МАТЕМАТИЧЕСКОЕ ПРОСВЕЩЕНИЕ

Третья серия

выпуск 12

Москва
Издательство МЦНМО
2008

УДК 51.009
ББК 22.1
М34

Издание осуществлено при поддержке РФФИ
(*издательский проект* № 07-01-07056).

РФФИ

Редакционная коллегия

Бугаенко В. О.	Винберг Э. Б.	Вялый М. Н.
Гальперин Г. А.	Глейзер Г. Д.	Гусейн-Заде С. М.
Дориченко С. А.	Егоров А. А.	Ильяшенко Ю. С.
Канель-Белов А. Я.	Константинов Н. Н.	Прасолов В. В.
Розов Н. Х.	Сосинский А. Б.	Тихомиров В. М.
Френкин Б. Р.	Ященко И. В.	

Главный редактор: Э. Б. Винберг Отв. секретарь: М. Н. Вялый

Адрес редакции:
119002, Москва, Б. Власьевский пер., д. 11, к. 301
(с пометкой «Математическое просвещение»)
Email: matpros@mccme.ru Web-page: www.mccme.ru/free-books

М34 **Математическое просвещение.** Третья серия, вып. 12. —
М.: МЦНМО, 2008. — 240 с.
ISBN 978-5-94057-354-8

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

УДК 51.009
ББК 22.1

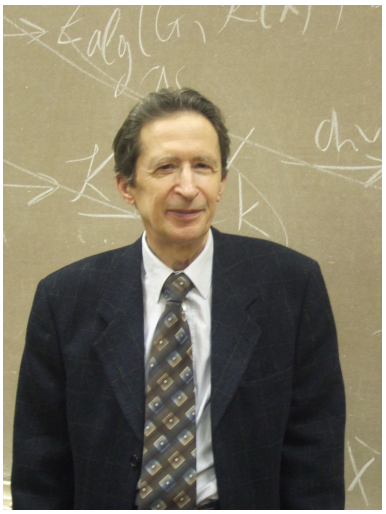
Фотографии на с. 3 сделаны С. Третьяковой (левые)
и А. Зобниным (правая)

ISBN 978-5-94057-354-8

© МЦНМО, 2008.

Поздравляем

Владимира Игоревича Арнольда



Эрнеста Борисовича Винберга

Алексея Брониславовича Сосинского

с 70-летием!

Содержание

Нам пишут

Задачный раздел

Математический мир

Лазарь Аронович Люстерник и его стихи

В. М. Тихомиров

Лазарь Аронович Люстерник (1899–1981) был выдающимся математиком, одним из плеяды московских математиков, начинавших творческую жизнь в конце десятых — начале двадцатых годов прошлого века. Он принадлежал ко второму поколению учеников Николая Николаевича Лузина, в которое входили еще Нина Карловна Бари и Михаил Алексеевич Лаврентьев.

Лазарь Аронович был глубоко и разносторонне талантливым человеком. Прежде всего, разумеется, в математике, где им были получены многочисленные фундаментальные результаты.[1)] Но помимо математической одаренности, Лазарь Аронович замечательно владел словом и пером, был великолепным рассказчиком, автором интересных воспоминаний о молодости московской математической школы.

Лазарь Аронович был большим знатоком поэзии и сам любил одаривать друзей и знакомых своими стихами, в которых всегда присутствовали легкость и веселость. Он был мастером застольной беседы, и в памяти современников сохранились многие его экспромты, передаваемые из уст в уста. Следующую эпиграмму Люстерника мне довелось слышать неоднократно.

Дело происходило в Казани, в 1942 году. Часто случается так, что в какой-то организационной структуре очень важную роль играют люди, ведающие хозяйственной частью. В ту пору в администрации Академии наук СССР (которая эвакуировалась в Казань) какой-то видный хозяйственный пост занимал человек, которого звали Ной Соломонович Гозенпуд. Ему Лазарь Аронович посвятил такие строки:

[1)] Вкладу Люстерника в теорию экстремума посвящена моя статья в пятом томе «Математического просвещения» за 2001 г.

Я высокой чести удостоен.
Не забыть торжественных минут:
Я предстал сегодня перед Ноем
Соломоновичем Гозенпуд.

У меня до сих пор в ушах стоит crescendo в исполнении П. С. Александрова: «Я предстал сегодня **перед НОЕМ**. . . »

А вот как описывает Л. А. Люстерник свое вхождение в лузинский математический мир, в круг математиков, известный под именем Лузитании:

Суровый двадцать первый год,
В научный двинулись поход. . .
Московский университет. . .
Хоть я пока и очень молод,
Хоть в полушубок я одет,
Но. . . брр. . . Какой собачий холод. . .
Каток в пустынном коридоре,
Горячие здесь только споры.

Примкнул с доверием безумным
Я к группе молодой и шумной.
Презрев классический анализ,
Здесь современным увлекались.
Пусть твой багаж не очень грузен —
Вперед! В себе уверен будь!
Великий бог — профессор Лузин —
Укажет нам в науке путь!

А далее вместе с учеником Д. Ф. Егорова Иваном Ивановичем Привaловым, примкнувшим к лузинскому направлению, выразительно характеризуются четверо из пятерых лузинских учеников первого поколения (не упомянут Михаил Яковлевич Суслин, скончавшийся в 1919 году):

А божество уж окружало созвездие полубогов:
Иван Иванович Привалов,
Димитр Евгеньевич Меньшов,
И Александров остро взвинчен,
И милый Павлик Урысон,
И философствующий Хинчин
И несколько других персон.

