бы потому, что в неявном виде появляются во многих задачах, предлагавшихся на олимпиадах для школьников. Такие задачи рассыпаны по всему следующему далее тексту [1)]. К большинству из них даны указания, а иногда и полные решения. Начнём со следующей задачи.

Задача 1 (XLIV Московская математическая олимпиада (1981), 9 кл., задача 5). У правильного 1981-угольника отмечены 64 вершины. Доказать, что существует трапеция с вершинами в отмеченных точках.

Указание. Рассмотрите все возможные прямые, продолжающие стороны и диагонали правильного n-угольника. Они разбиваются на n множеств («направлений») так, что все прямые одного направления параллельны, а прямые разных направлений — нет. Пусть в n-угольнике выделены k вершин. Если $k(k-1)/2 > n$, то согласно принципу Дирихле найдутся две параллельные прямые, пересекающие n-угольник в выделенных четырёх вершинах. Они и образуют трапецию (причём равнобокую), так как она симметрична относительно диаметра описанного вокруг n-угольника круга, перпендикулярного её основаниям; прямоугольником она быть не может, так как тогда её диагонали были бы тоже диаметрами этого круга, что невозможно в правильном нечётноугольнике.

Задача 1 равносильна следующей комбинаторной задаче. Пусть среди чисел от 0 до 1980 выбрано 64 числа. Тогда обязательно сумма по модулю 1981 каких-то двух различных выбранных чисел равна сумме по модулю

[1)] Некоторые задачи реально на олимпиадах не появлялись, но вполне могли бы быть.

1981 какой-то другой пары выбранных чисел[2)]. Для того чтобы убедиться в равносильности этих задач, достаточно занумеровать все вершины многоугольника по кругу. Другая равносильная формулировка: разность по модулю 1981 каких-то двух выбранных чисел равна разности по модулю 1981 каких-то двух других выбранных чисел. Действительно, если $a+b=c+d \bmod n$, то $a-c=d-b \bmod n$ и обратно. Возникает интересная и очень трудная задача: можно ли число 64 заменить меньшим, точнее: какое наибольшее подмножество можно выбрать в множестве $\{0, \ldots, 1980\}$ так, чтобы в нём все попарные разности были разными. Такие множества называются *разностными* и изучаются в комбинаторике.

Если заменить 1981 произвольным числом n, то верхнюю оценку для максимальной мощности k такого разностного множества можно получить в виде

$$k \leqslant \left\lfloor \frac{\sqrt{8n+1}+1}{2} \right\rfloor,$$

где $\lfloor\cdot\rfloor$ обозначает целую часть («пол»). Действительно, рассмотрим все различные попарные суммы. Их ровно $k(k-1)/2$ штук. По условию этих сумм должно быть не больше n, т. е. должно выполняться неравенство $k(k-1) \leqslant 2n$, из которого следует, что $k \leqslant (\sqrt{8n+1}+1)/2$. Можно наложить в определении разностного множества и более сильное ограничение: разности[3)] должны быть разными у любых двух упорядоченных пар чисел, даже если эти две пары содержат общее число. Таким образом, должны быть различны разности $a-b$ и $b-c$, и даже разности $a-b$ и $b-a$. Очевидно, это условие равносильно тому, что различными должны быть любые попарные суммы, например, разрешается паре состоять из равных чисел, т. е. для любых чисел a, b, c не должно выполняться равенство $a+b=2c$, а в случае чётного n не должно быть разности $a-b=n/2$. Тогда задача построения максимального разностного множества будет равносильна задаче выбора в правильном n-угольнике максимального множества вершин, среди которых не только не найдётся трапеции, но и не найдётся вершин, образующих равнобедренный треугольник (который можно рассматривать как вырожденную трапецию), а в случае чётного n ещё и не должно быть двух диаметрально противоположных вершин.

Задача 2 (вариант задачи 1). В правильном n-угольнике при нечётном n отмечено $\lceil(\sqrt{8n+1}+1)/2\rceil$ вершин. Доказать, что существует трапеция или равнобедренный треугольник с вершинами в этих точках.

[2)] Операция $a+b \bmod n$ называется сложением по модулю n, если её результат равен остатку от деления обычной суммы $a+b$ на n. Аналогично определяется и вычитание по модулю n.

[3)] Далее слова «по модулю n» опускаем.

Если разностное множество состоит из k чисел, то число $k(k-1)$ разностей по модулю n, образованных разными парами, должно быть не больше $n-1$, т. е. должно выполняться условие $k(k-1)+1 \leqslant n$. Вопрос, бывают ли разностные множества, у которых $k(k-1)+1=n$, представляет большой интерес. У этих множеств каждое число от 1 до $n-1$ представляется в виде разности по модулю n каких-то двух чисел из данного множества, причём единственным способом. На самом деле в комбинаторике обычно именно эти множества и называются *циклическими разностными множествами*. Ясно, что такие множества существуют только при нечётном n. Равносильная формулировка такая: если для данного множества M рассмотреть его циклические сдвиги $M+a \bmod n$, где $a=1,\ldots,n-1$, то любые два из этих сдвигов (в том числе и само $M=M+0$) имеют ровно одно общее число, и каждая пара чисел (x,y) принадлежит (ровно одному) сдвигу. Построенная система из $n=q^2+q+1$ множеств, $q=k-1$, обладает следующими свойствами. Каждое множество состоит из $q+1=k$ чисел, каждая пара различных чисел из множества $\{0,\ldots,n-1\}$ принадлежит ровно одному множеству. Указанное семейство множеств называется *конечной проективной плоскостью порядка q*. Известно, что если q есть степень простого числа, то такие плоскости действительно существуют, в частности в множестве $\{0,\ldots,1892\}$ существует[4] циклическое разностное множество из 44 чисел, а множества большего размера не существует. Приводить пример упомянутого разностного множества здесь неуместно, так как он достаточно громоздкий и проверка его правильности затруднительна. Вместо него приведём два примера циклических разностных множеств при $n=13$: это множества $\{0,1,3,9\}$ и $\{0,1,4,6\}$.

Что будет, когда n не равно степени простого, до конца не ясно. Известно, что если q равно $4t+1$ или $4t+2$ и при этом нельзя представить q в виде суммы квадратов двух целых чисел, то такого множества не существует[5]. Например, при $q=6$ эти условия не выполняются, т. е. в множестве $\{0,\ldots,42\}$ нет циклического разностного множества из 7 чисел. Это означает, что среди любых 7 вершин правильного 43-угольника найдётся либо трапеция, либо её вырожденный случай — равнобедренный треугольник.

Задача 3. В правильном 31-угольнике отмечены 7 вершин. Доказать, что существует трапеция или равнобедренный треугольник с вершинами в этих точках. Можно выделить 6 вершин так, что не существует ни трапеции, ни равнобедренного треугольника с вершинами в этих точках.

---

[4] Согласно теореме Зингера, сформулированной далее.

[5] Теорема Брука и Райзера, см. [13, 14].

§ 2. Разностные множества, конечные геометрии и блок-схемы

Введём понятия, о которых идёт речь в заголовке.

Блок-схемой[6] называется такое размещение v различных элементов по b блокам из k различных элементов каждый, что каждый элемент принадлежит ровно r блокам и каждая пара различных элементов появляется точно в λ блоках. Если $r = b$, то схема называется *симметричной*.

Задача 4. Докажите, что $bk = vr$, $r(k-1) = \lambda(v-1)$. Докажите, что в определении блок-схемы условие принадлежности каждого элемента равному числу блоков излишне (т. е. его можно вывести из остальных условий определения).

Множество $D = \{a_1, \ldots, a_k\}$ из k различных элементов множества $\{0, \ldots, v-1\}$ называется (v, k, λ)-*циклическим разностным множеством*, если для всякого $d \neq 0$ найдётся ровно λ таких упорядоченных пар (a_i, a_j), что $a_i - a_j \bmod v = d$. Связь таких множеств с блок-схемами указывает

Теорема 1. *Множество* $D = \{a_1, \ldots, a_k\} \subset \{0, 1, \ldots, v-1\}$ *является циклическим* (v, k, λ)-*разностным множеством тогда и только тогда, когда множества* $B_i = \{a_1 + i \bmod v,\ \ldots,\ a_k + i \bmod v\} \subset \{0, 1, \ldots, v-1\}$, *где* $i = 0, \ldots, v-1$, *являются блоками*

Множество называется *конечной проективной плоскостью*, если выполнены следующие условия[7] (обычно называемые аксиомами).

Ax1: *для любых двух различных точек существует, причём ровно одна, прямая, через них проходящая*;

Ax2: *любые две прямые имеют ровно одну общую точку*;

Ax3: *существуют четыре точки, из которых любые три не лежат на одной прямой.*

Изучением вопросов, связанных с проективными плоскостями, московские математики заинтересовались после войны, поэтому неудивительно, что на московской олимпиаде уже в 1946 г. во всех классах с 7 по 10 предлагалась следующая задача, в которой речь шла фактически о конечных проективных плоскостях.

Задача 5 (IX Московская математическая олимпиада (1946), второй тур, 7–8 кл., задача 5). Автобусная сеть города устроена следующим образом:

1) с любой остановки на любую другую остановку можно попасть без пересадки;

---

[6] Сейчас более моден термин 2-дизайн.

[7] Есть и другие равносильные аксиоматизации.

2) для любой пары маршрутов найдётся, и притом единственная, остановка, на которой можно пересесть с одного из этих маршрутов на другой;

3) на каждом маршруте ровно 3 остановки.

Сколько автобусных маршрутов в городе?

Вариант задачи (второй тур, 9–10 кл., задача 4): число маршрутов равно 57, и на каждом не менее трёх остановок. Сколько остановок могут иметь маршруты?

Указание. См. теорему 2. Ответ к основной задаче см. на левой части рис. 2 (с. 154).

Ещё две задачи, связанные с конечными геометриями (хотя сразу это не очевидно).

Задача 6 (XLVIII Московская математическая олимпиада (1985), 10 кл., задача 4). Даны 1985 множеств, каждое из которых состоит из 45 элементов, причём объединение любых двух множеств содержит ровно 89 элементов. Сколько элементов содержит объединение всех этих 1985 множеств?

Задача 7. В классе ученики ходят на 10 кружков, каждый кружок посещают четверо, и для любых двух кружков есть только один ученик, который ходит на оба кружка. Сколько может быть учеников в классе?

Решим для примера последнюю задачу. Приведём сразу ответ: 31 и 13. Рассмотрим задачу в следующей формулировке: даны 10 множеств из 4 элементов каждое, причём объединение любых двух содержит ровно 7 элементов. Сколько элементов может быть в объединении всех этих множеств? Укажите все возможные значения.

Будем проводить рассуждения иногда и для более общего случая, а именно, когда в каждом из множеств k элементов, а число множеств равно n. Число элементов в объединении всех n множеств обозначим m. Из условия следует, что любые два множества имеют ровно один общий элемент. Назовём эти множества «прямыми», а их объединение — «плоскостью». Тогда полученная «конечная геометрия» удовлетворяет двум «аксиомам» — любые две разные «прямые» имеют не более одной общей «точки», и через каждую точку проходит хотя бы одна прямая (далее кавычки опускаем). Очевидно, что если все n прямых имеют общую точку, то общее число точек на них $m = 1 + n(k - 1)$. Поскольку $k = 4$, один из возможных ответов в задаче: $m = 1 + 10 \cdot 3 = 31$. А что будет, если *не все* прямые имеют общую точку? Тогда каждый *пучок прямых* (т. е. множество всех прямых, проходящих через одну точку) содержит не более чем k прямых. Действительно, есть хотя бы одна прямая l, не входящая в него. Все прямые пучка пересекают l, причём в разных точках (ведь их общая точка не лежит на l), поэтому число прямых в пучке не больше k, а общее число точек на прямых этого пучка не больше $1 + k(k-1)$. Если в пучке k прямых, то точек на нём будет $1 + k(k-1)$. Докажем для числа прямых неравенство $n \leqslant 1 + k(k-1)$. Действительно, кроме прямой l есть не более $k(k-1)$ прямых, так как каждая прямая пересекает l в одной из k её точек, а через каждую такую точку проходит не более $k-1$ прямых, не считая самой l. Если в каждом пучке меньше k прямых, то точно так же доказывается, что $n \leqslant 1 + k(k-2)$. Так как в нашем случае $n = 10 > 1 + 4 \cdot 2$, найдётся пучок, в котором k прямых. Но тогда, как было уже доказано, $m \geqslant 1 + k(k-1)$.

Покажем, что тогда $m = 1 + k(k-1)$. Если $m > 1 + k(k-1)$, то найдётся точка A, не лежащая на прямых этого пучка. Рассмотрим проходящую через неё прямую. Она не совпадает с прямыми пучка (в силу выбора точки A) и пересекается с каждой из них, причём эти точки различны и не совпадают с A. Тогда на прямой $k+1$ точка, а это противоречит условию.

Остаётся привести пример «плоскости» с 13 точками и 10 прямыми.

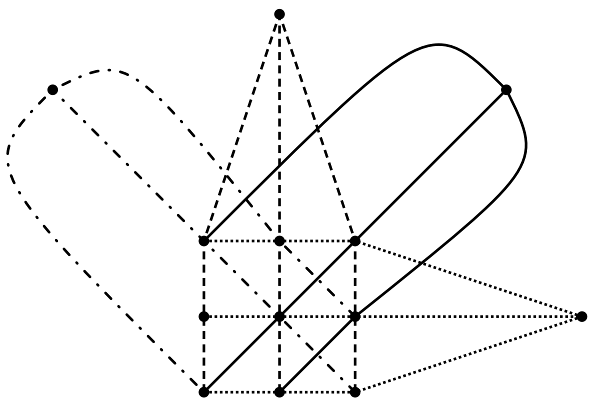


Рис. 1. «Плоскость» с 13 точками и 10 прямыми

В этом примере однотипные прямые очевидно имеют общую точку, так как образуют пучки. Прямые разного типа тоже попарно пересекаются, что менее очевидно, но легко проверяется. На самом деле даже можно нарисовать ещё 3 прямые так, чтобы любые две из 13 прямых попарно пересекались.

Равенство $n = 1 + k(k-1)$ возможно только в случае, когда в каждом пучке ровно k прямых. Докажем, что тогда через любую пару точек A, B проходит прямая (причём единственная). Действительно, проведя через A прямую l, не проходящую через B (если прямая проходит через B, то доказывать нечего, а какая-нибудь прямая через каждую точку проходит), рассмотрим пучок из k прямых, проходящих через B. Все они пересекают прямую l, причём в разных точках. Так как точек на прямой тоже k, одна из прямых этого пучка проходит через точку A прямой l, что и требовалось. Описанная плоскость состоит из $1 + k(k-1)$ точек, содержит столько же прямых, каждая из которых содержит k точек, в каждом пучке k прямых и выполнены две аксиомы: через любые две точки проходит единственная прямая и любые две прямые имеют общую точку. Это аксиомы проективной геометрии, а описанная плоскость является *конечной проективной плоскостью.* Однако неясно, при любом ли k существует такая «плоскость» на самом деле, т. е. возможно ли такое семейство конечных множеств. Если $q = k - 1$ есть степень простого числа, то это возможно. Выше это было фактически доказано в случае $q = 3$.

Если бы в условии задачи было $n > 1 + k(k-1)$ множеств, то тривиальный ответ $1 + (k-1) \cdot n$ был бы единственным, что по существу и доказано.

В случае $k = 4$ и $10 \leqslant n \leqslant 13$ кроме тривиального ответа $1 + 3 \cdot n$ есть ещё ответ 13, что фактически и было доказано (приведённый пример для 10 прямых дополняется до 13 прямых с соблюдением условий задачи и без увеличения числа точек).

Если в условии задачи будет не 10, а 9 множеств, то кроме ответа $1 + 9 \cdot 3 = 28$ будут ещё ответы $13, 12$. Для получения ответа 13 достаточно выбрать 9 прямых из указанных 10 так, чтобы какой-то пучок из 4 прямых содержался в выбранных девяти (очевидно, что этот ответ сохранится и во всех случаях $n \geqslant 4$). Для получения ответа 12 достаточно из 13 прямых, образующих плоскость с 13 точками, удалить 4 прямые, образующие пучок. Тогда оставшиеся 9 прямых содержат 12 точек (очевидно, что таким же образом получаем ответ 12 для любого n, $5 \leqslant n \leqslant 9$).

Покажем, что для $n = 8, 9$ других ответов нет. Докажем, что $m \geqslant 12$. Можно считать, что плоскость не содержит пучков с четырьмя прямыми (иначе уже на этом пучке 13 точек, а больше точек быть не может, как было доказано выше). Пусть точек, через которые проходит i прямых, имеется x_i. Подсчитывая двумя способами число пар «точка и проходящая через неё прямая», получаем уравнение $4n = 3x_3 + 2x_2 + x_1$. Подсчитывая двумя способами число пар прямых, получаем уравнение $n(n-1)/2 = 3x_3 + x_2$. В случае $n = 9$ из этих уравнений получаем $x_1 + x_2 = 0$, значит, $m = x_3 = 12$ и на плоскости 12 точек. В случае $n = 8$ имеем $x_1 + x_2 = 4$, значит,

$$m = x_3 + 4 = 4 + \frac{n(n-1)}{6} - \frac{x_2}{3} = 13 + \frac{1 - x_2}{3} \geqslant 12,$$

так как $x_2 \leqslant 4$, и очевидно $m < 14$, т. е. $m = 12, 13$.

В случае $n = 7$ аналогично получаем $x_1 + x_2 = 7$ и неравенство

$$14 \geqslant m = x_3 + 7 = 7 + 7 - \frac{x_2}{3} = 14 - \frac{x_2}{3} > 11,$$

т. е. $m = 12, 13, 14$. Возможность ответов $m = 12, 13$ уже доказана. Ответ $m = 14$ возможен только в случае $x_2 = 0, x_1 = 7$. Для построения такой «плоскости» достаточно построить плоскость с 7 точками и 7 прямыми (см. рис. 1) и добавить к каждой прямой по одной точке (разным прямым разные точки).

В случае $n = 6$ аналогично получаем $x_1 + x_2 = 9$ и неравенство

$$14 \geqslant m = x_3 + 9 = 9 + 5 - \frac{x_2}{3} = 14 - \frac{x_2}{3} \geqslant 11,$$

т. е. $m = 11, 12, 13, 14$. Ответ 11 получается, если из плоскости с 13 прямыми удалить два пучка (вместе содержащие 7 прямых). Оставшиеся 6 прямых покрывают оставшиеся 11 точек. Случай $m = 14$ невозможен, так как тогда $x_2 = 0, x_1 = 9$, значит, имеется 9 точек, через каждую проходит одна прямая, поэтому прямых не менее 9, что невозможно. Значит, при $n = 6$ ответ $m = 11, 12, 13$. В случае $n = 5$ имеем $x_1 + x_2 = 10$,

$$13 \geqslant m = x_3 + 10 = 10 + 3 + \frac{1 - x_2}{3} = 13 + \frac{1 - x_2}{3} \geqslant 10,$$

т. е. $m = 10, 11, 12, 13$. Ответы 12, 13 возможны, как было уже показано. Ответ 10 возможен, так как тогда $x_2 = 10, x_1 = 0 = x_3$, т. е. через 5 точек проходят 10 прямых, причём через каждую точку — ровно две. Чтобы убедиться в возможности такой конфигурации, достаточно провести на обычной плоскости 5 попарно не параллельных прямых так, чтобы никакие три не пересекались в одной точке. В случае $m = 11$ очевидно $x_3 = 1, x_2 = 7, x_1 = 3$. Такой случай также возможен, достаточно провести на обычной плоскости 5 прямых, три из них через одну точку, тогда на остальных двух будет по четыре точки попарных пересечений, а всего их будет 8 (с учётом точки пересечения трёх прямых), нужно ещё на каждой из трёх прямых, проходящих через одну точку, выбрать по одной точке — и конфигурация готова.

В случае $n = 4$ имеем $x_1 + x_2 = 10$,

$$12 \geqslant m = x_3 + 10 = 10 + 2 - \frac{x_2}{3} = 12 - \frac{x_2}{3} \geqslant 10,$$

т. е. $m = 10, 11, 12$. Ответ 10 получается, если провести на обычной плоскости 4 прямые с попарными точками пересечения (таких точек, в каждой из которых пересекаются ровно две прямые, будет 6) и ещё на каждой прямой выбрать по одной точке. Ответ 11 получается, если провести на обычной плоскости 4 попарно пересекающиеся прямые, из которых три проходят через одну точку, на них выбрать ещё по две точки, и ещё одну точку на четвёртой прямой. Случай $m = 12$ невозможен, так как тогда $x_2 = 0, x_3 = 2, x_1 = 10$, но четыре прямые не могут иметь две тройные точки пересечения (тогда прямых было бы пять).

В случае $n = 3$ имеем $x_1 + x_2 = 9$, $3 = 3x_3 + x_2$,

$$10 \geqslant m = x_3 + 9 = 9 + 1 - \frac{x_2}{3} = 10 - \frac{x_2}{3} \geqslant 9,$$

т. е. $m = 9, 10$. Ответ 9 получается, если провести на обычной плоскости 3 прямые с попарными точками пересечения (их будет 3) и ещё на каждой прямой выбрать по две точки. Ответ 10 тривиально возможен. В случае $n = 2$ очевидно возможен только тривиальный ответ.

Читатель может попробовать решить и более общую задачу: в семействе из n множеств по k элементов любые два множества имеют только один общий элемент. Сколько элементов может быть в объединении этих множеств? Получить полное решение этой задачи, по-видимому, очень трудно.

Приведённые задачи обобщает и уточняет следующая классическая

Теорема 2. *Пусть $q \geqslant 2$ — целое число. Для конечной проективной плоскости равносильны следующие шесть условий.*

(i) *Некоторая прямая содержит $q + 1$ точку.*

(ii) *Некоторая точка лежит ровно на $q + 1$ прямой.*

(iii) *Каждая прямая содержит $q + 1$ точку.*

(iv) *Каждая точка лежит ровно на $q + 1$ прямой.*

(v) *Плоскость содержит ровно $q^2 + q + 1$ точек.*

(vi) *На плоскости существует ровно $q^2 + q + 1$ прямых.*

Такая плоскость называется *конечной проективной плоскостью порядка q* и обозначается иногда $\mathrm{PG}(2, q)$. Доказательство можно найти в [13–15]. Однако несложно доказать эту теорему и самостоятельно. Связь проективных плоскостей с блок-схемами указывает следующая

Теорема 3. *Конечная проективная плоскость порядка q образует симметричную блок-схему с $v = q^2 + q + 1$ элементами, $b = v$ блоками по $k = q + 1$ элементов в каждом и $\lambda = 1$. Обратно, симметричная $(q^2 + q + 1, q + 1, 1)$-блок-схема образует плоскость $\mathrm{PG}(2, q)$.*

Доказательство её (сравнительно простое) опускается. Желающие могут найти его в [13, 14].

Примером (получающейся при $q = 2$) $(7, 3, 1)$-блок-схемы служит

$$\bigl\{\{1, 2, 7\}, \{3, 4, 7\}, \{2, 3, 5\}, \{1, 4, 5\}, \{1, 3, 6\}, \{2, 4, 6\}, \{5, 6, 7\}\bigr\}.$$

Вопрос о связи проективных плоскостей с разностными множествами рассмотрим позднее, а сейчас уместно ввести понятие конечной аффинной плоскости. Множество называется *конечной аффинной плоскостью*, если

Ax1: *для любых двух различных её точек существует, причём ровно одна, прямая, через них проходящая*;

Ax2: *через точку вне данной прямой проходит ровно одна не пересекающая её* (параллельная ей) *прямая*;

Ax3: *каждая прямая содержит не менее двух точек*;

Ax4: *существует не менее двух прямых*.

Справедлива аналогичная теореме 2

Теорема 4. *Пусть $q \geqslant 2$ — целое число. Для конечной аффинной плоскости равносильны следующие шесть условий.*

(i) *Некоторая прямая содержит q точек.*

(ii) *Некоторая точка лежит ровно на $q+1$ прямых.*

(iii) *Каждая прямая содержит q точек.*

(iv) *Каждая точка лежит ровно на $q+1$ прямых.*

(v) *Плоскость содержит ровно q^2 точек.*

(vi) *На плоскости существует ровно q^2+q прямых.*

Доказательство аналогично теореме 2 (его можно найти в [13]).

Связь аффинных плоскостей с блок-схемами указывает следующая

Теорема 5. *Конечная аффинная плоскость порядка q образует блок-схему с $v = q^2$ элементами, $b = v + q$ блоками по $k = q$ элементов в каждом и $\lambda = 1$. Обратно, любая $(q^2, q, 1)$-блок-схема образует плоскость $\mathrm{AG}(2, q)$.*

Доказательство (аналогичное теореме 3) можно найти в [13].

Примером (получающейся при $q = 3$) $(9, 12, 3, 1)$-блок-схемы служит $\bigl\{\{1,2,3\}, \{4,5,6\}, \{7,8,9\}, \{1,4,7\}, \{2,5,8\}, \{3,6,9\}, \{1,5,9\}, \{2,6,7\}, \{3,4,8\}, \{3,5,7\}, \{1,6,8\}, \{2,4,9\}\bigr\}$.

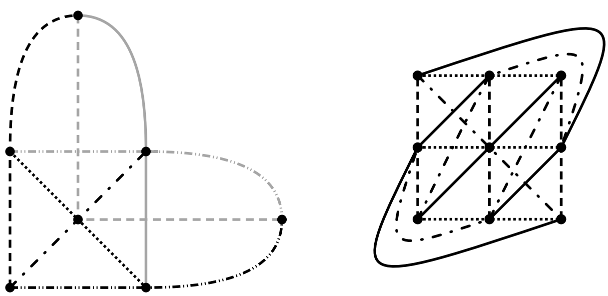


Рис. 2. Слева проективная плоскость $\mathrm{PG}(2,2)$ — плоскость Фано, справа аффинная плоскость $\mathrm{AG}(2,3)$.

Примеры проективной и аффинной плоскостей изображены на рис. 2.

Связь аффинных плоскостей с проективными указывает следующая

Теорема 6. *Аффинная плоскость порядка q существует тогда и только тогда, когда существует проективная плоскость порядка q.*

Доказательство (основанное на идее добавления бесконечно удалённых точек, образующих бесконечно удалённую прямую) можно найти в [13, 14].

2.1. Как можно построить конечные плоскости

Пусть $q = p^n$ — степень простого числа. Далее будет без доказательства использоваться следующий факт: существует *конечное поле* $\mathrm{GF}(q)$, состоящее из q элементов[8]. *Простое поле* $\mathrm{GF}(p)$ можно определить как множество чисел $\{0, 1, \ldots, p-1\}$, операции сложения и умножения в котором выполняются по модулю p, т. е. для нахождения суммы или произведения нужно вычислить обычную сумму или произведение и заменить её на остаток от деления на p. Читатель может сам проверить, что эти операции удовлетворяют тем же законам, что и операции сложения и умножения рациональных чисел, а именно, переместительному: $a+b \bmod p = b+a \bmod p$, $ab \bmod p = ba \bmod p$, сочетательному: $(a+b)+c = a+(b+c) \bmod p$, $(ab)c = a(bc) \bmod p$, распределительному: $a(b+c) = ab+ac$, и удовлетворяют тождествам $a+0=a$, $a\cdot 1 = a$, а также имеют однозначно определённые обратные операции вычитания $a-b \bmod p$ и деления $a/b \bmod p$, удовлетворяющие тождествам $(a-b)+b = a \bmod p$, $(a/b)b = a \bmod p$. Указанные выше свойства арифметических операций называются *аксиомами поля*[9]. Проверка их несложна, труднее всего доказывается возможность деления[10].

В случае $n > 1$ поле $\mathrm{GF}(p^s)$ можно определить как множество многочленов степени, меньшей n, с коэффициентами из простого поля $\mathrm{GF}(p)$. Сложение (и вычитание) многочленов определяется стандартным образом, т. е. коэффициенты складываются или вычитаются по модулю p, а умножение выполняется *по модулю данного неприводимого многочлена* $f(x)$ степени n с коэффициентами из поля $\mathrm{GF}(p)$, т. е. результат обычного умножения многочленов заменяется на остаток от деления на $f(x)$. Многочлен называется *неприводимым* над полем $\mathrm{GF}(p)$, если его нельзя разложить в произведение многочленов меньшей степени над тем же полем. Деление

[8] Такие поля называют полями порядка q, а обозначение напоминает о французском математике Эваристе Галуа, их открывшем.

[9] В отличие от аксиом геометрии Евклида выполнение аксиом поля для заданных операций на множестве $\mathrm{GF}(p)$ надо доказывать. Для поля рациональных чисел справедливость этих аксиом всем известна, поэтому можно считать их очевидными.

[10] Деление на нуль невозможно, так как из аксиом можно вывести, что $a \cdot 0 = 0$.

многочленов друг на друга с остатком определяется точно так же, как деление чисел с остатком, только вместо условия, что остаток от деления должен быть меньше делителя, используется условие, что степень остатка должна быть меньше степени делителя, т. е. многочлена $f(x)$. Доказательства того, что введённые выше арифметические операции в множестве $\mathrm{GF}(p^n)$ удовлетворяют всем аксиомам поля, и того факта, что такие поля при любом n и простом p действительно существуют, можно найти в книгах по алгебре[11)], например в [2, 7, 14].

Приведём пример построения конечного поля из 9 элементов. В нём фактически можно обойтись без использования многочленов над полем из 3 элементов, так как конструкция очень похожа на построение поля комплексных чисел. Рассмотрим множество $F_9 = \{\gamma_0, \ldots, \gamma_8\}$ из элементов вида (a, b), где $a, b = 0, \pm 1$. Определим на нём операцию сложения по формуле $(a, b) + (c, d) = (a + c, b + d)$, где $1 + 1 = -1$, $(-1) + (-1) = 1$, а всё остальное, как в обычном сложении. Операция умножения над числами $0, \pm 1$ берётся обычная, а операция умножения над парами (a, b), (c, d) определяется как $(ac - bd, ad + bc)$. Элемент $(0, 0)$ играет в этом поле роль нуля, а элемент $(1, 0)$ — роль единицы, в чём несложно убедиться. Элементы вида $(a, 0)$ образуют подполе в этом поле, состоящее из трёх элементов $(0, 0)$, $(1, 0)$, $(-1, 0)$. Для краткости их можно обозначать $0, 1, -1$. Выполнение операций в этом подполе сводится к выполнению указанных выше операций в множестве $\{0, 1, -1\}$. Элемент $(0, 1)$ при возведении в квадрат равен $(-1, 0)$, т. е. -1. Для любого (a, b) можно определить операцию вычисления обратного элемента относительно сложения (её можно назвать операцией смены знака): $-(a, b) = (-a, -b)$, где полагаем, что $-0 = 0$. Очевидно, что $(a, b) + (-(a, b)) = (0, 0) = 0$. После этого определяется операция вычитания: $(a, b) - (c, d) = (a, b) + (-c, -d)$, которая является обратной операцией к операции сложения. Для $(a, b) \neq (0, 0)$ можно ещё определить операцию вычисления обратного элемента относительно умножения: $(a, b)^{-1} = (-a, b)$, если $ab \neq 0$, а в остальных случаях $(a, 0)^{-1} = (a, 0)$, $(0, b)^{-1} = (0, -b)$. Несложно проверить, что $(a, b)^{-1} \cdot (a, b) = (1, 0)$.

Теорема 7. *Для любого q, равного степени простого числа, существует конечная проективная плоскость порядка q.*

Доказательство. Рассмотрим трёхмерное векторное пространство $\mathrm{GF}(q)^3$, т. е. множество троек (x_1, x_2, x_3), $x_i \in \mathrm{GF}(q)$, $i = 1, 2, 3$. Назовём две ненулевые тройки эквивалентными, если одна из них коллинеарна

[11)] В них также доказывается, например, что конечные поля порядка q существуют только для q, равных степени простого числа, и все поля равного порядка изоморфны, т. е. с алгебраической точки зрения одинаковы.

другой, т. е. $x_i = ay_i$, $i = 1, 2, 3$, $a \in \mathrm{GF}(q) \setminus \{0\}$. Класс эквивалентности троек назовём точкой проективной плоскости. В каждом классе эквивалентности ровно $q - 1$ ненулевых троек, поэтому число этих классов (число точек строящейся проективной плоскости) равно $(q^3 - 1)/(q - 1) = q^2 + q + 1$. Для произвольной ненулевой тройки $a = (a_1, a_2, a_3)$ рассмотрим двумерное подпространство в $\mathrm{GF}(q)^3$, состоящее из всех троек $x = (x_1, x_2, x_3) \in \mathrm{GF}(q)^3$, удовлетворяющих уравнению $(a, x) = a_1x_1 + a_2x_2 + a_3x_3 = 0$. Число таких троек равно q^2, из них одна нулевая, и все ненулевые разбиваются на $(q^2 - 1)/(q - 1) = q + 1$ классов коллинеарных троек, т. е. каждому такому двумерному подпространству можно сопоставить $q + 1$ точку строящейся проективной плоскости и назвать это множество прямой в этой плоскости. Любые два двумерных подпространства $(a, x) = 0$, $(b, x) = 0$ пересекаются по одномерному подпространству, ненулевые тройки которого определяют точку C строящейся проективной плоскости — (единственную) точку пересечения соответствующих прямых a и b. Число различных двумерных подпространств равно $(q^3 - 1)/(q - 1) = q^2 + q + 1$, так как подпространства $(a, x) = 0$, $(b, x) = 0$ совпадают тогда и только тогда, когда тройки a и b эквивалентны, следовательно, число прямых на строящейся проективной плоскости равно $q^2 + q + 1$. Через любые две точки A, C этой плоскости проходит единственная прямая a, а именно та, которая соответствует двумерному подпространству $(a, x) = 0$, натянутому на тройки из классов эквивалентности A, B. Теорема доказана. □

Теорема 8. *Для любого q, равного степени простого числа, существует конечная аффинная плоскость порядка q.*

Доказательство. Рассмотрим следующую блок-схему. Её точками являются упорядоченные пары $(x, y) \in \mathrm{GF}(q)^2$, количество которых q^2. Назовём прямой любое множество точек (пар), удовлетворяющих уравнению $ax + by = 1$, $ab \neq 0$. Число различных таких прямых равно $(q - 1)^2$. Добавим к ним ещё оси координат $(x, 0)$ и $(0, y)$ и все прямые, параллельные им, т. е. множества точек $\{(x, a)\colon x \in \mathrm{GF}(q)\}$, $\{(b, y), y \in \mathrm{GF}(q)\}$, а также все прямые, проходящие через начало координат, т. е. множества точек $\{(x, y)\colon y = kx \in \mathrm{GF}(q)\}$, $k \in \mathrm{GF}(q)\{0\}$. Число точек на каждой прямой равно q, а число всех прямых равно $(q-1)^2 + q + q + (q-1) = q^2 + q$. Через любую пару точек проходит ровно одна такая прямая. Для доказательства в случае точек (x_1, y_1), (x_2, y_2), не совпадающих с началом координат и не имеющих равных координат, достаточно проверить, что система двух уравнений $ax_1 + by_1 = 1$, $ax_2 + by_2 = 1$ относительно (a, b) имеет единственное решение (в остальных случаях всё очевидно). Аксиома о параллельности также может быть проверена непосредственно, но достаточно сослаться на теорему 5. □

2.2. Неожиданное явление плоскости Фано

Конечная проективная плоскость $\mathrm{PG}(2,2)$, изображённая на рис. 2, загадочным образом возникает в решении следующей задачи [12], опубликованной в сборнике головоломок [17], но фактически относящейся к серьёзной прикладной дисциплине — публичной криптографии.

Задача 8. Два шерифа соседних городов составили список из 7 подозреваемых в качестве серийного убийцы [13]. Потом каждый из них, проведя оперативно-разыскные действия, сократил список подозреваемых до двух человек. Эти списки различны, т. е. пересекаются только по одному подозреваемому, поэтому шерифы, обменявшись информацией, могут совместно арестовать убийцу (а в одиночку они этого сделать не могут). Но если эта информация будет перехвачена и станет известна жителям, то они поймут, кто убийца, и линчуют его, не дожидаясь ареста (список из семи подозреваемых им известен).

Как шерифам обменяться информацией, чтобы арестовать убийцу (и тем самым не допустить суда Линча)?

Задача может быть решена следующим образом (возможность придумать решение для случая 8 подозреваемых оставляется читателям).

Шерифы вначале нумеруют подозреваемых, далее подозреваемые называются точками [14], и один из шерифов объясняет другому, как построить на множестве из семи точек плоскость Фано. Потом каждый из них мысленно проводит прямую в этой плоскости через двоих своих подозреваемых, определяет оставшуюся (третью) точку этой прямой и сообщает её коллеге, а тот в ответ делает то же самое (сообщить явно две свои точки они не могут, так как тогда те, кто за ними шпионит, сразу определят общую точку и узнают убийцу, а по информации об одной точке прямая не определяется однозначно — таких прямых три). Возможны два случая: в первом обе прямые совпадают, а во втором — нет (далее будет ясно, что шпионы не смогут понять, какой из случаев реализовался).

Очевидно, что первый случай возможен только тогда, когда каждый шериф сообщил коллеге имя одного из подозреваемых этим коллегой (если первый подозревал A и B и сообщил коллеге имя C, а у второго шерифа получилась та же самая прямая с точками A, B, C, то второй сообщил имя A или B и подозревал соответственно B, C или A, C). В этом случае

[12] Об этой задаче и её решении мне сообщил А. В. Устинов.

[13] В книге [17] подозреваемых было 8, но потом для случая, когда их 7, было найдено решение на форуме http://mathoverflow.net/questions/203182/the-two-sheriffs-puzzle

[14] Как известно, Гильберт говорил, что после формулировки аксиом геометрии можно вместо точек, прямых и плоскостей говорить о столах, стульях и кружках пива.

шерифы сразу поймут, кто убийца (так как названные ими, очевидно, не являются убийцами), но шпионы об этом не узнают.

Во втором случае точка пересечения прямых очевидно указывает на убийцу. Но её нельзя найти, не зная самих прямых, — с точки зрения шпионов каждая из прямых может быть выбрана тремя способами, и пересекаться эти прямые могут в любой из пяти точек, отличных от двух, названных шерифами. Однако шерифы имеют больше информации, чем шпионы. Действительно, пусть список подозреваемых одного шерифа есть $\{A, B\}$, а назвал он точку C, тогда список второго шерифа, скажем, $\{A, D\}$ (списки должны иметь общую точку), а назвал он E. Точки C и E различны и отличаются от A, B, D (прямые $\{A, B, C\}$ и $\{A, D, E\}$ имеют только одну общую точку — точку A), шерифам (и шпионам) они известны, через них они могут провести прямую $\{C, E, F\}$ и найти ещё одну точку F, не совпадающую ни с A, B (потому, что прямые $\{A, B, C\}$ и $\{C, E, F\}$ пересекаются только в точке C), ни с D (прямые $\{A, D, E\}$ и $\{C, E, F\}$ пересекаются только в точке E). Таким образом, каждому из шерифов (и шпионов) ясно, что C, E, F выбывают из списка подозреваемых, и в нём остаются только A, B, D и ещё некий G (вне прямой лежит ровно четыре точки). Если теперь шерифы назовут двух своих подозреваемых, то в пересечении этих списков получится имя убийцы.

Но и шпионы могут сделать то же самое! Однако при этом они должны быть уверены, что реализовался именно второй случай, потому что в первом случае прямая $\{C, E, F\}$ (в обозначениях второго случая) совпала бы с прямой $\{A, B, C\}$ (в обозначениях первого случая) и предыдущий анализ потерял бы силу. Но определить, какой именно из случаев возник, шпионы очевидно не в состоянии.

В отличие от них шерифы легко замечают, что реализовался первый случай, вычисляют убийцу и для маскировки продолжают диалог так же, как и во втором случае, только называют не настоящие пары подозреваемых, а две другие пары (не лежащие на прямой $\{A, B, C\}$), и тем самым вводят шпионов в заблуждение (дезинформируя их об имени убийцы). Поэтому шпионы, понимая невозможность отличить друг от друга оба случая и соответственно верную информацию от дезинформации, вынуждены отказаться от планов линчевания.

2.3. И ЕЩЁ ОДНО ПОЯВЛЕНИЕ ПЛОСКОСТИ ФАНО

Начнём издалека и рассмотрим простейший пример кода, исправляющего одну ошибку. Допустим, нам нужно передать двоичное слово (x_1, x_2, x_3, x_4). Добавим к нему *проверочные символы* $x_5 = x_1 + x_3 + x_4$, $x_6 = x_1 + x_2 + x_4$, $x_7 = x_1 + x_2 + x_3$ (знак $+$ здесь обозначает сложение по модулю два;

символы x_1, x_2, x_3, x_4 называются *информационными*). Процедура вычисления по информационным символам проверочных и составления из них кодового слова (закодированного сообщения) называется кодированием (так же называется и само отображение исходного сообщения в кодовое слово). На языке матриц в рассматриваемом примере кодирование сводится к умножению некоторой матрицы M на транспонированный вектор $(x_1, x_2, x_3, x_4)^T$ (т. е. вектор, расположенный в столбец):

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix}.$$

Передаём закодированное сообщение $c = (x_1, \dots x_7)$ и получаем *зашумлённое сообщение* $r = c + e$, где $e = (e_1, \dots, e_7)$ — вектор ошибок. В нашем случае он имеет вес (сумму координат) 1, так как по предположению ошибка может произойти (если произойдёт) только в одной позиции. Например, возможно, $e = e_3 = (0, 0, 1, 0, 0, 0, 0)$. Тогда

$$r = c + e = (c_1, c_2, c_3 + 1, c_4, c_5, c_6, c_7) = (c_1, c_2, \bar{c}_3, c_4, c_5, c_6, c_7),$$

где $\overline{0} = 1, \overline{1} = 0$. Число 3 будет в рассматриваемом случае *позицией ошибки*. Для определения позиции ошибки (а значит, и обнаружения самой ошибки) можно вычислить *проверочные суммы*

$$S_1 = r_1 + r_3 + r_4 + r_5,$$
$$S_2 = r_1 + r_2 + r_4 + r_6,$$
$$S_3 = r_1 + r_2 + r_3 + r_7.$$

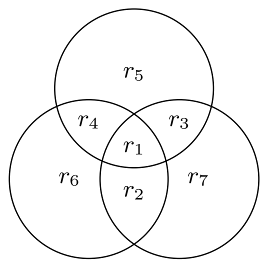


Рис. 3. Код Хэмминга с блоковой длиной 7

Построенный код является частным случаем кодов Хэмминга. Наглядно проверочные суммы изображены на рис. 3. Каждая сумма содержится в своём круге.