И далее:

Дни легендарной Лузитании,
Дни увлечений и исканий. . .

Мы в Лузина все влюблены,
К нему ревнуем мы друг друга.
Блеснуть хоть маленькой должны
Математической заслугой.
Я вспоминаю: каждый раз
Волнение тебя охватит,
Когда придешь в урочный час
В его квартиру на Арбате.

Очень рекомендую прочесть воспоминания Люстерника о молодости московской математической школы, опубликованные в журнале «Успехи математических наук», в томе XX, №3 за 1965 год и томе XXII №№1, 2 и 4 за 1967 год (откуда я позаимствовал строки его стихов).

Увы, все прекрасное когда-нибудь кончается. Вот как об этом сказал Лазарь Аронович:

А дальше все как будто просто —
Процесс естественного роста,
Тематика все расширялась,
Своей дорогой каждый шел —
И школа Лузина распалась
На ряд блестящих новых школ.

Из песни слова не выкинешь. Далее идут строчки:

Но был мучительно тяжелым
Процесс распада этой школы.

В вихре безумного времени — в середине тридцатых годов — некоторые ученики Лузина вели себя по отношению к нему недостойно.

Но не буду бередить старые раны. Никто из верных учеников Лузина не бросил камня в Люстерника. Через год после смерти Лузина вышел том, в котором были собраны работы Лузина по метрической теории функций. В этом томе Лазарь Аронович (который никогда не развивал лузинские темы) вместе с Ниной Карловной Бари, самой преданной ученицей Лузина, написал обзор лузинского творчества в этой ветви теории функций. Это можно воспринимать как покаяние.

* * * * * *

Весной 2007 года супруга Марка Иосифовича Вишика — ученика и близкого друга Лазаря Ароновича — Ася Моисеевна ознакомила меня с басней, написанной Л. А. Люстерником, по-видимому, где-то в середине шестидесятых годов. При этом было выражено пожелание, чтобы эта басня была опубликована. Редколлегия «Математического просвещения» предоставила место для опубликования, а я счел за благо привести еще некоторые строки из поэтического наследия замечательного человека —

Лазаря Ароновича Люстерника. А в качестве комментария современника событий, живо и точно описываемых в басне, я считаю долгом памяти заметить, что *именно второму* из двух ее героев мы обязаны тому, что писать подобные сочинения, не опасаясь за собственную жизнь, вообще оказалось возможным.

Басня

Л. А. Люстерник

Правителем в одном лесном массиве
Был мудрый Лев, жестокий и спесивый.
Зверье — от волка до певучей птахи —
Все жили в почитании и страхе.

Шли годы, и, состарясь, одряхлев,
Навек почил наш величайший Лев.
В последний путь владыку проводив,
Ждал нового вождя лесной массив.

Так, после шумных драк и бурных споров,
В правители был избран Боров.
И начал он с того, что влезши на пенек,
Покойного изматерил и вдоль, и поперек
В своей пространной речи.

Что будто Лев, от власти опьянев,
Не одного убил и покалечил,
Что будто все звериные заслуги
Себе присваивал, себя лишь восхвалял,
Что запустил дела во всей округе,
Что вообще он плохо управлял.

Стал Боров наводить порядки:
Объездил лес и дальние посадки,
Собрал затем он всю зверячью молодь
И бросил клич: «А ну-ка все на желудь!»

И звери, угодить ему дабы,
В лесу сажали лишь дубы.

Признаться надо, кроме желудей,
Правитель много выдвигал идей.
И хоть от них бывало мало толку,
«Ура!» ему кричали без умолку.

Зазнался постепенно толстый Боров,
Чуть ли не львиный проявляя норов.
С Лисой, министром иностранных дел,
Он не считался, слушать не хотел.

Медведь финансами ворочал, дело знал,
Но слишком часто на него ворчал —
Медведя вон! И так конца не видно...

К тому же стало всем обидно,
Что самая паршивая свинья
Считалася других умней и даровитей,
И норовила быть вершителем событий
Лишь потому, что Борову родня.

И вот, собравшись духом как-то раз,
Все сильные того лесного края
Изгнали Борова в запас.
И власть окончилась свиная.

Рядили эту новость вкривь и вкось
В самом лесу и за его пределом.
Прижать свиней — оно святое дело,
А то их, право, много развелось.

Но кто же твердо может поручиться,
Что вновь история не повторится,
Что новый власть имущий, осмелев,
Не рыкнет грозно, как покойный Лев,
Что он, как Боров вдруг не хрюкнет,
Когда ему седьмой десяток стукнет.

У этой басни нет морали:
Мораль давно перемарали.

В. М. Тихомиров, механико-математический факультет МГУ

Аттракторы динамических систем и философия общего положения

Ю. С. Ильяшенко

Мы повсюду видим эволюционные процессы, от движений атомов до динамики планет. Ньютон понял, что эти процессы описываются дифференциальными уравнениями и что эти уравнения полезно решать. За последующие 150 лет было понято, что большинство дифференциальных уравнений решить невозможно. Пуанкаре создал новую ветвь математики — качественную или геометрическую теорию дифференциальных уравнений. Она изучает геометрические свойства решений, непосредственно используя свойства правой части уравнения. Оказалось, что даже качественное поведение решения может быть очень сложным. Ситуация резко упрощается, если рассматривать только уравнения общего положения. С точки зрения физики, лишь последние и представляют интерес.

Исследование динамических систем можно условно разбить на три периода.

Период Ньютона: *дано дифференциальное уравнение. Решить его.*

Период Пуанкаре: *дано дифференциальное уравнение. Описать свойства его решений, не решая уравнение, а лишь используя свойства правой части.*

Период Андронова: *Не дано никакого дифференциального уравнения. Описать свойства его решений.*

Последнее высказывание звучит парадоксально. Однако важнейшие свойства дифференциальных уравнений *общего положения* на плоскости — всегда одни и те же. Эти свойства рассмотрены ниже и относятся к *предельному поведению* всех решений. Следовательно, чтобы узнать это поведение, нужно лишь убедиться, что уравнение — общего положения. Ниже показано, как это сделать на физическом уровне строгости. В размерности выше двух возникает сходная, но более сложная ситуация. Обсуждению этих тем и посвящена статья.

Yu. I. Ilyashenko, “Attractors of dynamical systems and philosophy of generic position”. Публикуется с любезного разрешения автора. Перевод Б. Р. Френкина.

Законы эволюции и дифференциальные уравнения. Рассмотрим некоторую физическую систему — скажем, искусственный спутник в гравитационном поле Земли или Солнечной системы (Солнца и планет). В каждый момент времени *состояние* этой системы описывается конечным количеством числовых параметров: $x_1, \dots, x_n$. Для спутника состояние определяется *положением и скоростью*, т. е. количество параметров равно шести: три координаты положения в пространстве и три компоненты вектора скорости. Множество этих параметров можно рассматривать как точку x в многомерном пространстве $\mathbb{R}^n$. *Закон эволюции* указывает, как меняется состояние системы; скорость этого изменения зависит только от состояния. Для спутника скорость изменения состояния (так называемая *фазовая скорость*) состоит из скорости и ускорения движения спутника. Отметим, что скорость движения не следует смешивать с фазовой скоростью. Итак, для каждого состояния x определяется такой вектор фазовой скорости $v(x)$, что производная от x по времени, которая обозначается $\dot{x}$ (то же самое, что $\frac{dx}{dt}$), удовлетворяет уравнению

$$\dot{x} = v(x). \tag{1}$$

Решить это уравнение — означает указать, каково будет состояние системы $x(t)$ в момент времени t. Чтобы сделать это однозначно, нужно лишь знать начальное состояние $x(0)$. Это утверждение называется *теоремой существования и единственности* решений дифференциальных уравнений.

Лапласовский детерминизм. Ньютон первым понял, что эволюционные процессы во Вселенной описываются дифференциальными уравнениями. Лаплас осознал, что теорема существования и единственности имеет философские следствия. Он выразил эту идею в следующих прекрасных словах:

«Разум, который для какого-нибудь момента знал бы все силы, действующие в природе, и относительное расположение ее составных частей, если бы он, кроме того, был достаточно обширен, чтобы подвергнуть эти данные анализу, обнял бы в единой формуле движения самых огромных тел во вселенной и самого легкого атома; для него не было бы ничего неясного, и будущее, как и прошлое, было бы у него перед глазами.» (Цит. по: С. Лаплас, «Изложение системы мира». Л.: Наука, 1982, с. 364–365.)

Геометрическая точка зрения на дифференциальные уравнения. Никто еще не написал дифференциальное уравнение, о котором мечтал Лаплас. Вернемся теперь на землю и рассмотрим простейшие примеры дифференциальных уравнений *с геометрической точки зрения*. Когда изменяется время, состояния системы $x(t)$ проходят кривую в фазовом

пространстве, которая называется *фазовой кривой* или *орбитой* уравнения (1). С точки зрения геометрии, найти орбиту — значит решить следующую задачу: *по данному векторному полю v и точке x_0 найти такую кривую в фазовом пространстве, что x_0 ей принадлежит и каждая точка x кривой — касательная к заданному вектору $v(x)$.*

Примеры. Радиальное поле. Если $v(x) = x$, то все орбиты (с единственным исключением) — открытые лучи, исходящие из нуля. Исключением является орбита $x(t) \equiv 0$. Она состоит только из нуля и называется *особой точкой* или *положением равновесия*.

Поворот на прямой угол. В этом примере x принадлежит плоскости, $v(x) = Ix$, что означает вектор x, повернутый на $\frac{\pi}{2}$. Орбиты этого поля — окружности с центром в нуле, а также положение равновесия (нуль).

Пуанкаре первым понял, что, вообще говоря, орбиты векторного поля можно описать геометрически, исходя из геометрии самого векторного поля $v(x)$.

Предельное поведение решений. Когда мы включаем электронное устройство, проходит короткое время, пока система пройдет переходный период и войдет в стационарный режим (который, вообще говоря, не является положением равновесия). Но этот переходный период краток лишь с точки зрения человека. Внутренние изменения в системе происходят очень быстро, так что ее «внутреннее время» очень быстро течет, и с точки зрения системы этот короткий переходный период очень велик (практически бесконечен). Поэтому стационарный режим можно охарактеризовать как *предельное поведение* решения.

Теорема Пуанкаре – Бендиксона. Для дифференциальных уравнений на плоскости задача о предельном поведении решений может быть решена в чисто геометрической постановке. Пусть плоскость разбита на гладкие кривые, которые не пересекаются попарно и сами с собой, причем кривая меняется гладко вместе с «начальной точкой», через которую она проходит. Пусть при этом все орбиты системы входят в некоторый большой круг и остаются там; такая система называется *диссипативной*. Для физических систем это соответствует некоторому предположению о *рассеянии энергии*. Тогда для предельного поведения любой кривой из этого семейства возможны следующие варианты:

a) орбита входит в состояние равновесия,

b) орбита обматывается вокруг замкнутой орбиты,

c) орбита обматывается вокруг многоугольника, образованного состояниями равновесия и орбитами, которые их соединяют (они называются *сепаратрисами* или *сепаратрисными связками*). Случаи a), b) и c) показаны на рис. 1.