Обратим внимание на некоторые его свойства. Его мощность (количество кодовых слов) равна $2^4 = 16$, сумма любых двух кодовых слов по модулю два опять является кодовым словом, расстояние кода равно трём (расстояние $d(a, b)$ между кодовыми словами a, b равно числу позиций, в которых они отличаются, а расстояние кода по определению равно минимальному расстоянию между различными кодовыми словами). Так как код имеет кодовое слово веса нуль (нулевое слово), а кодовое расстояние равно трём, кодовых слов веса 1 или 2 в нём нет. Для каждого кодового слова рассмотрим шар радиуса 1 с центром в нём. Этот шар содержит, кроме центра, ещё 7 двоичных наборов (вершин семимерного двоичного куба), получающихся, если в центральном наборе заменить ровно один из семи его символов на противоположный. Эти шары с центрами в кодовых словах не пересекаются[15)], поэтому в совокупности содержат $2^4 \cdot 8 = 2^7$ различных вершин куба, т. е. все эти вершины. Такие точные покрытия многомерного куба непересекающимися шарами называются *совершенными*, а соответствующие им коды — *совершенными кодами*.

Исходя только из свойства совершенности указанного кода, можно однозначно определить число кодовых вершин на третьем слое семимерного куба[16)].

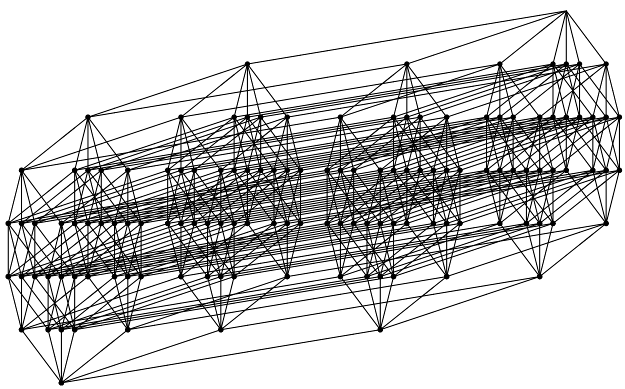


Рис. 4. Семимерный куб (условное изображение)

Для этого рассмотрим единичные сферы с центрами в кодовых словах веса три (сфера — это шар без центра). Заметим, что их пересечения со вторым слоем куба[17)] имеют мощность 3 (так как есть только три набора веса два, лежащих на данной сфере: действительно, среди координат центра сферы только три единицы, которые можно заменять на нули). Эти сечения не пересекаются, так как расстояние между центрами сфер равно трём. Поэтому число кодовых слов веса три не больше $\binom{7}{2} : 3 = 7$. А так как вершины второго слоя покрываются только шарами с центрами в третьем слое (шары с центрами в четвёртом и более высоких слоях до второго слоя

[15)] Если шары с центрами a, b имеют общую точку c, то $d(a,b) \leqslant d(a,c) + d(c,b) \leqslant 2$, что невозможно.

[16)] k-й слой куба состоит из всех вершин веса k и очевидно содержит $\binom{7}{k}$ вершин.

[17)] Все вершины одного слоя куба лежат на плоскости с уравнением $x_1 + \ldots + x_7 = k$, поэтому указанные пересечения можно рассматривать как сечения сфер плоскостью.

не достают), и код совершенный, то число кодовых слов веса три в точности равно 7. Вычислим, сколько вершин четвёртого слоя покрывается семью рассмотренными шарами. Каждый шар покрывает 4 вершины, эти сечения шаров плоскостью попарно не пересекаются, поэтому общее число покрытых вершин 4-го слоя равно $7 \cdot 4 = 28$. Непокрытых вершин в нём остаётся $\binom{7}{4} - 28 = 7$. В третьем слое непокрытых вершин $\binom{7}{3} - 7 = 28$, так как покрыты только центры шаров, а их семь. Непокрытые вершины третьего слоя можно покрыть только шарами с центрами в четвёртом слое, а каждый такой шар покрывает в третьем слое ровно 4 вершины. Значит, для покрытия оставшихся вершин третьего слоя нужно не менее $28/4 = 7$ шаров с центрами в четвёртом слое, а непокрытых вершин там ровно 7, значит, все их нужно использовать в качестве кодовых вершин (и центров шаров). Поэтому кодовых вершин веса 4 в точности 7. Соответствующие шары покрывают в пятом слое $7 \cdot 3 = 21$ вершину (шары попарно не пересекаются, так как их центры — кодовые слова), т. е. все его вершины. Кодовых слов на шестом слое быть не может, так как шар с центром в этом слое содержит вершины пятого слоя, а они уже покрыты. Остаётся единственная вершин седьмого слоя — единичная вершина, которая должна входить в код, чтобы её сфера покрыла шестой слой. Таким образом, предполагая существование совершенного кода с расстоянием три в семимерном кубе, можно точно установить его *весовой спектр*, а именно число его слов заданного веса. Он состоит из чисел $a_0 = 1$, $a_1 = 0$, $a_2 = 0$, $a_3 = 7$, $a_4 = 7$, $a_5 = 0$, $a_6 = 0$, $a_7 = 1$.

Посмотрим на кодовые слова веса три. Каждое из них определяет трёхэлементное подмножество в множестве $\{1, 2, 3, 4, 5, 6, 7\}$, состоящее из номеров позиций единиц в этом слове. Очевидно, что любые два из этих множеств имеют не более одного общего элемента (иначе расстояние между кодовыми словами было бы равно двум). Поэтому система из этих 7 троек образует *систему троек Штейнера*, т. е. каждая пара элементов (а их ровно $\binom{7}{2} = 21$) принадлежит ровно одной тройке (потому что семь троек содержат в точности 21 пару). На самом деле общий элемент у любых двух троек ровно один, так как если бы две тройки не пересекались, то остальные тройки, которые пересекаются с этими двумя не более чем по одному элементу, должны иметь один общий для всех элемент — тот, который не принадлежит двум первым тройкам. Но других общих элементов у них быть не может, значит, таких троек не более трёх, а всего троек не более пяти, в то время как их должно быть семь.

Поэтому система троек изоморфна конфигурации 7 прямых в проективной плоскости на 7 точках — плоскости Фано (см. рис. 2) А расстояние между любыми двумя кодовыми словами из третьего слоя равно 4. Из проведённых рассуждений следует также, что максимальное число вершин третьего слоя семимерного куба, попарные расстояния между которыми не меньше трёх (или четырёх), равно семи. (Коды, все вершины которых лежат на одном слое куба, называются *равновесными кодами*.) Таким образом, максимальная мощность кода веса три со словами длины 7 также равна семи.

§ 3. Примеры разностных множеств и теорема Зингера

Справедлива следующая

Теорема 9 (Зингер). *В проективной геометрии* $\mathrm{PG}(2, q)$, $q = p^r$, *прямые, взятые в качестве блоков, образуют симметричную блок-схему с параметрами* $v = q^2 + q + 1$, $k = q + 1$, $\lambda = 1$. *Эта схема циклическая, а точки любой прямой определяют циклическое* (v, k, λ)*-разностное множество.*

Доказательство (непростое) можно найти в [13, 14].

Вот пример $(31, 6, 1)$-разностного множества, построенного с помощью этой теоремы: $\{0, 1, 15, 19, 21, 24\}$. Можно, вычисляя все 30 попарных разностей по модулю 31, непосредственно убедиться, что все они разные и каждое число от 1 до 30 появляется среди них ровно один раз.

Применение построенного разностного множества к задаче 3 см. на рис. 5.

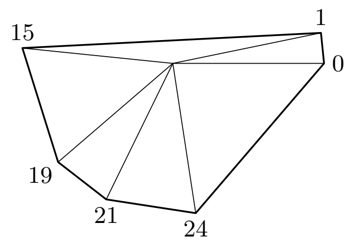


Рис. 5. Шестиугольник из вершин правильного 31-угольника без трапеций и равнобедренных треугольников

Вращая этот шестиугольник вокруг центра данного правильного 31-угольника, получаем 31 «вписанный» шестиугольник, любые два из которых имеют только одну общую вершину. Получим 31 множество, каждое из которых совпадает с множеством вершин соответствующего шестиугольника. Эти множества образуют модель проективной плоскости 5-го порядка.

Следующая задача подобна задаче 3, но существенно труднее.

Задача 9. В правильном 43-угольнике отмечены 7 вершин. Доказать, что существует трапеция или равнобедренный треугольник с вершинами в этих точках. Можно выделить 6 вершин так, что не существует ни трапеции, ни равнобедренного треугольника с вершинами в этих точках.

Указание. Если бы какой-то семиугольник не содержал ни трапеции, ни равнобедренного треугольника, то существовало бы $(43, 7, 1)$-разностное множество, а его не существует согласно упоминавшейся теореме Брука — Райзера.

Множество $\{0, 1, 15, 19, 21, 24\}$ превращается в разностное по модулю 43 множество $\{0, 1, 27, 31, 33, 36\}$, если «раздвинуть» интервал от 1 до 15, превратив его в интервал от 1 до 27. Непосредственно можно убедиться, что все попарные разности чисел этого множества по модулю 43 разные. Соответствующий ему шестиугольник см. на рис. 6.

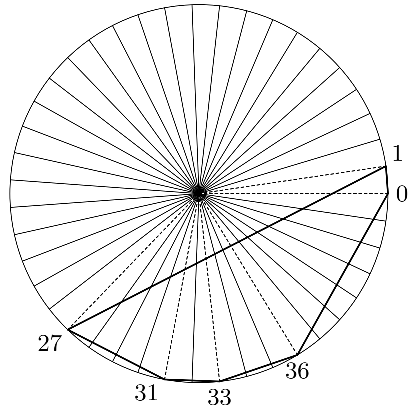


Рис. 6. Шестиугольник из вершин правильного 43-угольника без трапеций и равнобедренных треугольников

Приведём ещё примеры разностных множеств, которые нельзя получить из теоремы Зингера, но можно построить другими методами. Множество $\{2, 4, 5, 27, 31, 36\}$ является разностным по модулю 42. Можно, вычисляя все 30 попарных разностей по этому модулю, непосредственно убедиться, что все они разные. Множество $\{1, 12, 22, 29, 31, 34, 35\}$ является разностным по модулю 48. Зная эти примеры, читатель легко решит следующие задачи, подобные задаче 3.

Задача 10. В правильном 42-угольнике отмечены 7 вершин. Доказать, что существует или трапеция, или прямоугольник, или равнобедренный треугольник, или большая диагональ с вершинами в этих точках. Можно выделить 6 вершин так, что не существует ни трапеции, ни прямоугольника, ни равнобедренного треугольника, ни большой диагонали с вершинами в этих точках.

Задача 11. В правильном 48-угольнике отмечены 8 вершин. Доказать, что существует или трапеция, или прямоугольник, или равнобедренный треугольник, или большая диагональ с вершинами в этих точках. Можно выделить 7 вершин так, что не существует ни трапеции, ни прямоугольника, ни равнобедренного треугольника, ни большой диагонали с вершинами в этих точках.

Приведём пример ещё одной задачи подобного типа.

Задача 12. Можно ли в правильном 26-угольнике так отметить 8 вершин, что не будет существовать ни трапеция, ни равнобедренный треугольник с вершинами в этих точках? А можно ли это сделать так, чтобы не было ещё и прямоугольников?

Ответ на первый вопрос: можно. Пример указан на рис. 7.

Для проверки достаточно для каждой пары не диаметрально противоположных вершин (таких пар $4 \cdot 7 - 4 = 24$) найти наименьшую из двух

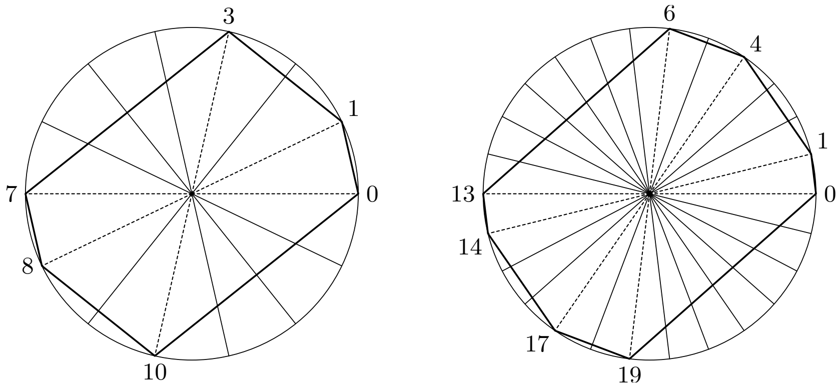


Рис. 7. *Шестиугольник из вершин правильного* 14*-угольника без трапеций и равнобедренных треугольников. Восьмиугольник из вершин правильного* 26*-угольника без трапеций и равнобедренных треугольников*

дуг данной окружности с концами в этих вершинах, и убедиться, что эти дуги все попарно различны по длине, за исключением пар диаметрально противоположных дуг. Так как упомянутых пар 12, достаточно вычислить длины 12 дуг. Если дуга соединяет вершины с номерами i, j, то в качестве её длины можно взять минимальное из чисел $|i-j|$, $26-|i-j|$.

На второй вопрос ответ отрицательный. Рассмотрим все $7\cdot 8/2=28$ прямых, проходящих через пары выбранных вершин. Из них две параллельны друг другу, так как стороны и диагонали правильного n-угольника образуют n классов попарно параллельных прямых. Они образуют равнобокую трапецию или прямоугольник (при нечётном n всегда получалась бы трапеция).

Указанный пример — частный случай следующего утверждения.

В правильном n-угольнике при $n=2(q^2+q+1)$, где $q=p^m$ — степень простого числа, можно так отметить $2(q+1)$ вершин, что не будет существовать ни трапеция, ни равнобедренный треугольник с вершинами в этих точках.

Его доказательство использует следующие два факта.

1. При $k=q^2+q+1$ в кольце вычетов $\mathbb{Z}_k$ по модулю k существует разностное множество из $q+1$ чисел (теорема Зингера).

2. Пусть в кольце $\mathbb{Z}_n=\{0,\ldots,n-1\}$ выбрано k чисел так, что все $k(k-1)$ попарных разностей по модулю n различны. К каждому из них прибавим n и добавим полученные k чисел к выбранному множеству. Получим подмножество из $2k$ чисел в множестве $\mathbb{Z}_{2n}=\{0,\ldots,2n-1\}$. Тогда равенство разностей $a-b=c-d \bmod 2n$ в этом подмножестве возможно, лишь когда $a-b=c-d=n \bmod 2n$ или $a-c=b-d \bmod 2n$. Используя эти факты, получим в кольце $\mathbb{Z}_n$ множество из $2q+2$ чисел.

Если в правильном n-угольнике выбрать $2q+2$ вершин, соответствующих этому множеству, то получим центрально-симметричный $(2q+2)$-угольник, из вершин которого нельзя образовать ни равнобедренный треугольник, ни трапецию.

Второе утверждение доказывается несложно. Действительно, если

$$\{a,b,c,d\}\subset\{0,\ldots,n-1\} \quad \text{или} \quad \{a,b,c,d\}\subset\{n,\ldots,2n-1\},$$

то равенство $a-b=c-d \bmod 2n$ невозможно, так как невозможно равенство $a-b=c-d \bmod n$. Если, например, $\{a,b,c\}\subset\{0,\ldots,n-1\}$, $d\geqslant n$, то $d-n\in\{0,\ldots,n-1\}$, и если $d-n\notin\{a,b,c\}$, то равенство $a-b=c-d \bmod 2n$ невозможно, так как иначе $a-b=c-(d-n) \bmod n$, а если $d-n\in\{a,b\}$, то $a-b=c-(d-n) \bmod n$ превращается, например, в $a-b=a-(d-n)=a-d \bmod n$, откуда $b=d$, что тоже невозможно, значит, остаётся только случай $d-n=c$, но тогда $d-c=n=b-a \bmod 2n$. Случай, когда $a,b,c\geqslant n$, а $d<n$, сводится к уже рассмотренному прибавлением n по модулю $2n$ к каждому из этих чисел.

Если $a,b<n$, а $c,d\geqslant n$, получаем или $c-n=a$, $d-n=b$, и тогда $a-c=b-d \bmod 2n$; или $c-n=b$, $d-n=a$, и тогда $a-b=(d-n)-(c-n)=$ $=d-c=c-d \bmod 2n$, т. е. $c-d=n=a-b \bmod 2n$; или $c-n\notin\{a,b\}$, или $d-n\notin\{a,b\}$, при этом в обоих случаях $a-b=(c-n)-(d-n) \mod 2n$, поэтому $a-b=(c-n)-(d-n) \mod n$, что возможно только при $a=c-n$, $b=d-n$, и тогда $a-c=n=b-d \bmod 2n$. Случай, когда $a,b\geqslant n$, а $c,d<n$, сводится к уже рассмотренному прибавлением n по модулю $2n$ к каждому из этих чисел.

Если $a,c<n$, а $b,d\geqslant n$, то $a-(b-n)=c-(d-n) \bmod 2n$, значит, $a-(b-n)=c-(d-n) \bmod n$, т. е. или $a=c$, $b-n=d-n$, поэтому $a-c=b-d \bmod 2n$, или $a=b-n$, $c=d-n$, т. е. $a-b=n=c-d \bmod 2n$.

Осталось рассмотреть случай, когда $a,d<n$, $b,c\geqslant n$. Тогда $a-(b-n)=$ $=(c-n)-d \bmod 2n$, поэтому $a-(b-n)=(c-n)-d \bmod n$, но тогда или $a=c-n$, $b-n=d$, т. е. $a-c=n=b-d \bmod 2n$, или $a=b-n$, $c-n=d$, т. е. $a-b=n=c-d \bmod 2n$.

Задача 13 (LXXIX Московская математическая олимпиада (2016), 11 кл., второй день). Можно ли отметить k вершин правильного 14-угольника так, что любой четырёхугольник с вершинами в отмеченных точках, имеющий две параллельные стороны, является прямоугольником, если: а) $k=6$; б) $k\geqslant 7$?

Задача 14. Можно ли в правильном 26-угольнике так отметить 9 вершин, что не существует ни трапеция, ни равнобедренный треугольник с вершинами в этих точках (но существуют прямоугольники)?

Следующий раздел, как это ни удивительно на первый взгляд, довольно тесно связан с предыдущими.

§ 4. Матрицы из нулей и единиц без прямоугольников

О таких матрицах фактически речь идёт в следующих олимпиадных задачах.

Задача 15 (9-я Всесоюзная математическая олимпиада (1975), 9–10 кл., 1-й день). В квадрате 13×13 нужно отметить центры k клеток, чтобы никакие четыре отмеченные точки не являлись вершинами прямоугольника со сторонами, параллельными сторонам квадрата. При каком наибольшем k это возможно?

Ответ: при $k = 13 \cdot 4$.

Задача 16 (22-я Шведская математическая олимпиада (1982 г.), задача 5). Все узлы решётки 12×12 покрашены в красный, белый или синий цвет. Покажите, что всегда найдутся четыре узла одного цвета, образующие прямоугольник со сторонами, параллельными сторонам решётки.

Их решения легко найти, прочитав доказательство следующей теоремы (найденной в 1950-е годы венгерским математиком Рейманом и с тех пор многократно переоткрывавшейся, в том числе и автором этой статьи).

Теорема 10. *Если в $(n \times n)$-матрице из нулей и единиц нет двух строк и двух столбцов, на пересечении которых стоят единицы (т. е. нет подматриц 2×2, заполненных единицами), то число единиц в матрице не больше $n(\sqrt{n - 3/4} + 1/2)$. Равносильная формулировка: если в квадратной таблице размера $n \times n$, $n > 2$, содержится более чем $n(1 + \sqrt{4n - 3})/2$ нулей, то в ней найдётся прямоугольник (четыре клетки, лежащие на пересечении двух строк и двух столбцов), состоящий из нулей.*

Чтобы доказать это, для i-й строки обозначим через M_i множество (и количество) столбцов, на пересечении которых с этой строкой стоят единицы. Число N единиц во всей таблице равно сумме чисел M_i. Можно считать, что различные множества M_i, M_j имеют не более одного общего столбца (если бы они имели пару общих столбцов, то в пересечении этих столбцов с i-й и j-й строками стояли бы одни единицы и лемма была бы уже доказана). Рассмотрим множество P_i всех различных пар столбцов из множества M_i. Число таких пар равно $M_i(M_i - 1)/2$. Из предыдущего утверждения следует, что множества P_i не пересекаются (не имеют общих пар столбцов). Поэтому число пар столбцов в объединении этих множеств равно сумме всех чисел $M_i(M_i-1)/2$. Но число пар столбцов в указанном объединении не больше чем $n(n-1)/2$. Поэтому имеем неравенство

$$\frac{M_1(M_1-1)}{2}+\ldots+\frac{M_n(M_n-1)}{2}\leqslant\frac{n(n-1)}{2},$$

т. е.

$$\sum_{i=1}^{n} M_i^2-\sum_{i=1}^{n} M_i\leqslant n(n-1).$$

Применяя неравенство Коши $n(a_1^2+\ldots+a_n^2)\geqslant(a_1+\ldots+a_n)^2$, получаем, что

$$\left(\sum_{i=1}^{n} M_i\right)^2-n\sum_{i=1}^{n} M_i\leqslant n^2(n-1),$$

т. е. $N^2-nN\leqslant n^2(n-1)$. Значит,

$$\left(N-\frac{n}{2}\right)^2=N^2-nN+\frac{n^2}{4}\leqslant\frac{n^2}{4}+n^2(n-1),$$

откуда следует неравенство

$$N\leqslant n\left(\sqrt{n-\frac{3}{4}}+\frac{1}{2}\right),$$

что и требуется.

В следующей задаче найдены условия, при которых неравенство теоремы 10 превращается в равенство.

Задача 17. Если в $(n\times n)$-матрице из нулей и единиц нет прямоугольников и число единиц в матрице равно $n(\sqrt{n-3/4}+1/2)$, то $n=q^2+q+1$, в каждой строке и каждом столбце ровно $q+1$ единиц, для любых двух строк найдётся (разумеется, единственный) столбец, в пересечении которого с этими строками стоят единицы, и аналогичное утверждение верно для столбцов.

Указание. Если $n(\sqrt{n-3/4}+1/2)$ — целое число, то $\sqrt{4n-3}$ тоже, поэтому $\sqrt{4n-3}=2q+1$, тогда $n=q^2+q+1$. Согласно доказательству теоремы 10 равенство $N=\sqrt{4n-3}$ имеет место тогда и только тогда, когда справедливо равенство

$$\frac{M_1(M_1-1)}{2}+\ldots+\frac{M_n(M_n-1)}{2}=\frac{n(n-1)}{2}$$

и во всех множествах поровну элементов. Из указанного равенства следует утверждение про столбцы. Аналогично доказывается и про строки.

Остаётся построить пример экстремальной таблицы в задаче 15. Это можно сделать, построив циклическую (в другой терминологии циркулянтную) таблицу (матрицу) без прямоугольников.

Циклической называется квадратная матрица, каждая строка которой получается циклическим сдвигом предыдущей строки на одну позицию. То есть циклическая $(n \times n)$-матрица имеет вид

$$\begin{pmatrix} a_0 & a_1 & \dots & a_j & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{j+1} & \dots & a_{n-2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_1 & a_2 & \dots & a_{j-1} & \dots & a_0 \end{pmatrix}.$$

Для построения циклической матрицы без прямоугольников рассмотрим любое множество $S = \{s_1, \dots, s_k\} \subset \mathbb{Z}_n$, в котором все разности $s_i - s_j \mod n$, где $i \neq j$, различны. Для всех $i = 1, \dots, k$ положим $a_{s_i} = 1$, а остальные a_j положим равными нулю.

Соответствующая циклическая матрица состоит из k циклических единичных диагоналей, проходящих через s_i-е позиции первой строки. Величины $s_i - s_j$ имеют смысл расстояния между этими диагоналями. Единицы, стоящие на одинаковых позициях в некоторых двух строках, относятся к разным циклическим диагоналям. Следовательно, если бы по две единицы в некоторых двух строках были расположены на одних и тех же позициях, то для каждой из строк эти единицы относились бы к различным (упорядоченным) парам циклических диагоналей, но это противоречит построению: расстояния между диагоналями не повторяются. Поэтому построенная матрица не содержит прямоугольников.

В качестве такого множества S можно взять $(q^2+q+1, q+1, 1)$-разностное множество Зингера (при $q = 3$ получается пример таблицы с 52 клетками для задачи 15). Число единиц в этой матрице в точности равно полученной в теореме 10 верхней оценке числа единиц $n(1 + \sqrt{4n-3})/2 = nk$, где $n = q^2 + q + 1$, $k = q + 1$.

Задача 18. Докажите, что любая циклическая матрица без прямоугольников может быть получена указанным выше способом из подходящего разностного множества.

Матрица, построенная на основе множества Зингера, фактически совпадает с матрицей, строки которой являются характеристическими функциями прямых конечной проективной плоскости порядка q. Тот факт, что матрица не содержит прямоугольников, вытекает из того, что любые две прямые проективной плоскости пересекаются ровно в одной точке.

Если не требовать дополнительно свойства цикличности, то $(n \times n)$-матрицу с k единицами на каждой строке, не содержащую прямоугольников, при $n = q^2 + q + 1$, $k = q + 1$ можно построить указанным выше способом, т. е. как *матрицу смежности точек и прямых* конечной проективной плоскости порядка q. Это несколько проще, так как не требует доказательства теоремы Зингера. Задача 17 показывает, что существование $(n \times n)$-матрицы без прямоугольников с максимально возможным числом единиц, равным $n(\sqrt{n - 3/4} + 1/2)$, равносильно существованию проективной плоскости с n точками.

Приведём более простой пример $(n \times n)$-матрицы без прямоугольников, содержащей приблизительно $n^{3/2}$ единиц. Этот пример предложил Э. И. Нечипорук в [11] для применения в теории сложности булевых функций. Через E_0 обозначим единичную матрицу размера $p \times p$, а через E_i — матрицу, получаемую из E_0 циклическим сдвигом строк на i позиций вниз.

Матрица H_p имеет вид

$$H_p = \begin{pmatrix} E_0 & E_0 & \dots & E_0 & \dots & E_0 \\ E_0 & E_1 & \dots & E_j & \dots & E_{p-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ E_0 & E_i & \dots & E_{ij} & \dots & E_{i(p-1)} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ E_0 & E_{p-1} & \dots & E_{(p-1)j} & \dots & E_{(p-1)^2} \end{pmatrix}.$$

Проверим, что матрица H_p не содержит прямоугольников. Воспользуемся разбиением указанной матрицы на горизонтальные и вертикальные полосы ширины p, нумеруя их от 0 до $p-1$. Заметим, что на пересечении i-й горизонтальной полосы и j-й вертикальной полосы находится матрица E_{ij}.

Предположим, что некоторые две строки и некоторые два столбца матрицы H_p в пересечении образуют «единичный» прямоугольник. Пусть эти строки расположены в i_1-й и i_2-й горизонтальных полосах, а столбцы — в j_1-й и j_2-й вертикальных полосах. Очевидно, $i_1 \neq i_2$ и $j_1 \neq j_2$, так как в любой строке и любом столбце матрицы E_k содержится ровно по одной единице.

Легко видеть, что для любой строки i-й горизонтальной полосы расстояние между единицами из l_1-й и l_2-й вертикальных полос, где $l_1 < l_2$, совпадает с $i(l_1 - l_2)$ по модулю p. В частности, согласно предположению совпадают по модулю p расстояния между единицами i_1-й и i_2-й полос на пересечении с j_1-м и j_2-м столбцами. Таким образом,

$$i_1(j_1 - j_2) \equiv i_2(j_1 - j_2) \bmod p,$$

откуда следует

$$(i_1 - i_2)(j_1 - j_2) \equiv 0 \bmod p,$$

что невозможно в силу $0 < |i_1 - i_2|, |j_1 - j_2| < p$.

Матрица H_p является матрицей Нечипорука [11] [18], в которой строки и столбцы нумеруются двойными индексами (a, b) и (x, y) соответственно, а единица стоит на пересечении строки (a, b) и столбца (x, y) в том и только том случае, когда $y \equiv ax + b \mod p$. Для столбцов следует принять лексикографический порядок нумерации:

$$(x, y) = (0, 0), (0, 1), \dots, (0, p-1), (1, 0), \dots, (1, p-1), \dots, (p-1, p-1),$$

а для строк несколько видоизменённый:

$$\begin{gathered}(a, b) = (0, 0), (0, 1), \dots, (0, p-1), (p-1, 0), (p-1, 1), \dots, (p-1, p-1), \\ (p-2, 0), (p-2, 1) \dots, (p-2, p-1), \dots, (1, 0), (1, 1), \dots, (1, p-1).\end{gathered}$$

Проверим: i-ю горизонтальную полосу такой матрицы определяет соотношение $a = -i \bmod p$, а j-ю вертикальную — соотношение $x = j$. Тогда позиции единиц матрицы в пересечении полос определяются из соотношения $y \equiv -ij + b \bmod p$, где b и y нумеруют строки и соответственно столбцы данной подматрицы. Это в точности матрица E_{ij}, что и требовалось.

Очевидно, число единиц в матрице (H_p) равно p^3.

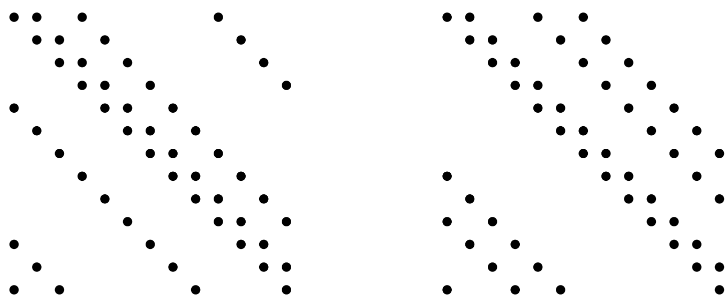
Матрица Нечипорука представляет из себя матрицу характеристических функций прямых конечной аффинной плоскости порядка p. Вместо p можно взять степень любого простого числа, если в качестве аффинной плоскости использовать координатную плоскость над конечным полем $\mathrm{GF}(q)$ (подобные вопросы рассматриваются, например, в [10]). Теперь рассмотрим семейство всех $q^2 + q$ прямых этой аффинной плоскости и заметим, что в ней через каждую точку проходит $q + 1$ прямая. Далее рассмотрим $(q^2 \times (q^2 + q))$-матрицу, в которой строки занумерованы точками плоскости $A(2, q)$, а столбцы — прямыми, причём на пересечении строки со столбцом стоит 1 тогда и только тогда, когда соответствующая точка лежит на соответствующей прямой. Эта матрица не содержит прямоугольников, имея $q + 1$ единиц в каждой строке и q единиц в каждом столбце. Из задачи 21 следует, что матрица, содержащая более $q^2(q + 1)$ единиц, обязательно содержит прямоугольник.

Задача 19. Постройте (25×25)-матрицу из нулей и единиц без прямоугольников с 5 единицами в каждой строке и в каждом столбце. Докажите, что аналогичную матрицу с 6 единицами в каждой линии построить нельзя. Дополните построенную (25×25)-матрицу до (25×30)-матрицы с 6 единицами в каждой строке и 5 единицами в каждом столбце так, чтобы в ней не появилось прямоугольников.

[18] Ранее эта матрица была построена в работе венгерских математиков Ковари, Турана и его супруги Веры Шош.

Задача 20. Постройте (13×13)-матрицу из нулей и единиц с 52 единицами без прямоугольников.

Указание. Возьмите разностное множество $\{0, 1, 3, 9\} \subset \mathbb{Z}_{13}$ и постройте циклическую матрицу, показанную слева.



Единицы в ней обозначены точками (а нули никак не обозначены). Можно взять другое разностное множество $\{0, 1, 4, 6\} \subset \mathbb{Z}_{13}$ и построить другую циклическую матрицу, показанную справа.

4.1. Проблема Царанкевича

Так называется задача, предложенная польским математиком Царанкевичем: заполнить матрицу размера $n \times m$ нулями и единицами так, чтобы единицы не образовывали прямоугольник данного размера (a, b) и единиц было максимальное число. Под прямоугольником понимается множество элементов матрицы, лежащих на пересечении a строк и b столбцов (любых, необязательно соседних). Булевы матрицы (т. е. матрицы из $0, 1$) без единичных прямоугольников размера (a, b) назовём (a, b)-*редкими*. Число единиц в булевой матрице — её *вес*. В случае $a = b = 2$ эта проблема была предметом теоремы 10. Следующая теорема (Эрдёша и Царанкевича) развивает эту тему дальше.

Теорема 11. *Вес $\nu(A)$ любой $(a, 2)$-редкой булевой $(n \times m)$-матрицы A удовлетворяет неравенству*

$$\nu(A)\Big(\frac{\nu(A)}{n} - 1\Big) \leqslant m(m-1)(a-1).$$

Доказательство. Пусть $\nu(A) = k$. Для доказательства соотношения

$$k\Big(\frac{k}{n} - 1\Big) \leqslant m(m-1)(a-1)$$

оценим двумя способами число горизонтальных (т. е. лежащих в одной строке) пар единиц в матрице. Обозначим число единиц в i-й строке через x_i.

Тогда число горизонтальных пар единиц равно

$$\frac{x_1(x_1-1)+\ldots+x_n(x_n-1)}{2}.$$

С другой стороны, для каждой из $m(m-1)/2$ пар столбцов имеется не более $a-1$ горизонтальных пар единиц, накрываемых этой парой столбцов (иначе существовала бы $(a,2)$-подматрица, заполненная единицами). Поэтому

$$x_1(x_1-1)+\ldots+x_n(x_n-1)\leqslant m(m-1)(a-1).$$

Так как $x_1+\ldots+x_n=k$ — общее число единиц в матрице, применяя неравенство выпуклости к функции $f(x)=x^2-x$, имеем

$$n\frac{k}{n}\Bigl(\frac{k}{n}-1\Bigr)=nf\Bigl(\frac{k}{n}\Bigr)=nf\Bigl(\frac{x_1+\ldots+x_n}{n}\Bigr)\leqslant f(x_1)+\ldots+f(x_n)=$$
$$=x_1(x_1-1)+\ldots+x_n(x_n-1)\leqslant m(m-1)(a-1),$$

ч. т. д. □

Задача 21. Если $(q^2\times(q^2+q))$-матрица из нулей и единиц не содержит прямоугольников, то её вес не больше $q^2(q+1)$.

Указание. Примените теорему 11.

Задача 22. В клетчатом прямоугольнике 11×52 клетки раскрашены в два цвета. Доказать, что найдутся три строки и три столбца, на пересечении которых стоят клетки одного цвета.

Указание. Примените рассуждения, подобные доказательству теоремы 11.

Естественным продолжением этого раздела является раздел

§ 5. Редкие множества и редкие матрицы

В следующей задаче речь идёт по существу о матрице из нулей и единиц, в которой нет не только прямоугольников, но и параллелограммов.

Задача 23 (12-я Всесоюзная олимпиада (1978), 9 кл., 2-й день). Дано простое число $p>3$. Рассмотрим на координатной плоскости множество M, состоящее из таких точек с целыми координатами (x,y), что $0\leqslant x<p$, $0\leqslant y<p$. Докажите, что можно отметить p различных точек множества M так, чтобы никакие четыре из них не лежали в вершинах параллелограмма и никакие три из них не лежали на одной прямой.

В связи с рассмотрением этой и подобных задач обобщим введённое выше понятие разностного множества.

Пусть на множестве G определена операция $+$, удовлетворяющая сочетательному закону и тождеству $x + 0 = x$. Такие множества назовём *полугруппами*[19]. Подмножество H полугруппы $(G, +)$ назовём (k, l)*-редким*, если оно не содержит подмножеств вида $A + B = \{a + b \mid a \in A,\ b \in B\}$, где $|A| = k$ и $|B| = l$ (здесь и далее мощность конечного множества M обозначается через $|M|$).

Полугруппу назовём *группой*, если для каждого её элемента x найдётся единственный такой элемент y, что $x + y = y + x = 0$. В случае группы определение редкого множества равносильно следующему: подмножество H группы $(G, +)$ называется (k, l)-редким, если для любых различных элементов $g_1, \ldots, g_k \in G$ справедливо неравенство

$$\left|\bigcap_{i=1}^{k} g_i H\right| < l, \quad \text{где} \ \ g_i H = \{g_i\} + H.$$

Проверим равносильность двух определений. Действительно, пусть для некоторых $g_1, \ldots, g_k \in G$ выполняется неравенство

$$\left|\bigcap_{i=1}^{k} g_i H\right| \geqslant l.$$

Поскольку

$$\{-g_1, \ldots, -g_k\} + \bigcap_{i=1}^{k} g_i H \subset H,$$

H не является (k, l)-редким в смысле первого определения.

Обратно, пусть $A + B \subset H$, $A = \{g_1, \ldots, g_k\}$, $|B| = l$. Поскольку

$$B \subset \bigcap_{i=1}^{k} (-g_i) H,$$

получаем

$$\left|\bigcap_{i=1}^{k} (-g_i) H\right| \geqslant l.$$

Значит, H не является (k, l)-редким в смысле второго определения.

Подмножество H группы $(G, +)$ назовём *разностным*, если для любых элементов $a, b, c, d \in H$ справедлива импликация

$$0 \neq a - b = c - d \quad \Rightarrow \quad (a = c)\ \&\ (b = d).$$

[19] Примером полугруппы служит множество векторов длины n с целыми неотрицательными координатами и покоординатной операцией сложения.

Пусть в группе $(G, +)$ операция сложения удовлетворяет тождеству $x + y = y + x$ и уравнение $x + x = 0$ имеет только нулевое решение[20]. Тогда можно проверить, что в группе $(G, +)$ подмножество H является разностным тогда и только тогда, когда для любых элементов $a, b, c, d \in H$ справедливо равенство

$$a + b = c + d \quad \Rightarrow \quad ((a = c) \,\&\, (b = d)) \vee ((a = d) \,\&\, (b = c)).$$

Далее 2-редкое множество означает $(2, 2)$-редкое. Покажем, что в группе $(G, +)$ определения разностного и 2-редкого подмножества равносильны. Пусть $H \subset G$ не является 2-редким, т. е. для некоторых элементов $a \neq b$, $c \neq d$ выполнено $a + c, a + d, b + c, b + d \in H$. Но тогда

$$0 \neq (b + c) - (a + c) = (b + d) - (a + d),$$

при этом $b + c \neq b + d$, значит, H не является разностным.

Пусть теперь H не является разностным, т. е. для некоторых элементов $a, b, c, d \in H$ выполняется $a + b = c + d$, при этом $a \neq c$, $a \neq d$. Но тогда $\{a, d\} + \{c - a, 0\} = \{a, b, c, d\} \subset H$, т. е. H не является 2-редким.

Обозначим через $(\mathrm{GF}(q)^n, +)$ группу, образованную упорядоченными наборами $(a_1, \ldots, a_n)$ элементов конечного поля $\mathrm{GF}(q)$ порядка q, в которой операция сложения определяется как покомпонентное сложение этих наборов: $(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$. Так как q^n будет степенью простого числа, если q — степень простого, существует поле $\mathrm{GF}(q^n)$ порядка q^n. По операции сложения оно образует группу, которую обозначим $(\mathrm{GF}(q^n), +)$. Известна следующая

Теорема 12. (i) *В группе* $(\mathrm{GF}(q)^2, +)$ *при нечётном* q *«парабола»* $\{(x, x^2) \mid x \in \mathrm{GF}(q)\}$ *является* 2*-редким подмножеством мощности* q.

(ii) *В группе* $(\mathrm{GF}(q)^3, +)$, *где* q *нечётно, «сфера»*

$$\{(x, y, z) \mid x^2 + y^2 + z^2 = \gamma\},$$

где $-\gamma$ *не является квадратом никакого элемента поля* $\mathrm{GF}(q)$, *является* 3*-редким подмножеством мощности* $q^2 - q$.

(iii) *В группе* $(\mathrm{GF}(q^t), +)$ *множество таких элементов* x, *что* $x^{\frac{q^t-1}{q-1}} = 1$, *является* $(t, t! + 1)$*-редким подмножеством мощности* $(q^t - 1)/(q - 1)$.

Доказательство. Докажем (i). Проверим, что из равенства для двумерных векторов над $\mathrm{GF}(q)$

$$(x, x^2) - (y, y^2) = (z, z^2) - (u, u^2) \neq (0, 0)$$

[20] Примером такой группы служит множество $\{0, 1, \ldots, n - 1\}$ с операцией сложения по модулю n при $n > 2$.

следует, что $x = z$ и $y = u$. Действительно, система уравнений

$$\begin{cases} x - y = a, \\ x^2 - y^2 = b \end{cases}$$

над этим полем при $a \neq 0$ эквивалентна системе

$$\begin{cases} x - y = a, \\ x + y = \dfrac{b}{a}, \end{cases}$$

которая имеет единственное решение.

Таким образом, рассматриваемая парабола является разностным, следовательно, 2-редким подмножеством в $\mathrm{GF}(q)^2$.

Утверждение (ii) фактически доказано У. Брауном в [3]. Точнее, он доказал, что пересечение любых трёх различных сфер

$$S(a, b, c) = \{(x, y, z) \mid (x-a)^2 + (y-b)^2 + (z-c)^2 = \gamma\}$$

состоит не более чем из двух точек. Теперь, если предположить, что сфера $S(0, 0, 0)$ не является 3-редким подмножеством, т. е. $A + B \subset S(0, 0, 0)$, где $|A| = |B| = 3$, то в силу того, что произвольную сферу $S(a, b, c)$ можно представить в виде $\{(a, b, c)\} + S(0, 0, 0)$, получим, что трёхэлементное множество B содержится в каждой из сфер $S(a, b, c)$, где $(-a, -b, -c) \in A$, что противоречит доказанному.

Доказательство того, что число точек сферы $S(0, 0, 0)$ равно $q^2 - q$, опускаем, так же как и весьма сложное доказательство (iii), найденное венгерскими математиками Роньяи, Колларом и Сабо в 1996 г. $\square$

Приведём пример 3-редкого множества в группе $\mathbb{Z}_3^3$, построенного методом Брауна. Указанная группа состоит из всех троичных наборов длины три от $(0, 0, 0)$ до $(2, 2, 2)$. Сложение в ней выполняется покомпонентно по модулю три, например $(1, 2, 0) + (2, 2, 1) = (0, 1, 1)$. К операции сложения по модулю три в группе $\mathbb{Z}_3 = \{0, 1, 2\}$ можно добавить операцию умножения по модулю три (и тогда эта группа превратится в поле $\mathrm{GF}(3)$) и рассмотреть в трёхмерном арифметическом пространстве $\mathrm{GF}(3)^3 = \{0, 1, 2\}^3$ сферу с центром в нуле $(0, 0, 0)$, определяемую уравнением $x^2 + y^2 + z^2 = 1$. Эта сфера состоит из 6 наборов (точек): $(0, 0, 1)$, $(0, 0, 2)$, $(0, 1, 0)$, $(0, 2, 0)$, $(1, 0, 0)$, $(2, 0, 0)$. Действительно, x^2 в поле $\mathrm{GF}(3)$ равен 0 или 1, а сумма трёх квадратов равна 1, только когда один из них 1, а остальные 0. Для проверки 3-редкости этого множества в группе $\mathbb{Z}_3^3$ достаточно проверить, что любая сдвинутая сфера $(x-a)^2 + (y-b)^2 + (z-c)^2$ пересекается со сферой $x^2 + y^2 + z^2 = 1$ не более чем в двух точках, в чём можно убедиться и непосредственной проверкой (в силу симметрии достаточно рассмотреть не все 26, а меньшее число сдвигов). Тогда и любые две сдвинутые сферы пересекаются не более чем в двух точках, потому что система уравнений

$$\begin{cases} (x-a')^2+(y-b')^2+(z-c')^2=1, \\ (x-a)^2+(y-b)^2+(z-c)^2=1 \end{cases}$$

линейной заменой переменных сводится к системе

$$\begin{cases} x^2+y^2+z^2=1, \\ (x-a'')^2+(y-b'')^2+(z-c'')^2=1 \end{cases}$$

и поэтому имеет столько же решений.

Далее (k,k)-редкую матрицу называем просто k-редкой. (k,k)-редкие матрицы называем просто k-редкими. Про них известна следующая

Теорема 13. (i) *Существует k-редкая $(n\times n)$-матрица с весом не более $C_k(n^{\frac{2k}{k+1}})$, где C_k — некоторая константа, зависящая от k и не зависящая от n.*

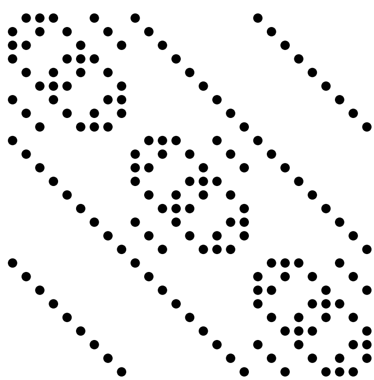
(ii) *В случае $k=2$ существует 2-редкая симметрическая $(n\times n)$-матрица с весом $(1+\varepsilon_n)n^{3/2}$, где $\varepsilon_n\to 0$ при $n\to\infty$.*

(iii) *В случае $k=3$ существует 3-редкая симметрическая $(n\times n)$-матрица с весом $(1+\varepsilon_n)n^{5/3}$, где $\varepsilon_n\to 0$ при $n\to\infty$.*

(iv) *Для $t\geqslant 2$ существует $(t,t!+1)$-редкая симметрическая $(n\times n)$-матрица с весом $(1+\varepsilon_n)n^{(2t-1)/t}$, где $\varepsilon_n\to 0$ при $n\to\infty$.*

Доказательство теоремы довольно сложное и здесь не приводится. Укажем только, что доказательство последних трёх пунктов основано на использовании теоремы 12 и асимптотического закона распределения простых чисел.

Основываясь на приведённом выше примере 3-редкого множества в группе $\mathbb{Z}_3^3$, построим 3-редкую симметричную (27×27)-матрицу, в которой в каждой строке и столбце ровно 6 единиц.



Из построения очевидна симметричность матрицы. Это её свойство даёт возможность построить по ней граф с 27 вершинами, каждая из которых соединена с 6 другими (регулярный граф степени 6). Такой граф не содержит подграфов $K_{3,3}$ — полных двудольных графов с тремя вершинами в каждой доле, содержащих всевозможные рёбра (этот граф известен как граф задачи о трёх домах и трёх колодцах). Граф по матрице строится следующим образом: вершина i соединяется ребром с вершиной j тогда и только тогда, когда элемент матрицы $a_{i,j}$, лежащий на пересечении i-й строки и j-го столбца, равен 1 (это граф, у которого матрица смежности вершин совпадает с данной матрицей A).

На рис. 8 можно увидеть, как выглядит симметричная, но не циклическая матрица порядка 125 без прямоугольников размера 3×7 с 16 единицами в каждой строке и каждом столбце, построенная методом п. (iii) теоремы 12.

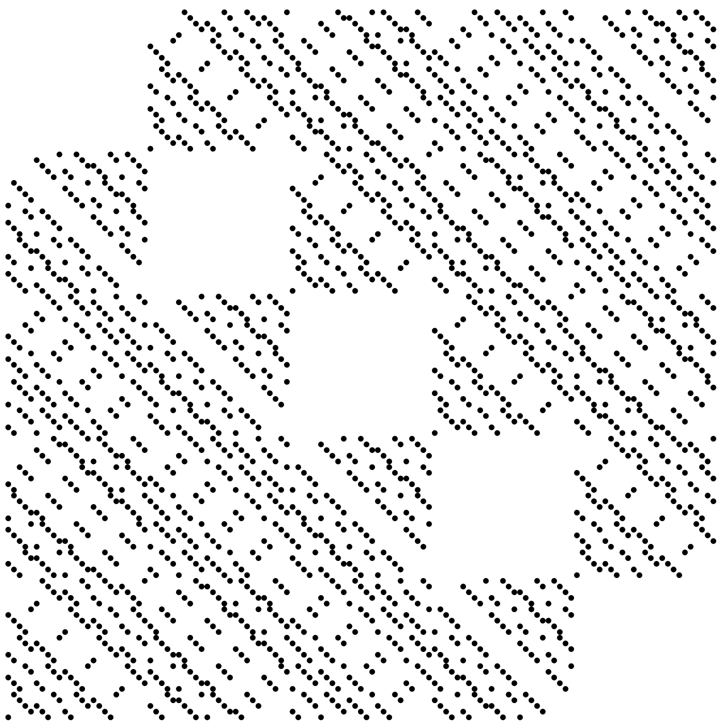


Рис. 8. Симметричная, но не циркулянтная, матрица порядка 125 *без прямоугольников* 3×7 *с* 16 *единицами на каждой линии*

Следующий параграф тесно связан с предыдущим, хотя сразу это не будет очевидно.

§ 6. Теорема Турана и экстремальные графы

На Всесоюзной олимпиаде некогда предлагалась [21)]

Задача 24 (3-я Всесоюзная математическая олимпиада (1969), 10 кл., второй день). В розыгрыше первенства страны по футболу участвуют 20 команд. Какое наименьшее число игр должно быть сыграно, чтобы среди любых трёх команд нашлись две, уже сыгравшие между собой?

На самом деле она является частным случаем следующей теоремы [16].

Теорема 14 (Мантель). *В компании из n человек среди любых трёх найдётся хотя бы одна пара незнакомых. Тогда число пар знакомых не больше $n^2/4$.*

Дальнейшим обобщением является

Теорема 15 (Туран). *Отрезки, соединяющие пары точек n-элементного множества, покрашены в белый и чёрный цвета так, что среди любых его $k+1$ точек найдётся хотя бы одна пара, соединённая белым отрезком. Тогда чёрных отрезков у этого множества не больше*

$$\frac{k-1}{2k}(n^2-r^2)+\frac{r(r-1)}{2}, \quad \text{где} \ \ n=kq+r,\ 0\leqslant r<k,\ q - \text{целое число,}$$

причём для любых n, k эта оценка достигается.

Пять доказательств теоремы можно найти в [1].

Попытки доказать теоремы, аналогичные теореме Турана, привели к созданию *теории экстремальных графов*. В ней получены, например, следующие результаты.

Обозначим через $t(n, G)$ наибольшее число рёбер в n-вершинном графе, при котором возможно отсутствие в нём подграфа, изоморфного данному графу G [22)]. В случае $G = K_r$, где K_r — полный граф на r вершинах, число $t(n, G) = t(n, K_r)$ найдено в теореме Турана. Если $G = K_{r,s}$ — полный двудольный граф, в одной доле которого r вершин, а в другой s, то про $t(n, G) = t(n, K_{r,s})$ известно следующее.

Теорема 16 (Ковари — Шош — Туран). *При $2 \leqslant r \leqslant s$ справедливо неравенство $t(n, K_{r,s}) < C(s^{1/r}n^{2-1/r} + n)$, где C — некоторая константа. При $r = s$ справедливо неравенство*

$$t(n, K_{r,r}) > cn^{2-2/(r+1)}.$$

---

21) Автору не довелось её решать на олимпиаде, так как он был классом младше, но задачу он с тех пор запомнил хорошо.

22) В теории экстремальных графов используется также обозначение $ex(n, G)$, но оно не напоминает о Туране.

Гипотеза Турана о том, что $t(n, K_{r,r}) > cn^{2-1/r}$, по-видимому, не доказана. Однако известна

Теорема 17 (Эрдёш — Реньи — Шош). *При $r = s = 2$ и $n = q^2 + q + 1$, где q — степень простого, справедливо неравенство*

$$t(n, K_{2,2}) \geqslant \frac{1}{2}q(q+1)^2;$$

при $n = q^2 - 1$, где $q = 2^m$, справедливо неравенство

$$t(n, K_{2,2}) \geqslant \frac{1}{2}q(q^2-2);$$

при любом n

$$n\frac{1+\sqrt{4n-3}}{4} \geqslant t(n, K_{2,2}) \gtrsim \frac{1}{2}n^{3/2}.$$

Доказательство. Для доказательства первого неравенства построим граф без циклов длины 4 с $n = q^2 + q + 1$ вершинами и $\frac{1}{2}q(q+1)^2$ рёбрами, где q — степень простого. Возьмём поле $\mathrm{GF}(q)$ и вспомним построение координатной проективной плоскости $\mathrm{PG}(2, q)$ над ним из п. 2.1. Её точками будут классы коллинеарности ненулевых троек (x, y, z), а прямыми — множества точек, удовлетворяющих равенству $ax + by + cz = 0$. Очевидно, коллинеарные тройки (a, b, c) и (a', b', c') определяют одну и ту же прямую, поэтому прямые тоже можно отождествить с классами коллинеарных троек. Число точек в $\mathrm{PG}(2, q)$, как и число прямых, равно $q^2 + q + 1$. Определим на множестве точек плоскости $\mathrm{PG}(2, q)$ граф, в котором пары классов ненулевых коллинеарных троек (x, y, z) и (a, b, c) соединяются ребром тогда и только тогда, когда $ax + by + cz = 0$ (это *полярное соответствие двойственности* между точками и прямыми в $\mathrm{PG}(2, q)$). Если точка не лежит на кривой $x^2 + y^2 + z^2 = 0$, то она соединяется с $q + 1$ прямой (это все прямые, через неё проходящие), т. е. степень соответствующей вершины графа равна $q + 1$. Поэтому сумма степеней таких вершин равна $(q^2 + q + 1 - (q + 1))(q + 1) = q^3 + q^2$. Если точка лежит на этой кривой, то среди проходящих через неё прямых есть и прямая, определяемая классом, содержащим тройку (x, y, z). Поэтому из соответствующей вершины графа выходит только q рёбер. Далее будет показано, что число точек на этой кривой в проективной плоскости $\mathrm{GF}(2, q)$ равно $q + 1$. Значит, сумма степеней этих вершин равна $(q + 1)q$. Следовательно, рассматриваемый граф имеет $q^2 + q + 1$ вершин и $(q^3 + q^2 + (q + 1)q)/2 = q(q + 1)^2/2$ рёбер. Любые две прямые в проективной плоскости $\mathrm{PG}(2, q)$ имеют ровно одну общую точку, поэтому в построенном графе нет циклов длины 4 (если бы вершины l, p, m, q образовывали цикл, то прямые, соответствующие вершинам l, m, проходили бы через точки, соответствующие вершинам p, q).

Покажем, что число точек на указанной кривой в проективной плоскости $\mathrm{GF}(2,q)$ равно $q+1$. Действительно, если q — степень двойки, то в поле $\mathrm{GF}(q)$ квадратные корни всегда существуют и определены однозначно, поэтому число ненулевых решений уравнения $x^2+y^2+z^2=0$ равно q^2-1. Значит, точек на кривой ровно $q+1$.

Пусть теперь $q\neq 2^m$. Число точек в пересечении данной кривой с плоскостью $z=0$ равно числу попарно неколлинеарных ненулевых решений уравнения $x^2+y^2=0$. Если из -1 не извлекается квадратный корень в поле $\mathrm{GF}(q)$ (иначе говоря, -1 — квадратичный невычет), то таких решений нет. Если же -1 есть квадратичный вычет, то неколлинеарных решений два (так как всего решений четыре: $(\pm x,\pm y)$). Число точек на кривой с $z\neq 0$ равно числу решений уравнения $x^2+y^2=-1$ в поле $\mathrm{GF}(q)$. Применяя утверждение задачи 25 (см. ниже), получаем в обоих случаях один ответ: число точек на рассматриваемой кривой в проективной плоскости $\mathrm{GF}(2,q)$ равно $q+1$.

Для доказательства второго неравенства построим граф без циклов длины 4 с $n=q^2-1$ вершинами и $\frac{1}{2}q(q^2-2)$ рёбрами. Рассмотрим поле $\mathrm{GF}(q)$, $q=2^m$, и определим граф на множестве вершин вида $(x,y)\in\mathrm{GF}(q)^2\setminus\{(0,0)\}$, соединив пары вершин (x,y) и (a,b) ребром тогда и только тогда, когда $ax+by=1$ (т. е. точка (x,y) лежит на прямой $aX+bY=1$ в координатном представлении аффинной плоскости над полем $\mathrm{GF}(q)$, указанном в п. 2.1). Если $(a,b)=(x,y)$, ребро не проводим. Такие исключительные точки лежат на окружности $x^2+y^2=1$ в конечной плоскости $\mathrm{GF}(q)^2$ над этим полем. Так как q — степень двойки, в поле $\mathrm{GF}(q)$ квадратные корни всегда существуют и определены однозначно, поэтому число решений уравнения $x^2+y^2=1$ равно q. Из неисключительных вершин (а их ровно q^2-q-1) выходит по q рёбер, так как на каждой прямой $aX+bY=1$ лежит по q точек. Из исключительных вершин выходит по $q-1$ ребру. Удвоенное общее число рёбер равно $(q^2-q-1)q+q(q-1)=q^3-2q$. Любые две прямые имеют не более одной общей точки, поэтому в построенном графе нет циклов длины 4.

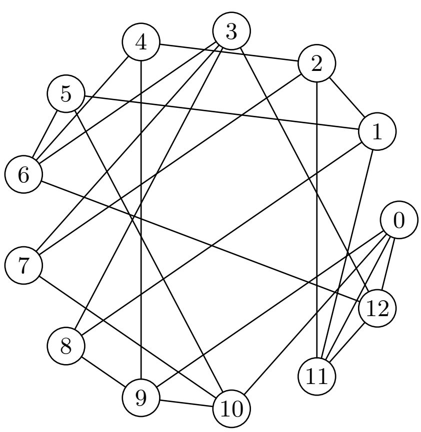
Для доказательства верхней оценки в третьем неравенстве построим по данному графу, не содержащему $K_{2,2}$, двудольный граф, удвоив каждую вершину и из дубликатов образовав вторую долю. Вершины из разных долей соединим ребром, если вершины исходного графа, из которых они были получены, соединялись ребром. Очевидно, что число рёбер в двудольном графе вдвое больше числа рёбер в исходном. Матрица смежности рёбер двудольного графа имеет число единиц, вдвое большее числа рёбер исходного графа, и не содержит прямоугольников из единиц. Действительно, эта матрица симметрична относительно главной диагонали и на диагонали стоят нули. Если бы она содержала прямоугольник, в двудольном графе были бы вершины a, b в одной доле и вершины $c \neq a$, $c \neq b$, $d \neq a$, $d \neq b$ в другой доле, образующие подграф $K_{2,2}$. Но тогда соответствующие 4 вершины исходного графа соединялись бы рёбрами (a, c), (a, d), (b, c), (b, d), т. е. образовывали подграф $K_{2,2}$, что невозможно. Согласно теореме 10 тогда число единиц в матрице не больше $n(1 + \sqrt{4n-3})/2$. Поэтому число рёбер в исходном графе не больше $n(1 + \sqrt{4n-3})/4$.

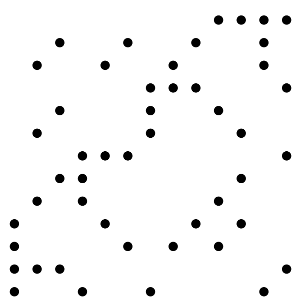
Для доказательства асимптотической нижней оценки в третьем неравенстве выберем простое $q = q_n$ так, чтобы $n \leqslant m = q^2 + q + 1$ и $q \sim \sqrt{n}$, для чего применим асимптотический закон распределения простых чисел Адамара и Валле Пуссена (из него следует, что при любом $\varepsilon > 0$ для достаточно больших n найдётся такое простое p, что $n < p < (1+\varepsilon)n$). Очевидно, что справедливо асимптотическое равенство $n \sim m$. Возьмём построенный выше граф без циклов длины 4 с m вершинами и $e = q(q+1)^2/2 \sim n^{3/2}/2$ рёбрами. Согласно задаче 26 (см. ниже) в нём найдётся подграф с n вершинами и не менее чем

$$e\frac{n(n-1)}{m(m-1)} \sim e \sim \frac{n^{3/2}}{2}$$

рёбрами. Очевидно, в нём нет циклов длины 4, так как их не было в объемлющем графе. □

Вот пример графа с 13 вершинами и 24 рёбрами без циклов длины 4 и его матрица смежности вершин — симметричная матрица без прямоугольников.





Это симметричная относительно главной диагонали (13×13)-матрица с 48 единицами, с 9 строками по 4 единицы и 4 строками по 3 единицы, не содержащая прямоугольников.

Задача 25. Если $q \neq 2^m$ и -1 является квадратичным вычетом в поле $\mathrm{GF}(q)$, то число точек на окружности $x^2+y^2=-1$ в плоскости $\mathrm{GF}(q)^2$ равно $q-1$, а если -1 является квадратичным невычетом, то число точек на окружности $x^2+y^2=-1$ равно $q+1$.

Указание. В первом случае существует элемент $i \in \mathrm{GF}(q)$, $i^2=-1$. Тогда число решений уравнения $x^2+y^2=a$, $a \neq 0$, равно общему числу решений систем $(x+iy)=u$, $(x-iy)=a/u$ при всех значениях ненулевого параметра $u \in \mathrm{GF}(q)$, т. е. равно $q-1$, так как при любом фиксированном $u \neq 0$ линейная система имеет единственное решение.

Если же -1 — невычет, то при любом y элемент $-y^2$ тоже невычет (иначе -1 — вычет). Пусть $QR \subset \mathrm{GF}(q)\setminus\{0\}$ — множество всех ненулевых вычетов (их количество, очевидно, $(q-1)/2$, так как корень из ненулевого элемента извлекается ровно двумя способами), а NR — множество всех невычетов (тогда их количество тоже $(q-1)/2$, так как количество ненулевых элементов $q-1$). Далее, пусть QR_+, NR_+ — количества квадратичных вычетов вида $a-1$, где соответственно $a \in QR$ и $a \in NR$. Число решений уравнения $x^2+1=-y^2$ вдвое больше общего числа всех решений уравнений $x^2+1=a$ с параметром $a \in NR$ (действительно, $-y^2$ при $y \neq 0$ пробегает всё множество NR, а при $y=0$ решений нет). Следовательно, оно равно $4NR_+$.

Заметим теперь, что число точек на гиперболе $x^2-y^2=-1$ вдвое больше общего числа решений уравнений $x^2+1=a$ при значениях параметра $a \in QR$. Если $a=1$, то решение одно ($x=0$), а в остальных случаях решений два. Поэтому число точек на гиперболе равно $4QR_+-2$. Но очевидно, что уравнение $x^2-y^2=-1$ имеет столько же решений, сколько и система $x+y=u$, $x-y=-1/u$, т. е. $q-1$. Отсюда $QR_+=((q-1)+2)/4=(q+1)/4$. Общее количество квадратичных вычетов, включая нулевой, равно

$$\frac{q-1}{2}+1=\frac{q+1}{2}.$$

С другой стороны, оно равно $QR_+ + NR_+$, поскольку $0-1=-1$ — невычет. Отсюда $NR_+=(q+1)/2-(q+1)/4=(q+1)4$. Значит, число точек на окружности $x^2+y^2=-1$ равно $q+1$.

Задача 26. Назовём средним числом рёбер в графе с v вершинами число $e/(v(v-1))$, где e — число рёбер в нём. Докажите, что в любом графе с m вершинами при любом $n \leqslant m$ найдётся подграф с n вершинами, у которого среднее число рёбер не меньше, чем у всего графа.

Указание. Для каждого подграфа G с n вершинами определим число рёбер $e(G)$ и просуммируем эти числа по всем $\binom{m}{n}$ подграфам. Каждое ребро будет входить в эту сумму $\binom{m-2}{n-2}$ раз, потому что оно принадлежит ровно $\binom{m-2}{n-2}$ подграфам (каждый из них определяется выбором $n-2$ вершин из числа $m-2$ вершин данного графа, отличных от концов рассматриваемого ребра). Поэтому сумма равна $e\binom{n-2}{m-2}$, где e — число рёбер в данном графе. Из принципа Дирихле следует, что один из подграфов с n вершинами имеет не менее

$$\frac{e\binom{m-2}{n-2}}{\binom{m}{n}} = \frac{en(n-1)}{m(m-1)}$$

рёбер. Деля на $n(n-1)$, получаем требуемое.

Теорема 17 была усилена в 1980-е годы молодым (тогда) венгерским математиком Золтаном Фюреди[23].

Теорема 18 (Фюреди). *При $n=q^2+q+1$, где $q \geqslant 15$ — степень простого, $t(n, K_{2,2}) = \frac{1}{2}q(q+1)^2$. При любом $q \geqslant 13$ имеем $t(n, K_{2,2}) \leqslant \frac{1}{2}q(q+1)^2$.*

Задача 27 (Олимпиада «Студент и научно-технический прогресс», 1981 г., городской тур, II секция; [9], с. 81). В компании из 1981 человека каждый имеет не меньше 45 знакомых. Доказать, что можно выбрать четырёх человек и посадить их за круглый стол так, чтобы каждый сидел рядом со своими знакомыми.

Задача 28. На конгрессе из 1893 участников все, кроме 44, имеют по 44 знакомых, а эти 44 имеют по 43 знакомых. Доказать, что может случиться так, что никаких четырёх человек нельзя будет посадить за стол между знакомыми.

Ещё две теоремы без доказательства.

Теорема 19 (Ковари — Шош — Туран — Фюреди).

$$\frac{1}{2}\sqrt{s}n^{3/2} - cn^{4/3} \leqslant t(n, K_{2,s}) \leqslant \frac{1}{2}\sqrt{s}n^{3/2} + \frac{n}{4}\ .$$

Теорема 20. *При $r = s = 3$ справедливы неравенства*

$$cn^{5/2} \leqslant t(n, K_{3,3}) \leqslant Cn^{5/2} \quad \text{(Браун)},$$

а при $r \geqslant 4$, $s \geqslant r!+1$ — неравенство

$$t(n, K_{r,s})) > C_r(n^{2-1/r}) \quad \text{(Коллар — Роньяи — Сабо)}.$$

Ещё кое-что на тему теоремы Турана можно прочитать в [8, 12].

[23] Между прочим, победителем одной из международных олимпиад.

Список литературы

[1] *Айгнер М., Циглер Г.* Доказательства из книги. М.: Бином, 2015.

[2] *Артин Э.* Геометрическая алгебра. М.: Наука, 1969.

[3] *Браун У. Г.* Графы, не содержащие графа Томпсена // Кибернетический сборник. Вып. 18. М.: Мир, 1981. С. 34–38.

[4] *Васильев Н. Б., Егоров А. А.* Задачи Всесоюзных математических олимпиад. М.: Наука, 1988.

[5] *Васильев Н. Б., Гутенмахер В. Л., Раббот Ж. М., Тоом А. Л.* Заочные математические олимпиады. М.: Наука, 1987.

[6] *Гальперин Г. А., Толпыго А. К.* Московские математические олимпиады. М.: Просвещение, 1986.

[7] *Гашков С. Б.* Современная элементарная алгебра. М.: МЦНМО, 2006.

[8] *Гашков С. Б.* a-Диаметры и турановские графы // Математическое просвещение. Сер. 3. Вып. 12. М.: МЦНМО, 2008. С. 161–175.

[9] *Григорян А. А., Конягин С. В., Садовничий В. А.* Задачи студенческих математических олимпиад. М.: МГУ, 1987.

[10] *Картеси Ф.* Введение в конечные геометрии. М.: Наука, 1980.

[11] *Нечипорук Э. А.* Об одной булевской матрице // Доклады АН СССР. 1966. Т. 169(4). С. 765; Проблемы кибернетики. Вып. 21. С. 237–240. М.: Наука, 1969.

[12] *Райгородский А., Шабанов Л.* Об одной «олимпиадной» задаче про графы расстояний // Квант. 2015. № 3. С. 7–10.

[13] *Таранников Ю. В.* Комбинаторные свойства дискретных структур и приложения к криптологии. М.: МЦНМО, 2011.

[14] *Холл М.* Комбинаторика. М.: Мир, 1970.

[15] *Яглом И. М., Яглом А. М.* Неэлементарные задачи в элементарном изложении. М.: Эдиториал УРСС, 2006.

[16] *Mantel W.* // Wisk Opgaven. 1907. V. 10. P. 60–61.

[17] *Winkler P.* Mathematical puzzles: a connoisseur's collection. A. K. Peters, 2004.

Сергей Борисович Гашков, мехмат МГУ

sbgashkov@gmail.com

Теорема Семереди — Троттера

Ф. К. Нилов, А. А. Полянский, Н. А. Полянский

§ 1. Введение

Пал Эрдёш любил ставить «детские» вопросы, которые скорее похожи на пазлы, чем на серьёзные исследовательские проблемы. Зачастую математики с азартом набрасывались на такие задачи, и нередко выяснялось, что у одной проблемы существует несколько решений, основанных на различных глубоких идеях. Ровно так и сложилось с теоремой Семереди — Троттера.

Однажды Эрдёш сформулировал следующую гипотезу. Любые n прямых и n точек на плоскости образуют не более $cn^{4/3}$ инциденций для некоторой не зависящей от n константы c. Мы говорим, что точка и прямая образуют *инциденцию*, если точка лежит на прямой. То есть гипотеза Эрдёша была более строгой, чем тривиальная оценка сверху n^2 на число инциденций. Объяснение, почему в показателе стоит $4/3$, а не меньшая константа, будет дано в начале § 2.

В 1983 году два математика, Эндре Семереди и Уильям Томас Троттер, дали положительный ответ на поставленный вопрос. Более того, они доказали следующую теорему [5].

Теорема 1. *Любые n прямых и m точек на плоскости образуют не более $O((mn)^{2/3} + m + n)$ инциденций.*

Данную теорему неоднократно передоказывали. Упомянем следующие три доказательства: короткое вероятностное [6] (на русском языке изложено в [8, с. 127–128]) и два, основанных на идее «декомпозиции плоскости на клетки». Одно [3, раздел 4.5] из этих двух доказательств более «грубое». Другое [2] более «гладкое» и использует полиномиальный метод. Подробнее о данном методе читатель может прочитать, например, в [1].

Первый автор частично поддержан фондом «Династия»; второй — грантами РФФИ № 15–31–20403 (мол_а_вед), № 15–01–99563 А, № 15–01–03530 А; третий — грантом РФФИ № 16–01–00440 А.

Цель настоящей заметки — познакомить читателей с доказательством [2], основанным на полиномиальном методе. Статья состоит из двух частей: в § 2 будет изложено доказательство теоремы Семереди — Троттера в случае $n=m$ (читатель с лёгкостью сможет самостоятельно доказать случай $n \neq m$), использующее полиномиальный метод; в § 3 будет предложена подборка задач, в которую включены три их типа: задачи, решение которых позволяет доказать теорему Семереди — Троттера (по сути повторяющие сделанное в § 2), задачи, развивающие некоторые идеи, используемые при доказательстве, а также задачи, связанные с применением теоремы Семереди — Троттера. Изначально данная подборка задач служила основой проекта [7] Турнира городов в 2014 году. Позже второй автор использовал материалы данной заметки на просеминаре по комбинаторной геометрии для студентов-бакалавров в МФТИ. С решениями читатели могут ознакомиться в [7].

Задачи, которые непосредственно нужны для доказательства теоремы Семереди — Троттера, обозначены кружком.

§ 2. Доказательство теоремы Семереди — Троттера при $n = m$

Прежде чем перейти к доказательству теоремы, убедимся в существовании такой константы $c > 0$, что можно построить n прямых и n точек, для которых суммарное количество инциденций будет не меньше $cn^{4/3}$. Заметим, что достаточно рассматривать большие значения n. Для фиксированного $n > 1$ можно найти такое натуральное k, что $2k^3 \leqslant n < 2(k+1)^3 \leqslant 16k^3$. Рассмотрим $2k^3 < n$ точек на плоскости $\{(x, y)\colon 1 \leqslant x \leqslant k,\ 1 \leqslant y \leqslant 2k^2\}$ с целыми x, y, а также $k^3 < n$ прямых $\{y = ax + b\colon 1 \leqslant a \leqslant k,\ 1 \leqslant b \leqslant k^2\}$ с целыми a, b. Тогда для целого x, $1 \leqslant x \leqslant k$, имеем $1 \leqslant y = ax + b \leqslant k^2 + k^2 = 2k^2$, т. е. каждая прямая проходит через k точек из выбранного множества. Следовательно, суммарное число инциденций равно $k \cdot k^3 = k^4 > 2^{-16/3} n^{4/3}$.

2.1. Слабая оценка на число инциденций

Докажем следующую лемму, которая даёт слабую оценку на число инциденций между точками и прямыми.

Лемма 1. *Пусть на плоскости расположено n прямых и m точек. Тогда общее число инциденций не превосходит $n + m^2$.*

Доказательство. Заметим, что если прямая проходит только через одну из m точек, то она участвует в одной инциденции. Поэтому такие прямые суммарно участвуют не более чем в n инциденциях. Покажем, что прямые, содержащие по крайней мере две точки, суммарно участвуют не более чем в m^2 инциденциях. Действительно, через данную пару точек может проходить лишь одна прямая. Поскольку всего пар точек $m(m-1)/2$ и каждая из рассматриваемых прямых проходит через одну такую пару, число образованных ими инциденций не превосходит

$$2\frac{m(m-1)}{2} = m(m-1) < m^2. \qquad \square$$

2.2. Алгебраический подход к декомпозиции плоскости на клетки

Приведём несколько простых определений и лемм.

Множеством нулей Z_f многочлена $f(x,y) \in \mathbb{R}[x,y]$ называется множество всех точек (x,y), для которых $f(x,y)=0$. Будем называть *степенью* многочлена $f(x,y) \in \mathbb{R}[x,y]$ наибольшее значение $i+j$ по всем его мономам вида $x^i y^j$ с ненулевым коэффициентом.

Следующие две леммы несложно следуют из теоремы Безу. Приведём доказательства, в которых нам не потребуется эта теорема.

Лемма 2. *Пусть $f(x,y) \in \mathbb{R}[x,y]$ — многочлен степени d. Тогда любая прямая либо пересекает Z_f не более чем в d точках, либо целиком содержится в множестве Z_f.*

Доказательство. Заметим, что любую прямую можно параметризовать как

$$\{(x,y)\colon x = a_1 t + b_1,\ y = a_2 t + b_2,\ t \in \mathbb{R}\},$$

где $a_1, a_2, b_1, b_2 \in \mathbb{R}$ $(a_1^2 + a_2^2 \neq 0)$ — фиксированные числа. Поэтому все точки, лежащие в пересечении прямой и Z_f, определяются уравнением $f(a_1 t + b_1, a_2 t + b_2) = 0$. Поскольку последнее уравнение имеет степень не выше d относительно t, у него либо не более d решений, либо в качестве решения подойдёт любое t, т. е. прямая либо пересекает Z_f в не более чем d точках, либо целиком содержится в Z_f. $\square$

Лемма 3. *Пусть $f(x,y) \in \mathbb{R}[x,y]$ — многочлен степени d. Тогда число прямых, содержащихся в Z_f, не превосходит d.*

Доказательство. Предположим, что Z_f содержит k прямых. Тогда рассмотрим точку, которая не принадлежит Z_f (почему найдётся такая точка?), и проведём через неё прямую, которая пересекает каждую из k прямых, содержащихся в Z_f, и не проходит через точки пересечения этих прямых (количество таких точек конечно). Тогда из леммы 2 получаем, что число точек пересечения с Z_f не превосходит d, т. е. и число прямых, содержащихся в Z_f, не превосходит d. $\square$

Следующая лемма потребует введения нового определения.

Многочлен $f(x, y)$ будем называть *r-делящим* (где $r \geqslant 1$) для данного конечного множества точек $A \subset \mathbb{R}$, если в каждой компоненте связности множества $\mathbb{R}^2 \setminus Z_f$ содержится не более $|A|/r$ точек из A.

Лемма 4. *Пусть даны конечные множества $A_1, \ldots, A_m \subset \mathbb{R}^2$. Тогда существует многочлен степени не выше d, где $C^2_{d+2} - 1 \geqslant m$, который будет 2-делящим многочленом для каждого из множеств $A_1, \ldots, A_m$.*

Доказательство. Воспользуемся отображением (которое называется отображением Веронезе), переводящим точки плоскости в точки из $\mathbb{R}^n$, где $n = C^2_{d+2} - 1$:

$$\varphi(x, y) := (x, y, x^2, xy, y^2, \ldots, x^d, x^{d-1}y, \ldots, xy^{d-1}, y^d) \in \mathbb{R}^n.$$

Здесь каждой координате в $\mathbb{R}^n$ соответствует пара (i, j), для которой выполняются неравенства $0 \leqslant i$, $0 \leqslant j$, $1 \leqslant i + j \leqslant d$ (нетрудно убедиться, что количество таких пар в точности n). Тогда конечные множества A_i перейдут в конечные множества $\varphi(A_i)$ (отметим, что количество получившихся множеств не превосходит размерность пространства). Применим теперь теорему о бутерброде (см. [4, теорема 3.1.2]):

Теорема 2. *Пусть даны конечные множества $A_1, \ldots, A_d \subset \mathbb{R}^d$. Тогда существует такая гиперплоскость, что в каждом из открытых полупространств, образованных данной гиперплоскостью, содержится не более $\lfloor |A_i|/2 \rfloor$ точек из A_i для каждого i (некоторые точки могут лежать в гиперплоскости).*

Значит, существует такая гиперплоскость

$$a_{0,0} + a_{1,0}x_{1,0} + a_{0,1}x_{0,1} + a_{2,0}x_{2,0} + a_{1,1}x_{1,1} + a_{0,2}x_{0,2} + \ldots + a_{0,d}x_{0,d} = 0,$$

что в каждом из полупространств, образованных этой гиперплоскостью, находится не более $|A_i|/2$ точек из $\varphi(A_i)$. Легко убедиться, что многочлен

$$f(x, y) = a_{0,0} + a_{1,0}x + a_{0,1}y + a_{2,0}x^2 + a_{1,1}xy + a_{0,2}y^2 + \ldots + a_{0,d}y^d$$

будет 2-делящим для каждого из множеств $A_1, \ldots, A_m$. $\square$

Лемма 5. *Для любого конечного множества $A \subset \mathbb{R}^2$ существует многочлен степени не выше $7\sqrt{r}$, который будет r-делящим.*

Доказательство. Выберем такое целое неотрицательное m, что $2^m < r \leqslant 2^{m+1}$. Докажем, что существует многочлен, который будет 2^{m+1}-делящим для множества A. Для этого будем действовать по индукции. На первом шаге выбираем многочлен $f_0(x, y) = 1$, который является 2^0-делящим для A. Пусть мы построили 2^i-делящий многочлен $f_i(x, y)$, т. е. Z_{f_i} делит плоскость на компоненты, в каждой из которых находится не более $|A|/2^i$ точек. Заметим, что количество компонент, которые содержат более $|A|/2^{i+1}$ точек, меньше 2^{i+1}. Обозначим через ℓ их количество, а через A_j — совокупность точек, лежащих в j-й компоненте, содержащей более $|A|/2^{i+1}$ точек (но по предположению индукции не более $|A|/2^i$). Применим лемму 4 к множествам $A_1, \ldots, A_\ell$. Тогда найдётся многочлен $g_{i+1}(x, y)$ степени не выше $k = [\sqrt{2^{i+2}}]$ (так как $C^2_{k+2} - 1 \geqslant 2^{i+1} > \ell$), который будет 2-делящим для $A_1, \ldots, A_\ell$. Следовательно, многочлен $f_{i+1}(x, y) = g_{i+1}(x, y) \cdot f_i(x, y)$ является 2^{i+1}-делящим для A. Таким образом, по индукции мы построим многочлен $f_{m+1}(x, y)$, который будет 2^{m+1}-делящим (тем более r-делящим). Так как

$$f_{m+1}(x, y) = g_1(x, y) g_2(x, y) \ldots g_{m+1}(x, y),$$

степень многочлена $f_{m+1}(x, y)$ равна сумме степеней многочленов $g_i(x, y)$, т. е. не превосходит

$$\sum_{i=1}^{m+1} \sqrt{2^{i+2}} < \sqrt{2^{m+3}} \frac{1}{1 - 2^{-1/2}} = \sqrt{2^{m+1}} \frac{2}{1 - 2^{-1/2}} < 7\sqrt{r}. \qquad \square$$

2.3. Завершение доказательства теоремы Семереди — Троттера в случае $n = m$

Обозначим через $I(L', P')$ число инциденций, образованных прямыми из множества L' и точками из множества P', т. е. число таких пар (l, p), что $l \in L'$, $p \in P'$ и $p \in l$.

Пусть на плоскости расположено n прямых (обозначим их множество через L) и n точек (обозначим их множество через P). Используя лемму 5, построим r-делящий многочлен $f(x, y)$ степени не более $7\sqrt{r}$ для данного множества точек P (позже мы подберём значение величины r). Обозначим через $L_0 \subset L$ множество прямых, которые содержатся в Z_f, а через $P_0 \subset P$ — множество точек, лежащих на Z_f. Пусть многочлен f поделил плоскость на s частей: множество точек в i-й части будем обозначать через P_i, а множество прямых, пересекающих i-ю часть, — через L_i.

Заметим, что

$$I(L, P) = I(L_0, P_0) + I(L \setminus L_0, P_0) + \sum_{i=1}^{s} I(L_i, P_i).$$

Оценим каждое из слагаемых в правой части. Во-первых, $I(L_0, P_0) < 7n\sqrt{r}$, поскольку $|P_0| \leqslant n$ и по лемме 3 имеем $|L_0| < 7\sqrt{r}$. Аналогично получаем, что $I(L \setminus L_0, P_0) < 7n\sqrt{r}$, так как по лемме 2 каждая прямая из $L \setminus L_0$

(их не более чем n) будет пересекать Z_f не более чем в $7\sqrt{r}$ точках. Перейдём к оценке последнего слагаемого. Для этого воспользуемся слабой оценкой из леммы 1

$$\sum_{i=1}^{s} I(L_i, P_i) \leqslant \sum_{i=1}^{s}(|P_i|^2 + |L_i|).$$

Поскольку каждая прямая из $L \setminus L_0$ проходит не более чем через $7\sqrt{r}$ точек в Z_f, она входит не более чем в $7\sqrt{r}+1 \leqslant 8\sqrt{r}$ множеств L_i. Отсюда

$$\sum_{i=1}^{s} |L_i| \leqslant 8n\sqrt{r}.$$

Кроме того,

$$\sum_{i=1}^{s} |P_i|^2 \leqslant \max |P_i| \sum_{i=1}^{s} |P_i| \leqslant \frac{n^2}{r}.$$

Поэтому в итоге мы получаем, что

$$I(L, P) \leqslant 22n\sqrt{r} + \frac{n^2}{r}.$$

Выбирая $r = n^{2/3}$, получаем, что $I(L, P) \leqslant 23n^{4/3}$. Теорема Семереди — Троттера при $m = n$ доказана. □

§ 3. Подборка задач

3.1. Инциденции множеств

Пусть $X = \{x_1, \ldots, x_n\}$ — произвольное семейство подмножеств m-элементного множества $Y = \{y_1, \ldots, y_m\}$. Назовём пару (x_i, y_j) *инциденцией,* если $y_j \in x_i$. Через $I(X, Y)$ будем обозначать число инциденций, образованных элементами из X и Y. Во всех задачах этого параграфа мы считаем, что для некоторого $r \in \mathbb{N}$ выполняется $|x_i \cap x_j| \leqslant r$ для любых $i \neq j$.

Замечание. Инциденции можно воспринимать следующим образом. Рассмотрим такую таблицу размера $m \times n$, что в клетке, находящейся на пересечении i-й строки и j-го столбца, стоит звёздочка тогда и только тогда, когда $y_i \in x_j$. Таким образом, вопрос о числе инциденций равносилен вопросу о том, сколько звёздочек стоит в таблице.

Задача 1. Пусть $r = 1$. Докажите, что
а)$^\circ$ $I(X, Y) \leqslant m^2 + n$, $I(X, Y) \leqslant n^2 + m$;
б) $I(X, Y) \leqslant \sqrt{n(m^2 - m)} + n$, $I(X, Y) \leqslant \sqrt{m(n^2 - n)} + m$.

Задача 2. Докажите, что $I(X, Y) \leqslant \sqrt{mr(n^2 - n)} + m$.

Задача 3. Пусть $r = 1$. Найдите $\max I(X, Y)$

а) при $n \leqslant 3$;

б) при $m \geqslant C_n^2$.