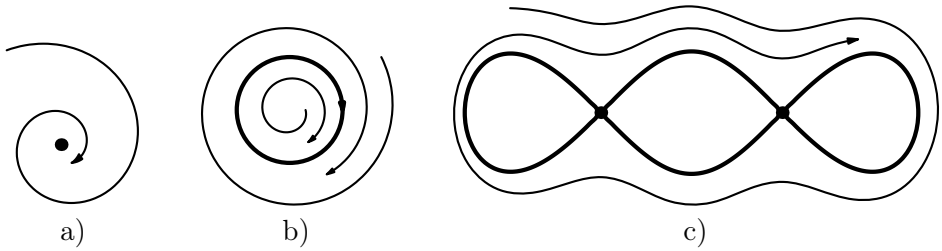


Рис. 1. *Плоские ω-предельные множества*

Такая классификация непосредственно вытекает из известной *теоремы Пуанкаре – Бендиксона*, которая стала одним из крупнейших успехов топологического подхода к дифференциальным уравнениям.

Общее положение Поведение, описанное выше, не очень сложно, но и не очень просто. Предельные множества типа c) могут быть сложными. Положение спасает тот факт, что *тип c) — не общего положения*, а потому не должен возникать в системах физического происхождения. Говоря подробнее, если процесс не подчинен никакому закону сохранения или соотношению симметрии, то следует ожидать, что для системы (1), моделирующей этот процесс, не выполняется никакое условие типа *равенства*.

Например, линейные операторы, естественно связанные с уравнением (1) (скажем, линеаризация поля в положениях равновесия или производная отображения Пуанкаре) не должны иметь собственных значений, равных 0 или 1 по абсолютной величине. Особые точки дифференциальных уравнений общего положения на плоскости могут быть только трех типов: a) сёдла, b) узлы, c) фокусы, см. рис. 2.

Что более важно, *векторное поле общего положения на плоскости не имеет седловых связок*. Действительно, любую связку между двумя седлами можно разрушить малым возмущением, см. рис. 3. Наивное представление о *свойствах общего положения* было формализовано Р. Томом в форме *теоремы трансверсальности*. Том был одним из создателей *тео-*

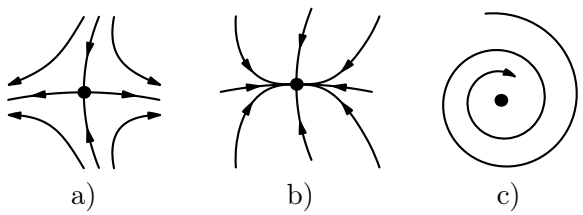


Рис. 2. *Особые точки общего положения на плоскости*

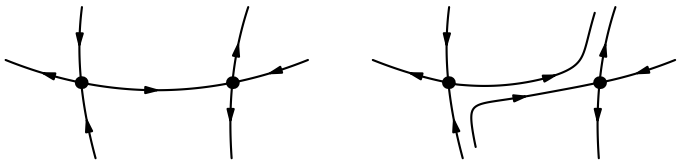


Рис. 3. *Седловая связка и ее разрушение*

рии катастроф, которая изучает и классифицирует особенности систем, находящихся в общем положении.

Теорема Андронова Как следствие предыдущих рассмотрений, Андронов получил следующую теорему:

Физический процесс без симметрий и законов сохранения, моделируемый плоской диссипативной системой, имеет конечное количество предельных режимов для решений. Каждый из этих режимов либо является положением равновесия, либо периодичен.

Действительно, предельными режимами могут быть только положения равновесия или периодические траектории: вариант с), как уже сказано выше, требует наличия седловой связки и потому невозможен для типичного поля. При этом для типичного поля вдоль любой периодической траектории отображение Пуанкаре имеет производную, отличную от единицы (то есть любая периодическая траектория либо притягивает, либо отталкивает). Как следствие, в достаточно малой окрестности такой траектории не содержится других периодических траекторий. Все особые точки типичного векторного поля — сёдла, узлы и фокусы, поэтому в достаточно малой окрестности любой из них также нет ни других положений равновесия, ни (не выходящих за эту окрестность) периодических траекторий.

С другой стороны, все предельные режимы сосредоточены в поглощающем круге из определения диссипативности. Если их бесконечно много, они должны куда-то накапливаться, что противоречит только что сказанному. Поэтому предельных режимов (как положений равновесия, так и периодических траекторий) может быть лишь конечное число.

Мечта середины века. В середине прошлого века некоторые специалисты мечтали обобщить теорему Андронова на случай высших размерностей. А именно, они ожидали, что в предыдущем утверждении можно заменить «плоский» на «многомерный». В конце 50-х годов Смейл опубликовал эту гипотезу вместе с подробным описанием, как должна выглядеть динамическая система общего положения на компактном многообразии. Описанные им системы ныне составляют важный класс и называются

системами Морса – Смейла. Однако оказалось, что они не общего положения.

Как только появилась статья Смейла, специалисты старшего поколения сообщили ему, что в статьях Картрайта, Литлвуда и Левинсона были построены динамические системы *с бесконечным количеством периодических орбит*, причем это свойство выдерживает малые возмущения.