При каких условиях достигается максимум?

Задача 4. Квадрат 13×13 разбит на единичные квадратики. Центры некоторых из них отмечены так, что нет прямоугольника с вершинами в отмеченных точках и сторонами, параллельными сторонам квадрата. Найдите наибольшее возможное число отмеченных точек.

Задача 5. Сто (или a) мышей вместе грызут 1000 (или b) кусков сыра. Каждая мышь может попробовать несколько кусков сыра, сделав в каждом из них по одной дырке. Любые две мыши сделали дырки не более чем в 10 (или c) общих кусках сыра. Докажите, что число дырок не больше

а) 11 000 (или $b + a\sqrt{bc}$);

б) 10 500 (или $\dfrac{b + \sqrt{b^2 + 4bca(a-1)}}{2}$).

3.2. Теорема о бутерброде

Задача 6. На плоскости расположено конечное количество точек. Докажите, что найдётся такая прямая, что в каждой из открытых полуплоскостей, на которые она делит плоскость, будет не больше половины всех точек.

Задача 7. а) Докажите, что если на плоскости даны красные и синие точки в общем положении, то найдётся прямая, которая делит плоскость на две такие открытые полуплоскости, что в каждой из них находится не более половины красных и не более половины синих точек.

б) Докажите, что если в пространстве даны красные, синие и зелёные точки в общем положении, то найдётся плоскость, которая делит пространство на два таких открытых полупространства, что в каждом из них находится не более половины точек каждого цвета.

В пункте 3.4 нам пригодится следующее обобщение задачи 7 (см. п. 2.2, теорема 2):

Теорема о бутерброде. *Пусть даны конечные множества $A_1, \ldots, \ldots, A_d \subset \mathbb{R}^d$. Тогда существует такая гиперплоскость, что в каждом из открытых полупространств, образованных данной гиперплоскостью, будет не более $\lfloor |A_i|/2 \rfloor$ точек из A_i для каждого i (некоторые точки могут лежать в гиперплоскости).*

Задача 8. а) Пусть на плоскости дано $2n$ точек общего положения, из них n красных и n синих. Докажите, что их можно разделить на пары таким образом, что каждая пара будет состоять из точек разных цветов, а отрезки, соответствующие парам, не будут пересекаться.

б)[1] Пусть в пространстве дано $3n$ точек общего положения, из них n красных, n синих и n зелёных. Докажите, что их можно разделить на тройки таким образом, что каждая тройка будет состоять из точек разных цветов, а треугольники, соответствующие тройкам, не будут пересекаться.

Задача 9. Два вора украли ожерелье с двумя концами, состоящее из платиновой цепочки, на которую нанизаны драгоценные камни d видов. Воры не знают ценности каждого камня, поэтому хотят поделить камни каждого вида поровну (известно, что камней каждого вида чётное количество). Чтобы потерять как можно меньше платины, воры хотят сделать наименьшее число разрезов. Могут ли они поделить ожерелье с помощью

а) $(d-1)$ разрезов?

б) d разрезов?

3.3. Конструктивная геометрия

Мы будем говорить, что n точек и n прямых на плоскости образуют *конфигурацию* n_d из точек и прямых, если на любой данной прямой лежит ровно d данных точек и через любую данную точку проходит ровно d данных прямых, т. е. число инциденций равно nd.

Задача 10. Постройте две различные конфигурации а) 9_3; б) 10_3.

Задача 11°. а) Постройте для любого n такой пример из n прямых и n точек, что число инциденций, задаваемое этими прямыми и точками на плоскости, больше, чем $c'n^{4/3}$ для некоторой константы $c' > 0$, не зависящей от n.

б) Постройте для любых n и m такой пример из n прямых и m точек, что число инциденций, задаваемое этими прямыми и точками на плоскости, больше, чем $c''((nm)^{2/3} + n + m)$ для некоторой константы $c'' > 0$, не зависящей от n и m.

3.4. Алгебраические мотивы в геометрии

Воспользуемся терминологией из п. 2.2.

Задача 12°. Пусть $f(x, y)$ — многочлен степени d. Докажите, что любая прямая либо пересекает Z_f не более чем в d точках, либо целиком содержится в множестве Z_f.

---

[1] К сожалению, до сих пор неизвестно элементарное (т. е. без использования теоремы о бутерброде) решение этой задачи.

Задача 13°. Пусть $f(x, y)$ является многочленом степени d. Докажите, что число прямых, содержащихся в Z_f, не превосходит d.

Задача 14°. Покажите, что количество мономов степени не выше d от двух переменных ровно C_{d+2}^2.

Задача 15. Докажите, что для конечного множества $A \subset \mathbb{R}^2$ существует r-делящий многочлен степени $[r]$.

Здесь каждой координате в $\mathbb{R}^n$ соответствует пара (i, j), для которой выполняются неравенства $0 \leqslant i$, $0 \leqslant j$, $1 \leqslant i + j \leqslant d$.

Задача 16°. Пусть даны конечные множества $A_1, \ldots, A_m \subset \mathbb{R}^2$. Докажите, что существует многочлен степени не выше k, где $C_{k+2}^2 - 1 \geqslant m$, который будет 2-делящим многочленом для каждого из данных множеств.

Задача 17°. Докажите, что для конечного множества $A \subset \mathbb{R}^2$ существует r-делящий многочлен степени не выше $c\sqrt{r}$, где c — некоторая константа (например, можно показать, что $c \leqslant 7$).

3.5. Доказательство теоремы Семереди — Троттера

Пусть $I(L', P')$ — число инциденций, образованных прямыми из множества L' и точками из множества P', т. е. число таких пар (l, p), что $l \in L'$, $p \in P'$ и $p \in l$.

Пусть на плоскости отмечены множество L из n прямых и множество точек P из n точек. Пользуясь задачей 17, построим r-делящий многочлен $f(x, y)$ для данного множества точек P (значение величины r подберём позже). Обозначим через $L_0 \subset L$ множество отмеченных прямых, которые содержатся в Z_f, а через $P_0 \subset P$ множество отмеченных точек, лежащих на Z_f. Пусть многочлен f поделил плоскость на s частей: множество отмеченных точек в i-й части будем обозначать через P_i, а множество отмеченных прямых, пересекающих i-ю часть, через L_i.

Задача 18°. Докажите, что существуют такие константы c_1, c_2, c_3, что
а) $I(L_0, P_0) \leqslant c_1 n\sqrt{r}$;
б) $I(L \setminus L_0, P_0) \leqslant c_2 n\sqrt{r}$;
в) $\displaystyle\sum_{i=1}^{s} I(L_i, P_i) \leqslant c_3\Big(\frac{n^2}{r} + n\sqrt{r}\Big)$.

Задача 19°. Выбрав нужное r, докажите теорему Семереди — Троттера в случае $n = m$.

Задача 20°. Докажите теорему Семереди — Троттера в общем случае.

3.6. Применения теоремы Семереди — Троттера

Задача 21. Докажите, что существует такая константа c, что для любых n точек на плоскости число треугольников единичной площади с вершинами в данных точках не превосходит $cn^{7/3}$.

Задача 22. а) Докажите, что число прямых, каждая из которых содержит не менее $k > 2$ различных точек m-элементного множества P, равно $O(m^2/k^3 + m/k)$.

б) Докажите, что такие прямые задают $O(m^2/k^2 + m)$ инциденций с данным множеством точек P.

Задача 23 (Теорема Бека). Пусть P — множество точек на плоскости, а L — множество прямых, проходящих по меньшей мере через две точки из P. Тогда найдутся такие константы $c_1, c_2 > 0$, не зависящие от P и L, что выполняется одно из двух условий:

1. Найдётся прямая из L, которая содержит по крайней мере $c_1|P|$ точек.
2. $|L| \geqslant c_2|P|^2$.

Задача 24. Пусть $A \subset \mathbb{R}$ — конечное множество. Докажите, что существует такая константа $c > 0$, что

$$\max\{|A + A|; |A \cdot A|\} \geqslant c|A|^{5/4},$$

где

$$A + A = \{a_1 + a_2 \colon a_1 \in A,\ a_2 \in A\},$$
$$A \cdot A = \{a_1 \cdot a_2 \colon a_1 \in A,\ a_2 \in A\}.$$

Список литературы

[1] *Dvir Z.* Incidence Theorems and Their Applications // Foundations and Trends in Theoretical Computer Science. 2012. V. 6, № 4. P. 257–393. https://arxiv.org/pdf/1208.5073v2.pdf

[2] *Kaplan H., Matoušek J., Sharir M.* Simple Proofs of Classical Theorems in Discrete Geometry via the Guth-Katz Polynomial Partitioning Technique // Discrete Comput. Geom. 2012. V. 48, № 3. P. 499–517. http://arxiv.org/abs/1102.5391v1

[3] *Matoušek J.* Lectures on Discrete Geometry. New York: Springer-Verlag, 2002. (Graduate Texts in Math.; V. 212).

[4] *Matoušek J.* Using the Borsuk — Ulam theorem: Lectures on Topological Methods in Combinatorics and Geometry. Berlin: Springer-Verlag, 2003.

[5] *Szemerédi E., Trotter W. T.* Extremal problems in discrete geometry // Combinatorica. 1983. V. 3, iss. 3. P. 381–392.

[6] *Székely L.* Crossing numbers and hard Erdős problems in discrete geometry // Combin. Probab. Comput. 1997. V. 6, № 3. P. 353–358.

[7] *Нилов Ф., Полянский А., Полянский Н.* Инциденции точек и прямых, проект 26-й летней конференции Турнира городов.
http://www.turgor.ru/lktg/2014/7/index.htm

[8] *Тао Т.* Структура и случайность. М.: МЦНМО, 2017.

Фёдор Константинович Нилов, мехмат МГУ
nilovfk@gmail.com

Александр Андреевич Полянский, МФТИ, Технион, ИППИ РАН
alexander.polyanskii@yandex.ru

Никита Андреевич Полянский, ИППИ РАН
nikitapolyansky@gmail.com

Преподавание и популяризация математики

Вложения в плоскость графов с вершинами степени 4

А. Б. Скопенков*

В этой методической заметке приводится доказательство интересной и важной гипотезы В. А. Васильева [1] о критерии планарности графа с вершинами степени 4 и некоторой дополнительной («крестовой») структурой. Эта гипотеза относится к числу тех замечательных проблем, возникших в современной математике, формулировка и доказательство которых доступны школьнику, знакомому с основами теории графов. Она была впервые доказана В. О. Мантуровым [2], см. также [3]. В настоящей заметке приведено более простое изложение доказательства, а также даны пояснения для начинающих [1)].

Полуребром графа называется пара из ребра и его концевой вершины (или, неформально, конца ребра). *Графом с крестовой структурой* (кратко *X-графом*) называется граф, степень каждой вершины которого равна 4,

* Работа выполнена при поддержке РФФИ, грант № 15–01–06302, грантами фонда Саймонса и стипендией фонда Д. Зимина «Династия».

1) Эта заметка написана по материалам цикла задач [6], представленного на Летней конференции Турнира городов в 2005 г. А. Каибхановым, Д. Пермяковым и автором. Она выложена в архив в августе 2010 г. Поставленный в ней вопрос (задача 2) послужил отправной точкой для интересных исследований [3, 4].

Редколлегией сборника при публикации внесены некоторые изменения в аннотацию. Обновляемая авторская версия: `https://arxiv.org/abs/1008.4940`

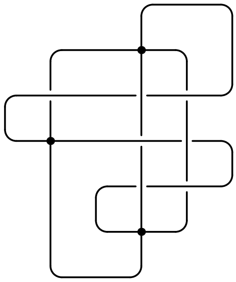


Рис. 1

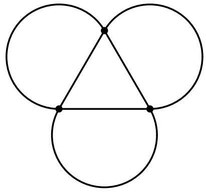


Рис. 2

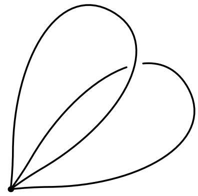


Рис. 3

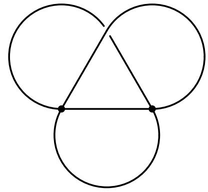


Рис. 4

причём для каждой вершины фиксировано разбиение четырёх входящих в неё полурёбер на две пары.

Вот примеры X-графов. Они изображены на плоскости (с самопересечениями) так, что при обходе вокруг каждой вершины полурёбра из первой пары и полурёбра из второй пары чередуются (т. е. проходятся в порядке 1212, а не 1122).

X-Граф называется *X-планарным*, если его можно изобразить без самопересечений на плоскости так, что при обходе вокруг каждой вершины полурёбра из первой пары и полурёбра из второй пары чередуются.

Например, X-граф на рис. 1 является X-планарным, ибо он «не отличается как X-граф» от изображённого на рис. 2.

Заметим, что не любой планарный X-граф X-планарен. Действительно, X-графы «восьмёрка» (рис. 3) и «трилистник» (рис. 4) планарны, но не X-планарны.

Общая вершина двух путей на X-графе, не имеющих общих рёбер, называется *точкой перекрестья*, если один из этих путей проходит по полурёбрам из одной пары, выходящим из этой вершины. (Тогда второй путь проходит по полурёбрам из другой пары.)

Теорема планарности графов с крестовой структурой. *X-Граф X-планарен тогда и только тогда, когда он не содержит двух несамопересекающихся циклов без общих рёбер, имеющих ровно одну вершину перекрестья.*

Замечания. (а) Слово «несамопересекающихся» можно опустить[2].

[2] Чтобы обосновать это замечание, покажем, что если в X-графе есть два цикла K_1 и K_2 ровно с одной точкой перекрестья A, то есть и два несамопересекающихся цикла с тем же свойством. Для этого рассмотрим несамопересекающийся цикл K_1^+ из рёбер цикла K_1, содержащий вершину A. Аналогично определим цикл K_2^+. Тогда K_1^+ и K_2^+ и будут искомыми циклами.

(б) Слова «без общих рёбер, имеющих ровно одну вершину перекрестья» нельзя заменить на «пересекающихся только по одной вершине, являющейся вершиной перекрестья» (см. пример на рис. 4).

Доказательство необходимости в теореме. Пусть, напротив, некоторый X-граф с несамопересекающимися циклами K_1 и K_2, имеющими ровно одну вершину A перекрестья, X-планарен. Цикл K_1 делит плоскость на две части. Лишь в вершине A при движении по циклу K_2 мы переходим из одной части в другую, а в остальных общих вершинах остаёмся в той же части. Противоречие. □

Задача 1. Если в X-графе найдутся два цикла с нечётным числом точек перекрестья, то найдутся и два цикла ровно с одной точкой перекрестья.

Задача 2 (для исследования). Сформулируйте определения $*$-графа и $*$-планарности для графов, степень каждой вершины которых равна 4. (*Указание*: полурёбра, выходящие из каждой вершины, можно разбить на три пары или на две тройки...) Найдите соответствующие критерии $*$-планарности.

Для одного из определений $*$-графа и $*$-планарности решение приведено в [4] и [5]. Насколько мне известно, для других вариантов вопрос открыт!

В оставшейся части заметки приводится *доказательство достаточности в теореме.*

Цикл в графе называется *эйлеровым*, если он проходит по каждому *ребру* ровно по одному разу.

Пусть в графе степени 4 задан эйлеров цикл. Назовём две вершины P и Q *скрещивающимися*, если они идут вдоль эйлерова цикла в порядке $PQPQ$ (а не $PPQQ$). Назовём эйлеров цикл *удобным*, если вершины графа можно так разбить на два множества, что никакие две вершины из одного множества не скрещиваются.

Идею доказательства можно пояснить на следующей красивой задаче[3)].

Задача 3. Связный граф степени 4 планарен тогда и только тогда, когда в нём найдётся удобный эйлеров цикл.

Решение. *Достаточность.* Пусть вершины разбиты на два множества требуемым образом. Построим несамопересекающийся цикл S на плоскости, рёбра которого соответствуют всем рёбрам удобного эйлерова цикла и идут в том же порядке. Каждой вершине графа отвечают две вершины

[3)] В дальнейшем она не используется формально, а служит лишь для *мотивировки* понятий поворачивающего и сильно поворачивающего эйлерова цикла. Поэтому задачу 3 и её решение можно пропустить.

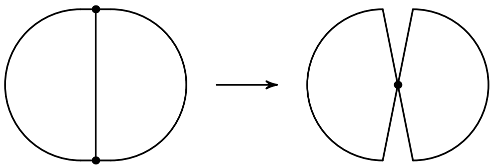


Рис. 5

цикла S. Соединим каждую пару вершин цикла S, отвечающую вершине *первого* множества (из определения удобности), несамопересекающейся ломаной *внутри* цикла S. Эти ломаные можно взять попарно непересекающимися, поскольку соответствующие вершины первого множества не скрещиваются. Аналогично соединим пары вершин цикла S, отвечающие вершинам *второго* множества, несамопересекающимися попарно непересекающимися ломаными *вне* цикла S. Стянем в плоскости каждую проведённую ломаную в точку (рис. 5). Получим вложение графа в плоскость.

Необходимость. Будем называть *гранями* связные куски, на которые распадается плоскость при разрезании по всем рёбрам плоского графа. Начнём двигаться из некоторой вершины A, причём из каждой вершины будем выходить по ребру, соседнему по грани с тем, по которому пришли. По рёбрам разрешается проходить не более чем по одному разу. Будем так двигаться, пока возможно. Завершиться это движение может только в A. Более того, мы вернёмся в A по ребру, лежащему в одной грани с начальным ребром (иначе мы ещё можем продолжить движение). По окончании движения получим цикл T', проходящий через каждую вершину по парам рёбер, лежащих в одной грани (в том числе и через A, как показано ранее). Если T' не эйлеров, то из некоторой его вершины B выходят рёбра, не принадлежащие T'. Пройдём из B по циклу T', а затем продолжим движение так же, как при построении цикла T'. В итоге получим больший цикл, также проходящий через каждую вершину по рёбрам, лежащим в одной грани, и потому несамопересекающийся. Таким образом можно увеличивать цикл, пока он не будет содержать все рёбра графа.

Докажем, что построенный эйлеров цикл удобен. Расцепим этот цикл в каждой вершине, соединив в плоскости расцеплённые точки отрезками (рис. 6). Объединение рёбер полученного графа, не совпадающих с проведёнными отрезками, разбивает плоскость на две части. Включим в первое (второе) множество вершин исходного графа те вершины, которые отвечают проведённым отрезкам, лежащим во внутренней (внешней) части. □

Пусть в X-графе имеется удобный эйлеров цикл T. По нему можно построить вложение X-графа в плоскость, как в задаче 3. При каком условии на T полученное вложение будет «X-вложением»? Ясно, что T должен

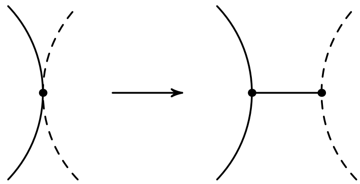


Рис. 6

быть *поворачивающим*, т. е. в каждой вершине последовательно проходить по полурёбрам из разных пар, выходящим из этой вершины. Этого условия недостаточно. Цикл T должен быть *сильно поворачивающим*, т. е. при движении по циклу T (в одном произвольном направлении) мы должны входить в каждую вершину оба раза по полурёбрам одной и той же пары.

Достаточность в теореме вытекает из следующих трёх лемм.

Лемма о планарности. *Если в X-графе существует удобный сильно поворачивающий эйлеров цикл, то X-граф X-планарен.*

Лемма о поворачивающем цикле. *В любом связном X-графе существует поворачивающий эйлеров цикл.*

Лемма о дополнительных свойствах. *Пусть X-граф не содержит двух несамопересекающихся циклов без общих рёбер, имеющих ровно одну вершину перекрестья. Тогда любой поворачивающий эйлеров цикл является удобным и сильно поворачивающим.*

Доказательство[4] леммы о планарности. Построим несамопересекающийся цикл S на плоскости, рёбра которого соответствуют всем рёбрам удобного эйлерова цикла и идут в том же порядке. Каждой вершине графа отвечают две вершины цикла S.

Соединим каждую пару вершин цикла S, отвечающую вершине *первого* множества (из определения удобности), несамопересекающейся ломаной *внутри* цикла S. Эти ломаные можно взять попарно непересекающимися, поскольку соответствующие вершины первого множества не скрещиваются. Аналогично соединим пары вершин цикла S, отвечающие вершинам *второго* множества, несамопересекающимися попарно непересекающимися ломаными *вне* цикла S.

Стянем в плоскости каждую проведённую ломаную в точку (рис. 5). Получим вложение X-графа в плоскость. Поскольку взятый эйлеров цикл сильно поворачивающий, при обходе вокруг каждой вершины полурёбра из первой и из второй пары чередуются. Значит, это вложение является «X-вложением». □

[4] Это доказательство, кроме последнего абзаца, повторяет решение задачи 3.

Доказательство леммы о поворачивающем цикле (аналогичное доказательству критерия существования эйлерова цикла). Начнём двигаться из некоторой вершины A. Будем двигаться, меняя пару полуребра в каждой вершине и проходя по рёбрам не более чем по одному разу, пока возможно. Так как из каждой вершины выходит поровну полурёбер обеих пар, завершиться это движение может только в A. Более того, мы вернулись в A по полуребру, не парному начальному полуребру (иначе мы ещё можем выйти по полуребру другой пары, а значит, движение не завершилось). По окончании движения получим поворачивающий цикл F.

Если F не эйлеров, то из некоторой его вершины B выходят рёбра, не принадлежащие F. Пройдём из B по циклу F, а затем продолжим движение так же, как при построении цикла F. В итоге получим больший поворачивающий цикл. Таким образом можно увеличивать цикл, пока он не будет содержать все рёбра X-графа. $\square$

Доказательство сильной поворачиваемости в лемме о дополнительных свойствах. Пусть, напротив, найдётся такая вершина A, что поворачивающий цикл T входит в неё первый раз по полуребру одной пары, а второй — по полуребру другой пары. Обозначим через T_1 цикл, соответствующий части цикла T от первого выхода из A до второго входа в A. Обозначим через T_2 цикл, соответствующий остатку цикла T. Тогда T_1 и T_2 — циклы, поворачивающие во всех вершинах, кроме вершины A, являющейся для них вершиной перекрестья. Если путь поворачивает в вершине, то эта вершина не может быть для него точкой перекрестья с другим путём. Значит, остальные вершины не являются для циклов T_1 и T_2 точками перекрестья. Но такой пары циклов нет по предположению. $\square$

Доказательство удобности в лемме о дополнительных свойствах. Построим вспомогательный граф $Q(T)$. Вершины графа $Q(T)$ — те же, что у исходного графа. Две вершины графа $Q(T)$ соединяются ребром, если они скрещиваются (относительно цикла T).

Удобность цикла T равносильна двудольности графа $Q(T)$, что, в свою очередь, равносильно отсутствию в $Q(T)$ циклов нечётной длины.

Пусть поворачивающий цикл T неудобен. Возьмём наименьший цикл A нечётной длины $2k+1 \geqslant 3$ в $Q(T)$.

Так как цикл A минимален, скрещиваются только соседние его вершины. Пройдём по эйлерову циклу T, обозначая появляющиеся вершины цикла A через $Y_1, Y_2, \ldots, Y_{4k+2}$: каждая из этих вершин получит два номера, отличающиеся на 3. Более аккуратно: обозначим через

- T отображение из $\{1, 2, \ldots, n\}$ в множество вершин исходного графа, выражающее порядок обхода эйлерова цикла T,

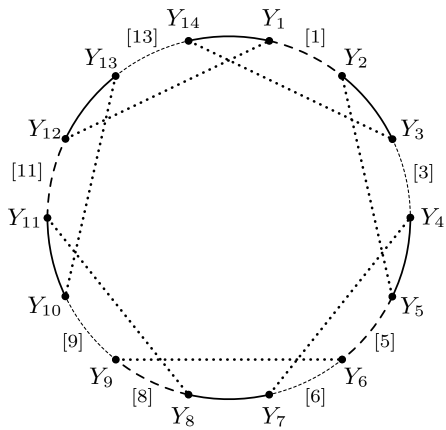


Рис. 7

- $1 \leqslant y_1 < y_2 < \ldots < y_{4k+2} \leqslant n$ числа, образами которых являются вершины цикла A,
- Y_j вершину $T(y_j)$.

Без ограничения общности можно считать, что $Y_2 = Y_5$, $Y_4 = Y_7$, $\ldots$, $Y_{4k} = Y_1$, $Y_{4k+2} = Y_3$.

Положим

$$[i] := (T(y_i), T(y_i + 1), \ldots, T(y_{i+1}))$$

для каждого $i \in \{1, 2, \ldots, 4k + 1\}$. (Неформально, это «отрезок эйлерова цикла T, проходимый между Y_i и Y_{i+1}». Чтобы строго объяснить, что это такое, и нужно рассматривать T как отображение.)

Возьмём первый цикл (рис. 7):

$$[1], [5], \ldots, [4l - 7], [4l - 3], \overline{[4l]}, [4l + 3], [4l + 7], \ldots, [4k - 5], [4k - 1],$$

где $l := [(k + 1)/2]$. Здесь путь $[4l]$ проходится против эйлерова цикла T, а остальные пути — по циклу T.

(Вот неформальное объяснение этого построения для $k = 3$, см. рис. 7. Пройдём по циклу T из $Y_{12} = Y_1$ в Y_2, затем из $Y_2 = Y_5$ в Y_6, затем против цикла T из $Y_6 = Y_9$ в Y_8, затем по циклу T из $Y_8 = Y_{11}$ в Y_{12}.)

Возьмём второй цикл, «симметричный» первому (рис. 7):

$$[3], [7], \ldots, [4m - 5], [4m - 1], \overline{[4m + 2]}, [4m + 5], [4m + 9], \ldots, [4k - 3], [4k + 1],$$

где $m = k - l$. Здесь путь $[4m + 2]$ проходится против цикла T, а остальные пути — по циклу T.

(Вот неформальное объяснение этого построения для $k = 3$, см. рис. 7. Пройдём по циклу T из $Y_{14} = Y_3$ в Y_4, затем против цикла T из $Y_7 = Y_4$ в Y_6, затем по циклу T из $Y_6 = Y_9$ в Y_{10}, затем из $Y_{10} = Y_{13}$ в Y_{14}.)

У построенных двух циклов одна общая вершина $Y_{2k} = Y_{2k+3}$. Первый цикл выходит из неё против цикла T, а входит по циклу T. Как уже доказано, цикл T сильно поворачивающий. Поэтому первый цикл в обоих случаях идёт по полурёбрам одной пары. Аналогично второй цикл проходит через эту вершину по полурёбрам другой пары. Таким образом, у этих циклов единственная точка перекрестья. Противоречие. $\square$

Благодарности

Благодарю редколлегию сборника «Математическое просвещение» за полезные замечания и обсуждения.

Список литературы

[1] *Васильев В. А.* Инварианты и когомологии первого порядка для пространств вложений самопересекающихся кривых в $\mathbb{R}^n$ // Изв. РАН. Сер. матем. 2005. Т. 69, № 5. С. 3–52.

[2] *Мантуров В. О.* Доказательство гипотезы В. А. Васильева о планарности сингулярных зацеплений // Изв. РАН. Сер. матем. 2005. Т. 69, № 5. С. 169–178.

[3] *Мантуров В. О.* Четырёхвалентные графы с крестовой структурой // Математическое просвещение. Сер. 3. Вып. 15. М.: МЦНМО. 2011. С. 128–137.

[4] *Friesen T.* A generalization of Vassiliev's planarity criterion. `http://arxiv.org/abs/1210.1539`

[5] *Friesen T., Manturov V.* Embeddings of $*$-graphs into 2-surfaces. `http://arxiv.org/abs/1212.5646`

[6] `http://olympiads.mccme.ru/lktg/2005/3/index.htm`

[7] `https://arxiv.org/abs/1008.4940`

Аркадий Борисович Скопенков, МФТИ, НМУ
`skopenko@mccme.ru`, `http://www.mccme.ru/~skopenko/`

Избранные задачи экзамена по дискретному анализу

А. А. Полянский, П. Б. Тарасов

Дискретный анализ — один из фундаментальных математических курсов, читаемый А. М. Райгородским на факультете инноваций и высоких технологий МФТИ. Преподаватели кафедры дискретной математики МФТИ уже неоднократно делились на страницах «Математического просвещения» методическими материалами, которыми они пользуются при проведении семинаров (см. [2, 3]).

В данной короткой статье мы предложим несколько интересных задач, которые предлагались на устном экзамене по дискретному анализу, проходившем в июне 2015 года. Отличительными чертами этих задач является то, что их условия имеют необычную формулировку, а решения состоят из двух частей: во-первых, студентам необходимо понять, к какой теореме курса данная задача сводится, во-вторых, нужно доказать соответствующие теоремы. Это было сделано для того, чтобы студенты, которые «заучили» билеты не вдумываясь, не смогли распознать теоремы, спрятанные под формулировками задач.

Решения задач мы разбирать в рамках статьи не будем. При желании читатель с лёгкостью сможет найти теоремы, которые нужны для решения задач: для этого достаточно обратиться к подсказкам и списку литературы в конце статьи.

Отметим, что каждую задачу смогла решить приблизительно половина студентов, которым она доставалась. На потоке прикладной математики и информатики обучается приблизительно 100 студентов, каждому студенту доставалось две задачи из списка в 20 задач (ниже предложены лишь 16 из них), т. е. каждую задачу пытались решить около 10 человек. В статье задачи расположены в порядке их сложности.

Первый автор частично поддержан грантами РФФИ № 15–31–20403 мол_а_вед, № 15–01–99563 А, № 15–01–03530 А.

Авторы выражают благодарность сотрудникам кафедры дискретной математики (особенно А. Б. Скопенкову) за замечания, которые позволили улучшить формулировки задач.

Задачи

1. В скале расположено n комнат-пещер, и некоторые из них соединены коридорами (коридор соединяет две комнаты), при этом из любой комнаты в любую другую ведёт ровно один путь, возможно проходящий через другие комнаты. Какое минимальное количество коридоров необходимо пройти, чтобы посетить все комнаты, если стартовать и заканчивать надо в первой комнате?

2. Среди любых ли 8 теннисистов найдётся такая четвёрка, что каждые двое хоть раз играли друг против друга, либо такая тройка, что никакие двое не играли друг против друга?

3. В городе N живёт 2016 моноциклистов, причём среди любых 65 из них найдутся по крайней мере два знакомых. Докажите, что нельзя так раскрасить моноциклы в 31 цвет, чтобы на велопараде любые два владельца моноциклов одного цвета были незнакомы.

4. Есть N альпинистов, которые любят ходить парами в горы. Каждые два альпиниста однажды вместе посетили либо Кавказ, либо Альпы, либо Гималаи. Известно, что среди любых 20 альпинистов найдутся двое, которые вместе посетили Кавказ или Альпы, а среди любых 30 найдутся двое, которые вместе посетили Кавказ или Гималаи. Докажите, что при достаточно большом N найдётся 1000 таких альпинистов, что каждая пара из 1000 альпинистов посетила Кавказ.

5. В волшебном замке пять лестниц между шестью этажами каждый день меняют своё расположение. Известно, что каждый день можно попасть с каждого этажа на каждый (по лестнице можно попасть только с одного этажа на другой, на промежуточном сойти не получится). Могло ли произойти, что на протяжении трёх лет схема переходов между этажами ни разу не повторилась?

6. Семирукий инопланетянин хочет попасть на борт корабля NASA, чтобы позавтракать с космонавтами. Для того чтобы войти на корабль, нужно ввести пароль следующим образом. Каждую минуту инопланетянин может внести одну руку в кувшин. После этого сканер, находящийся внутри кувшина, распознаёт руку инопланетянина и запоминает эту руку. Требуется ввести правильную последовательность из 4 рук (возможно, что одну руку нужно ввести 4 раза подряд; сканер помнит только последние 4 введённых объекта). Инопланетянин не помнит пароль от входа (а может быть, вообще не знает). Через какое наименьшее время он сможет гарантированно насладиться пакетиком настоящего английского чая?

7. В королевстве 116 городов. Для любых двух городов, не соединённых дорогой, сумма количества дорог из первого города и количества дорог из второго города не меньше 118. Докажите, что король может выехать из столицы, проехать по всем городам и вернуться назад, не посетив никакой город дважды.

8. В средневековом государстве между замками проложена сеть непересекающихся дорог, идущих от замка к замку. Если перекрыть все дороги, ведущие к некоторому замку, то его можно захватить. Какое наименьшее число дорог заведомо достаточно перекрыть, чтоб захватить хотя бы один замок?

9. Президент Тридевятого Царства отдал приказ тысяче министров заняться строительством городов. Министры решили, что любая тройка министров объединится для строительства своего города (другие министры не участвуют в этом) и соединит его авиалинией с теми городами, в строительстве которых участвовал ровно один министр из этих трёх. По окончанию проекта по строительству городов и авиалиний Президент хочет объехать всю страну с визитом, побывав в каждом городе лишь один раз. Сможет ли он это сделать?

10. Группа из 10 000 жуликов сформировала 5000 банд по 25 жуликов в каждой (жулик может одновременно входить в несколько банд). Детективу хочется уничтожить все банды, для этого достаточно посадить в тюрьму по одному жулику из каждой банды. Докажите, что детективу достаточно посадить в тюрьму 1600 жуликов, чтобы уничтожить все банды.

11. В городе живёт 2015 человек. Вася узнал новость и решил её распространить, при этом другие жители города не знают эту новость. Известно, что на следующий день было совершено 2015 звонков и в результате эту новость узнали все. Напишите формулу для подсчёта количества возможных различных схем совершённых звонков (две схемы, отличающиеся порядком следования звонков, считаются одинаковыми).

12. В Техасе проживает 1000 бандитов. Известно, что они образовали банды по 45 человек в каждой. Шерифу поступила информация о том, что у любых двух банд есть по крайней мере один общий представитель. Помогите шерифу понять, какое наибольшее число банд находится в его штате.

13. Тысяча школьников города Новые Васюки вышли на парад. Известно, что дети ходят в 300 кружков. Остап Бендер хочет раздать учащимся пилотки двух цветов (красные и синие) так, чтобы среди представителей одного кружка разность (по модулю) между количеством людей в красных пилотках и в синих пилотках не превосходила 150. Докажите, что Остап Бендер может справиться с поставленной задачей.

14. Существует ли группа из $C_{7^3}^{7^2}$ человек, в которой нет $7C_{7^3}^{7}$ человек, попарно знакомых или незнакомых?

Подсказки

1. Воспользуйтесь соотношением между количеством рёбер и количеством вершин в дереве (см. [1, задача 2.2.1]).
2. Вспомните (и докажите), чему равно число Рамсея $R(4,3)$ (см. [1, задача 4.1.1]).
3. Воспользуйтесь соотношением между кликовым числом и числом независимости графа (см. [1, задача 3.1.3]).
4. Воспользуйтесь конечностью чисел Рамсея (см. [1, задача 4.1.2]).
5. Воспользуйтесь формулой Кэли (см. [1, задача 2.2.3]).
6. Воспользуйтесь свойствами последовательности де Брёйна (см. [1, задача 2.5.7]).
7. Воспользуйтесь критерием Дирака гамильтоновости графа (см. [1, задача 2.6.2]).
8. Докажите, что в планарном графе существует вершина степени не более 5 (см. [1, задача 2.4.3]).
9. Воспользуйтесь гамильтоновостью графа 1-пересечений 3-элементных множеств n-элементного множества (см. [1, задача 2.6.5]).
10. Воспользуйтесь теоремой об оценке сверху для системы общих представителей (см. [4, теорема 3.1]).
11. Воспользуйтесь формулой для числа унициклических графов (см. [1, задача 2.2.5]).
12. Воспользуйтесь теоремой Эрдёша — Ко — Радо (см. [1, задача 5.1.3]).
13. Воспользуйтесь теоремой об оценке сверху уклонения в гиперграфе (см. [5, лекция 26]).
14. Воспользуйтесь нижней оценкой для чисел Рамсея, основанной на векторных пространствах (теорема Франкла — Уилсона, см. [5, лекция 17]).

Список литературы

[1] *Глибичук А. А., Дайняк А. Б., Ильинский Д. Г. и др.* Элементы дискретной математики в задачах. М.: МЦНМО, 2016.

[2] *Ильинский Д., Купавский А., Райгородский А., Скопенков А.* Дискретный анализ для математиков и программистов (подборка задач) // Математическое просвещение. Сер. 3. Вып. 17. М.: МЦНМО, 2013. С. 162–181.

[3] *Ильинский Д. Г., Райгородский А. М., Скопенков А. Б.* Независимость и доказательства существования в комбинаторике // Математическое просвещение. Сер. 3. Вып. 19. М.: МЦНМО, 2015. С. 164–177.

[4] *Райгородский А. М.* Системы общих представителей в комбинаторике и их приложения в геометрии. М.: МЦНМО, 2009.

[5] *Райгородский А. М.* Дискретный анализ, видеолекции.
`http://lectoriy.mipt.ru/course/Maths-DiscreteMathematics-13L`

Александр Андреевич Полянский, МФТИ, Технион, ИППИ РАН
`alexander.polyanskii@yandex.ru`

Павел Борисович Тарасов, МФТИ
`tarasov.p.b@gmail.com`

Нам пишут

Отклик на статью В. М. Журавлёва и П. И. Самовола «Экспоненциальные диофантовы уравнения и сумма цифр числа»

Н. Н. Осипов

В статье В. М. Журавлёва и П. И. Самовола [1] приведена задача 10 (с. 187):

Решить уравнение $3^n + 100 = 7^m$ *в натуральных числах.*

Данное уравнение имеет единственное решение $(m, n) = (3, 5)$. Показать это можно разными способами.

Первый способ. Пусть $m > 3$ и $n > 5$. Перепишем уравнение в виде

$$7^3(7^a - 1) = 3^5(3^b - 1), \tag{1}$$

где $a = m - 3$ и $b = n - 5$. Докажем, что (1) неразрешимо в натуральных числах.

Имеем $7^a \equiv 1 \pmod{3^5}$. Заметим, что $\mathrm{ord}_{3^5}(7) = 81$ (здесь и далее $\mathrm{ord}_x(y)$ обозначает *порядок числа* y *по модулю* x, т. е. наименьшее натуральное число z, для которого $y^z \equiv 1 \pmod{x}$). Значит, a делится на 81 и, как следствие, левая часть уравнения (1) должна делиться на $7^{81} - 1$. Одним из делителей числа $7^{81} - 1$ является 811. Значит, $3^b \equiv 1 \pmod{811}$. Далее заметим, что $\mathrm{ord}_{811}(3) = 810$, поэтому b делится на 810 и правая часть уравнения (1) должна делиться на число $3^{810} - 1$, делителем которого является 3889. Значит, $7^a \equiv 1 \pmod{3889}$. Наконец, $\mathrm{ord}_{3889}(7) = 1944 = 2^3 \cdot 3^5$. В частности, a делится на 3^5. Но $7^{(3^5)} - 1$ делится на 3^6, поэтому $7^a - 1$ должно делиться на 3^6, что противоречит (1). $\square$

Второй способ. Он основан на теории *уравнений Пелля* (см., например, [2, 3]). Ограничимся лишь наброском решения, оставляя детали заинтересованному читателю.

Как видно из сравнения по модулю 8, числа m и n должны быть нечётными, что позволяет записать уравнение в виде

$$7X^2 - 3Y^2 = 100, \tag{2}$$

где $X = 7^{(m-1)/2}$ и $Y = 3^{(n-1)/2}$. Уравнение (2) имеет несколько бесконечных серий решений $(X, Y) = (X_l, Y_l)$, $l = 0, 1, 2, \ldots$, но только три из них содержат решения, удовлетворяющие условию $Y \equiv 0 \pmod 3$. Эти серии таковы:

$$7X_l + Y_l\sqrt{21} = (140 - 30\sqrt{21})(55 + 12\sqrt{21})^l,$$
$$(49 \pm 9\sqrt{21})(55 + 12\sqrt{21})^l, \quad l = 0, 1, 2, \ldots$$

Для этих серий, как можно убедиться, из сравнения $Y \equiv 0 \pmod{3^3}$ вытекает сравнение $Y \equiv 0 \pmod{53}$. Таким образом, при $n \geqslant 7$ решений нет. $\square$

Замечание. Поскольку, как отмечено выше, n нечётно, второй способ фактически решает уравнение $3^n + 100 = 7X^2$.

Список литературы

[1] *Журавлёв В. М., Самовол П. И.* Экспоненциальные диофантовы уравнения и сумма цифр числа // Математическое просвещение. Сер. 3. Вып. 20. М.: МЦНМО, 2016. С. 167–199.

[2] *Barbeau E. J.* Pell's equation. New-York: Springer-Verlag, 2003.

[3] *Бугаенко В. О.* Уравнения Пелля. М.: МЦНМО, 2010.

Николай Николаевич Осипов, Сибирский федеральный университет (Красноярск)

nnosipov@rambler.ru

Этюд о рекуррентных соотношениях*

А. С. Волостнов, А. Б. Скопенков, Ю. Н. Яровиков

Мы демонстрируем важный метод работы с рекуррентными соотношениями на простых примерах его применения (§ 1). Один из них — «олимпиадная» задача (утверждение 1), возникшая из новой оригинальной детали в доказательстве *локальной леммы Ловаса* (§ 2). Мы приводим несколько определений и формулировок, поясняющих метод *разложения многочлена от оператора сдвига*, вместе со ссылками на более подробное изложение (§ 3). Формально § 3 не использует предыдущие параграфы, поэтому чтение заметки можно начинать и с него. Но лучший способ познакомиться с методом — разобрать простые примеры его применения (§ 1).

§ 1. Применения к «олимпиадной» задаче

Начнём с простых примеров, поясняющих основную идею.

Пример 1. Если $a_1 = 1$, $a_2 = 2$ и $a_{k+2} \geqslant 2a_{k+1} - a_k$ при любом $k > 0$, то $a_k \geqslant k$ при любом k.

Доказательство. Неравенство $a_{k+2} \geqslant 2a_{k+1} - a_k$ можно переписать в виде $(a_{k+2} - a_{k+1}) - (a_{k+1} - a_k) \geqslant 0$. Обозначим $b_k = a_{k+1} - a_k$. Тогда $b_1 = 1$ и $b_{k+1} - b_k \geqslant 0$. Следовательно, $b_k \geqslant 1$ при любом k. Отсюда $a_{k+1} \geqslant a_k + 1$. Поскольку $a_1 = 1$, то $a_k \geqslant k$ при любом k, что и требовалось доказать. □

Пример 2. Если $a_1 = 1$, $a_2 = 2$ и $a_{k+2} \geqslant 5a_{k+1} - 6a_k$ при любом $k > 0$, то $a_k > 0$ при любом k.

Доказательство. Неравенство $a_{k+2} \geqslant 5a_{k+1} - 6a_k$ можно переписать в виде $(a_{k+2} - 2a_{k+1}) - 3(a_{k+1} - 2a_k) \geqslant 0$. Обозначим $b_k = a_{k+1} - 2a_k$. Тогда $b_1 = 0$ и

$$b_{k+1} - 3b_k = a_{k+2} - 2a_{k+1} - 3(a_{k+1} - 2a_k) = a_{k+2} - 5a_{k+1} + 6a_k \geqslant 0,$$

---

* Эта заметка возникла из обсуждений на семинарах по дискретному анализу на факультете инноваций и высоких технологий МФТИ.

Второй автор поддержан грантом фонда Д. Зимина «Династия» и стипендией фонда Саймонса.

следовательно, $b_{k+1} \geqslant 3b_k$. Отсюда $b_k \geqslant 0$ при любом k, т. е. $a_{k+1} - 2a_k \geqslant 0$, $a_{k+1} \geqslant 2a_k$. Так как $a_1 > 0$, то $a_k > 0$ при любом k, что и требовалось доказать. $\square$

Следующее утверждение возникает при доказательстве локальной леммы Ловаса (§ 2). Оно предлагалось в качестве задачи на студенческой олимпиаде МФТИ в 2015 г. [4]. Мы приведём доказательство, развивающее идею доказательства примера 2.

Утверждение 1. *Дана последовательность* $a_0, a_1, a_2, \ldots$ *и целое число* $d \geqslant 2$. *Известно, что* $a_0 = a_1 = \ldots = a_d = 1$ *и* $a_{k+1} \geqslant a_k - a_{k-d}/(4d)$ *при любом* $k \geqslant d$. *Тогда все числа* a_k *положительные.*

Доказательство. Обозначим

$$f(x) := x^{d+1} - x^d + \frac{1}{4d}.$$

Тогда $f(1) > 0$. Имеем

$$f\Bigl(\frac{d}{d+1}\Bigr) = -\frac{1}{d}\Bigl(1 + \frac{1}{d}\Bigr)^{-d-1} + \frac{1}{4d} < 0,$$

так как величина $(1 + 1/d)^{d+1}$ убывает и равна 4 при $d = 1$. Следовательно, у многочлена $f(x)$ есть корень α, где $0 < \alpha < 1$. Имеем

$$f(x) = f(x) - f(\alpha) = (x^{d+1} - \alpha^{d+1}) - (x^d - \alpha^d) =$$
$$= (x - \alpha)\bigl(x^d - (1-\alpha)x^{d-1} - \alpha(1-\alpha)x^{d-2} - \ldots - \alpha^{d-1}(1-\alpha)\bigr).$$

Обозначим (аналогично разобранным примерам)

$$b_k := a_k - (1-\alpha)a_{k-1} - \alpha(1-\alpha)a_{k-2} - \ldots - \alpha^{d-1}(1-\alpha)a_{k-d}.$$

Тогда

$$0 \leqslant a_{k+1} - a_k + \frac{a_{k-d}}{4d} = b_{k+1} - \alpha b_k$$

для любого k. Здесь неравенство выполнено по условию, а равенство — ввиду вышеприведённого разложения для $f(x)$.

Так как $0 < \alpha < 1$, отсюда по индукции $b_k > 0$ для любого k. Из определения b_k по индукции выводим, что $a_k > 0$. $\square$

Замечание. Немного более громоздкое изложение получается при помощи языка *формальных степенных рядов* [4, первое решение задачи 5]. Ещё одно доказательство [2, задача 6.2.15.c], [4, второе решение задачи 5] основано на доказательстве неравенства $a_{k+t} \geqslant a_k(1 - 1/d)^t$ для любых $k, t \geqslant 0$. До этой оценки для чисел a_n трудно догадаться (но можно догадаться, основываясь на развиваемой идее!).

§ 2. Применение к доказательству локальной леммы Ловаса

Обсуждение понятия независимости, его применения к доказательствам существования, а также вероятностного языка в комбинаторике см. в [3], [2, § 6.2]. Здесь мы сразу приведём окончательные формулировки.

Подмножества A и B конечного множества M называются *независимыми*, если $|A \cap B| \cdot |M| = |A| \cdot |B|$. При $B \neq \varnothing$ это равносильно тому, что доля множества $A \cap B$ в B равна доле множества A в M.

Подмножество A конечного множества M называется *независимым от набора подмножеств* $B_1, \ldots, B_k \subset M$, если A независимо с любым подмножеством, являющимся пересечением нескольких (возможно, одного) множеств из $B_1, \ldots, B_k$.

Локальная лемма Ловаса в симметричной форме. *Пусть* $A_1, \ldots, A_n$ — *подмножества конечного множества. Пусть для некоторого* d *и любого* k

- *доля подмножества* A_k *не меньше* $1 - 1/(4d)$,
- *среди данных подмножеств существует набор из не менее чем* $n - d$ *подмножеств, от которого* A_k *не зависит.*

Тогда $A_1 \cap \ldots \cap A_n \neq \varnothing$.

Замечание. Приводимое доказательство леммы похоже на доказательство в [3], [2, § 6.2]. Отличие, во-первых, в том, что явно выделено нижеприведённое утверждение 2, позволяющее *свести* лемму к утверждению 1 (а не проводить доказательство аналитического утверждения 1 на комбинаторном языке внутри доказательства леммы). Во-вторых, в том, что мы по-другому доказываем утверждение 1 (в § 1; см. замечание в конце § 1).

Утверждение 2. *Пусть* $A_1, \ldots, A_{k+1}$ — *подмножества конечного множества* M. *Если* A_{k+1} *не зависит от набора* $A_1, \ldots, A_{k-d}$, *то*

$$|A_1 \cap \ldots \cap A_k| - |A_1 \cap \ldots \cap A_{k+1}| \leqslant |A_1 \cap \ldots \cap A_{k-d}| \cdot \Big(1 - \frac{|A_{k+1}|}{|M|}\Big).$$

Доказательство. Имеем

$$\begin{aligned} |A_1 \cap \ldots \cap A_k| - |A_1 \cap \ldots \cap A_{k+1}| &= |A_1 \cap \ldots \cap A_k \cap \overline{A_{k+1}}| = \\ &= |A_1 \cap \ldots \cap A_{k-d} \cap \overline{A_{k+1}} \cap A_{k-d+1} \cap \ldots \cap A_k| \leqslant \\ &\leqslant |A_1 \cap \ldots \cap A_{k-d} \cap \overline{A_{k+1}}| \overset{(*)}{=} |A_1 \cap \ldots \cap A_{k-d}| \cdot \frac{|\overline{A_{k+1}}|}{|M|} = \\ &= |A_1 \cap \ldots \cap A_{k-d}| \cdot \Big(1 - \frac{|A_{k+1}|}{|M|}\Big). \end{aligned}$$

Здесь $\overline{A_{k+1}}$ — дополнение подмножества A_{k+1}; равенство $(*)$ выполнено в силу независимости подмножества A_{k+1} от набора $A_1, \ldots, A_{k-d}$. $\square$

Доказательство локальной леммы Ловаса. Обозначим через M данное конечное множество. Для каждого k обозначим

$$a_k := \begin{cases} \max\Bigl\{\Bigl|\bigcap\limits_{i\in S} A_i\Bigr|/|M|\colon S\subset\{1,2,\ldots,n\},\ |S|=k\Bigr\}, & k\geqslant 1,\\ 1, \quad k\leqslant 0. \end{cases}$$

Для любого (одного!) k предположим без ограничения общности, что

$$\frac{|A_1\cap\ldots\cap A_k|}{|M|} = a_k$$

и что A_{k+1} не зависит от набора $A_1, \ldots, A_{k-d}$. Тогда

$$a_k - a_{k+1} \leqslant \frac{|A_1\cap\ldots\cap A_k| - |A_1\cap\ldots\cap A_{k+1}|}{|M|} \leqslant \\ \leqslant \frac{|A_1\cap\ldots\cap A_{k-d}|}{|M|}\cdot\Bigl(1-\frac{|A_{k+1}|}{|M|}\Bigr) \leqslant \frac{a_{k-d}}{4d},$$

где второе неравенство справедливо по утверждению 2. По утверждению 1 получаем $|A_1\cap\ldots\cap A_n| = a_n|M| > 0$. $\square$

§ 3. Многочлены от оператора сдвига (набросок)

Будем рассматривать *последовательности* вещественных чисел и *отображения* множества всех последовательностей в себя.

Пусть $E\{a_n\} := \{a_n\}$ — тождественный оператор. *Сдвигом* последовательности $\{a_n\}$ называется последовательность $Ta_n := a_{n+1}$. *Последовательностью разностей* последовательности $\{a_n\}$ называется последовательность $\Delta a_n := a_{n+1} - a_n$.

На множестве отображений (множества всех последовательностей в себя) естественно определяются операции суммы и умножения на число. Тогда $\Delta = T - E$.

Упражнение. (1) Приведите пример некоммутативности композиции отображений.

(2) Любое ли отображение имеет обратное по сложению? А по композиции?

(3) Выполняется ли ассоциативность для умножения отображений на числа? А для композиции отображений?

(4) Выполняется ли дистрибутивность для сложения и композиции отображений?

Несмотря на некоммутативность композиции отображений, степени одного отображения коммутируют между собой. Поэтому *многочлен* от отображения определён. Значит, рекуррентное уравнение

$$c_k a_{n+k} + \ldots + c_1 a_{n+1} + c_0 a_0 = 0$$

можно записать в виде

$$(c_k T^k + \ldots + c_1 T + c_0 E)\{a_n\} = 0.$$

Метод *разложения многочлена от оператора сдвига* заключается в разложении на множители многочлена $c_k t^k + \ldots + c_1 t + c_0$. Этим методом фактически доказаны примеры 1, 2 и утверждение 1: разобранные доказательства фактически используют разложение на множители многочленов $x^2 - 2x + 1$, $x^2 - 5x + 6$ и $x^{d+1} - x^d + 1/(4d)$. Этим методом можно доказать следующий замечательный результат, полезнейший для приложений.

Теорема о решениях линейного однородного рекуррентного уравнения. *Пусть P — многочлен, корни которого — числа $\lambda_1, \ldots, \lambda_k \in \mathbb{C}$ с кратностями $l_1, \ldots, l_k$. Если $P(T)\{a_n\} = 0$, то существуют такие многочлены $f_1, \ldots, f_k$, что $\deg f_j < l_j$ и $a_n = f_1(n)\lambda_1^n + \ldots + f_k(n)\lambda_k^n$.*

Эта теорема несложно выводится из следующих утверждений.

(1) *Метод вариации постоянной.* Если $P(T)(T - \lambda E)^l a_n = 0$ для многочлена P и целого $l > 0$, то для последовательности $b_n := a_n \lambda^{-n}$ имеем $P(T)\Delta^l b_n = 0$.

(2) Если λ — корень многочлена P кратности l (у P могут быть и другие корни), то $P(T)[f(n)\lambda^n] = 0$ для любого числа n и многочлена f степени меньше l.

(3) Если $\Delta^l b_n = \lambda^n n^k$ для некоторых чисел l, k, $\lambda \geqslant 0$, то $b_n = g(n)\lambda^n + h(n)$ для некоторых многочленов h степени меньше l, а также g степени не больше $l + k$ при $\lambda = 1$ и степени не больше k при $\lambda \neq 1$.

(4) Для любых различных чисел $\lambda_1, \ldots, \lambda_k \in \mathbb{C}$ и $l_1, \ldots, l_k \in \mathbb{Z}_+$ последовательности $n^i \lambda_j^n$, $j = 1, \ldots, k$, $i = 0, \ldots, l_j$, линейно независимы.

(*Указание*: рассмотрите предел при $n \to \infty$.)

Предлагаем попытаться самостоятельно доказать эти утверждения. О рассмотренных вопросах см. [1, гл. V, § 4].

Список литературы

[1] *Гельфонд А. О.* Исчисление конечных разностей. М.: Эдиториал УРСС, 2012.

[2] *Глибичук А. А., Дайняк А. Б., Ильинский Д. Г. и др.* Элементы дискретной математики в задачах. М.: МЦНМО, 2016.
`http://www.mccme.ru/circles/oim/discrbook.pdf`

[3] *Ильинский Д. Г., Райгородский А. М., Скопенков А. Б.* Независимость и доказательства существования в комбинаторике // Математическое просвещение. Сер. 3. Вып. 19. М.: МЦНМО, 2015. С. 164–177. http://arxiv.org/abs/1411.3171

[4] *Карасёв Р. Н.* Студенческая олимпиада по математике МФТИ. http://rkarasev.ru/common/upload/2015-05-sol.pdf

Алексеевич Сергеевич Волостнов, МФТИ
gyololo@rambler.ru

Аркадий Борисович Скопенков, МФТИ, НМУ
www.mccme.ru/~skopenko

Юрий Николаевич Яровиков, МФТИ
yu-rovikov@ya.ru

По мотивам задачника

О минимальных прямых и эллипсах Штейнера

А. А. Заславский

Пусть дан неравносторонний треугольник ABC. Его можно перевести в правильный аффинным преобразованием. Обратное преобразование переводит описанную и вписанную окружности правильного треугольника в эллипсы, гомотетичные друг другу относительно общего центра — центра тяжести данного треугольника. Эти эллипсы называются *эллипсами Штейнера*. Известны следующие экстремальные свойства эллипсов Штейнера: вписанный эллипс имеет наибольшую площадь среди всех эллипсов, вписанных в данный треугольник, а описанный — наименьшую площадь среди всех описанных. Целью данной заметки является вывод ещё одного свойства эллипсов Штейнера. Однако двигаться к этой цели мы будем обходным путём.

Сначала рассмотрим следующую известную задачу.

На плоскости даны n точек. Найти прямую, сумма квадратов расстояний до которой от данных точек минимальна. Такую прямую будем называть *минимальной прямой*.

Примечание. В математической статистике минимальная прямая называется главной компонентой. Это прямая, для которой набор проекций данных точек имеет наибольшую дисперсию. Известна также механическая интерпретация: если поместить в данные точки одинаковые массы, то минимальная прямая будет осью, относительно которой полученная система масс имеет наименьший момент инерции.

Утверждение 1. *Минимальная прямая проходит через центр тяжести данных точек.*

Доказательство. Будем рассматривать плоскость как комплексную, причём начало координат поместим в центр тяжести данных точек (этого соглашения будем придерживаться и в дальнейшем). Тогда этим точкам будут соответствовать комплексные числа $z_1, \ldots, z_n$, сумма которых равна нулю.

Рассмотрим прямую, параллельную действительной оси, с уравнением

$$z - \bar{z} = 2it.$$

Расстояние от точки z_j до этой прямой равно $\left|\frac{z_j - \bar{z}_j}{2i} - t\right|$. Следовательно, сумма квадратов равна

$$\sum_{j=1}^{n} \left(\frac{z_j - \bar{z}_j}{2i}\right)^2 + nt^2 \geqslant \sum_{j=1}^{n} \left(\frac{z_j - \bar{z}_j}{2i}\right)^2. \tag{1}$$

Поскольку направление осей можно выбрать произвольно, это означает, что сумма квадратов расстояний до любой прямой, не проходящей через центр тяжести, больше, чем до параллельной ей прямой, проходящей через него. Заметим, что (1) можно интерпретировать как частный случай теоремы Гюйгенса — Штейнера о моментах инерции. □

Итак, минимальную прямую надо искать среди прямых, проходящих через начало координат. Зададим произвольную такую прямую параметрическим уравнением $z = te^{i\varphi}$, $t \in R$. Расстояние от точки z_j до этой прямой найдём, минимизируя функцию $(z_j - te^{i\varphi})(\bar{z}_j - te^{-i\varphi})$ по t. Просуммировав затем по j, получаем, что сумма квадратов равна

$$\frac{1}{4}\Big(2\sum_j z_j\bar{z}_j - e^{-2i\varphi}\sum_j z_j^2 - e^{2i\varphi}\sum_j \bar{z}_j^2\Big).$$

Следовательно, нахождение минимальной прямой эквивалентно определению максимума функции

$$f(\varphi) = e^{-2i\varphi}\sum z_j^2 + e^{2i\varphi}\sum \bar{z}_j^2.$$

Если $\sum z_j^2 = 0$, эта функция не зависит от φ. В противном случае выберем направление осей так, чтобы $\sum z_j^2$ было действительным положительным числом (это условие будем считать выполненным и в дальнейшем). Тогда максимум f достигается при $\varphi = n\pi$ и минимальной прямой является действительная ось. Таким образом, доказано

Утверждение 2. *Либо минимальной является любая прямая, проходящая через центр тяжести данных точек (такую систему точек будем называть вырожденной), либо существует единственная минимальная прямая.* □

Для невырожденной системы точек справедлив следующий факт, о котором автору сообщила В. Ипатова, в то время 11-классница.

Утверждение 3. *Существуют две точки, обладающие следующим свойством: сумма квадратов расстояний от данных точек до любой проходящей через такую точку прямой постоянна. Эти точки симметричны относительно центра тяжести данных точек и лежат на прямой, перпендикулярной минимальной.*

Доказательство. Рассуждая так же, как при доказательстве предыдущего утверждения, получаем, что искомая точка z_0 должна удовлетворять соотношению

$$\sum_j (z_j - z_0)^2 = 0,$$

которое с учётом равенства $\sum z_j = 0$ приводится к виду

$$z_0^2 = -\frac{1}{n}\sum_j z_j^2.$$

Так как $\sum z_j^2 > 0$, этому равенству удовлетворяют две точки, лежащие на мнимой оси и симметричные относительно начала координат. □

Будем теперь искать такую точку z_{n+1}, при добавлении которой к данным точкам получается вырожденная система.

Утверждение 4. *Существуют две точки z_{n+1}, обладающие указанным свойством. Эти точки лежат на прямой, перпендикулярной минимальной, и симметричны относительно центра тяжести данных точек.*

Доказательство. Так как при добавлении к точкам $z_1, \ldots, z_n$ точки z_{n+1} центр тяжести системы смещается в точку $\frac{z_{n+1}}{(n+1)}$, искомая точка удовлетворяет соотношению

$$\sum_{j=1}^{n}\left(z_j - \frac{z_{n+1}}{n+1}\right)^2 + \left(\frac{n}{n+1}z_{n+1}\right)^2 = 0.$$

Следовательно,

$$z_{n+1}^2 = -\frac{n+1}{n}\sum_{j=1}^{n} z_j^2 = (n+1)z_0^2. \qquad \square$$

Перейдём теперь к приложению полученных результатов для случая $n = 3$. Как и прежде, будем считать, что данным точкам соответствуют комплексные числа a, b, c, причём $a + b + c = 0$. Прежде всего отметим следующий факт.

Утверждение 5. *Система из трёх точек вырождена тогда и только тогда, когда эти точки являются вершинами правильного треугольника.*

Доказательство. Вырожденность системы из точек a, b, c равносильна равенству $a^2+b^2+c^2=0$. Но тогда

$$ab+bc+ca=\frac{(a+b+c)^2-a^2-b^2-c^2}{2}=0$$

и по теореме Виета числа a, b, c являются корнями уравнения $z^3-abc=0$, т. е. вершинами правильного треугольника. □

Теперь мы наконец можем сформулировать наш основной результат.

Теорема. *Минимальная прямая неравностороннего треугольника содержит большую ось его эллипсов Штейнера.*

Доказательство. Известно (см., например, [1, с. 54–55]), что фокусы вписанного эллипса Штейнера треугольника с вершинами a, b, c являются корнями производной многочлена $(z-a)(z-b)(z-c)$. Значит, при $a+b+c=0$ они удовлетворяют уравнению

$$3z^2=-(ab+bc+ca)=\frac{a^2+b^2+c^2}{2},$$

т. е. лежат на минимальной прямой. □

Следствие. *Точки z_0, z_{n+1}, определённые в утверждениях* 3, 4, *лежат на малой оси эллипсов Штейнера, а расстояние от них до центра равно соответственно $f/\sqrt{2}$ и $f\sqrt{2}$, где f — расстояние между центром и фокусом описанного эллипса Штейнера.*

Доказательство. Утверждение непосредственно следует из приведённого уравнения для фокусов с учётом формул для z_0 и z_{n+1}, доказанных в утверждениях 3, 4. □

Последнее утверждение можно сформулировать в виде следующей задачи.

Задача [2, с. 250, задача 6]. Пусть точка D лежит на малой оси эллипсов Штейнера треугольника ABC на расстоянии $f\sqrt{2}$ от его центра, где f — расстояние от центра описанного эллипса Штейнера до его фокуса. Докажите, что C лежит на малой оси эллипсов Штейнера треугольника ABD.

(*А. А. Заславский*)

Интересно, можно ли решить эту задачу, не повторив весь пройденный нами путь?

В заключение приведём набросок другого доказательства теоремы. Введём систему координат, в которой описанный эллипс Штейнера имеет уравнение

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.$$

Тогда вершины треугольника имеют координаты (ax_i, by_i), где (x_i, y_i), $i = 1, 2, 3,$ — координаты вершин некоторого правильного треугольника, вписанного в единичную окружность. По утверждению 1 минимальная прямая проходит через начало координат, следовательно, её можно задать параметрическими уравнениями $x = \alpha t$, $y = \beta t$, где $\alpha^2 + \beta^2 = 1$. Найдя расстояния от вершин треугольника до этой прямой, получим задачу нахождения условного экстремума относительно (α, β). Можно показать, что её решением является собственный вектор матрицы

$$\begin{pmatrix} a^2 \sum x_i^2 & ab \sum x_i y_i \\ ab \sum x_i y_i & b^2 \sum y_i^2 \end{pmatrix}.$$

Поскольку вершины правильного треугольника образуют вырожденную систему с нулевой суммой, эта матрица диагональна. Значит, минимальная прямая содержит ось эллипса.

Заметим, что это рассуждение переносится на случай произвольной размерности, т. е. верно следующее обобщение теоремы: минимальная прямая вершин симплекса содержит наибольшую из осей описанного около него эллипсоида, который при аффинном преобразовании, переводящем симплекс в правильный, переходит в сферу. Напротив, утверждения 3 и 4 верны только в плоском случае.

Список литературы

[1] *Акопян А. В., Заславский А. А.* Геометрические свойства кривых второго порядка. М.: МЦНМО, 2011.

[2] Математическое просвещение. Сер. 3. Вып. 20. М.: МЦНМО, 2016.

Алексей Александрович Заславский, ЦЭМИ РАН

alzasl@yandex.ru

О разбиениях многогранника на выпуклые части

Р. Н. Карасёв

§ 1. Введение

В нашей статье мы обсудим факты, относящиеся к разбиению выпуклых многогранников в евклидовом пространстве произвольной размерности. Для начала мы сформулируем их как утверждения про многоугольники на плоскости. Читатель может попробовать доказать их самостоятельно, прежде чем продолжить чтение статьи; но это необязательно. Далее для этих утверждений мы сформулируем многомерные аналоги и докажем их; заметим, что даже двумерные утверждения у нас будут доказаны с выходом в пространство большей размерности.

Эта статья развивает тему задачи 6.9 (автор В. В. Произволов) из «Математического просвещения» [2]. Об источниках и обобщениях этой задачи см. Дополнение к задаче 6.9, с. 274–275.

Утверждение 1.1. *Пусть участок земли имеет форму выпуклого m-угольника, его стороны занумерованы. Внутри участка вбиты менее m столбов. Тогда участок можно разрезать на m выпуклых многоугольников $X_1, \ldots, X_m$ так, что каждая часть X_i пересекает границу участка в точности по стороне номер i и ни один столб не оказывается строго внутри ни одной из частей X_i.*

Утверждение 1.2. *Пусть участок земли имеет форму выпуклого m-угольника, его стороны занумерованы и на участке рассыпаны N монет. Тогда для любых положительных чисел $n_1, \ldots, n_m$, в сумме дающих N, участок можно разрезать на m выпуклых многоугольников $X_1, \ldots, X_m$ так, что в части X_i, включая её границу, будет не менее n_i монет.*

Утверждение 1.3. *Пусть участок земли имеет форму выпуклого m-угольника, его стороны занумерованы. По участку распределено месторождение золота, пусть всего золота на участке $Z > 0$. Тогда для любых положительных чисел $z_1, \ldots, z_m$, в сумме дающих Z, участок* *можно разрезать на m выпуклых многоугольников $X_1, \ldots, X_m$ так, что в части X_i будет ровно z_i золота.*

Столбы и монеты в предыдущих утверждениях следует считать точечными. В утверждении 1.3 может быть не вполне ясно, что такое *распределение золота на участке*, далее это будет пояснено при формулировке многомерного варианта — теоремы 2.4; вообще различие между утверждениями 1.2 и 1.3 чисто техническое. Следующее утверждение на плоскости мы для большей строгости сформулируем уже в терминах точек:

Утверждение 1.4. *Пусть на плоскости дан выпуклый m-угольник. Его вершины и ещё несколько точек внутри него покрашены в синий цвет, ещё менее m точек внутри него покрашены в красный цвет, при этом никакие три из покрашенных точек не лежат на одной прямой. Тогда существует необязательно выпуклый многоугольник с вершинами во всех синих точках, содержащий все красные точки.*

Здесь *необязательно выпуклым многоугольником* мы называем замкнутую область, ограниченную замкнутой ломаной без самопересечений.

§ 2. Многомерные формулировки

Структура наших рассуждений будет такова, что даже для доказательства утверждений на плоскости понадобится выход в пространство большей размерности. Поэтому и сами утверждения нам естественно сформулировать в многомерном случае. Читатель может представлять себе случай размерности 3, в котором эти утверждения вполне имеют смысл и нетривиальны.

Нам будет удобно определить *выпуклый многогранник* как ограниченное пересечение конечного числа полупространств в $\mathbb{R}^n$, где полупространство — это множество решений нетривиального линейного неравенства $a_1x_1 + \ldots + a_nx_n \geqslant b$.

В литературе обычно выпуклый многогранник определяется иначе — как выпуклая оболочка конечного множества точек[1]. Эквивалентность этих двух определений неочевидна и требует дополнительных соображений, которые мы здесь приводить не будем. Читатель может поразмышлять об этом самостоятельно или открыть учебник [5, с. 52 и след.] или [8, с. 55].

Размерностью выпуклого многогранника $X \subset \mathbb{R}^n$ будем называть минимальное целое k, для которого X можно поместить в k-мерное аффинное подпространство $A^k \subseteq \mathbb{R}^n$. Для выпуклого многогранника $X \subset \mathbb{R}^n$ раз-

[1] *Выпуклая оболочка множества* $V \subset \mathbb{R}^n$ — это множество всевозможных *выпуклых комбинаций* элементов V, обозначаемое $\operatorname{conv} V = \left\{\sum_{v\in V} a_v v\colon \sum_{v\in V} a_v = 1 \text{ и все } a_v \geqslant 0\right\}$.

мерности n рассмотрим подпространства $\{H_i\}$, пересечением которых он является. Если набор этих подпространств минимален, т. е. при выкидывании из него некоторого подпространства пересечение увеличивается, то *гипергранями* X мы будем называть множества $F_i = X \cap \partial H_i$, где ∂H_i — гиперплоскость, ограничивающая H_i. Следующие два утверждения мы не доказываем и даём в качестве упражнения.

Упражнение 2.1. Докажите, что гиперграни n-мерного выпуклого многогранника имеют размерность $n-1$.

Упражнение 2.2. Докажите, что однозначно определён минимальный набор полупространств, дающий в пересечении данный выпуклый многогранник размерности n.

Сформулируем теперь многомерное обобщение утверждения 1.1.

Теорема 2.3. *Пусть X — n-мерный выпуклый многогранник, и пусть $F_1, \ldots, F_m$ — его гиперграни. Предположим, что внутри X дано конечное множество V из менее чем m точек. Тогда X можно разбить на выпуклые многогранники $X_1, \ldots, X_m$ так, что каждый X_i будет пересекать границу многогранника по соответствующей гиперграни F_i и ни одна точка множества V не попадёт внутрь ни одной части X_i.*

Далее нам надо строго сформулировать многомерное обобщение утверждения 1.3. Предположим, что в выпуклом многограннике X задана какая-то плотность $\rho \geqslant 0$ (её можно считать интегрируемой по Лебегу или хотя бы по Риману) и она нормирована условием $\int_X \rho(x)\,dx = 1$. Будем говорить, что в X распределена *единичная масса* с данной плотностью. Тогда нужное нам утверждение будет звучать так:

Теорема 2.4. *Пусть X — выпуклый многогранник и $F_1, \ldots, F_m$ — его гиперграни. Предположим, что в X задана плотность ρ единичной полной массы. Пусть также заданы положительные числа $y_1, \ldots, y_m$ с единичной суммой. Тогда X можно разбить на выпуклые многогранники $X_1, \ldots, X_m$ так, что каждый X_i будет пересекать границу многогранника по соответствующей гиперграни F_i и масса части X_i будет равна y_i.*

Мы также выведем многомерное обобщение утверждения 1.4 о существовании необязательно выпуклого многогранника с заданным множеством вершин, содержащего данное конечное множество точек:

Следствие 2.5. *Пусть в $\mathbb{R}^n$ дан выпуклый многогранник с m гипергранями. Его вершины и ещё несколько точек внутри него покрашены в синий цвет, ещё менее m точек внутри него покрашены в красный цвет, при этом никакие $n+1$ из покрашенных точек не лежат в одной* *гиперплоскости. Тогда существует необязательно выпуклый многогранник с вершинами во всех синих точках, содержащий все красные точки.*

Нужно пояснить, что такое *необязательно выпуклый многогранник* в размерности большей двух.

В данном случае под необязательно выпуклым многогранником будем подразумевать такое объединение выпуклых многогранников в $\mathbb{R}^n$, которое кусочно-линейно гомеоморфно n-мерному симплексу. Наглядные рассуждения об определении необязательно выпуклого многогранника читатель может найти в [1]. Определение понятия «кусочно-линейный гомеоморфизм» содержится в [4, § 5]. А тем, кто проявит серьёзный интерес к кусочно-линейной топологии, мы рекомендуем классический учебник [3].

При таком определении всякий выпуклый многогранник является многогранником[2)].

Заметим также, что понятие *вершина многогранника* в невыпуклом случае тоже требует своего определения[3)]. Для следствия 2.5 граница получающегося в его доказательстве многогранника будет состоять из выпуклых $(n-1)$-мерных многогранников, и утверждение теоремы следует понимать так, что в качестве вершин этих многогранников используются все синие точки и только они.

§ 3. Доказательство теоремы 2.4 о делении меры

Воспользуемся классическим способом свести утверждение о произвольном выпуклом многограннике к утверждению о самом простом из возможных многогранников — о симплексе.

Определение 3.1. Выпуклая оболочка $n+1$ точки в $\mathbb{R}^n$ называется *симплексом*, если она не содержится ни в каком аффинном подпространстве размерности менее n.

Упражнение 3.2. Если $v_0, v_1, \ldots, v_n$ — вершины симплекса S, то всякая точка $x \in S$ однозначно задаётся в виде выпуклой комбинации

$$x = x_0 v_0 + x_1 v_1 + \ldots + x_n v_n, \quad x_0 + x_1 + \ldots + x_n = 1.$$

Упорядоченный набор чисел $x_0, x_1, \ldots, x_n$ называется *барицентрическими координатами* в симплексе.

---

2) Хотя и это утверждение надо строго проверить!

3) Точка p многогранника P называется его *вершиной*, если для любой прямой ℓ найдётся такая сколь угодно близкая к p точка $p' \in P$, что на прямой $\ell' \ni p'$, параллельной ℓ, найдётся сколь угодно близкая к p' точка, не принадлежащая P.

Обсуждение понятия вершины многогранника см. в [7].

Упражнение 3.3. Докажите, что симплекс имеет $n+1$ гипергрань.

Мы будем использовать следующий исключительно полезный факт:

Лемма 3.4. *Всякий выпуклый многогранник является сечением симплекса некоторым аффинным подпространством. Более точно: всякий выпуклый многогранник можно представить в виде сечения симплекса большей размерности так, что каждая гипергрань симплекса в сечении будет давать гипергрань многогранника, а не вырождаться в грань меньшей размерности или пустое множество.*

Это известное и полезное утверждение. Например, его можно доказать, воспользовавшись полярностью ([5, § 2.3] или [8, с. 145]) и сведя утверждение о сечении к утверждению о проекции.

Доказательство теоремы 2.4. С учётом предыдущей леммы будем считать $X = L \cap S$ для некоторого аффинного подпространства $L \subseteq \mathbb{R}^n$ и симплекса $S \subset \mathbb{R}^n$, а его гиперграни обозначим $F_0, \ldots, F_n$, здесь $n+1$ равно m из условия теоремы. (Гиперграни здесь занумерованы по-другому, это не вызовет путаницы.)

Разбиения симплекса на выпуклые многогранники $C_0, \ldots, C_n$ будем делать очень простым способом: выбирать точку в симплексе x и брать в качестве C_i выпуклую оболочку x и F_i, т. е. пирамиду с основанием F_i и вершиной x. Очевидно, что для исходного многогранника $X = L \cap S$ (L — некоторое аффинное подпространство) множества $X_i = C_i \cap L$ будут давать разбиение требуемого в теореме вида. Пусть вершины симплекса — это $v_0, \ldots, v_n$ (нумерацию зафиксируем так, чтобы $v_i \notin F_i$). Представим некоторую точку $x \in S$ в барицентрических координатах:

$$x = x_0 v_0 + x_1 v_1 + \ldots + x_n v_n.$$

Если на сечении $L \cap S$ задана некоторая плотность, то построим отображение $f\colon S \to S$, в барицентрических координатах заданное формулой

$$f(x)_i = \int\limits_{L \cap C_i(x)} \rho(t)\, dt, \quad i = 0, 1, \ldots, n,$$

т. е. координаты являются массами частей $L \cap C_i(x)$. Ясно, что

$$f(x)_0 + f(x)_1 + \ldots + f(x)_n = 1$$

и числа $f(x)_i$ — это барицентрические координаты какой-то точки в S. Отображение f обладает важным свойством: если $x_i = 0$, то соответствующее $y_i = 0$, потому что размерность $L \cap C_i(x)$ при $x_i = 0$ становится меньше размерности L и масса $L \cap C_i(x)$ обнуляется. Определим *грань симплекса* (более общее понятие, чем гипергрань) как множество решений некоторой системы уравнений $x_i = 0$, $i \in I$ для некоторого $I \subset \{0, 1, \dots, n\}$. С помощью понятия грани мы можем переформулировать свойства построенного отображения: f непрерывно и *переводит каждую грань симплекса в неё саму.*

Теорема 2.4 теперь свелась к сформулированной ниже теореме 3.5. □

Теорема 3.5. *Если отображение симплекса $f\colon S \to S$ непрерывно и переводит каждую грань симплекса в неё саму, то оно сюръективно, $f(S) = S$.*

По существу эта теорема эквивалентна классической теореме [13]:

Теорема 3.6 (Кнастер — Куратовский — Мазуркевич, 1929). *Если n-мерный симплекс S с гипергранями $F_0, \dots, F_n$ так покрыт множествами $V_0, \dots, V_n$, что $F_i \cap V_i = \varnothing$ для любого i и либо все V_i открыты, либо все они замкнуты, то $\bigcap_{i=0}^n V_i \neq \varnothing$.*

Эта теорема имеет глубокие связи с другими классическими вопросами, такими как определение размерности[4)], теорема Брауэра о неподвижной точке [9] и т. п. Интересующемуся читателю рекомендуем книги [6, 14] про теоремы такого типа и их многочисленные приложения в комбинаторике.

Сведение теоремы 3.5 к теореме 3.6. Пусть дана точка $z \in S$ с барицентрическими координатами $z_0, z_1, \dots, z_n$ и мы хотим найти такое x, что $f(x) = z$. Будем считать все координаты z_i положительными, иначе мы можем перейти в грань симплекса S, отбросив нулевые координаты, и воспользоваться индукцией по размерности; здесь важно, что f переводит грани в грани.

Пусть $y_0(x), y_1(x), \dots, y_n(x)$ — барицентрические координаты точки $f(x)$. Положим $V_i = \{x \in S\colon y_i(x) \geqslant z_i\}$. Эти множества замкнуты и удовлетворяют условиям теоремы 3.6, а значит, они должны иметь общую точку. Но так как сумма y_i равна сумме z_i, то в этой общей точке $y_i(x) = z_i$, как мы и хотели. □

Отметим, что на самом деле можно сначала доказать теорему 3.5, заметив по индукции, что при данных условиях отображение f имеет степень один, а потом уже вывести из неё теорему 3.6, как это сделано в [10, Lemma 9.2]. Но мы приведём более элементарное рассуждение для доказательства теоремы Кнастера — Куратовского — Мазуркевича, основанное на другом классическом факте [16].

[4)] Подмножество в $\mathbb{R}^m$ называется *n-мерным*, если любое его достаточно мелкое открытое покрытие покрывает какую-то его точку не менее $n+1$ раза.

Триангуляция n-мерного симплекса — такое его разбиение на n-мерные симплексы, что любые два из них пересекаются по их общей грани [5]. В этом определении грань может иметь любую размерность; если размерность равна -1, то грань является пустым множеством.

Теорема 3.7 (Шпернер, 1928). *Вершины n-мерного симплекса помечены числами $0, 1, \ldots, n$. Вершины некоторой его триангуляции помечены теми же числами таким образом, что любая вершина на $(n-1)$-мерной грани исходного симплекса, противолежащей его вершине k, помечена числом, отличным от k. Тогда обязательно существует симплекс триангуляции, на вершинах которого есть все числа от 0 до n. Более того, количество таких симплексов нечётно.*

Набросок вывода теоремы 3.6 из теоремы 3.7. Каждому множеству V_i сопоставим определённый цвет. В триангуляции симплекса S покрасим каждую вершину каждого из маленьких симплексов в цвет одного из V_i, которым она принадлежит. Тогда на грани F_i отсутствует цвет множества V_i. По теореме 3.7 найдётся маленький симплекс, в вершинах которого присутствуют все цвета, т. е. он задевает все V_i. Будем брать всё более мелкие триангуляции. Переходя к пределу и используя компактность симплекса S, мы получим общую для всех V_i точку, если все эти множества замкнуты. Случай открытых множеств можно вывести из случая замкнутых, читатель может проделать это самостоятельно; на самом деле мы случай открытых множеств не использовали. □

Теорема Шпернера на плоскости может быть известна некоторым читателям. Мы докажем её классическим способом через рассуждение с *комнатами и дверями*, которое очень наглядно в плоском случае и работает в произвольной размерности.

Доказательство теоремы 3.7. Используем индукцию по размерности. Нульмерный случай очевиден. Далее рассмотрим гипергрань F_n, она является симплексом размерности $n-1$, и на ней нет цвета n. Значит, на ней есть нечётное число маленьких $(n-1)$-мерных симплексов с цветами $0, 1, \ldots, n-1$. Посмотрим на триангуляцию всего S, назовём её маленькие n-мерные симплексы *комнатами*. Комнаты разделены *стенками* — $(n-1)$-мерными симплексами. Стенку мы заменим на *дверь*, если на её вершинах стоят цвета $0, 1, \ldots, n-1$ в некотором порядке. Тогда

(a) количество дверей, ведущих за пределы симплекса S, нечётно (по предположению индукции);

[5] Заметим, что определение триангуляции в `https://ru.wikipedia.org/wiki/лемма_Шпернера` некорректно.

(б) любая разноцветная комната имеет ровно одну дверь;

(в) любая из остальных комнат либо не имеет ни одной, либо имеет две двери.

Рассмотрим граф, вершины которого — комнаты, а рёбра — двери между ними. Сложив количества дверей в каждой комнате, ввиду (а) получим нечётную сумму. Ввиду (в) существуют разноцветные комнаты, а ввиду (б) их количество нечётно. □

Приведённое рассуждение с комнатами и дверями на самом деле можно рассматривать как некоторое утверждение о степени отображения, см. статью [15], где эта мысль должным образом развивается.

§ 4. Доказательство утверждений 2.3 и 2.5 о конечном множестве точек

Вывод теоремы 2.3 из теоремы 2.4. Пусть $k = |V| < m$. Заменим каждую точку $v \in V$ на плотность ρ_v, равномерно распределённую по шарику радиуса ε с центром в v и имеющую интеграл, равный $1/k$. Сложим все такие плотности и получим плотность ρ, годящуюся для теоремы 2.4. Применим эту теорему с равными весами $y_i = 1/m < 1/k$. Тогда мы получим требуемое разбиение X на $X_1(\varepsilon), \dots, X_m(\varepsilon)$, в котором

$$\int\limits_{X_i(\varepsilon)} \rho(x)\, dx = \frac{1}{m}$$

при всех $i = 1, \dots, m$. Их этого следует, что ни одно из множеств $X_i(\varepsilon)$ не содержит шара с центром в $v \in V$ радиуса ε, иначе интеграл был бы не менее $1/k > 1/m$.

Теперь нам надо устремить ε к нулю и воспользоваться тем, что все наши разбиения параметризовались точками некоторого симплекса размерности $m-1$, т. е. множество всех разбиений оказывается компактно. Таким образом, мы можем взять последовательность $\varepsilon_n \to 0$ так, что $X_i(\varepsilon_n) \to X_i$ в некотором разумном смысле, например, в смысле метрики Хаусдорфа (см. определение в `https://ru.wikipedia.org/wiki/Метрика_Хаусдорфа`). В пределе мы увидим, что никакое X_i не сможет содержать никакую точку $v \in V$ внутри себя. □

Для доказательства следствия 2.5 нам понадобится ещё одна лемма:

Лемма 4.1. *Пусть $W \subset \mathbb{R}^n$ — конечное множество точек в общем положении, $|W| \geqslant n + 1$, F — гипергрань в* $\operatorname{conv} W$. *Тогда существует многогранник с вершинами W, одна из граней которого совпадает с F.*

Доказательство. Проведём индукцию по $|W|$. При $|W| = n+1$ всё очевидно. Будем обозначать через $\operatorname{int} S$ внутренность множества S.