С тех пор вопрос о том, *каковы свойства динамических систем общего положения*, является одним из главных в этой области. Он породил множество достижений, но всё еще остается нерешенным в полной общности. Один из его частных случаев приведен в конце этой статьи.

Подкова Смейла. Вместо того, чтобы изучать работы предшественников, довольно длинные и сложные, Смейл попытался понять, как вообще могло случиться, что динамическая система может устойчиво иметь счетное количество периодических орбит? Бродя вдоль пляжа Копакабана в Рио, он придумал простой ответ, впоследствии назвнный *подкова Смейла*.

Со времен Пуанкаре было понятно, что дифференциальные уравнения и итерации отображений — ветви одной и той же теории. Поэтому ответ Смейла формулируется в терминах двумерных отображений. Отображение подковы Смейла f строится как композиция отображений прямоугольника, показаных на рис. 4 и описанных ниже.

Отображение f_1 сжимает заштрихованный прямоугольник D в горизонтальном направлении и растягивает в вертикальном. Отображение f_2 сгибает растянутый прямоугольник в подкову. Отображение f_3 передвигает подкову так, чтобы она пересекла D, как показано на рисунке.

Это отображение имеет бесконечное количество периодических орбит и другие замечательные свойства, устойчивые относительно малых возмущений.

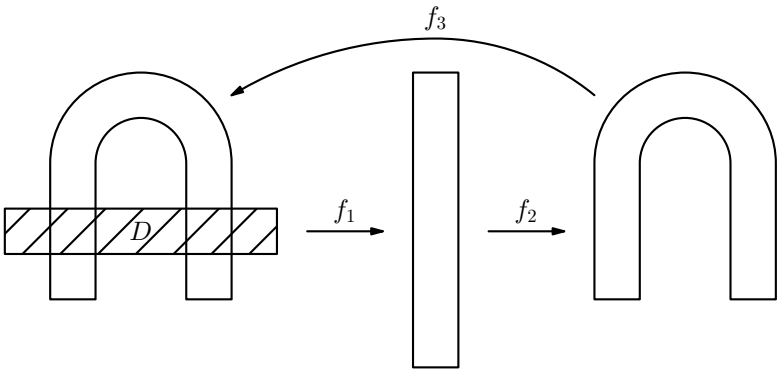


Рис. 4. *Подкова Смейла*

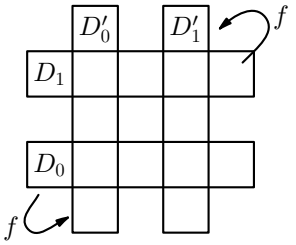


Рис. 5. *Упрощенная подкова Смейла*

На рис. 5 показан еще более простой вариант, который также называют подковой Смейла. Возьмем единичный квадрат и разобьем его на пять равных горизонтальных прямоугольников. Пусть D_0 и D_1 — соответственно второй и четвертый прямоугольник снизу. Разобьем тот же квадрат на пять равных вертикальных прямоугольников. Пусть D'_0 и D'_1 — второй и четвертый прямоугольник слева. Положим $D = D_0 \cup D_1$, $D' = D'_0 \cup D'_1$, и пусть f — отображение, которое сжимает D_j в 5 раз по горизонтали, растягивает в 5 раз по вертикали и параллельно переносит на место D'_j $(j = 0, 1)$. Таким образом, f — кусочно аффинное отображение, заданное одной формулой на D_0 и другой — на D_1. Отображение f можно продолжить до диффеоморфизма сферы, но нас интересует ограничение этого диффеоморфизма на D, которое уже определено выше. Если, соответственно, все итерации отображения f корректно определены в некоторой точке $x \in D$ и принадлежат D, то мы говорим, что x обладает *полной орбитой* относительно f. Множество всех точек с полной орбитой обозначается Λ. *Оказывается, $\Lambda = C' \times C'$ — декартово произведение двух канторовых множеств.*

Для любой точки $x \in \Lambda$ можно определить ее *судьбу* как двустороннюю последовательность из нулей и единиц:

$$\omega = \ldots\omega_{-n}\ldots\omega_{-1}\omega_0\ldots\omega_n\ldots$$

А именно, $\omega_n = j \Leftrightarrow f^n(x) \in D_j$. Оказывается, *любую последовательность из нулей и единиц можно реализовать как судьбу одной и только одной точки.*

Как следствие получаем, что любая точка, судьба которой — периодическая последовательность, сама периодична. Поскольку существует бесконечное количество периодических последовательностей, f имеет бесконечное количество периодических точек.

Чувствительность к начальным условиям и опровержение лапласовского детерминизма. Элементарный анализ отображения подковы Смейла показывает, что для любой пары точек $x, y \in \Lambda$, с точностью

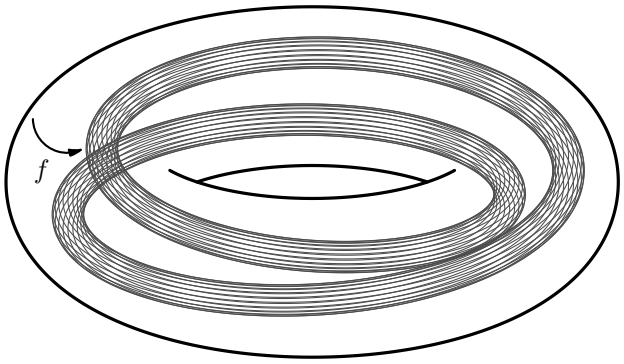


Рис. 6. *Соленоид Смейла – Вильямса*

до 5^{-n} совпадающих, их судьбы совпадают на первых n шагах (как вперед, так и назад). После этого их судьбы могут различаться произвольным образом, как если кто-то бросает монету. Расстояние между точками орбит после этих n шагов будет порядка 1. Этот эффект называется *чувствительностью к начальным условиям*.