Если $\operatorname{int}\operatorname{conv} W \cap W = \varnothing$, то $\operatorname{conv} W$ и есть искомый многогранник. Иначе пусть F' — другая грань $\operatorname{conv} W$ и

$$W' = (F' \cup \operatorname{int}\operatorname{conv} W) \cap W.$$

Ясно, что $W' \subseteq W$ и W' не содержит какую-то из вершин грани F, так как иначе F и F' совпали бы. Следовательно, $|W'| < |W|$. Кроме того, $F' \cap W$ содержит как минимум n точек, а $\operatorname{int}\operatorname{conv} W \cap W$ — как минимум одну, значит, $|W'| \geqslant n+1$.

Применим предположение индукции к W' и F'. Получим некоторый многогранник Y' с вершинами в W'. Возьмём многогранник

$$Y = \overline{(\operatorname{conv} W) \setminus Y'}$$

(черта сверху у нас обозначает замыкание). Его граница состоит из границы $\operatorname{conv} W$ без относительной внутренности грани F' и границы Y' без той же относительной внутренности грани F'. Это будет необязательно выпуклый многогранник, множество вершин которого совпадает с W, и одна из его граней — F. □

Доказательство следствия 2.5. Пусть W — синие точки, а V — красные точки. Положим $X = \operatorname{conv} W$, и пусть $\{F_i\}_{i=1}^m$ — множество гиперграней X. Применим теорему 2.3 к X и множеству V. Получим такое разбиение X на множества X_i, что $X_i \cap \partial X = F_i$ и $V \cap \operatorname{int} X_i = \varnothing$ для всех $1 \leqslant i \leqslant m$.

Разобьём точки из $W \cap \operatorname{int} X$ на множества W_i так, чтобы выполнялось $W_i \subset X_i$. Положим также $W_i' = W \cap F_i$.

Рассмотрим такие $1 \leqslant i \leqslant m$, что $W_i \neq \varnothing$. Тогда к множеству $W_i \cup W_i'$ и гиперграни F_i применима лемма 4.1, которая даёт некоторый многогранник Y_i, в числе вершин которого состоят все точки из W_i. Заметим, что $Y_i \subseteq X_i$, следовательно, $\operatorname{int} Y_i \cap V = \varnothing$, а в силу общего положения точек $Y_i \cap V = \varnothing$.

Положим

$$Y = \overline{X \setminus \Big(\bigcup_{\substack{1 \leqslant i \leqslant m,\\ W_i \neq \varnothing}} Y_i \Big)}.$$

Можно показать, что Y — многогранник в смысле используемого нами определения, мы полагаемся здесь на интуицию читателя, хотя строгое объяснение этого факта требует некоторых технических усилий. Вершины Y совпадают с множеством W; $Y \supset V$, так как для всех $1 \leqslant i \leqslant m$, $W_i \neq \varnothing$ имеем: $Y_i \cap V = \varnothing$. □

§ 5. Заключение

Изложенные результаты по сути взяты из статьи [11]. Изложение близких к рассмотренным в этой заметке вопросов можно найти в записках лекций [10]; современные результаты о разбиении выпуклого тела на выпуклые части равной меры можно посмотреть в [12]; более продвинутые варианты теоремы Кнастера — Куратовского — Мазуркевича можно найти в статье [15] и упомянутых в ней ссылках. Последовательное изложение затронутых в этой заметке вопросов можно найти в книгах [6, 14].

Благодарности

Автор благодарит А. Б. Скопенкова за многочисленные полезные замечания.

Список литературы

[1] *Долбилин Н. П.* Жемчужины теории многогранников. М.: МЦНМО, 2012.

[2] Математическое просвещение. Сер. 3. Вып. 6. М.: МЦНМО, 2002. С. 134. Задача 6.9.

[3] *Рурк К., Сандерсон Б.* Введение в кусочно линейную топологию. М.: Мир, 1974.

[4] *Скопенков А. Б.* Алгебраическая топология с геометрической точки зрения. М.: МЦНМО, 2015.

[5] *Циглер Г. М.* Теория многогранников. М.: МЦНМО, 2014.

[6] *Шашкин Ю. А.* Неподвижные точки. М.: Наука, 1989. (Популярные лекции по математике; Вып. 60).

[7] *Akopyan A., Bárány I., Robins S.* Algebraic vertices of non-convex polyhedra. `https://arxiv.org/abs/1508.07594`

[8] *Barvinok A.* A course in convexity. Providence, RI: AMS, 2002. (Graduate Studies in Math.; V. 54).

[9] *Brouwer L.* Über Abbildung von Mannigfaltigkeiten // Math. Annalen. 1910. Bd. 71. S. 97–115.

[10] *Karasev R.* Geometry of measures: partitions and convex bodies. `http://rkarasev.ru/common/upload/mes_partition.pdf`

[11] *Karasev R. N.* Partitions of a polytope and mappings of a point set to facets // Discrete Comput. Geom. 2005. V. 34, № 1. P. 25–45.

[12] *Karasev R., Hubard A., Aronov B.* Convex equipartitions: the spicy chicken theorem // Geometriae Dedicata. 2014. V. 170, № 1. P. 263–279.

[13] *Knaster B., Kuratowski C., Mazurkiewicz S.* Ein Beweis des Fixpunktsatzes für n-dimensionale Simplexe // Fundamenta Mathematicae. 1929. V. 14, № 1. P. 132–137.

[14] *Matoušek J.* Using the Borsuk — Ulam theorem: Lectures on Topological Methods in Combinatorics and Geometry. Berlin: Springer-Verlag, 2003.

[15] *Musin O. R.* KKM type theorems with boundary conditions. https://arxiv.org/abs/1512.04612

[16] *Sperner E.* Neuer Beweis für die Invarianz der Dimensionszahl und des Gebietes // Abh. Math. Sem. Univ. Hamburg. 1928. Bd. 6. S. 265–272.

Роман Николаевич Карасёв, МФТИ, ИППИ РАН

r_n_karasev@mail.ru, http://www.rkarasev.ru/en/

От школьной задачи к элементам высшей алгебры

В. М. Журавлёв, П. И. Самовол

§ 1. Введение

В задачнике «Математического просвещения», вып. 20 [8] предложена следующая задача.

Задача 1. а) В клетках квадрата 5×5 стоят знаки «+» и «−». Можно положить пятиклеточный крест центральной клеткой на клетку квадрата и поменять все знаки, закрытые крестом, на противоположные. Можно ли с помощью таких операций все знаки поменять на противоположные?

(*Р. Г. Женодаров*)

б) Дан граф, в вершинах которого стоят знаки «+» и «−». Разрешается выбрать вершину и поменять знаки на противоположные в ней и в смежных вершинах. Докажите, что такими действиями можно заменить все знаки на противоположные. (*И. В. Митрофанов*)

Отметим, что условия и решения указанной и аналогичных задач публиковались и раньше.

Любители компьютерных игр, возможно, вспомнят, что случай квадрата 5×5, т. е. задачи 1а), попал в качестве головоломки в компьютерную игру «Код да Винчи».

Случай квадрата 8×8 предлагался на Конкурсе имени А. П. Савина «Математика 6–8» 2007/08 уч. г. в журнале «Квант» [7].

Задача 2. За один ход разрешается одновременно перекрасить в противоположный цвет любую клетку шахматной доски, а также все клетки, имеющие с ней общую сторону. Можно ли за несколько ходов перекрасить в противоположный цвет все клетки доски? (*И. Акулич*)

Кроме того, было проведено небольшое математическое исследование, связанное с указанной задачей и её обобщениями. Мы хотим не только предложить читателям решение задачи 1, но также познакомить их с результатами этого исследования и предложить некоторые новые задачи, возникшие в этой связи. Часть этих материалов доступна школьникам.

В дальнейшем будем использовать терминологию раскрасок, которая применялась в более ранних формулировках этой задачи.

Можно сказать, что началом этого математического исследования послужила статья Игоря Акулича [3]. Он не рассматривал задачу в контексте графов, а изучал обобщения задач 1а) и 2 для квадратов, прямоугольников и других фигур, которые можно вырезать из клетчатой бумаги. Им были рассмотрены случаи квадратных досок $n \times n$ при $n \leqslant 28$ и некоторых прямоугольных досок.

На самом деле вопрос существования решения в задаче 1 был заменён И. Акуличем на вопрос поиска количества решений для заданной фигуры. Здесь необходимо дать уточнение. Если в какую-либо клетку делается не менее двух ходов, то, уменьшив число ходов в эту клетку на 2, мы приходим к такому же результату. Это означает, что нам достаточно рассматривать комбинации ходов, у которых ход в клетку либо сделан один раз, либо не сделан вовсе. Остальные комбинации мы будем считать эквивалентными указанным. После таких пояснений можно говорить о количестве различных наборов ходов, подразумевая количество различных классов эквивалентности.

Предположим, мы отметили клетки, в которые надо сделать ход. Пусть в отмеченных клетках стоит 1, в неотмеченных 0. Попробуем понять, каким условиям должна удовлетворять полученная конфигурация.

Заметим, что с каждой отмеченной клеткой обязано соседствовать чётное число отмеченных клеток (т. е. или ни одной, или две, или четыре), а с каждой неотмеченной клеткой — нечётное число отмеченных клеток (т. е. одна или три). Действительно, рассмотрим любую неотмеченную клетку A. Так как при ходе в любую отмеченную соседнюю клетку клетка A поменяет цвет, после всех ходов она поменяет цвет нечётное число раз, если соседствует с нечётным числом отмеченных клеток. Тогда в итоге её цвет станет противоположным исходному.

Рассмотрим любую отмеченную клетку B. Так как при ходе в любую отмеченную соседнюю клетку клетка B поменяет цвет, то после всех ходов в соседние отмеченные клетки она поменяет цвет чётное число раз, если соседствует с чётным числом отмеченных клеток. Сверх того, она один раз поменяет цвет при ходе в саму клетку B, и в итоге её цвет станет противоположным исходному.

Таким образом, «динамическая» задача (где клетки то и дело меняют цвет) преобразуется в «статический» вариант, где нужно всего лишь отметить некоторые клетки доски так, чтобы *с каждой отмеченной клеткой соседствовало чётное число отмеченных клеток, а с каждой неотмеченной — нечётное число отмеченных клеток*.

Использовав компьютер, И. Акулич нашёл, что для досок $n \times n$, $n \leqslant 28$, решение существует, причём для $n = 1, 2, 3, 6, 7, 8, 10, 12, 13, 15, 18, 20, 21, 22, 25, 26, 27$ и 28 оно единственно. Авторам удалось проверить единственность решения также для $n = 36$, 37, 38. Следовательно, в этих случаях решение обладает симметрией относительно всех осей симметрии самой доски (иначе появились бы дополнительные решения, полученные поворотами и отражениями).

Решение для $n = 1$ — это просто единственная отмеченная клетка. При $n = 2$ имеем четыре закрашенных клетки. Примеры решений для $n = 3, 6, 7, 8$ изображены на рис. 1 (по словам И. Акулича, решения для этих n ещё удалось подобрать «вручную»).

Ходы нужно сделать в отмеченные клетки.

Для $n = 5$ (рис. 2, слева) и $n = 17$ (рис. 2, справа) имеется по 4 решения, которые получаются друг из друга поворотами.

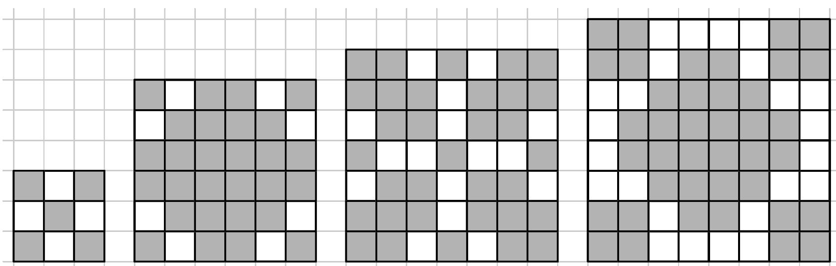


Рис. 1

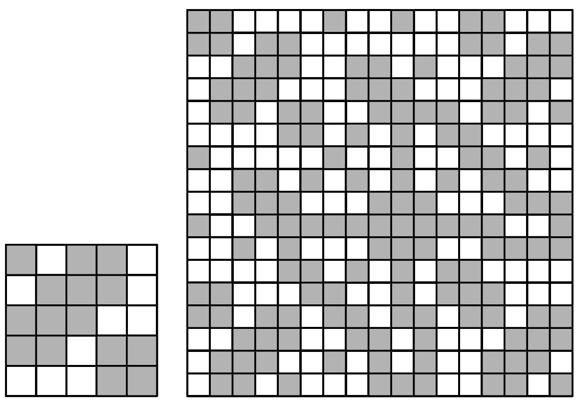


Рис. 2

Для квадрата 4×4 существует 16 различных наборов ходов. Все эти наборы получаются из 5 конфигураций с помощью поворотов и отражений (рис. 3).

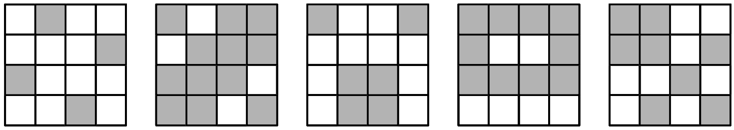


Рис. 3

Для $n = 14$ и 24 также имеется по 16 решений. Для $n = 11$ число решений достигает 64, для $n = 9$ и 16 оно равно 256, при $n = 23$ число решений резко «прыгает» до 16 384, а при $n = 19$ — до 65 536. И. Акулич отметил, что каждое из фигурирующих здесь чисел (1, 4, 16, 64, 256, 16 384 и 65 536) является целой неотрицательной степенью четвёрки. При этом появляются конфигурации, не обладающие ни осевой, ни поворотной симметрией. Например, одна из них для доски 9×9 изображена на рис. 4.

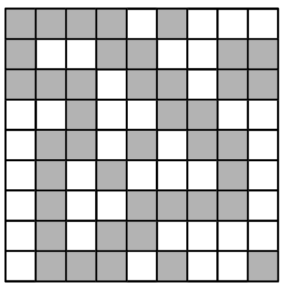


Рис. 4

И. Акуличем в статье [3] были сформулированы следующие вопросы.

Вопрос 1. *Для любого ли n можно отметить требуемым образом клетки квадрата $n \times n$?*

Вопрос 2. *Если да, то всегда ли количество способов, которыми можно это сделать, является целой неотрицательной степенью числа 4?*

Вопрос 3. *Для любых ли m и n можно отметить требуемым образом клетки прямоугольника $m \times n$?*

Вопрос 4. *Если да, то всегда ли количество способов, которыми можно это сделать, является целой неотрицательной степенью числа 2?*

Вопрос 5. *Существует ли такое m, что для любого n решение для прямоугольника $m \times n$ единственно?*

Вопрос 6. *Существует ли хотя бы одна фигура, которую можно вырезать из клетчатой бумаги (возможно, с дырками) и клетки которой нельзя отметить требуемым образом?*

Конечно, с помощью компьютера нельзя перебрать все варианты досок. Чтобы ответить на часть вопросов, достаточно переложить задачу на язык графов.

§ 2. Графы

Каждую клетку фигуры заменим вершиной графа. Если клетки являются соседями, то соединим вершины ребром. Так каждой доске или фигуре из клеток можно сопоставить граф[1)]. Это обобщение задачи было опубликовано в статьях [5] и [6].

Задача 3 [6]. Вершины графа окрашены в два цвета (чёрный и белый), за один ход разрешается одновременно перекрасить в противоположный цвет любую вершину графа и все смежные с ней вершины (т. е. соединённые с ней ребром). Можно ли за несколько ходов перекрасить в противоположный цвет все вершины графа?

Оказалось, что в такой общей формулировке задачу решить легче, чем в частном случае для квадратных досок.

Решение задачи 3. *Первый способ.* Заметим, что очерёдность ходов не играет никакой роли. Если выбрать некоторый набор вершин для ходов, то тем самым определится конечная раскраска графа.

Проведём индукцию. Если вершина одна, то просто покрасим её.

Предположим теперь, что мы имеем подходящий набор ходов для любого графа с k вершинами, и рассмотрим граф с $k+1$ вершиной. Обозначим вершины графа через $A_1, A_2, \ldots, A_k, A_{k+1}$.

Отбросив некоторую вершину A_i, получим граф с k вершинами, и для него по нашему предположению существует требуемый набор ходов (при котором все вершины поменяют цвет на противоположный). Если в первоначальном графе вершина связана рёбрами с нечётным числом покрашенных вершин, то этот набор ходов подойдёт и для графа с $k+1$ вершиной.

Однако возможен случай, когда для каждой вершины A_i, $1 \leqslant i \leqslant k+1$, мы нашли такой набор ходов на оставшихся k вершинах, что вершина A_i соединена с чётным числом покрашенных вершин. Если мы проделаем один за другим наборы ходов для двух разных вершин $A_i \neq A_j$, то все вершины останутся с начальным цветом, кроме вершин A_i и A_j. Это означает, что

[1)] В статье рассматриваются графы без петель.

мы можем перекрасить в противоположный цвет любые две выбранные вершины, не перекрашивая остальные вершины.

Значит, если в графе чётное число вершин, то нужно перекрашивать каждую пару вершин, пока все они не изменят цвет на противоположный.

Если в графе нечётное число вершин, то граф должен содержать вершину, у которой чётное число соседних вершин. Действительно, если такой вершины не существует, то общее число «соседей» у всех вершин графа нечётно, но это невозможно, поскольку общее число соседей в два раза больше, чем количество рёбер в графе.

Выберем эту вершину и перекрасим её вместе с чётным числом всех её соседей. При этом мы перекрасили в противоположный цвет нечётное число вершин. Так как в графе нечётное количество вершин, осталось неперекрашенным чётное количество вершин. Разобьём эти вершины на пары и перекрасим так, как обсуждали ранее.

Итак, требуемая последовательность ходов всегда существует. □

Мы полностью решили задачу 1. Более того, получили ответы на некоторые вопросы И. Акулича, а именно: ответ на шестой вопрос отрицательный — таких фигур нет. И, как следствие, имеем положительный ответ на первый и третий вопросы, т. е. требуемым образом всегда можно отметить клетки любого прямоугольника и, в частности, квадрата.

Из нашего решения получаем

Следствие 1. *Если в графе из каждой вершины выходит чётное число рёбер, то, чтобы получить требуемую последовательность ходов, нужно просто сходить в каждую вершину.*

Расширим вопрос 4 и докажем более сильное утверждение о графах.

Задача 4 [6]. Для графов, вершины которых окрашены в два цвета (чёрный и белый), количество различных наборов ходов, позволяющих перекрасить в противоположный цвет все вершины графа, является целой неотрицательной степенью числа 2. Наборы ходов мы считаем различными, если отличаются наборы вершин, куда сделаны ходы. Как и прежде, ходом называется одновременная перекраска в противоположный цвет некоторой вершины графа и всех смежных (соединённых ребром) с ней вершин.

Применим к «нашим доскам» теорему Лагранжа о том, что порядок подгруппы делит порядок группы. Чуть позже мы углубимся в теорию групп, а сейчас предложим решение, адаптированное для школьников.

Решение задачи 4. *Первый способ.* Рассмотрим граф с d вершинами. Дальнейшие рассуждения мы могли бы проводить для любой раскраски графа. Для простоты будем считать все вершины белыми.

Рассмотрим множество всевозможных наборов ходов в вершины графа. Поскольку в любую вершину ход либо сделан, либо нет, различных наборов ровно 2^d. При подсчёте мы учитываем «нулевой» набор ходов, при котором ни в одну вершину ходы не делаются.

Выделим подмножество наборов ходов, которые оставляют все вершины графа белыми, т. е. не меняют исходной раскраски графа. Количество таких наборов обозначим через s. Очевидно, что это подмножество содержит «нулевой» набор, поэтому $s > 0$. Назовём это подмножество «нейтральным».

Будем считать, что два набора ходов принадлежат одному классу, если результаты их независимого применения к фиксированной (белой) раскраске вершин графа совпадают. Пусть k обозначает количество таких классов. Докажем, что в каждом классе ровно s наборов ходов.

Пусть h_1 и h_2 — два набора ходов из одного класса. Рассмотрим их объединение (двойной ход в одну и ту же вершину графа приравниваем к отсутствию хода).

Заметим, что объединение наборов h_1 и h_2 лежит в нейтральном подмножестве. Действительно, каждая вершина после применения объединения h_1 и h_2 поменяет цвет чётное количество раз и, следовательно, не поменяет исходную раскраску.

Если набор ходов h_1 объединить с объединением h_1 и h_2, то получим набор ходов h_2. Значит, h_2 получается объединением набора ходов h_1 с некоторым уникальным набором ходов из нейтрального подмножества. Следовательно, количество элементов в данном классе не больше, чем количество элементов в нейтральном подмножестве, т. е. не больше s.

С другой стороны, если мы возьмём какой-нибудь набор ходов, то в том же классе лежит объединение исходного набора ходов с любым набором ходов из нейтрального подмножества. Следовательно, в этом классе число наборов не меньше чем s.

В итоге получаем, что в каждом классе ровно s наборов ходов. Отметим, что и в классе наборов ходов, перекрашивающих все вершины графа в противоположный цвет, также s элементов.

Итак, все наборы ходов разбились на k классов по s элементов, т. е. $ks = 2^d$. Следовательно, и k, и s являются степенями двойки. Что и требовалось доказать. $\square$

§ 3. Раскраски и системы сравнений

Итак, мы знаем, что для любого графа искомый набор ходов всегда существует. Но как его найти?

Сопоставим каждому двуцветному графу систему линейных сравнений с коэффициентами 0 и 1 (над полем $\mathbb{Z}_2$). При этом искомый набор ходов будет соответствовать некоторому решению этой системы.

Обозначим вершины графа через $A_1, A_2, \ldots, A_d$. Пусть переменная a_i принимает значение 1, если вершина A_i отмечена, и 0, если вершина A_i не отмечена. Пусть вершины $A_{i_1}, \ldots, A_{i_k}$ — смежные с вершиной A_i. В качестве i-го сравнения системы возьмём сравнение $a_i + a_{i_1} + \ldots + a_{i_k} \equiv 1 \pmod 2$. Таким образом, i-е сравнение системы выражает для вершины A_i условие, что у неотмеченной вершины нечётное число отмеченных соседок.

Систему линейных сравнений можно решить методом Гаусса последовательного исключения неизвестных. Для шага метода последовательного исключения неизвестных можно воспользоваться любым из уравнений системы. Мы из некоторого имеющегося сравнения выражаем любую из входящих в него переменных и, подставляя полученное выражение в остальные сравнения, уменьшаем тем самым количество неизвестных и сравнений. При этом могут образоваться сравнения $0 \equiv 0$ или $1 \equiv 1$, которые можно отбросить.

Для примера найдём все наборы ходов для графа рис. 5, который отвечает прямоугольнику 2×5.

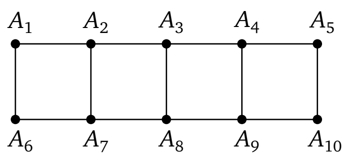


Рис. 5

Получим следующую систему сравнений (вершине A_i графа соответствует i-я строка составленной системы):

$$\begin{cases}
a_1 + a_2 + a_6 \equiv 1 \pmod 2,\\
a_1 + a_2 + a_3 + a_7 \equiv 1 \pmod 2,\\
a_2 + a_3 + a_4 + a_8 \equiv 1 \pmod 2,\\
a_3 + a_4 + a_5 + a_9 \equiv 1 \pmod 2,\\
a_4 + a_5 + a_{10} \equiv 1 \pmod 2,\\
a_1 + a_6 + a_7 \equiv 1 \pmod 2,\\
a_2 + a_6 + a_7 + a_8 \equiv 1 \pmod 2,\\
a_3 + a_7 + a_8 + a_9 \equiv 1 \pmod 2,\\
a_4 + a_8 + a_9 + a_{10} \equiv 1 \pmod 2,\\
a_5 + a_9 + a_{10} \equiv 1 \pmod 2.
\end{cases}$$

Решением системы будет:

$$\begin{cases} a_1 = a_5 = a_8 = a_{10} + 1, \\ a_3 = a_6 = a_{10}, \\ a_2 = a_4 = a_7 = a_9 = 0. \end{cases}$$

Переменная a_{10} является свободной и принимает одно из двух значений 0 или 1. Следовательно, система имеет два решения и для прямоугольника 2×5 есть два различных набора ходов (два способа отметить клетки).

Мы уже знаем, что для любого графа система, соответствующая раскраскам, совместна.

Совместность системы мы можем доказать и по-другому. Тем самым мы найдём ещё один способ решения задачи 3.

Предложение 1. *Сумма степеней всех вершин графа чётна*[2]*.*

Доказательство. Достаточно разрезать все рёбра графа пополам. Тогда получим, что удвоенное число рёбер графа равно сумме степеней всех вершин графа. Что и требовалось доказать. □

Решение задачи 3. *Второй способ* [5]. Докажем, что в процессе решения системы, соответствующей графу, не получится сравнение $0 \equiv 1$.

Если мы складываем несколько сравнений системы (а ничего другого по сути мы делать не можем: все операции исключения неизвестных являются операциями почленного сложения — так устроены сравнения по модулю 2), то для получения единицы в правой части мы должны сложить нечётное число сравнений.

Рассмотрим подграф исходного графа, вершинам которого соответствуют складываемые сравнения. Для получения нулевого коэффициента при каждой из соответствующих переменных степени всех вершин рассматриваемого подграфа должны быть нечётны. Но в силу предложения 1 не существует ни одного графа с нечётным числом вершин, степени которых все нечётны. Следовательно, система, отвечающая графу, совместна. Что и требовалось доказать. □

С помощью систем линейных сравнений получим другое несложное решение задачи 4.

Решение задачи 4. *Второй способ* [5]. Пусть t — число свободных переменных, получающихся при решении системы. Тогда общее количество решений системы, соответствующей некоторому графу, равняется 2^t. Что и требовалось доказать. □

Например, если $t = 0$, то система имеет единственное решение.

---

[2] Степень вершины графа — это количество рёбер, содержащих эту вершину.

§ 4. Пятый вопрос

Ответ на этот вопрос был дан в статье [5].

Рассмотрим граф, вершины которого — центры клеток прямоугольника размером $m \times n$, а соседними считаем центры клеток, имеющих общую сторону. Сколько для него существует решений — выяснить непросто. Пятый вопрос звучит так: «Существует ли такое m, что для любого n решение единственно?»

Ответ отрицательный. Более того, для любого m существует такое n, что количество решений равно 2^m. Более того, для каждого данного m множество таких n бесконечно!

Чтобы это доказать, расставим в m клетках крайнего левого столбца произвольным образом 0 и 1. Условие, что у каждой отмеченной вершины чётное число отмеченных соседок, а у каждой неотмеченной вершины нечётное число отмеченных соседок, однозначно определяет второй столбец. Первый и второй столбцы определяют третий, и так далее...

Пример для $m = 2$

a	$a+b+1$	$a+1$	0	a	$a+b+1$	$a+1$	0	...
b	$a+b+1$	$b+1$	0	b	$a+b+1$	$b+1$	0	...

Пример для $m = 3$

a	$a+b+1$	$a+c+1$	$b+c+1$	$c+1$	0	c	$b+c+1$	...
b	$a+b+c+1$	0	$a+b+c$	$b+1$	0	b	$a+b+c+1$	...
c	$b+c+1$	$a+c+1$	$a+b+1$	$a+1$	0	a	$a+b+1$	...

Пример для $m = 4$

a	$a+b+1$	$a+c+1$	$b+c+d+1$	0	$b+c+d$	$a+c+1$	$a+b+1$	...
b	$a+b+c+1$	d	$a+b+d+1$	0	$a+b+d$	$d+1$	$a+b+c$	...
c	$b+c+d+1$	a	$a+c+d+1$	0	$a+c+d$	$a+1$	$b+c+d$	...
d	$c+d+1$	$b+d+1$	$a+b+c+1$	0	$a+b+c$	$b+d+1$	$c+d+1$	...

Доказать, что при любом m в таблице бесконечно много столбцов, состоящих только из нулей (это и означает, что для соответствующих n количество наборов ходов равно 2^m), довольно просто. Рассмотрим всевозможные пары соседних столбцов (B, C). По каждой такой паре однозначно строится следующий столбец D. Таким образом, задано отображение $(B, C) \to (C, D)$.

Поскольку множество различных пар столбцов конечно, рано или поздно произойдёт зацикливание. Возникший цикл не может обладать предпериодом. Дело в том, что пара столбцов (B, C) однозначно определяет не только следующий за ними столбец D, но и предшествующий им столбец A.

Осталось вспомнить, что к рассматриваемой нами таблице слева с соблюдением правила «у каждой отмеченной вершины чётное число отмеченных клеток, а у каждой неотмеченной нечётное» можно приписать только столбец из одних нулей. Значит, когда произойдёт зацикливание, мы вновь увидим нулевой столбец.

§ 5. Группы

Наш граф обозначим через Γ, а его вершины через $A_1, A_2, \ldots, A_d$.

Цвет вершины графа заменим числом: пусть, например, вместо белого будет 1, а вместо чёрного 0. Существует ровно 2^d различных расстановок чисел 0, 1 в вершинах графа (двуцветных раскрасок графа).

Множество всех двуцветных раскрасок графа превратим в векторное пространство V над полем $\mathbb{Z}_2$. Для этого достаточно определить сумму любых двух раскрасок графа, поставив в каждой вершине сумму чисел из этих раскрасок.

Обозначим через v_i, $i=1, \ldots, d$, раскраску, у которой в вершине A_i стоит 1, а в остальных вершинах нули. В качестве элементов базиса векторного пространства V можно взять все векторы $v_i, \ldots, v_d$. Раскраске, состоящей из одних нулей (все вершины графа покрашены чёрным), соответствует нулевой вектор $\overrightarrow{0}$. Раскраске, состоящей из одних единиц (все вершины графа покрашены белым), соответствует вектор $w = v_1 + \ldots + v_d$.

Пусть оператор $g_i\colon V \to V$ действует следующим образом: $g_i(v) = v_i + v$, где $v \in V$. Таким образом, оператор прибавляет 1 к числу, стоящему в вершине A_i (сумма рассматривается по модулю 2), при этом числа в остальных вершинах графа не меняются (можно считать, что к ним прибавляется 0).

Рассмотрим группу операторов G_d, порождённую всеми элементами g_i, т. е. множество, составленное из всевозможных сумм элементов g_i с коэффициентами из $\mathbb{Z}_2$. Группа G_d абелева, её порядок $|G_d|$ равен 2^d. При этом

$$G_d \cong \underbrace{\mathbb{Z}_2 \oplus \ldots \oplus \mathbb{Z}_2}_{d} \cong \mathbb{Z}_2^d.$$

Обозначим через s_i оператор «хода» в вершину A_i, т. е. прибавление 1 к числу в вершине A_i и её соседях. Значения чисел в остальных вершинах графа не меняются. Рассмотрим группу S_Γ, порождённую всеми элементами s_i.

Предложение 2. *Группа S_Γ является подгруппой группы G_d.*

Доказательство. Очевидно, что s_i равняется сумме $g_i + \sum_j g_j$, где индекс j пробегает множество соседних вершин для A_i. □

Следствие 2. *Группа S_Γ абелева. Порядок группы S_Γ делит порядок группы G_d, т. е. является делителем числа 2^d.*

Мы имеем два принципиально различных случая.

1. Группа S_Γ изоморфна группе G_d, т. е. $S_\Gamma \cong G_d \cong \mathbb{Z}_2^d$.

Тогда $g_i \in S_\Gamma$ для всех i и, следовательно, из любой расстановки чисел $0, 1$ в вершинах графа можно получить любую другую расстановку при помощи суммы подходящих элементов s_i. В частности, существует только один способ требуемой перекраски.

Случай изоморфизма групп осуществляется, например, для квадратов 2×2 или 3×3.

2. Группа S_Γ является собственной подгруппой группы G_d, т. е. $S_\Gamma \subset G_d$, $S_\Gamma \neq G_d$.

Как следует из доказанного выше, элемент $g_1 + g_2 + \ldots + g_d$ и в этом случае принадлежит группе S_Γ: $g_1 + g_2 + \ldots + g_d \in S_\Gamma$. Однако теперь нельзя из любой таблицы получить любую другую, и способов перекраски больше одного. Количество различных способов перекраски делит порядок группы.

Примерами для этого случая являются квадраты 4×4 или 5×5.

Составим матрицу, соответствующую рассматриваемой системе сравнений. Если определитель этой матрицы над полем $\mathbb{Z}_2$ равен 1, то группы изоморфны. Если этот определитель равен 0, то реализуется второй случай.

§ 6. Многочлены Чебышёва

Можно ли определить, для каких квадратов $n \times n$ или прямоугольников $m \times n$ имеется только одно решение?

Решение будет единственным тогда и только тогда, когда определитель системы не равен нулю в поле $\mathbb{Z}_2$. Но поскольку мы имеем дело с коэффициентами 0 и 1, то вначале попытаемся найти этот определитель в кольце целых чисел.

Итак, рассмотрим прямоугольник $m \times n$ и его граф (рис. 6) с вершинами $A_1, A_2, \ldots, A_{mn}$.

Матрицу системы, соответствующей прямоугольной решётке, обозначим $B_{m,n}$. Она выглядит так:

$$B_{m,n} = \begin{pmatrix} H_n & E_n & 0 & \ldots & 0 & 0 & 0 \\ E_n & H_n & E_n & 0 & \ldots & 0 & 0 \\ 0 & E_n & H_n & E_n & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & E_n & H_n & E_n & 0 \\ 0 & 0 & \ldots & 0 & E_n & H_n & E_n \\ 0 & 0 & 0 & \ldots & 0 & E_n & H_n \end{pmatrix},$$

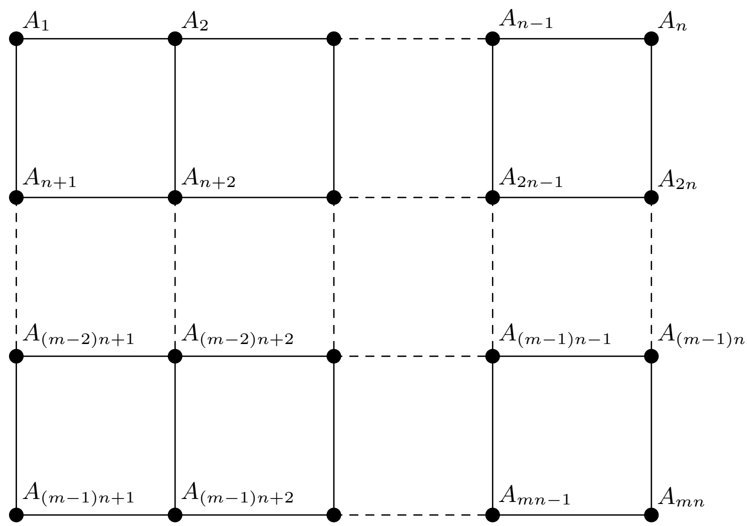


Рис. 6

где матрица H_n определена ниже, а E_n — единичная матрица размера $n \times n$. Определитель матрицы $B_{m,n}$ мы выразим через произведение собственных значений.

Рассмотрим тензорное произведение m-мерного пространства, в котором выделен базис $e_1, e_2, \ldots, e_m$, и n-мерного пространства, в котором выделен базис $f_1, f_2, \ldots, f_n$. Первый сомножитель будет отвечать строкам решётки, а второй — столбцам. Будем рассматривать $B_{m,n}$ как матрицу линейного оператора в базисе $e_i \otimes f_k$.

Действие оператора можно записать так:

$$B_{m,n}\colon \ e_i \otimes f_k \mapsto H_m e_i \otimes f_k + e_i \otimes L_n f_k.$$

Матрицы операторов H_m размера $m \times m$ и L_n размера $n \times n$ имеют следующий вид:

$$H_m = \begin{pmatrix} 1 & 1 & 0 & \ldots & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & \ldots & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 1 & 1 \end{pmatrix}, \qquad L_n = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & \ldots & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 1 & 0 \end{pmatrix}.$$

Для нахождения собственных значений операторов H_m и L_n найдём вначале определитель следующей матрицы размера $n \times n$:

$$C_n(x) = \begin{vmatrix} x & 1 & 0 & \dots & 0 & 0 & 0 \\ 1 & x & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & x & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & x & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 & x & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 & x \end{vmatrix}.$$

Разложим определитель по первой строке, а затем по первому столбцу. Получаем рекуррентное соотношение:

$$C_n(x) = xC_{n-1}(x) - C_{n-2}(x).$$

Положим $C_0(x) = 1$. Начало последовательности находим прямым вычислением: $C_1(x) = x$, $C_2(x) = x^2 - 1$.

Члены последовательности можно выразить через многочлены Чебышёва второго рода $U_0(y) = 1$, $U_1(y) = 2y$, $U_{n+1}(y) = 2yU_n(y) - U_{n-1}(y)$. Для этого достаточно сделать замену переменных $x = 2y$.

Корни многочленов Чебышёва равны

$$y = \cos\frac{k\pi}{n+1}, \quad k = 1, \dots, n.$$

Поэтому корни многочленов $C_n(x)$ равны

$$x = 2y = 2\cos\frac{k\pi}{n+1}, \quad k = 1, \dots, n.$$

Для нахождения собственных значений оператора H_m нужно положить $x = 1 - \lambda$. Поэтому собственные значения оператора H_m равны:

$$\lambda_k = 1 - 2\cos\frac{k\pi}{m+1}, \quad k = 1, \dots, m.$$

Для нахождения собственных значений оператора L_n нужно положить $x = -\mu$. Поэтому собственные значения оператора L_n равны

$$\mu_j = -2\cos\frac{j\pi}{n+1}, \quad j = 1, \dots, n.$$

Собственные значения матрицы $B_{m,n}$ равны $\lambda_k + \mu_j$.

Тогда её определитель равен

$$\det B_{m,n} = \prod_{k,\,j}(\lambda_k + \mu_j) = \prod_{k,\,j}\left(1 - 2\cos\frac{k\pi}{m+1} - 2\cos\frac{j\pi}{n+1}\right),$$

где $k = 1, \dots, m$; $j = 1, \dots, n$.

Итак, доказана

Теорема 1. *Для графа* Γ, *отвечающего прямоугольнику* $m \times n$,
1) *группа* S_Γ *изоморфна группе* G_{mn}, *если*

$$\prod_{k,\,j}\left(1 - 2\cos\frac{k\pi}{m+1} - 2\cos\frac{j\pi}{n+1}\right) \equiv 1 \pmod 2;$$

2) *группа* S_Γ *является собственной подгруппой группы* G_{mn}, *если*

$$\prod_{k,\,j}\left(1 - 2\cos\frac{k\pi}{m+1} - 2\cos\frac{j\pi}{n+1}\right) \equiv 0 \pmod 2.$$

Следствие 3. *Группа* S_Γ *является собственной подгруппой группы* G_{mn}, *в частности, для прямоугольников* $m \times n$, *где*
а) $m = 3q - 1$, $n = 2t - 1$ *или* $m = 2q - 1$, $n = 3t - 1$;
б) $m = 5q - 1$, $n = 5t - 1$, $q, t \in \mathbb{N}$.

Доказательство. а) В случае $m = 3q - 1$, $n = 2t - 1$ посмотрим на сомножитель с $k = \dfrac{m+1}{3} = q$ и $j = \dfrac{n+1}{2} = t$. Имеем

$$1 - 2\cos\frac{k\pi}{m+1} - 2\cos\frac{j\pi}{n+1} = 1 - 2\cos\frac{\pi}{3} - 2\cos\frac{\pi}{2} = 0.$$

Поскольку произведение собственных значений содержит нулевой сомножитель, определитель равен нулю. Остаётся применить теорему 1.

Аналогично в случае $m = 2q - 1$, $n = 3t - 1$ определитель также равен нулю.

Следовательно, для прямоугольников с длинами сторон $m = 3q - 1$, $n = 2t - 1$ или $m = 2q - 1$, $n = 3t - 1$ мы имеем не менее двух решений.

б) В случае $m = 5q - 1$, $n = 5t - 1$ посмотрим на сомножитель с $k = 3q$ и $j = t$. Имеем

$$1 - 2\cos\frac{k\pi}{5q} - 2\cos\frac{j\pi}{5t} = 1 - 2\cos\frac{3\pi}{5} - 2\cos\frac{\pi}{5} = 1 + 2\frac{\sqrt{5}-1}{4} - 2\frac{\sqrt{5}+1}{4} = 0.$$

Поскольку произведение собственных значений содержит нулевой сомножитель, определитель равен нулю. Опять применим теорему 1. Следовательно, для прямоугольников с длинами сторон $m = 5q - 1$, $n = 5t - 1$ ($t \in \mathbb{N}$) мы также имеем более одного решения. $\square$

Следствие 4. *Для квадратных досок* $n \times n$, *где* $n = 6t - 1$ *или* $n = 5t - 1$ *имеется не менее двух решений.*

Эти результаты согласуются со статистикой вычислений для квадратов $n \times n$, $n \leqslant 28$, проведённых И. Акуличем [3]. Как было раньше отмечено, число решений для квадратов $n \times n$ при $n = 4, 5, 9, 11, 14, 17, 19, 23, 24$ больше 2.

Выпадает случай $n = 16$, поскольку этот случай не подпадает под следствие 4. Более того, тогда определитель не равен 0 в кольце целых чисел, но, поскольку он чётен, он равен нулю в кольце Z_2.

Похожая техника нахождения определителя через собственные значения матрицы оператора с помощью многочленов Чебышёва применялась для подсчёта количества разбиений прямоугольника на «домино», см. [4].

§ 7. Ацтекский диамант

Кроме прямоугольников, можно посмотреть на другие фигуры на клетчатой доске. В качестве примера рассмотрим ацтекский диамант порядка n, см. рисунки ниже. У диаманта n-го порядка по $2n$ вертикальных и горизонтальных рядов клеток, а всего $2n(n + 1)$ клеток.

В графе, отвечающему ацтекскому диаманту, все вершины имеют чётный порядок, поэтому одним из решений всегда является набор ходов во все вершины диаманта.

Как и ранее, поставим вопрос о количестве решений для ацтекского диаманта порядка n.

Приведём результаты для $n \leqslant 10$.

Ацтекский диамант для $n = 1$ — это просто квадрат 2×2. Как мы знаем, в этом случае имеется только одно решение.