В двух последовательных опытах с реальными физическими системами невозможно достичь идеального совпадения начальных условий. Малая, физически пренебрежимая ошибка через довольно короткое время приведет к резкому различию между орбитами. Значит, *невозможно предсказать долговременное поведение решений динамических систем с чувствительностью к начальным условиям*.

Странные аттракторы. Недостаток предыдущего примера в том, что «почти все» точки из D не имеют полных орбит относительно отображения подковы Смейла. Смейл и Вильямс построили отображение полнотория D в себя, см. рис. 6, со следующими свойствами:

– для всех точек полнотория корректно определены орбиты в направлении вперед;

– эти орбиты притягиваются к множеству $\Lambda \subset D$, которое называется *соленоидом*;

– динамика на соленоиде сходна с отображением подковы Смейла; в частности, имеется чувствительность к начальным условиям и бесконечное количество периодических орбит.

Все эти свойства устойчивы относительно малых возмущений.

Соленоид Смейла – Вильямса дает пример *странного аттрактора*, который резко отличается от притягивающей особой точки или периодической орбиты.

Разные типы аттракторов: совпадают ли они в случае общего положения? Любая диссипативная динамическая система имеет притягивающее множество — *максимальный аттрактор*, — к которому приближаются все орбиты. Но это множество может быть слишком большим: в численных экспериментах наблюдатель видит лишь его небольшую часть, *вблизи которой почти все орбиты проводят почти всё время*. Это множество называется *статистическим аттрактором*. Пример приведен на рис. 7.

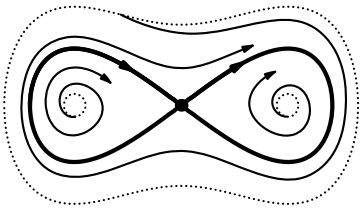


Рис. 7. *Несовпадение максимального и статистического аттракторов*

В этом примере максимальный аттрактор — восьмеркообразная фигура, а статистический — седловая точка. Но этот пример — не общего положения: имеются две седловые связки, которые можно разрушить малыми возмущениями.

Следующая проблема далека от решения: *верно ли, что в случае общего положения максимальный и статистический аттракторы совпадают*? Точнее, *верно ли, что для динамической системы общего положения f статистический аттрактор A становится максимальным, если ограничить f на некоторую окрестность аттрактора A*?

Дальнейшая информация.

По плоским динамическим системам:

А. Андронов, А. Витт, С. Хайкин. *Теория колебаний*. М.: Физматгиз, 1959.

По странным аттракторам и чувствительности к начальным условиям:

D. Ruelle, F. Takens. *On the nature of turbulence* // Commun. Math. Phys., 1971. Vol. 20. P. 167–192.

J. Palis, W. de Melo. *Geometric theory of dynamical systems*. Berlin, Heidelberg: Springer, 1982.

По свойствам динамических систем общего положения и по теории катастроф:

A. Katok, B. Hasselblatt. *Introduction to the modern theory of dynamical systems*. Cambridge, 1994.

V. Arnold. *Catastrophe theory*. Springer Encyclopaedia in Math., vol. 5, 1994.

По различным типам аттракторов:

J. Milnor. *On the concept of attractor* // Commun. Math. Phys., 1985. Vol. 99, no. 2. P. 177–196.

A. Gorodetski, Yu. Ilyashenko. *Minimal and strange attractors* // International Journal of Bifurcation and Chaos, 1996. Vol. 6, no. 6. P. 1177–1183.

Ю. С. Ильяшенко, Cornell University, USA; МГУ и НМУ; МИРАН, Москва

Размышления об исследовательских задачах для школьников*

А. Б. Скопенков†

Введение. Эта заметка содержит некоторые соображения об исследовательской работе школьников по математике, а также информацию о конкретном опыте. Здесь говорится о *научно*-исследовательской работе, хотя исследовательские задачи можно использовать также и при *обучении*.

Я привожу ссылки на некоторые удачные работы школьников и рекомендации, как найти задачу для исследования, как подготовить работу и доклад, в каких конференциях школьников участвовать; сформулированы общие *требования* к работам. Естественно, я даже не пытаюсь дать ответ на главный вопрос: как решать задачу [13].

Большинство приводимых соображений не оригинально. Однако опыт автора говорит о необходимости еще раз высказать эти соображения.

Благодарю В. Д. Арнольда, М. Н. Вялого, Н. Н. Константинова, В. М. Тихомирова, Д. В. Трещева и Б. Р. Френкина за полезные обсуждения.

Постановка проблемы. Многим школьникам интересно решать исследовательские задачи, в которых конечный результат может быть даже неизвестен изначально, а естественно появляется в процессе работы. Такой интерес полезно поддерживать и развивать — это одна из форм развития творческих способностей, которая для многих школьников может оказаться наиболее удачной. Кроме того, обычно ученику интереснее изучать теорию в том случае, когда он сразу же применяет ее к конкретным задачам.

Сравнительно недавно стала разрабатываться технология приучения школьников к творческой работе в области математики, когда им даются «исследовательские задачи». Исследовательские задачи полезны для

*Полный обновляемый текст находится по адресу:
www.mccme.ru/circles/oim/issl.pdf

†Частично поддержан Российским Фондом Фундаментальных Исследований, Гранты номер 05-01-00993, 07-01-00648a и 06-01-72551-NCNILa, Грантами Президента РФ НШ-4578.2006.1 и МД-4729.2007.1, а также стипендией П. Делиня, основанной на его Премии Бальзана 2004 года.

творческого развития школьников, для учителей и даже для самой математики.

We should not forget that the solution of any worthwhile problem very rarely comes to us easily and without hard work; *it is rather the result of intellectual effort of days or weeks or months. Why should the young mind be willing to make this supreme effort*? *The explanation is probably the instinctive preference for certain values*, *that is*, *the attitude which rates intellectual effort and spriritual achievement higher than material advantage. Such a valuation can be only the result of a long cultural development of environment and public spirit which is difficult to accelerate by governmental aid or even by more intensive training in mathematics. The most effective means may consist of transmitting to the young mind the beauty of intellectual work and the feeling of satisfaction following a great and successful mental effort.* (G. Szegö)[1)]

Естественной формой для обсуждения и решения исследовательских задач являются научные конференции школьников[2)]. Их проводится довольно много — от Летней Конференции Турнира Городов[3)] до конференций, на которых иногда награждаются работы, выполненные не самостоятельно, или не проверяются полные тексты доказательств в награждаемых работах. К сожалению, таких конференций немало.

Отсутствие четкой связи между наградой и доступным для проверки результатом (т. е. публикацией) *резко отрицательно* сказывается на прогрессе науки и развращает школьников (даже изначально талантливых

[1)] *Не следует забывать, что решение любой стóящей проблемы очень редко приходит к нам легко и без труда*; *чаще это результат интеллектуальных усилий, длившихся днями, неделями или месяцами. Что побудит молодой ум делать такие чрезвычайные усилия*? *Объяснение, вероятно, состоит в инстинктивном предпочтении определенных ценностей, то есть в подходе, при котором интеллектуальное усилие и духовное достижение ставятся выше, чем материальная выгода. Такая оценка может быть лишь результатом долгого культурного развития среды и общественного мнения, — развития, которое трудно ускоритъ правительственной помощью или даже более интенсивным обучением математике. Может быть, самое эффективное средство состоит в том, чтобы передать молодому уму ощущение красоты интеллектуальной работы и чувство удовлетворения, которое следует за большим и успешным мыслительным усилием.* (Г. Сегё)

[2)] Такие конференции отличаются от научных тем, что предполагают награды и доклады для неспециалистов. Поэтому школьнику, сделавшему научную работу, полезно участвовать не только в научных конференциях по данной тематике, но и в школьных.

[3)] См. `www.mccme.ru/turgor/lktg`. Эти конференции проводятся с 1989 г. под руководством Н. Н. Константинова и (с 2000 г.) С. А. Дориченко (сам я работаю в жюри Летних Конференций с 1997 г.). Ввиду высоких требований к мотивировкам (для жюри) и к доказательствам (для школьников) участники Летних Конференций приобретают солидный опыт в решении исследовательских задач. Некоторым школьникам в процессе работы на Летней Конференции (или продолжая эту работу после) удается получить новые научные результаты, которые докладываются на научных конференциях и публикуются в рецензируемых журналах.

и добросовестных). Многие школьники стараются «получить» *побольше* результатов, а их *проверка и публикация* отходит на второй план. После награждения появляются другие интересные дела (в частности, новые задачи, за решение которых можно получить новые награды). В итоге замечательные идеи часто остаются непроверенными и неопубликованными: трудно взяться за решение проблемы, за которое другим человеком уже получена награда. Если же к такой проблеме через несколько лет все-таки возвращаются, то часто обнаруживаются ошибки. В итоге нередко оказывается, что вклад награжденного автора в решение проблемы *отрицателен*. Поэтому вопрос о *публикации* работ школьников имеет исключительно важное значение.

Как найти задачу для исследования? *Исследовательские задачи должны, с одной стороны, быть доступны для решения, понятны и интересны школьнику, а, с другой стороны, быть математически содержательными.*

Ведь если задача не имеет математического содержания, то усилия школьника по ее решению и проверке доказательства не вполне оправданы. Если же задача интересна школьнику не по своей сути, а благодаря авторитету руководителя или желанию поехать на конференцию, то это обычно приводит к низкому качеству работы: докладчик не в состоянии дать четкие понятные формулировки своих *результатов* и *этапов доказательства*, а также явно отделить одно от другого. Лучшей задачей для исследования является проблема, которая просто и четко формулируется, но трудно решается. (При этом задача может быть уже решенной в науке — тогда школьник должен об этом знать и всегда упоминать при выступлении.)

Желательно, чтобы задачу поставил школьнику человек, имеющий представление о какой-нибудь актуальной области математики, опыт собственной научной работы и вкус к просто формулируемым задачам. Таким человеком может быть как сильный школьный учитель, так и профессиональный математик. Конечно, школьник и сам может придумать себе задачу, однако она не всегда будет иметь серьезное математическое содержание и еще реже — «продолжение».

Вот примеры удачных задач для исследования.

(1) *Доказать, что существует непрерывная функция $f(x, y)$ двух переменных на квадрате $0 \leqslant x \leqslant 1$, $0 \leqslant y \leqslant 1$, не представимая в виде суперпозиции $\chi(\varphi(x) + \psi(y))$, т. е. функции одного переменного от суммы функции от икс и функции от игрек.*

(2) *Доказать, что через точку внутри трехгранного угла можно провести сечение так, чтобы точка оказалась центром тяжести полученного треугольника.*

Первая задача была поставлена А. Н. Колмогоровым на семинаре для первокурсников. Решение было получено студентом первого курса В. И. Арнольдом и опубликовано в УМН. Вторая задача из репертуара В. М. Тихомирова и давалась школьникам. Обе они имеют «продолжение»: в первом случае — решение тринадцатой проблемы Гильберта [1,18], во втором — кандидатскую диссертацию.