Для ацтекского диаманта порядка 2 (т. е. при $n = 2$) имеем четыре решения, все они показаны на рис. 7. Как видим, два решения получаются друг из друга симметрией относительно вертикальной оси.

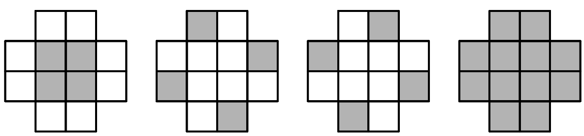


Рис. 7

При $n = 3$, $n = 6$, $n = 7$ и $n = 10$ имеем по одному решению, т. е. нужно сходить по разу во все клетки диаманта и других решений нет.

При $n = 4$ и $n = 5$ имеем по 16 решений, см. рис. 8, 9. Здесь и далее мы не показываем решение с набором ходов во все клетки диаманта и решения, получающиеся из приведённых поворотами и отражениями.

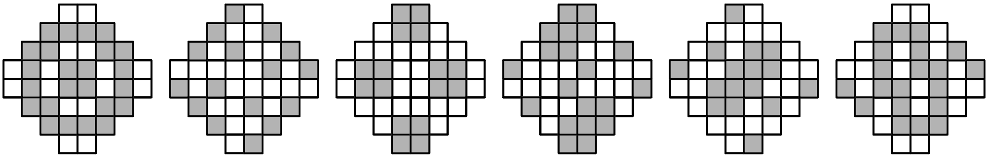


Рис. 8

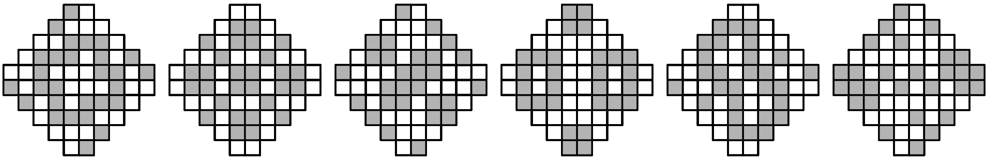


Рис. 9

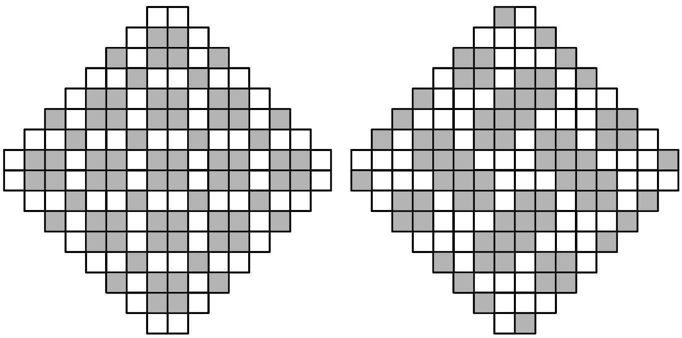


Рис. 10

При $n = 8$ (как и для $n = 2$) имеем 4 решения (рис. 10).

При $n = 9$ имеем 256 решений.

Как видим в проверенных случаях, количество решений является не только степенью двойки, но также степенью четвёрки.

Попытаемся продвинуться в поисках тех значений n, когда имеется только одно решение, т. е. группа S_Γ совпадает с G_d.

Составим систему сравнений по модулю 2, но при этом нумеровать клетки будем не как в случае квадрата и прямоугольника, а немного по-другому. Используя шахматную раскраску диаманта, мы видим, что чёрные клетки соответствуют графу прямоугольника $n(n+1)$. То же самое можно сказать о белых клетках.

Занумеровав вершины соответствующим образом, см. рис. 11, придём к системе сравнений, матрица которой имеет вид

$$D_n = \begin{pmatrix} E_m & K_m \\ K_m^T & E_m \end{pmatrix},$$

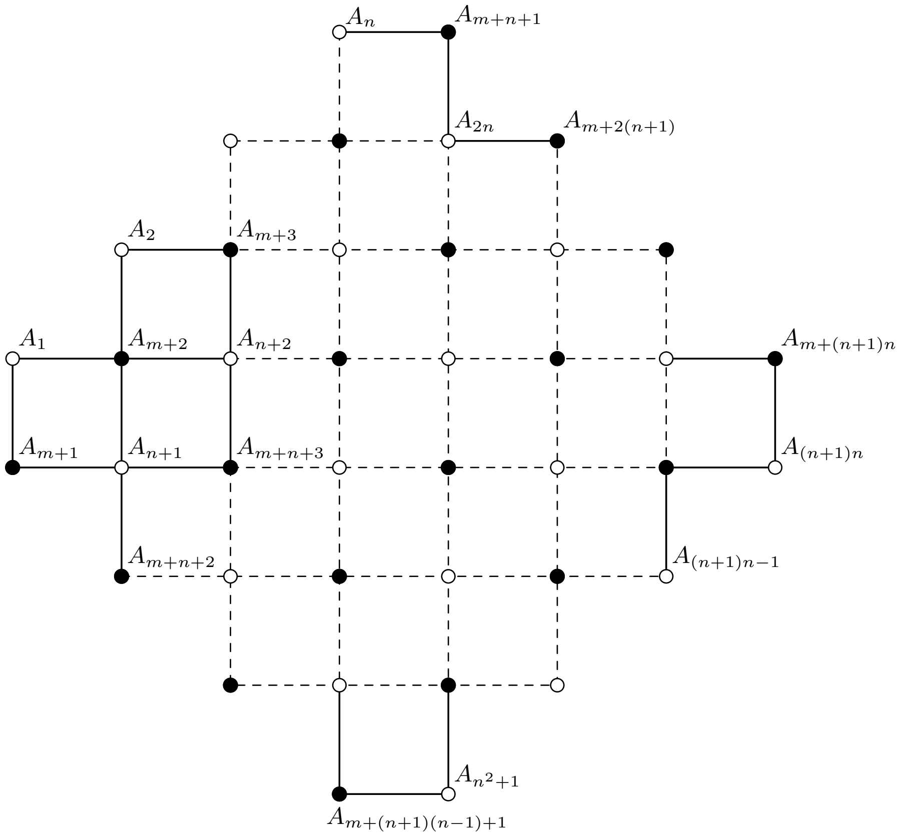


Рис. 11

где $m = n(n+1)$, E_m — единичная матрица, матрица K_m определена ниже, а K_m^T — транспонированная матрица.

Матрицу K_m можно рассматривать как кронекерово произведение матриц: $K_m = A_n \otimes A_n^T$, где матрица A_n имеет размер $n \times (n+1)$ и равна

$$A_n = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Теперь нам понадобится решить одну задачу по алгебре для первокурсников.

Задача 5 [9]. Доказать, что если A, B, C, D — квадратные матрицы порядка n, причём C или D — невырожденная матрица и $CD = DC$, то

$$\left\| \begin{matrix} A & B \\ C & D \end{matrix} \right\| = \|AD - BC\|.$$

Доказательство. Достаточно рассмотреть произведение

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} C^{-1} & D \\ 0 & -C \end{pmatrix} \quad \text{или} \quad \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} D & 0 \\ -C & D^{-1} \end{pmatrix}.$$

Что и требовалось доказать. □

Используя эту задачу, получим

$$\det D_n = \left\| \begin{matrix} E_m & K_m \\ K_m^T & E_m \end{matrix} \right\| = \|E_m E_m - K_m K_m^T\| = \|E_m - K_m K_m^T\|.$$

Положим $P_m = K_m K_m^T$. Наша цель — найти спектр матрицы P_m. Для этого воспользуемся следующей теоремой. Её доказательство читатели могут провести самостоятельно или найти в курсе линейной алгебры.

Теорема 2 (Кронекер). *Докажите следующие свойства кронекеровского произведения матриц*:

1) $(A \otimes B)^T = A^T \otimes B^T$;

2) *если* A, B, C, D — *матрицы такого размера, что существуют произведения* AC *и* BD, *то* $(A \otimes B)(C \otimes D) = AC \otimes BD$;

3) *пусть* A *и* B — *квадратные матрицы размеров* $n \times n$ *и* $m \times m$; *если* $\lambda_1, \ldots, \lambda_n$ — *собственные значения матрицы* A, *а* $\mu_1, \ldots, \mu_m$ — *собственные значения матрицы* B, *то собственными значениями матрицы* $A \otimes B$ *являются* $\lambda_i \mu_j$, *где* $i = 1, \ldots, n$, $j = 1, \ldots, m$.

Итак, используя свойства кронекеровского произведения, получаем

$$P_m = K_m K_m^T = (A_n \otimes A_n^T)(A_n \otimes A_n^T)^T = \\ = (A_n \otimes A_n^T)(A_n^T \otimes A_n) = (A_n A_n^T) \otimes (A_n^T A_n).$$

Матрица $A_n A_n^T$ является симметрической квадратной матрицей порядка n, и

$$A_n A_n^T = \begin{pmatrix} 2 & 1 & 0 & \ldots & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & \ldots & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 1 & 2 \end{pmatrix}.$$

Её собственные значения можно найти, как в предыдущем параграфе, они равны $\lambda_k = 2 - 2\cos\dfrac{k\pi}{n+1}$, $k = 1, \ldots, n$.

Матрица $A_n^T A_n$ является симметрической квадратной матрицей порядка $n+1$, и

$$A_n^T A_n = \begin{pmatrix} 1 & 1 & 0 & \ldots & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & \ldots & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & \ldots & 0 & 1 & 1 \end{pmatrix}.$$

Чтобы найти её собственные значения, придётся ещё немного поработать.

Найдём вспомогательный определитель матрицы порядка $n+1$, который является многочленом от переменной x:

$$F_{n+1}(x) = \begin{Vmatrix} x-1 & 1 & 0 & \ldots & 0 & 0 & 0 \\ 1 & x & 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & x & 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & 1 & x & 1 & 0 \\ 0 & 0 & \ldots & 0 & 1 & x & 1 \\ 0 & 0 & 0 & \ldots & 0 & 1 & x-1 \end{Vmatrix}.$$

Разложим определитель по первой строке, а затем по первому столбцу. Полученные определители разложим по нижней строке и последнему столбцу. Получим

$$F_{n+1}(x) = (x-1)^2 C_{n-1}(x) - 2(x-1)C_{n-2}(x) + C_{n-3}(x).$$

Вспоминая рекуррентное соотношение

$$C_n(x) = xC_{n-1}(x) - C_{n-2}(x),$$

упростим выражение до следующего

$$F_{n+1}(x) = (x-2)C_n(x).$$

Чтобы найти собственные значения матрицы $A_n^T A_n$, мы должны положить $x = 2 - \mu$ и решить уравнение

$$F_{n+1}(2-\mu) = (2 - \mu - 2)C_n(2-\mu) = 0.$$

Таким образом, одно из собственных значений матрицы $A_n^T A_n$ равно нулю: $\mu_0 = 0$, а остальные равны

$$\mu_j = 2 - 2\cos\frac{j\pi}{n+1}, \quad j = 1, \ldots, n.$$

По теореме 2, пункт 3 собственные значения матрицы P_m равны $\lambda_k\mu_j$, $k = 1, \ldots, n$, $j = 0, \ldots, n$, а собственные значения матрицы $E_m - P_m$ равны $1 - \lambda_k\mu_j$.

Тогда имеем

$$\det D_n = \det(E_m - P_m) = \\ = \prod_{k,\,j}(1 - \lambda_k\mu_j) = \prod_{k,\,j}\left(1 - 4\Bigl(1 - \cos\frac{k\pi}{n+1}\Bigr)\Bigl(1 - \cos\frac{j\pi}{n+1}\Bigr)\right),$$

где $k = 1, \ldots, n$, $j = 0, \ldots, n$. Итак, доказана

Теорема 3. *Для графа* Γ, *отвечающего ацтекскому диаманту порядка* n, *выполнено следующее*:

1) *группа* S_Γ *изоморфна группе* $G_{2n(n+1)}$, *если*

$$\prod_{k,\,j}\left(1 - 4\Bigl(1 - \cos\frac{k\pi}{n+1}\Bigr)\Bigl(1 - \cos\frac{j\pi}{n+1}\Bigr)\right) \equiv 1 \pmod 2;$$

2) *группа* S_Γ *является собственной подгруппой группы* $G_{2n(n+1)}$, *если*

$$\prod_{k,\,j}\left(1 - 4\Bigl(1 - \cos\frac{k\pi}{n+1}\Bigr)\Bigl(1 - \cos\frac{j\pi}{n+1}\Bigr)\right) \equiv 0 \pmod 2.$$

Следствие 5. *Группа* S_Γ *является собственной подгруппой группы* $G_{2n(n+1)}$, *в частности, для ацтекского диаманта порядка* n, *где*

$$\text{а) } n = 3q - 1; \quad \text{б) } n = 5q - 1, \quad q \in \mathbb{N}.$$

Доказательство. а) В случае $n = 3q - 1$ посмотрим на сомножитель с $k = j = q = (n+1)/3$. Имеем

$$1 - 4\Bigl(1 - \cos\frac{k\pi}{n+1}\Bigr)\Bigl(1 - \cos\frac{j\pi}{n+1}\Bigr) = 1 - 4\Bigl(1 - \cos\frac{\pi}{3}\Bigr)\Bigl(1 - \cos\frac{\pi}{3}\Bigr) = 0.$$

Поскольку произведение собственных значений содержит нулевой сомножитель, определитель равен нулю.

Следовательно, для ацтекского диаманта порядка $n = 3q - 1$ мы имеем не менее двух решений.

б) В случае $n = 5q - 1$ посмотрим на сомножитель с $k = 3q$ и $j = q$. Имеем

$$1 - 4\Big(1 - \cos\frac{k\pi}{n+1}\Big)\Big(1 - \cos\frac{j\pi}{n+1}\Big) = 1 - 4\Big(1 - \cos\frac{3\pi}{5}\Big)\Big(1 - \cos\frac{\pi}{5}\Big) = 0.$$

Значит, определитель равен нулю, поскольку произведение собственных значений содержит нулевой сомножитель. Следовательно, для ацтекского диаманта порядка $n = 5q - 1$ мы также имеем не менее двух решений. $\square$

§ 8. Упражнения

Задача 6 (Н. Агаханов, [2]). Клетки доски 8×8 раскрашены в шахматном порядке. Одним ходом разрешается перекрасить любую клетку в цвет одной из соседних с ней клеток. Можно ли с помощью таких перекрашиваний изменить цвет всех клеток на противоположный? (Соседними считаются клетки, имеющие общую сторону.)

Задача 7 (С. Токарев, XXIV Турнир городов 2002/03, [10]). В каждой клетке таблицы размером 4×4 стоит знак «+» или «−». Разрешено одновременно менять знаки на противоположные в любой клетке и во всех клетках, имеющих с ней общую сторону. Сколько разных таблиц можно получить, многократно применяя такую операцию?

Задача 8 (С. Токарев, [1]). В каждой клетке таблицы $n \times n$ записано число 1 или -1. Известно, что для каждой клетки произведение всех чисел в клетках, имеющих с ней общую сторону, равно 1. Докажите, что в любых двух клетках, симметричных относительно центра таблицы, записаны одинаковые числа.

Задача 9. Найдите последовательность ходов, перекрашивающую клетки доски $n \times n$ в противоположный цвет, для $n = 10$, 12, 13, 15, 18, 20, 21, 22, 25, 26, 27, 28, 36, 37, 38.

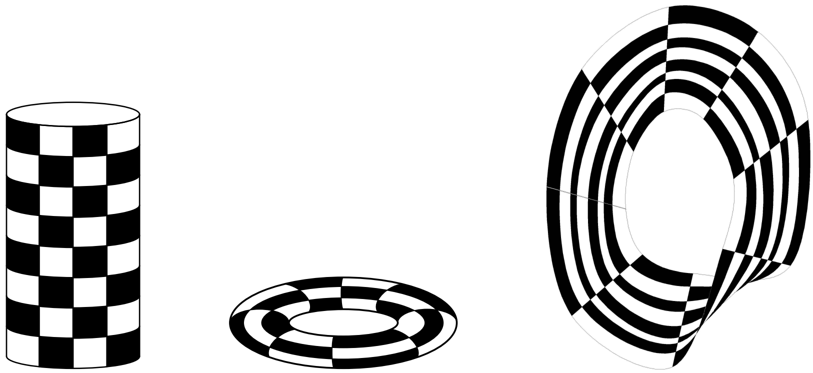
Задача 10. Найдите все последовательности ходов, перекрашивающие клетки доски $n \times n$ в противоположный цвет, для $n = 14$.

Задача 11 [5]. Постройте таблицу из § 4 для $m = 5$.

Задача 12 [6]. За один ход разрешается одновременно перекрасить в противоположный цвет любую клетку шахматной доски, а также все клетки, имеющие с ней общую сторону. Найдите последовательность ходов, перекрашивающую в противоположный цвет:

а) цилиндрическую шахматную доску, склеенную из доски 8×8 (рис. 12*а*);

б) тороидальную шахматную доску, склеенную из доски 8×8 (рис. 12*б*);



а) *б*) *в*)

Рис. 12

в) доску в форме листа Мёбиуса, склеенную из доски 8×8 (рис. 12*в*). Нарисуйте соответствующие графы.

Задача 13 [6]. За один ход разрешается одновременно перекрасить в противоположный цвет любую клетку доски, а также все клетки, в которые можно попасть из неё ходом коня. Найдите последовательности ходов, перекрашивающие в противоположный цвет клетки квадратных досок размеров 3×3, 4×4, и постройте соответствующие графы.

Задача 14. Клетки доски 8×8 раскрашены в шахматном порядке. За один ход можно выбрать клетку доски, и одновременно перекрасить в противоположный цвет все клетки, имеющие с ней общую сторону, при этом сама клетка не перекрашивается. Можно ли за несколько ходов перекрасить в противоположный цвет все клетки доски?

В заключение мы хотим отойти от двух красок и квадратных досок и перейти к многоцветным задачам.

Необходимо отметить, что исследование подобных многоцветных задач сопряжено с серьёзными трудностями. В частности, даже в трёхцветном случае существуют примеры раскрасок гексагональных досок, все клетки которых нельзя перекрасить в один цвет (вместе с клеткой перекрашиваются все соседние с ней по стороне) со следующей заменой цветов:

$$\text{белый} \to \text{серый} \to \text{чёрный} \to \text{белый}.$$

Задача 15 [6]. Приведите пример раскраски трёхцветной гексагональной доски, все клетки которой нельзя перекрасить в один цвет описанным образом.

Задача 16 [6]. За один ход разрешается одновременно перекрасить любую клетку гексагональной шахматной доски (доски Глинского) (рис. 13)

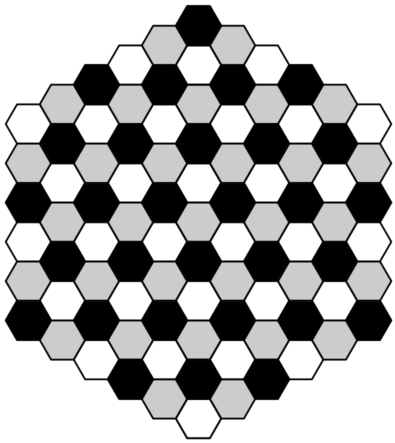


Рис. 13

и все клетки, имеющие с ней общую сторону, с заменой цветов:

$$\text{белый} \to \text{серый} \to \text{чёрный} \to \text{белый}.$$

Можно ли за несколько ходов перекрасить все клетки доски в белый цвет?

Как, зная решение, при котором все клетки доски Глинского перекрашиваются в белый цвет, получить решение, при котором все клетки доски Глинского перекрашиваются в чёрный цвет?

Задача 17 [6]. Докажите, что если для произвольной трёхцветной гексагональной доски решение существует, то число этих решений является целой неотрицательной степенью числа 3.

Вернёмся к двуцветным раскраскам.

Вопрос 2 оказался крепким орешком. И ответ на него неизвестен авторам. Возможно, нужно учитывать достаточно много симметрий квадрата.

Задача 18 (для исследования). Найдите, при каких n для доски $n \times n$ имеется ровно одно решение.

Задача 19 (для исследования). Найдите ответ на вопрос 2. Другими словами, докажите или опровергните, что для квадратной доски $n \times n$ количество способов поменять цвет клеток на противоположный является целой неотрицательной степенью числа 4.

Задача 20 (для исследования). Найдите, при каких n для ацтекского диаманта порядка n имеется ровно одно решение.

Задача 21 (для исследования). Докажите или опровергните, что для ацтекского диаманта порядка n количество способов поменять цвет клеток на противоположный — целая неотрицательная степень числа 4.

§ 9. Решения и указания к упражнениям

6. Рассмотрим клетку, которую мы перекрашиваем последней. К моменту её перекрашивания все остальные клетки должны были бы изменить цвет на противоположный. Значит, в этот момент все её соседние клетки — одного с ней цвета и мы эту клетку перекрасить не можем.

Эту задачу несложно обобщить, переложив её на язык графов. Каждую клетку доски мы можем заменить вершиной графа. Если клетки являются соседями, то соединим вершины ребром графа. Отметим, что такое обобщение задачи 6 в терминах графов не усложнит её решения.

7. Мы уже знаем, что количество разных таблиц будет степенью двойки. Поскольку из данной таблицы можно получить таблицу с любыми знаками в первых трёх строках, число различных таблиц не меньше чем 2^{12}. Это число будет искомым ответом: нетрудно убедиться, что первые три строки однозначно определяют четвёртую.

8. Заметим, что если заданы все числа первой строки, то все остальные числа таблицы определяются однозначно. (По первой строке заполняем вторую, затем третью и т. д.) Укажем два способа заполнения таблицы. При этом из первого способа будет следовать симметричность таблицы относительно её диагонали, идущей из левого нижнего угла в правый верхний, а из второго способа — симметричность относительно другой диагонали.

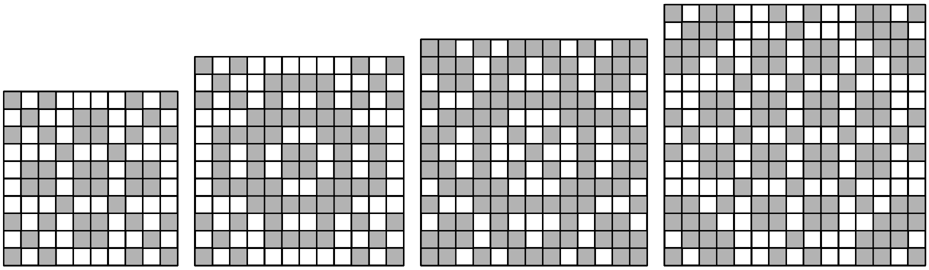
Первый способ. Вторую и последующие строки заполняем слева направо: во вторую вписываем $n-1$ число, в третью $n-2$ числа, в четвёртую $n-3$ числа и т. д., в самую нижнюю строку (в левый нижний угол таблицы) вписываем одно число. Затем в каждую из пустых клеток записываем число так, чтобы таблица оказалась симметричной относительно диагонали, идущей из левого нижнего угла в правый верхний. Построенная таблица удовлетворяет условию задачи.

Второй способ. Аналогичен первому, но строки заполняются справа налево (во вторую строку вписывается $n-1$ число и т. д., в самую нижнюю, т. е. в правый нижний угол таблицы, — одно число). Пустые клетки заполняем так, чтобы таблица оказалась симметричной относительно диагонали, идущей из левого верхнего угла в правый нижний.

Поскольку таблица с заданной первой строкой существует только одна, она совпадает с построенными, т. е. симметрична относительно каждой из своих больших диагоналей. Из симметричности относительно диагоналей следует симметричность относительно центра таблицы.

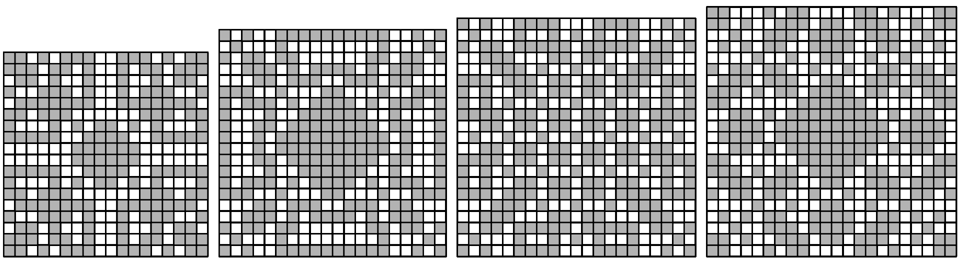
9. См. рис. 14, 15, 16, 17.

10. См. рис. 18.



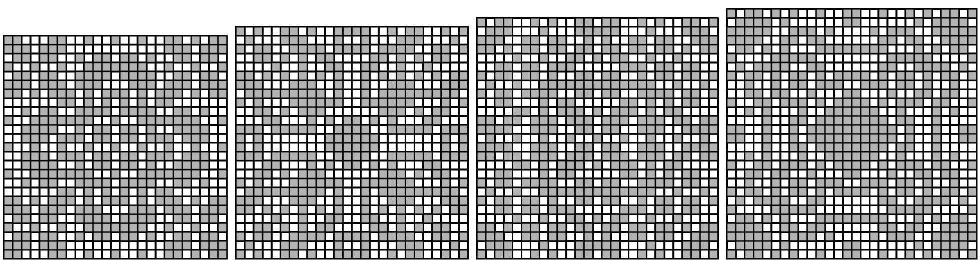
$n = 10$ $n = 12$ $n = 13$ $n = 15$

Рис. 14



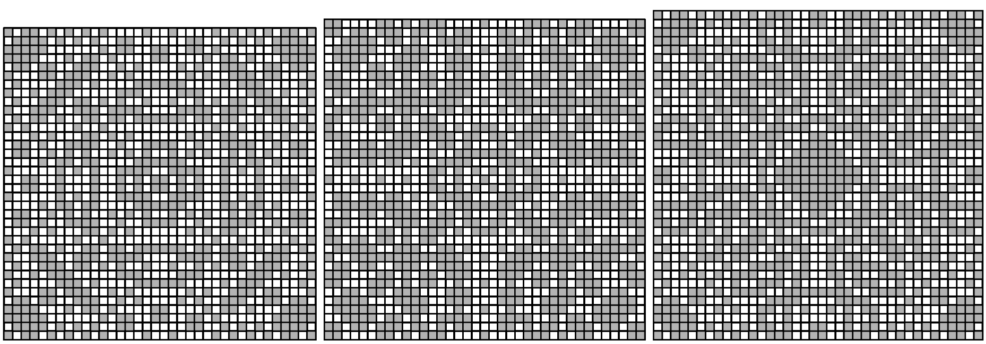
$n = 18$ $n = 20$ $n = 21$ $n = 22$

Рис. 15



$n = 25$ $n = 26$ $n = 27$ $n = 28$

Рис. 16



$n = 36$ $n = 37$ $n = 38$

Рис. 17

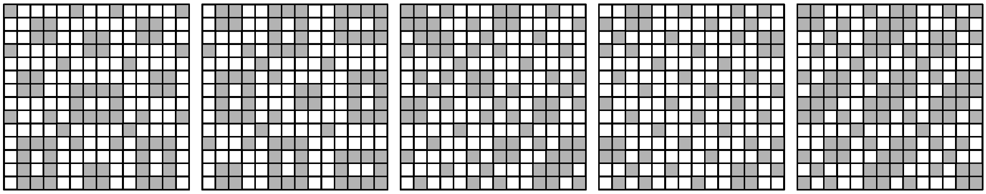


Рис. 18

Таблица 1

a	$a+b+1$	$a+c+1$	$b+c+d+1$	e	$b+c+e+1$	a	$a+c+e+1$	$c+e$	
b	$a+b+c+1$	d	$a+b+d+e+1$	$d+1$	$a+b+c$	$b+1$	0	b	
c	$b+c+d+1$	$a+e$	$a+c+e$	$c+1$	$a+b+d+e$	c	$a+c+e+1$	$a+e$	$\mapsto$
d	$c+d+e+1$	b	$a+b+d+e+1$	$b+1$	$c+d+e$	$d+1$	0	d	
e	$d+e+1$	$c+e+1$	$b+c+d+1$	a	$a+c+d+1$	e	$a+c+e+1$	$a+c$	

	$a+b$	e	$a+b+d+e+1$	$e+1$	$a+b$	$c+e$	$a+c+e$	$a+1$	
	$a+b+c+1$	d	$a+b+d+e+1$	$d+1$	$a+b+c$	$b+1$	0	b	
$\mapsto$	$b+c+d$	$c+1$	0	c	$b+c+d+1$	$a+e$	$a+c+e$	$c+1$	$\mapsto$
	$c+d+e+1$	b	$a+b+d+e+1$	$b+1$	$d+e+c$	$d+1$	0	d	
	$d+e$	a	$a+b+d+e+1$	$a+1$	$d+e$	$a+c$	$a+c+e$	$e+1$	

	$b+c+e$	$e+1$	$b+c+d$	$a+c+1$	$a+b+1$	$a+1$	0	a	$\dots$
	$a+b+c+1$	d	$a+b+d+e+1$	$d+1$	$a+b+c$	$b+1$	0	b	$\dots$
$\mapsto$	$a+b+d+e$	c	$a+c+e+1$	$a+e$	$b+c+d$	$c+1$	0	c	$\dots$
	$c+d+e+1$	b	$a+b+d+e+1$	$b+1$	$c+d+e$	$d+1$	0	d	$\dots$
	$a+c+d$	$a+1$	$b+c+d$	$c+e+1$	$d+e+1$	$e+1$	0	e	$\dots$

11. См. табл. 1.

12. Вершины, куда необходимо сделать ход, на графах обозначены чёрным цветом.

а) Граф для цилиндрической доски 8×8 см. на рис. 19 наверху слева.

б) Граф для тороидальной доски 8×8 см. на рис. 19 внизу. Поскольку из любой вершины графа тороидальной доски $n \times n$ для $n \geqslant 3$ выходит ровно 4 ребра, одной из подходящих раскрасок будет раскраска с ходом в каждую вершину.

в) Граф для листа Мёбиуса, склеенного из доски 8×8, см. на рис. 19 наверху справа.

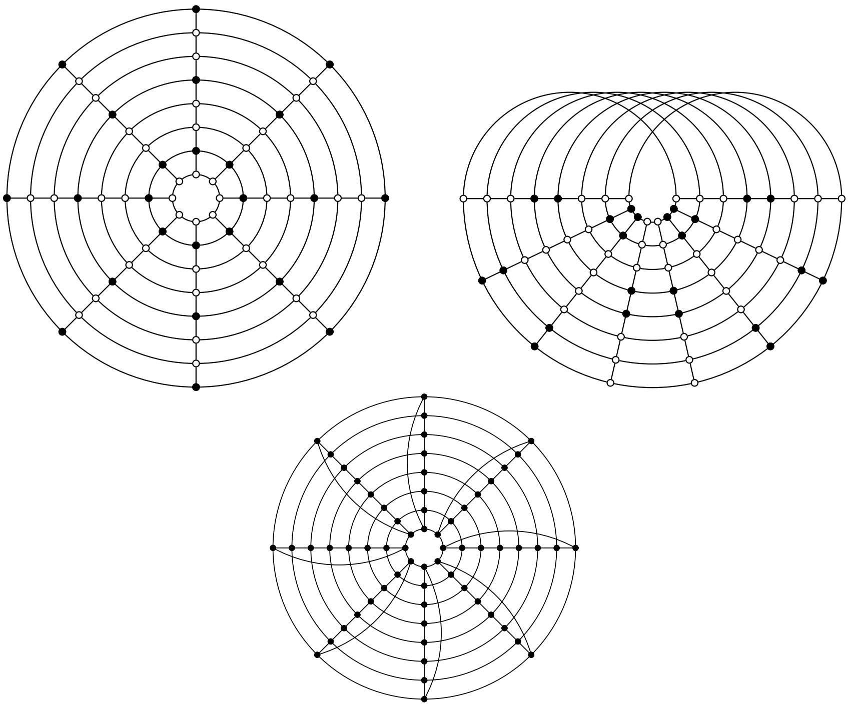


Рис. 19

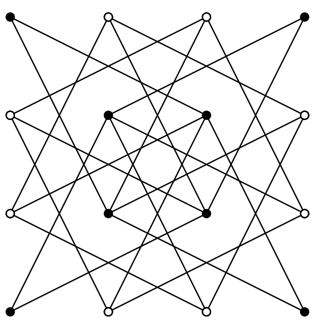


Рис. 20

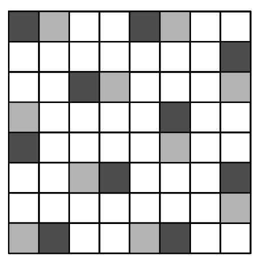


Рис. 21

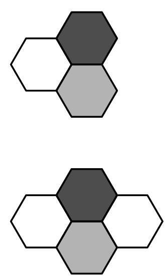


Рис. 22

13. *Указание.* В случае 3×3 граф представляет собой восьмирёберный цикл и изолированную точку. В случае 4×4 см. рис. 20.

14. См. рис. 21. Ходы в клетки, отмеченные чёрным, перекрашивают все чёрные клетки и не трогают белые клетки доски. И наоборот, ходы в клетки, отмеченные серым, перекрашивают все белые клетки и не трогают чёрные клетки доски.

15. См. рис. 22.

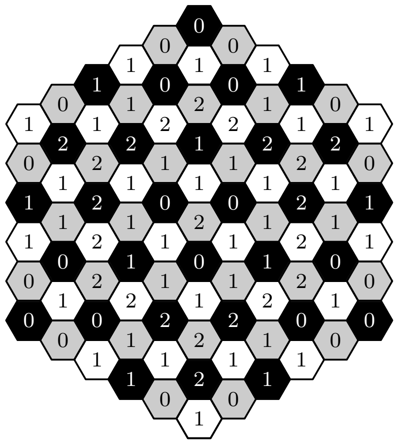


Рис. 23

16. Одно из возможных решений (для белой раскраски) см. на рис. 23. В каждой ячейке записано количество ходов в эту ячейку. Конечно, при решении этой задачи можно применить все методы, о которых мы говорили ранее. Можно также попытаться составить систему линейных уравнений с коэффициентами $0, 1, 2$ (над полем вычетов по модулю 3), но не будем заставлять читателя решать эту систему из 91 уравнения с 91 неизвестным.

17. *Указание.* С учётом того, что решение существует, проведите рассуждения, аналогичные решению задачи 4, и получите соотношение $ks = 3^n$, где n — число вершин графа, k — число классов, в каждом из которых по s элементов.

Список литературы

[1] *Агаханов Н. Х., Богданов И. И., Кожевников П. А. и др.* Математика. Областные олимпиады. М.: Просвещение, 2010. С. 29, задача 200.

[2] *Агаханов Н. Х., Богданов И. И., Кожевников П. А. и др.* Математика. Областные олимпиады. М.: Просвещение, 2010. С. 54, задача 385.

[3] *Акулич И.* Призрак Леонардо // Квант. 2008. № 1. С. 26–29.

[4] *Вялый М. Н.* Пфаффианы или искусство расставлять знаки // Математическое просвещение. Сер. 3. Вып. 9. М.: МЦНМО, 2005. С. 129–142.

[5] *Дорофеев В., Спивак А.* Раскраски графов и линейные уравнения // Квант. 2011. № 4. С. 39–42.

[6] *Журавлёв В., Самовол П.* Охота на призрак Леонардо // Квант. 2011. № 4. С. 36–38.

[7] Конкурс им. А. П. Савина «Математика 6–8», задача 5 // Квант. 2007. № 4. С. 27.

[8] Математическое просвещение. Сер. 3. Вып. 20. М.: МЦНМО, 2016. С. 249, задача 2.

[9] Сборник задач по алгебре / Под ред. А. И. Кострикина. М.: МЦНМО, 2009. С. 48, задача 16.14.

[10] *Толпыго А. К.* Тысяча задач Международного математического Турнира городов. М.: МЦМНО, 2010. С. 179, XXIV Турнир городов (2002/03), задача 46.

Валерий Михайлович Журавлёв, ПАО «Туполев», Москва, Россия

zhuravlevvm@mail.ru

Пётр Исаакович Самовол, Ben-Gurion University of the Negev, Beer-Sheva, Israel

pet12@012.net.il

О поиске медианы массива за линейное время

А. С. Малистов

В сборнике «Математическое просвещение», сер. 3, вып. 11 (М.: МЦНМО, 2007) на с. 164 опубликована следующая задача 11:

Дано $2n+1$ грузов попарно различной массы и чашечные весы без гирь. Докажите, что за $100n$ взвешиваний можно найти *медиану* (т. е. средний по массе груз). (*Фольклор*)

Рассмотрим следующую более общую задачу.

Описать алгоритм поиска медианы массива за линейное время.

Прежде чем мы подробно опишем требуемый алгоритм, определимся с терминологией. Напомним, что такое медиана массива, что значит время работы алгоритма и в каком случае это время можно считать линейным.

Пусть дано конечное линейно упорядоченное множество M, содержащее n объектов $\{x_1, x_2, \ldots, x_n\}$. Это означает, что для любых двух его элементов задано отношение порядка $\leqslant$, удовлетворяющее условиям рефлексивности ($\forall\, a\ a \leqslant a$), транзитивности ($\forall\, a, b, c\ \ a \leqslant b,\ b \leqslant c\ \Rightarrow\ a \leqslant c$) и антисимметричности ($\forall\, a, b\ \ a \leqslant b,\ b \leqslant a\ \Rightarrow\ a = b$). Если упорядочить все элементы множества M по возрастанию, то i-й *порядковой статистикой* называется i-й по возрастанию элемент. Если n — нечётное число, то *медианой* множества M называется $((n+1)/2)$-я статистика, которая находится ровно посередине. Если n — чётное число, то медиана не может быть однозначно определена и различают нижнюю и верхнюю медианы с индексами $n/2$ и $n/2+1$ соответственно. Иногда в качестве медианы в случае чётного n берут среднее арифметическое между нижней и верхней медианами. Нам требуется описать алгоритм поиска медианы за линейное время, но мы будем решать более общую задачу поиска i-й порядковой статистики за линейное время, которая покрывает задачу поиска медианы.

Теперь попробуем понять, что значит время работы алгоритма и в каком случае это время называют линейным. Чтобы исключить неоднозначность в определении времени, требуется абстрактная модель компьютера с универсальными инструкциями. Такие абстрактные компьютеры называются *моделями вычислений* или, по-другому, *вычислительными моделями*. Хронологически самой первой такой моделью считается *машина Тьюринга*, которая, правда, недостаточно хорошо моделирует современные компьютеры. Мы будем использовать модель машины с произвольным доступом к памяти, которая гораздо лучше подходит для современных вычислительных устройств. Это некоторый абстрактный компьютер с памятью, состоящей из ячеек, адреса которых нумеруются последовательно, начиная с нуля. Каждая ячейка может хранить целое число, ограниченное по модулю некоторым положительным числом L. Значение L зависит от входных данных решаемой на компьютере задачи. Кроме того, компьютер имеет конечное число регистров для проведения арифметических операций. Разрешены операции чтения чисел из памяти в регистр и записи из регистра в память, арифметические операции сложения, умножения, вычитания, целочисленного деления, взятия остатка. За одну операцию также можно сравнить значения любых двух чисел и, в зависимости от результата, перейти к любому шагу алгоритма. Кроме того, разрешён непрямой доступ к памяти, когда адрес обрабатываемой ячейки может быть задан в одном из регистров. *Временем работы* алгоритма называется число операций, которые алгоритм выполняет для решения задачи.

Пусть элементы множества M записаны в последовательных ячейках памяти нашего компьютера. Адреса этих ячеек находятся в диапазоне $[s, s+n-1]$, где s — начальный адрес, с которого начинается вход алгоритма. Требуется предложить алгоритм, который найдёт i-ю порядковую статистику входного массива. Отметим, что элементы множества M необязательно должны быть числами и могут иметь произвольное происхождение. Важно лишь, чтобы их можно было записать в ячейки памяти компьютера, и должна существовать возможность сравнивать эти объекты, чтобы определить, какой элемент меньше, а какой больше. Под этой возможностью понимается, что существует вспомогательная процедура, принимающая на вход два адреса ячеек памяти, которые содержат элементы a и b, сравнивает эти элементы и возвращает 1, если $a \leqslant b$, и 0 в противном случае. Время работы этой процедуры принимается условно за единицу.

Говорят, что алгоритм выполняется за *линейное время*, если количество шагов алгоритма ограничено многочленом первой степени от n для всех $n \in \mathbb{N}$. Иначе говоря, существует такой многочлен $an + b$, что для любого входа длины n время работы алгоритма не превысит $an + b$. Обратим внимание на распространённую ошибку. Увеличение входа, скажем, вдвое вовсе не означает, что алгоритм, работающий за линейное время, станет тратить времени ровно в два раза больше. Более того, это время вообще может оказаться не определённым однозначно, так как существует огромное количество различных входов длины n и каждый из них может требовать разное число операций. Линейное время означает лишь, что число таких операций ограничено сверху линейным многочленом. Иногда используют альтернативное определение, которое требует, чтобы существовали такие константы c и n_0, что время работы алгоритма меньше cn для всех $n > n_0$. Нетрудно убедиться, что эти определения эквивалентны. Второе следует из первого, если задать $c = |a| + |b|$, $n_0 = 1$, а первое следует из второго, если считать, что $a = c$, а b — это максимальное время работы для всех входов с длиной не больше n_0.

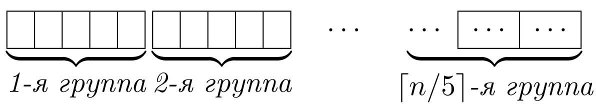
Существует универсальная запись, которая обобщает оценку времени работы алгоритма на случай не только линейных функций. Пусть с входными данными связан некоторый целочисленный параметр n, например, количество чисел в массиве. Этот параметр n часто называют функцией длины входа. Будем говорить, что алгоритм выполняется за $O(f(n))$, если существуют такие константы C и n_0, что для всех $n > n_0$ число операций, которые выполняет алгоритм на любом входе длины n, не превышает $Cf(n)$. Тогда фраза «алгоритм работает за линейное время» эквивалентна фразе «алгоритм работает за время $O(n)$».

Найти медиану массива, а также любую другую порядковую статистику можно нехитрым способом, предварительно отсортировав массив по возрастанию. Так как мы используем машину с произвольным доступом к памяти, после сортировки можно обратиться к ячейке с адресом $s + i - 1$, чтобы получить i-ю статистику (s — адрес первой ячейки отсортированного массива). Известные алгоритмы быстрой сортировки, например сортировка слиянием, работают за время $O(n \log_2 n)$. При этом для любого n, начиная с некоторого n_1, всегда существует вход длины n, на котором эта верхняя оценка достижима, то есть число операций больше $cn \log_2 n$ для некоторой ненулевой константы c. Если не использовать внутреннюю структуру элементов массивов, а опираться лишь на попарные сравнения элементов, то не существует алгоритма сортировки, который работал бы за линейное время. Тем не менее, если сортировать массив не требуется, а нужно лишь найти i-ю порядковую статистику, то сделать это можно за линейное время. Алгоритм, который мы опишем, был придуман Блюмом, Флойдом, Праттом, Ривестом и Тарьяном и опубликован в 1973 году [1]. Иногда его называют BFPRT-алгоритмом по первым буквам фамилий разработчиков.

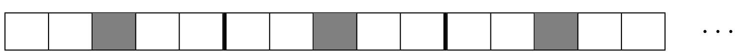
Сперва опишем вспомогательную процедуру, которая называется *разбиением массива*. Дан массив, состоящий из n элементов, и дополнительный элемент x. Необходимо упорядочить элементы массива таким образом, чтобы сначала шли элементы, не превосходящие x (т. е. все такие a, для которых $a \leqslant x$), а затем все остальные элементы. Оказывается, сделать такое разбиение можно за линейное время, причём не используя существенно дополнительную память. Нам потребуется всего лишь два дополнительных счётчика. В начале алгоритма первый счётчик должен указывать на первый элемент массива, а второй счётчик — на последний. Первый счётчик будет увеличивать своё значение на единицу до тех пор, пока для элемента a, на который он указывает, выполняется $a \leqslant x$. Второй счётчик должен уменьшать своё значение на единицу до тех пор, пока для элемента b, на который он указывает, неверно, что $b \leqslant x$. Когда первый счётчик станет указывать на элемент a, больший, чем x, а второй на такой элемент b, что $b \leqslant x$, необходимо поменять элементы a и b местами, а затем продолжить процедуру. Алгоритм заканчивает работу, когда второй счётчик перестаёт быть больше первого. Число изменений каждого счётчика не превышает n, а число сравнений элементов и их возможных перестановок не превосходит[1] $\lfloor n/2 \rfloor$.

Теперь мы можем описать *основной алгоритм*, который должен найти i-ю порядковую статистику.

А1. Входной массив разбивается на одинаковые небольшие группы, например на $\lceil n/5 \rceil$ групп по 5 элементов в каждой, кроме, возможно, одной группы, в которой может быть меньше элементов. Элементы в каждой группе стоят по порядку: в первой группе находятся элементы с 1-го по 5-й, во второй — с 6-го по 10-й, и т. д.



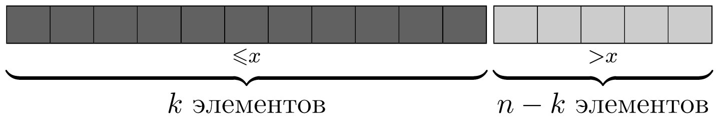
А2. Сначала каждая из маленьких групп сортируется по возрастанию любым известным методом сортировки, а затем в каждой отсортированной группе выбирается медиана. Если $n \leqslant 5$, то работа алгоритма на этом заканчивается.



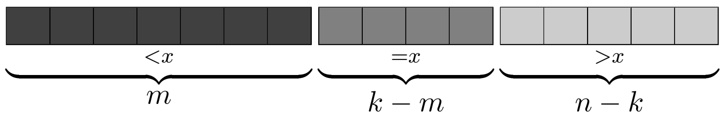
А3. С помощью того же алгоритма для $\lceil n/5 \rceil$ определяется *верхняя* медиана x из $\lceil n/5 \rceil$ медиан, найденных на втором шаге (другими словами, $\lceil \lceil n/5 \rceil /2 \rceil$-я порядковая статистика в массиве медиан).

А4. С помощью процедуры *разбиения массива*, описанной выше, входной массив делится относительно медианы медиан x. Пусть в нижнюю часть разбиения попало k элементов, а в верхнюю часть попало $n - k$ элементов.

[1] Напомним, что $\lfloor t \rfloor$ обозначает наибольшее целое число, не превосходящее t, а $\lceil t \rceil$ — наименьшее целое число, не меньшее чем t.



A5. С помощью процедуры, аналогичной *разбиению массива*, нижняя часть входного массива делится на две части: в первую входят все числа, которые не равны x (то есть меньше x), а во вторую — те, которые равны x. Пусть элементов, меньших x, оказалось ровно m.



A6. Если $m < i \leqslant k$, то возвращается значение x. Если $i < m$, то процедура вызывается повторно для нижней части разбиения. Если $i > k$, то процедура вызывается повторно для верхней части разбиения, но ищется $(i-k)$-я порядковая статистика.

Корректность алгоритма достаточно очевидно вытекает из описания последнего шага. На шестом шаге мы повторно запускаем алгоритм на уменьшенной выборке, корректно меняя искомый индекс статистики, если потребуется. Алгоритм всегда завершается за конечное число шагов, так как разбиение на четвёртом и пятом шагах всегда уменьшает размер обрабатываемого массива.

Теперь разберёмся, почему алгоритм работает за линейное время. Главную роль в этом играет медиана медиан x, относительно которой производится разбиение. Дело в том, что половина медиан, найденных на втором шаге, меньше или равна медиане медиан x. Более точно, таких медиан будет не меньше чем $\lceil \lceil n/5 \rceil /2 \rceil$. Исключим из рассмотрения маленькую группу, в которой может быть менее пяти элементов, и группу, которая включает медиану медиан x. Внутри каждой оставшейся полной группы, в которой медиана меньше или равна x, находятся 5 элементов, три из которых вместе с медианой меньше или равны x. Таким образом, количество Q элементов, не превышающих x, удовлетворяет следующему неравенству:

$$Q \geqslant 3\left(\left\lceil \frac{\lceil n/5 \rceil}{2} \right\rceil - 2\right) \geqslant 3\left(\frac{n}{10} - 2\right) = \frac{3n}{10} - 6.$$

Аналогично количество элементов, которые больше или равны x, не меньше $3n/10 - 6$. Отсюда следует, что к шестому шагу остаётся на дальнейшую обработку не более чем $\min\{7n/10 + 6, n-1\}$ элементов (даже если $7n/10 + 6$ больше n, как минимум один элемент выкидывается — это медиана медиан x).

Пусть $T(n)$ — максимальное время работы алгоритма по всем входам длины n. Индукцией по n получаем, что для выполнения шагов 1, 2, 4 и 5 требуется линейное время работы. Пусть это время ограничено многочленом an. Тогда $T(n)$ удовлетворяет следующему неравенству:

$$T(n) \leqslant an + T\left(\left\lceil \frac{n}{5} \right\rceil\right) + T\left(\min\left\{n-1, \left\lfloor \frac{7n}{10} + 6 \right\rfloor\right\}\right). \tag{1}$$

Пусть $T_0 = \max_{n \leqslant 700} T(n)$ — максимальное время по всем входам длины не больше 700. Нам осталось доказать, что существует такая константа c, что $T(n) < cn$ для всех $n \in \mathbb{N}$. Если эту константу взять больше, чем T_0, то это сразу докажет наше утверждение для всех $n \leqslant 700$. Для $n > 700$ требуется шаг индукции. Если $n > 700$, то

$$\min\left\{n-1, \left\lfloor \frac{7n}{10} + 6 \right\rfloor\right\} = \frac{7n}{10} + 6,$$

поэтому согласно (1) и предположению индукции получаем

$$T(n) \leqslant an + c\left\lceil \frac{n}{5} \right\rceil + c\left\lfloor \frac{7n}{10} + 6 \right\rfloor \leqslant$$
$$\leqslant an + c\left(\frac{n}{5} + 1\right) + \frac{7cn}{10} + 6c = cn + \left(an - \frac{cn}{10} + 7c\right).$$

Неравенство будет верным, если выбрать константу c такой, что

$$an - \frac{cn}{10} + 7c < 0$$

для всех $n > 700$. Решая последнее неравенство относительно c и учитывая, что $n/10 > 7$ при $n > 700$, получаем, что достаточно выбрать

$$c > \frac{an}{n/10 - 7} = \frac{10a}{1 - 70/n}.$$

Подойдёт $c = 12a$, так как при $n > 700$ всегда $12a > \dfrac{10a}{1 - 70/n}$.

Список литературы

[1] *Blum M., Floyd R. W., Pratt V., Rivest R. L., Tarjan R. E.* Time bounds for selection // Journal of computer and system sciences. V. 7, № 4. 1973. P. 448–461.

Алексей Сергеевич Малистов, ООО «Яндекс»

alexey@malistov.ru

Задачник

Условия задач

В этом разделе вниманию читателей предлагается подборка задач разной степени сложности, в основном трудных. Надеемся, что эти задачи окажутся интересными как для сильных школьников, интересующихся математикой, так и для студентов-математиков.

Мы обращаемся с просьбой ко всем читателям, имеющим собственные подборки таких задач, присылать их в редакцию. И, разумеется, мы с удовольствием будем публиковать свежие авторские задачи.

В скобках после условия задачи приводится фамилия автора (уточнения со стороны читателей приветствуются).

1. Какая из двух кривых длиннее: эллипс $\left\{(x,y)\colon \dfrac{x^2}{2}+y^2=1\right\}$ или синусоида $\{(x,\sin x)\colon 0\leqslant x\leqslant 2\pi\}$?

   (*Л. Радзивиловский*)

2. Докажите равенство

$$\left(\sum_{i=1}^{n} x_i\right)^n - \sum_{j=1}^{n}(x_1+\ldots+\widehat{x}_j+\ldots+x_n)^n + \\ + \sum_{j_1<j_2}(x_1+\ldots+\widehat{x}_{j_1}+\ldots+\widehat{x}_{j_2}+\ldots+x_n)^n+\ldots+ \\ + (-1)^{|J|}\sum_{j_1<\ldots<j_{|J|}}(x_1+\ldots+\widehat{x}_{j_1}+\ldots+\widehat{x}_{j_{|J|}}+\ldots+x_n)^n+\ldots+ \\ + (-1)^{n-1}\sum_{i=1}^{n}x_i^n = n!\prod_{i=1}^{n}x_i,$$

   где $\widehat{x}_j$ означает, что соответствующий член опускается.

   (*А. Я. Канель-Белов*)

3. Сеть железных дорог представляет собой дерево (неориентированный конечный связный граф без циклов). По сети проходят маршруты электричек, посредством которых можно проехать от любой станции до любой (возможно, с пересадками). Электричка может повернуть назад лишь на конечных станциях маршрута. Количество тупиков (висячих вершин, т. е. вершин степени 1) в данной сети равно n.
   а) Каково наименьшее возможное количество маршрутов, если от любой станции до любой можно проехать, возможно с пересадками?
   (*Фольклор*)
   б) Каково наименьшее возможное количество маршрутов, если от любой станции до любой можно проехать не более чем с одной пересадкой?
   (*Б. Р. Френкин*)

4. На плоскости отмечено n прямых общего положения, т. е. никакие три не пересекаются в одной точке, никакие две не параллельны и любые три точки пересечения либо не лежат на одной прямой, либо лежат на одной из отмеченных. Сколькими различными способами можно добавить *хорошую* прямую (т. е. не проходящую через точку пересечения двух отмеченных)? Два способа считаются *одинаковыми*, если один можно получить из другого, непрерывно двигая новую прямую так, чтобы она всё время оставалась *хорошей*. (*Фольклор*)

5. Многочлены $P(x)$ и $Q(x)$ таковы, что при всяком целом x найдётся такое целое y, что $P(x) = Q(y)$. Докажите, что найдётся такой многочлен R, что $P(x) = Q(R(x))$ при всех x. Что будет, если условие задачи ослабить, т. е. потребовать, чтобы указанное y нашлось для бесконечно многих целых x? (*А. Я. Канель-Белов*)

6. *По мотивам задачи М. Патерсон и Д. Стинсона* [1].
   а) По кругу стоят n мудрецов, у каждого на голове шапка одного из k цветов. Каждый мудрец видит всех оставшихся. Мудрецы по порядку (по часовой стрелке) говорят либо «пас», либо предполагаемое название цвета своей шапки (в зависимости от того, что они видят и сколько кругов прошло). Все распределения цветов равновероятны. Мудрецы могут заранее согласовать свои ответы. Их цель — чтобы первый, назвавший свой цвет, не ошибся. Какую максимальную вероятность этого они могут обеспечить? (*И. В. Митрофанов*)
   б) Король решил казнить n мудрецов. Их поставят в ряд друг за другом (так, чтобы все смотрели в одном направлении), на каждого наденут шляпу белого или чёрного цвета. Каждый мудрец будет видеть шляпы всех впереди стоящих. У каждого мудреца по очереди (от последнего к первому) спросят цвет его шляпы, и если он угадает, то его помилуют

(но уже по окончании опроса). Мудрецам разрешили договориться заранее, но оказалось, что k из них безумны (а кто — неизвестно). Безумный мудрец называет случайный цвет вне зависимости от договорённостей. Какое максимальное количество мудрецов может гарантированно спастись? (*М. Фадин*)

7. Радиус озера n м. Барон Мюнхгаузен имеет большой запас дощечек длины 1 м каждая и утверждает, что с помощью этих дощечек он может добраться до середины озера. Дощечка считается отрезком, и класть её можно так, чтобы каждый конец был на берегу или на другой дощечке.
а) Не хвастает ли барон?
б) Докажите, что для некоторой константы $C > 0$ при всех достаточно больших n ему не хватит Cn^3 дощечек. (*А. Я. Канель-Белов*)

8. (Задача на исследование.) Дано N-элементное множество M, $N \to \infty$, и случайное отображение $f\colon M \to M$.
а) Каково наиболее вероятное число элементов у множества $f(M)$?
б) Оцените n при условии $f^{(n)}(M) = f^{n+1}(M)$.
в) Оцените мощность множества $S = f^{(n)}(M)$.
г) Пусть ограничение f на S есть перестановка. Оцените число её циклов. Постарайтесь получить информацию о распределении описанных выше величин. (*Фольклор*)

9. В выпуклом многограннике M степень каждой вершины равна 5, а у всех граней, кроме, может быть, грани A, число сторон делится на 3. Докажите, что число сторон грани A тоже делится на 3. (*И. В. Митрофанов*)

10. Пусть A — матрица порядка n с комплексными коэффициентами, собственные значения которой по модулю не превосходят 1. Докажите, что
$$\|A^n\| \leqslant \frac{n}{\ln 2}\|A^{n-1}\|.$$
($\|B\| = \sup_{\|x\|\leqslant 1} \|Bx\|$, где $x \in \mathbb{C}^n$.) (*Ф. В. Петров*)

11. Пусть $a, b > 0$, $M = (a+b)/2$, $G = \sqrt{ab}$. Докажите равенство
$$\int\limits_{-\infty}^{+\infty} \frac{dx}{\sqrt{(x^2+a^2)(x^2+b^2)}} = \int\limits_{-\infty}^{+\infty} \frac{dx}{\sqrt{(x^2+M^2)(x^2+G^2)}}.$$
(*К. Ф. Гаусс*)

12. а) Область между двумя параллельными прямыми раскрашена в 2 цвета. Докажите, что найдётся отрезок длины 1 с концами одного цвета.
(*Л. А. Емельянов*)

б) Область между двумя параллельными плоскостями раскрашена в 4 цвета. Докажите, что найдётся отрезок длины 1 с концами одного цвета.

(*А. Я. Канель-Белов, Д. Черкашин, В. Воронов*)

Уточнение условия

Условие задачи 20.4 (вып. 20, с. 250) было сформулировано неточно. Приводим точную формулировку.

Задача 20.4. Последовательность $\{a_n\}$ называется *линейной рекуррентой порядка* k, если для некоторых $b_1, \ldots, b_k$ при всех $n \geqslant k$ выполняется равенство

$$b_0 a_n + b_1 a_{n-1} + \ldots + b_k a_{n-k} = 0.$$

Пусть $b_0 = 1$, $a_i, b_i \in \mathbb{Z}$ при всех i. Докажите, что либо последовательность $\{a_n\}$ содержит член, имеющий не менее 2016 различных простых делителей, либо $a_n = c_n d^n$ для некоторой периодической последовательности целых чисел $\{c_n\}$ и некоторого целого d.

Дополнение к задаче 6.9

В далёком 1978 году на отборочный тур к Всесоюзной олимпиаде школьников Г. А. Гальпериным была предложена замечательная

Задача. Прожектор освещает угол $2\pi/n$. Дано n точек, в каждой стоит по прожектору. Докажите, что прожекторы можно развернуть так, чтобы они осветили всю плоскость.

В. М. Гальперин (тогда десятикласник) придумал очень красивое решение этой задачи. Позже он вместе с автором задачи написал статью [2].

Эту задачу в дальнейшем обобщил В. В. Произволов, и это обобщение было опубликовано в нашем сборнике (сер. 3, вып. 6, с. 134):

Задача 6.9. Дан выпуклый n-угольник и n точек внутри него. Каждой точке сопоставляется сторона n-угольника (разным точкам — разные стороны) и рассматриваются треугольники, построенные на точках и соответствующих сторонах. Докажите, что можно так установить соответствие, чтобы получившиеся треугольники

а) не перекрывались;

б) покрывали внутренность многоугольника. (*В. В. Произволов*)

Если отправить точки на бесконечность, то как раз получается задача о прожекторах.

Решению обобщённой задачи были посвящены статьи [3, 4]. Очень красивое топологическое решение придумал Р. М. Карасёв. Развитию этой темы посвящена его статья [5] в настоящем сборнике.

Задача В. В. Произволова имеет обобщение и для неевклидовой плоскости — если расположить вершины многоугольника на абсолюте и рассмотреть модель Кэли — Клейна. В то же время Г. А. Гальперину принадлежит принципиально другое обобщение этой задачи, которое и предлагается читателям:

Задача 6.9$'$. Прожектор освещает бесконечный угол величиной в 1 градус. Разрешается располагать произвольным образом любое конечное количество прожекторов на плоскости так, чтобы они осветили целиком всю плоскость. Какое наименьшее число прожекторов потребуется, если это

а) евклидова плоскость;

б) плоскость Лобачевского? (*Г. А. Гальперин*)

Список литературы

[1] *Paterson M. B., Stinson D. R.* Yet another hat game // Electron. J. Combin. 2010. V. 17, № 1. P. 1–12.

[2] *Гальперин В., Гальперин Г.* Освещение плоскости прожекторами // Квант. 1981. № 11. С. 28–30.

[3] *Петров Ф. В., Рукшин С. Е.* Теоремы о покрывающих и непересекающихся треугольниках и их обобщения // Математическое просвещение. Сер. 3. Вып. 8. М.: МЦНМО, 2004. С. 222–228.

[4] *Гальперин Г. А.* Геометрическое решение проблемы В. В. Произволова // Математическое просвещение. Сер. 3. Вып. 8. М.: МЦНМО, 2004. С. 229–236.

[5] *Карасёв Р. Н.* О разбиениях многогранника на выпуклые части // Математическое просвещение. Сер. 3. Вып. 21. М.: МЦНМО, 2017. С. 224–234.

Решения задач из прошлых выпусков

7.7. Условие. W — бесконечное слово (сверхслово), $u \neq v$ — два его различных подслова. Докажите, что имеет место одна из трёх возможностей:

- Существуют такие s и t, что sut — подслово в W, а svt нет.
- Сверхслово W содержит сколь угодно большие участки, свободные от вхождения слова u.
- Некоторая комбинация букв в сверхслове W повторяется более 1000 раз подряд. (*А. Я. Канель-Белов*)

Решение. Первоначальные сведения по комбинаторике слов читатель может найти в замечательной книге [1].

Будем считать, что бесконечное вправо сверхслово U *подчинено сверхслову* W (обозначение: $U < W$), если все подслова конечной длины в U являются также подсловами сверхслова W. Если первая альтернатива задачи не выполняется, то замена любого вхождения u в такое сверхслово U на вхождение v приводит к появлению сверхслова $U' < W$. Рассмотрим теперь следующие случаи.

1) Слово u лексикографически меньше слова v (напомним, что если одно слово — начало другого, то слова лексикографически несравнимы). Тогда замена любого вхождения u на v приводит к лексикографическому увеличению бесконечного вправо сверхслова. Рассмотрим сверхслово U, лексикографически максимальное[1)] среди всех сверхслов, подчинённых W. Тогда в U слово u входить не может и, стало быть, в слове U есть сколь угодно длинные куски, свободные от вхождения u. Поскольку $U < W$, этим же свойством обладает и сверхслово W.

2) Слово u лексикографически больше слова v. Действуем аналогично предыдущему случаю, рассматривая лексикографически минимальное сверхслово $U < W$.

3) $v = ut$ и t — непустое слово. Пусть первая альтернатива задачи не выполняется. Возьмём произвольное n и в слове ut сделаем последовательно

[1)] В решении задачи 2.9 (см. [2]) содержится доказательство существования лексикографически минимального правого сверхслова. Оно без изменений проходит для множества сверхслов, подчинённых слову W, а также с заменой минимальности на максимальность.

n замен u на v. Получим слово $U' < W$, содержащее n-ю степень слова t. Но тогда и W тоже содержит n-ю степень слова t. Поскольку n произвольно, выполняется третья альтернатива задачи.

4) $u = vt$ и t — непустое слово. Если третья альтернатива не выполняется, то найдётся такое $n \geqslant 1$, что vt^n — подслово в W, а слово vt^{n+1} — нет. Поскольку W бесконечно, в него входит подслово $u' = ut^{n-1}t' = vt^n t'$, где t' и t имеют одинаковую длину и $t' \neq t$. При замене u на v возникает подслово $v' = vt^{n-1}t'$. Слова u' и v' имеют общее начало vt^{n-1}, а затем в слове u' стоит t, в слове v' стоит t', не равное t. Поскольку длины слов t и t' равны, эти слова лексикографически сравнимы, но тогда сравнимы v' и u'. Замена u на v приводит к замене u' на v', и мы приходим к первым двум случаям. Задача решена.

Упражнение. Если $uv = vu$, то для некоторого слова s выполняются равенства $u = s^n$, $v = s^m$, где m, n — натуральные числа.

Комментарий. Задача возникла из доказательства совпадения нильрадикала и радикала Джекобсона для мономиальных алгебр (см. [3–5]).

Доказательство существования лексикографически минимального правого сверхслова использует идею *компактности*. (Подробнее см. [6]. Связь с понятием компактности в математическом анализе обсуждается в решении задачи 7.2, см. [7].) Ниже приведён ряд упражнений на эту идею.

1. Пусть $\{v_i\}$ — набор слов неограниченной длины над конечным алфавитом. Тогда найдётся сверхслово V, каждое подслово которого является подсловом одного из слов этого набора.

2. Известно, что человечество бессмертно, но каждый человек смертен и количество людей в каждом поколении конечно. Тогда найдётся бесконечная мужская цепочка, идущая от Адама.

3. Докажите, что хроматическое число графа, если оно конечно, равно максимуму хроматических чисел его конечных подграфов. (*Указание*: см. решение задачи 7.2 в [7].)

4. В парламенте у каждого депутата не более трёх врагов. Докажите, что парламент можно разбить на две палаты так, чтобы у каждого парламентария было не более одного врага в своей палате. (Если A — враг B, то B — враг A.) Для конечного парламента решение см. в [8].

Список литературы

[1] *Саломаа А.* Жемчужины теории формальных языков. М.: Мир, 1986.

[2] Математическое просвещение. Сер. 3. Вып. 6. М.: МЦНМО. 2002. С. 145–147.

[3] *Belov A., Gateva-Ivanova T.* Radicals of monomial algebras // First International Tainan — Moscow Algebra Workshop (Tainan, 1994). Berlin: W. de Greyer, 1996. P. 159–169.

[4] *Белов А. Я., Борисенко В. В., Латышев В. Н.* Мономиальные алгебры // Алгебра-4. Итоги науки и техники. Соврем. матем. и её прил. Темат. обзор. М.: ВИНИТИ, 2002. Т. 26. С. 35–214.

[5] *Belov A. Ya., Borisenko V. V., Latyshev V. N.* Monomial algebras // J. Math. Sci. 1997. V. 87, № 3. P. 3463–3575.

[6] *Канель-Белов А. Я., Трепалин А. С., Ященко И. В.* Олимпиадный ковчег. М.: МЦНМО, 2016. С. 30.

[7] Математическое просвещение. Сер. 3. Вып. 8. М.: МЦНМО. 2002. С. 259–260.

[8] *Канель-Белов А. Я., Ковальджи А. К.* Как решают нестандартные задачи. М.: МЦНМО, 2016. С. 59–60.

(*А. Я. Канель-Белов*)

11.9. Условие. Можно ли множество рациональных точек единичной сферы раскрасить в два цвета (чёрный и белый) так, что если три точки отвечают концам трёх ортогональных векторов, то одна из них будет чёрной, а две другие — белыми? (*Д. Муштари*)

Решение. Рассмотрим решение уравнения $x^2 + y^2 + z^2 = 1$ в рациональных числах. Пусть q есть наименьшее общее кратное их знаменателей. Тогда числа $x' = xq$, $y' = yq$, $z' = zq$ взаимно просты в совокупности и среди них ровно одно нечётное и два чётных. (Рассмотрите остатки по модулю 4.) Следовательно, два вектора (x_1', y_1', z_1') и (x_2', y_2', z_2') могут быть ортогональны, только если разные координаты нечётные, а тройка таких векторов может оказаться попарно ортогональной, только если в одном нечётна координата x', в другом — координата y', в третьем — z'. Красим целочисленные точки с нечётной x'- или y'-координатой в чёрный цвет, а целочисленные точки с нечётной z'-координатой — в белый. Рациональную точку (x, y, z) красим так же, как соответствующую точку (x', y', z'). Получаем искомую раскраску.

Замечание. Отметим, что таким образом раскрасить *все* (а не только рациональные) точки единичной сферы невозможно. См. задачу 10.8.

(*А. Я. Канель-Белов*)

13.5. Условие. Известно, что в любом треугольнике расстояние между центрами O и I описанной и вписанной окружностей выражается через их радиусы R и r с помощью *формулы Эйлера*: $OI^2 = R^2 - 2Rr$. Докажите обобщение этой формулы: если в треугольник вписан эллипс с фокусами F_1, F_2 и малой осью ℓ, то $R^2\ell^2 = (R^2 - OF_1^2)(R^2 - OF_2^2)$.

(*А. А. Заславский*)

Решение 1 обобщает доказательство формулы Эйлера для окружности.

Лемма 1. *Пусть F_1, F_2 — фокусы эллипса, ℓ — длина его малой оси, D_1, D_2 — основания перпендикуляров, опущенных из F_1, F_2 на касательную к эллипсу. Тогда $4D_1F_1 \cdot D_2F_2 = \ell^2$.*

Доказательство. Пусть T — точка касания, a — длина большой полуоси, I — центр эллипса, f — расстояние от фокуса до центра эллипса (таким образом, $\ell^2/4 = a^2 - f^2$), F_1' — точка, симметричная F_1 относительно касательной, см. рис. 1. Тогда $F_1'F_2 = 2a$ по оптическому свойству эллипса [1, с. 13] и ID_1 — средняя линия треугольника $F_1F_2F_1'$. Таким образом, точка D_1 (и аналогично D_2) лежит на окружности с центром I и радиусом a. Поэтому утверждение леммы эквивалентно равенству $D_1F_1 \cdot D_2F_2 = ID_1^2 - IF_1^2$.

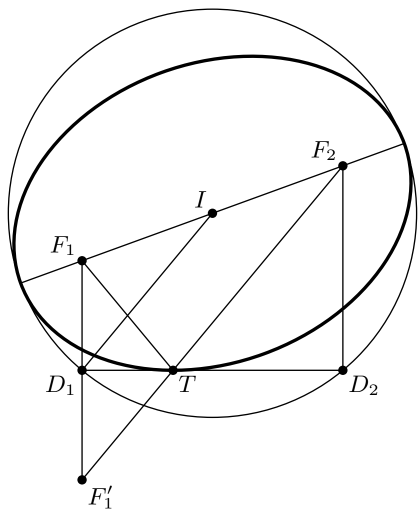


Рис. 1

Пусть теперь I' — проекция точки I на D_1F_1. Тогда

$$ID_1^2 - IF_1^2 = I'D_1^2 - I'F_1^2 = (I'D_1 + I'F_1)(I'D_1 - I'F_1).$$

Множители правой части равны (в том или другом порядке) D_1F_1 и D_2F_2, что и требовалось. □

Лемма 2 (обобщение леммы о трезубце). *Пусть в треугольник ABC вписан эллипс с фокусами F_1, F_2. Пусть O — центр описанной окружности треугольника, L_1, L_2 — точки её пересечения с лучами AF_1, AF_2* (см. рис. 2). *Тогда $F_1L_1 \cdot F_2L_2 = BL_1 \cdot BL_2$.*

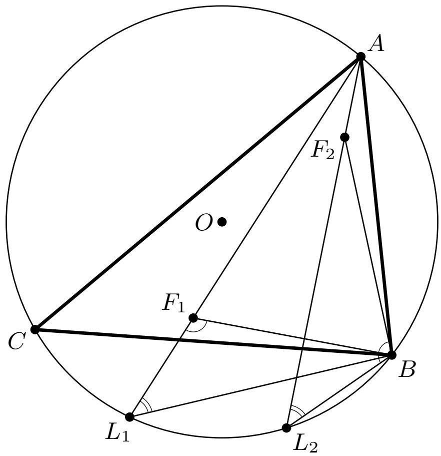


Рис. 2

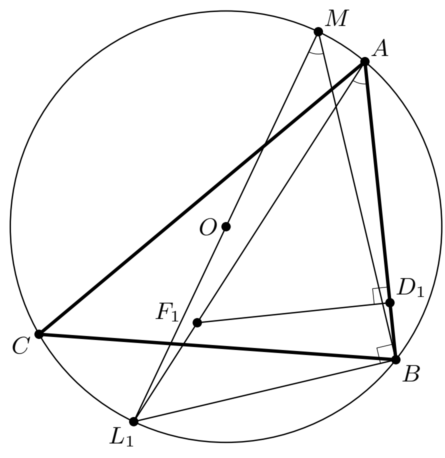


Рис. 3

Доказательство. С учётом изогонального свойства эллипса [1, с. 15],

$$\angle BF_1L_1 = \angle BAF_1 + \angle ABF_1 = \\ = \angle CAF_2 + \angle CBF_2 = \angle CBL_2 + \angle CBF_2 = \angle L_2BF_2.$$

При этом $\angle AL_1B = \angle AL_2B$, так как они опираются на одну и ту же дугу. Значит, $\triangle BF_1L_1 \sim \triangle F_2BL_2$, откуда следует нужное равенство. $\square$

Проведём теперь в описанной окружности диаметр L_1M и опустим из F_1 перпендикуляр F_1D_1 на AB (см. рис. 3). Вписанные углы BML_1 и D_1AF_1 опираются на одну дугу, поэтому прямоугольные треугольники BML_1 и D_1AF_1 подобны. Следовательно, $F_1D_1 : AF_1 = BL_1 : ML_1$, т. е.

$$2R \cdot F_1D_1 = AF_1 \cdot BL_1.$$

Опустив из F_2 перпендикуляр F_2D_2 на AB, аналогично получаем

$$2R \cdot F_2D_2 = AF_2 \cdot BL_2.$$

Применяя леммы 1 и 2, приходим к равенству

$$R^2\ell^2 = AF_1 \cdot F_1L_1 \cdot AF_2 \cdot F_2L_2. \qquad (*)$$

Заметим теперь, что $R^2 - OF_1^2 = (R+OF_1)(R-OF_1)$ — степень (со знаком минус) точки F_1 относительно описанной окружности треугольника ABC, и аналогичное верно для F_2. Поэтому формула из условия задачи равносильна равенству $(*)$. (*А. А. Заславский, Б. Р. Френкин*)

Решение 2. Использование комплексных чисел позволяет не опираться на доказательство для окружности. Пусть ABC — данный треугольник, A', B', C' — точки, симметричные F_1 относительно BC, CA, AB. Из оптического свойства эллипса [1, с. 13] следует, что каждый из отрезков F_2A', F_2B', F_2C' равен большой оси вписанного эллипса.

Будем считать, что описанная окружность треугольника является единичной окружностью комплексной плоскости. Пусть a, b, c, f_1, f_2, a', b', c' — комплексные числа, соответствующие точкам A, B, C, F_1, F_2, A', B', C'. Точки F_1 и F_2 изогонально сопряжены относительно треугольника [1, с. 15], и из формулы Морли [2, с. 94] получаем

$$f_1 + f_2 + abc\overline{f_1 f_2} = a + b + c. \qquad (1)$$

Теперь найдём большую ось эллипса. Например, для точки C' имеем

$$\frac{c' - a}{b - a} = \frac{\overline{f_1} - \bar{a}}{\bar{b} - \bar{a}}.$$

Поскольку $a\bar{a} = b\bar{b} = 1$, получаем

$$F_2C'^2 = (f_2 - c')(\overline{f_2} - \bar{c}') = f_1\overline{f_1} + f_2\overline{f_2} + \\ + \frac{f_1 f_2}{ab} + ab\overline{f_1 f_2} - \left(\frac{1}{a} + \frac{1}{b}\right)(f_1 + f_2) - (a + b)\overline{(f_1 + f_2)} + \frac{a}{b} + \frac{b}{a} + 2.$$

Напишем аналогичные выражения для $F_2A'^2$ и для $F_2B'^2$ и рассмотрим $(F_2A'^2 + F_2B'^2 + F_2C'^2) : 3$. Эта сумма симметрично зависит от a, b, c и, следовательно, может быть выражена через $a + b + c$, $ab + bc + ca$ и abc. Но, используя соотношение (1) и сопряжённое к нему, можно выразить $a + b + c$ и $ab + bc + ca$ через abc. Согласно теореме Понселе большая ось эллипса зависит только от f_1, f_2, поэтому после проведения всех выкладок члены, содержащие abc, уничтожатся и мы получим:

$$F_2C'^2 = (1 - f_1\overline{f_1})(1 - f_2\overline{f_2}) + (f_1 - f_2)(\overline{f_1} - \overline{f_2}).$$

Подставив в это выражение

$$f_1\overline{f_1} = \frac{OF_1^2}{R^2}, \quad f_2\overline{f_2} = \frac{OF_2^2}{R^2}, \quad (f_1 - f_2)(\overline{f_1} - \overline{f_2}) = \frac{F_1F_2^2}{R^2},$$

умножив его на R^4 и вычтя $F_1F_2^2R^2$, получим требуемое равенство.

Примечание. В приведённом решении никак не используется, что в треугольник вписан именно эллипс, а не гипербола. Поэтому формула верна и для гиперболы, если под ℓ подразумевать её мнимую ось.

Список литературы

[1] *Акопян А., Заславский А.* Геометрические свойства кривых второго порядка. М.: МЦНМО, 2011.

[2] *Прасолов В. В.* Рассказы о числах, многочленах и фигурах. М.: Фазис, 1997.

(*А. А. Заславский*)

19.2. Условие. В пространстве произвольным образом расположено несколько многогранников (возможно, пересекающихся). Доказать, что в пространстве можно расположить некоторое множество точек так, чтобы каждый многогранник содержал не менее одной точки внутри себя и чтобы любые два многогранника одинакового объёма содержали внутри себя одно и то же число точек. (*Г. А. Гальперин*)

Решение. Условие задачи можно переформулировать на языке системы линейных уравнений. Занумеруем всевозможные пересечения наших многогранников M_α и их дополнений, имеющих ненулевой конечный объём, числами $i=1, \ldots, k$, и пусть x_i — количество точек в i-м множестве V_i. Каждый многогранник M_α составлен из таких множеств V_i. Поэтому равенство количеств точек в двух многогранниках равного объёма будет выражаться соотношением вида $\sum x_i = \sum x_j$, а условие баланса выразится в виде системы уравнений и неравенств вида

$$\sum_{V_i \subseteq M_{\alpha_k}} x_i = \sum_{V_j \subseteq M_{\beta_k}} x_j, \quad x_i > 0,\ x_j > 0,$$

где $\mathrm{Vol}(M_{\alpha_k}) = \mathrm{Vol}(M_{\beta_k})$.

Указанная система совместна: подставим вместо каждого x_i объём множества V_i — все равенства выполнятся автоматически. Кроме того, все коэффициенты — целые.

Нам, однако, надо найти *целочисленное решение* этой системы. Поскольку система однородна, достаточно найти рациональное решение, поскольку все x_i можно умножить на кратное всех знаменателей. Остаётся воспользоваться следующей леммой.

Лемма. *Если система линейных уравнений и неравенств с рациональными коэффициентами и свободными членами имеет ненулевое решение, то она имеет и рациональное ненулевое решение.*

Доказательство. Если линейное неравенство нестрогое, то множество его решений есть объединение множества решений системы, где оно заменено на уравнение, и другой системы, где оно заменено на строгое неравенство. Таким образом, достаточно рассмотреть случай системы уравнений и строгих неравенств.

Выберем одно уравнение, выразим из него какую-либо переменную и подставим в остальные. Свойство уравнений и неравенств иметь рациональные коэффициенты и свободные члены при этом сохраняется. Проведя спуск по количеству уравнений, либо получим единственное решение системы (и оно рационально), либо приходим к системе строгих неравенств (если их множество пусто, то решением является любая точка пространства).

Если мы имеем решение системы строгих линейных неравенств, то его достаточно малая окрестность также состоит из решений в силу непрерывности линейной функции. Но в этой окрестности найдётся рациональное решение. □

Замечание 1. Похожим образом решается следующая классическая задача. *В стаде* 101 *корова. Если удалить любую, то стадо можно разбить на* 2 *стада по* 50 *коров равной массы. Доказать, что веса всех коров равны.*

Замечание 2. Одномерный случай рассматриваемой задачи используется в одном из решений *третьей проблемы Гильберта*: *доказать, что куб и правильный тетраэдр неравносоставленны.*

(*А. Я. Канель-Белов*)

20.1. Условие. Частица движется по прямой линии, при этом направление движения может меняться. В каждый момент времени ускорение частицы не превосходит 1 м/с^2 по абсолютной величине. Через одну секунду после начала движения частица вернулась в начальную точку. Докажите, что её скорость через 0,5 с после начала движения не превосходит 0,25 м/с.

(*А. Колчев*)

Решение. Пусть все промежутки времени выражены в секундах, а промежутки длины — в метрах. Пусть $\nu(T)$ — скорость, $a(t)$ — ускорение частицы в каждый момент времени. По условию задачи $|a(t)| = |\nu'(t)| \leqslant 1$ и $\int_0^1 \nu(t)\,dt = 0$. Требуется оценить $\nu(0{,}5)$.

Рассмотрим модуль этой величины:

$$|\nu(0{,}5)| = |\nu(0{,}5) - 0| = \left|\nu(0{,}5)\int\limits_0^1 dt - \int\limits_0^1 \nu(t)\,dt\right| = \left|\int\limits_0^1 (\nu(0{,}5) - \nu(t))\,dt\right|.$$

Используем теорему Лагранжа:

$$\nu(0{,}5) - \nu(t) = \nu'(c(t)) \cdot (0{,}5 - t),$$

где $c(t) \in [0{,}5; t]$. Отсюда

$$|\nu(0{,}5)| = \left|\int\limits_0^1 \nu'(c(t)) \cdot (0{,}5 - t)\right| dt \leqslant \int\limits_0^1 |\nu'(c(t)) \cdot (0{,}5 - t)|\, dt =$$

$$= \int\limits_0^1 |\nu'(c(t))| \cdot |(0{,}5 - t)|\, dt.$$

Но $|\nu'(t)| \leqslant 1$. Следовательно,

$$|\nu(0{,}5)| \leqslant \int\limits_0^1 |0{,}5 - t|\, dt = \int\limits_0^{0{,}5} (0{,}5 - t)\, dt + \int\limits_{0{,}5}^1 (t - 0{,}5)\, dt = \frac{1}{4}.$$

(*А. Колчев*)

Опечатки, замеченные в выпуске 20

Страница,	строка	Напечатано	Следует читать
241,	18 сверху	возбужения	возбуждения
266,	14 снизу	последним	предпоследним
269,	задача 2.8	6, 2–145	6, 142–145

Информация для авторов

1. Сборник «Математическое просвещение» предназначен для широкого круга математиков-исследователей и преподавателей, а также студентов, старшеклассников и всех, кто интересуется математикой. Издание публикует материалы по различным областям математики, а также по вопросам её истории и преподавания, интересные и доступные указанной аудитории.

2. Сборник «Математическое просвещение» не имеет возможности публиковать статьи, содержащие существенно новые научные результаты, оценка которых доступна лишь специалистам в данной области математики. Он также не публикует материалы по текущим вопросам преподавания математики в школе и вузах.

3. Сборник выходит, как правило, 1 раз в год, весной. Редакция просит авторов представлять материалы по электронной почте на адрес `matpros@mccme.ru` или `matpros@ya.ru` в виде двух файлов `pdf` и `tex` (с дополнительными файлами рисунков и т. п., если требуется). Допускается присылка статей, набранных в Ворде.

4. Просим обратить внимание, что материалы принимаются в чёрно-белом исполнении.

5. Редакция благодарна авторам за оформление ссылок на литературу аналогично опубликованным выпускам сборника, см. `http://www.mccme.ru/free-books/matpros.html`

6. В конце статьи необходимо указать для каждого автора:

1) имя, отчество (если есть), фамилию;
2) место работы/обучения;
3) электронный адрес для дальнейшей переписки.

7. Авторы опубликованных статей имеют право на 2 экземпляра сборника каждый. О порядке передачи экземпляров можно обращаться на `matpros@mccme.ru` или `matpros@ya.ru`

Издательство Московского центра
непрерывного математического образования

119002, Москва, Большой Власьевский пер., 11. Тел. (499) 241–08–04.

Отпечатано в ООО «Типография „Миттель-Пресс“».
г. Москва, ул. Руставели, д. 14, стр. 6.
Тел./факс +7 (495) 619–08–30, 647–01–89.
E-mail: mittelpress@mail.ru

Подписано в печать 14.03.2017 г. Формат 70×100 $^1/_{16}$. Бумага офсетная.
Печать офсетная. Печ. л. 18. Тираж 1000 экз. Заказ №