Благодаря красоте и наглядности топологической теории графов она является одним из удачных источников исследовательских задач: см., например, [2,8,9,16–18].

Много хороших задач для исследования можно найти в материалах Летних Конференций Турнира Городов[3)]. Другой естественный способ найти задачу для исследования — работать в кружке-семинаре, на котором предлагаются и обсуждаются задачи для исследования (возможно, наряду с учебной деятельностью). Такой кружок может проводиться в течение учебного года или на летней (зимней, ...) школе.

Например, сам я веду миникурсы по основам топологии в летней школе «Современная Математика» (с 2001 г.) и в Кировской Летней Многопредметной Школе (с 1993 г. с перерывами). Веду кружки «Математический семинар»[4)] в СУНЦ МГУ и «Олимпиады и математика» в МЦНМО (с 2003 г.; основная цель этого кружка — работа с потенциальными участниками Всероссийской математической олимпиады.[5)]).

Задачи для исследования предлагаются также на Московской математической конференции школьников, открывшейся 9.12.2007 [6)] (председатель жюри и программного комитета чл.-корр. РАН Д. В. Трещев). Похожая традиция рассылать школьникам задачи для исследования существовала раньше в «Кванте».

Требования к научной работе.[7)]

Решение проблемы должно быть получено самим школьником, а текст работы — написан им самостоятельно. (*Это не исключает возможность и необходимость консультаций научного руководителя.*)

[4)] С 1994 г.; до 2001 г. совместно с В. Н. Дубровским. Этот кружок продолжает традицию «Физико-математического семинара» и «Научного общества учащихся», которые вели В. Н. Дубровский, А. Н. Земляков, Е. Л. Сурков и А. П. Веселов. См. `www.mccme.ru/circles/oim/matsem.pdf`.

[5)] См. `www.mccme.ru/circles/oim`.

[6)] См. `www.mccme.ru/mmks`

[7)] Эти требования относятся также к студенческим, аспирантским и другим научным работам. По мнению автора, если уж работа школьника называется *научной*, то к ней должны применяться стандартные требования. Другое дело, что *руководство* школьником, при котором он способен сделать научную работу, отличается от руководства студентом.

Текст должен содержать ясные формулировки и полные доказательства результатов, т. е. работа должна быть ориентирована на публикацию в научно-популярном или реферируемом научном журнале.

Это требование необходимо, поскольку в первом приближении польза человечеству от научной работы происходит благодаря появлению проверенного общедоступного текста, т. е. публикации в рецензируемом журнале.[8)] См. замечания в конце раздела «Постановка проблемы». Поэтому, как правило, научными премиями *для профессиональных математиков* награждаются только работы, *опубликованные* в рецензируемых журналах. Поскольку серьезное рецензирование и публикация занимают некоторое время (от полугода), этот принцип неприменим к награждению работ *школьников*.

Однако современные технические средства позволяют выдвинуть разумное и реалистичное *промежуточное* условие для награждения школьных работ: *выкладывание работ на сервере* `www.arxiv.org` (с согласия руководителя, с указанием его фамилии и с предложением высылать замечания).[9)] Это условие выгодно отличается от простого наличия рекомендаций доведением результата до пользователя, публичностью и ответственностью. Замечу, что создание специальных сайтов для выкладывания *научных* работ школьников представляется излишним.

Чтобы работа соответствовала вышеприведенным требованиям, автор должен иметь хорошую *общематематическую* подготовку. К сожалению, иногда к «научной» работе привлекаются школьники, у которых вызывает трудности даже обязательная программа математической школы. Это приводит к ситуации, когда автор «научной» работы неспособен дать четкие формулировки основного результата и необходимых определений (не

[8)] Оговорка [4]: Most things that an article such as this one can say have at least one counterexample in the practice of some natural born genius. Authors of articles such as this one know that, but in the first approximation they must ignore it, or nothing would ever get done.

(Большинство утверждений, которые можно высказать в статье вроде этой, имеют хотя бы один контрпример в практике настоящего прирожденного гения. Авторы таких статей это знают, но в первом приближении должны это игнорировать, иначе никогда ничего не получится.)

[9)] Хотя выкладывание на `www.arxiv.org` не приравнивается к публикации, оно дает возможность специалистам ознакомиться с результатами автора и прислать замечания. Кроме того, оно предполагает серьезную ответственность автора: помещение некачественной работы (или ее удаление автором, после которого остаются фамилия автора и название работы) негативно влияет на его репутацию. Поэтому выкладывание работ на этом сервере все более популярно среди активно работающих математиков. Для выкладывания работы достаточно рекомендации математика, уже выложившего свою работу; при этом специально оговаривается, что от рекомендателя не требуется проверки рекомендуемой работы. На этот сервер могут быть выложены работы на русском языке (см. инструкции на `www.mccme.ru/mmks`).

говоря уже о доказательстве). Такая ситуация позорна прежде всего для руководителя работы.

Почти во всех работах — и школьных, и «взрослых», — на которые мне приходилось писать отрицательные рецензии, содержалось *несколько* плохо проверенных результатов. По моему мнению, для науки и для авторов было бы полезней, если бы был *один* хорошо проверенный результат.

Пожелание об ориентации работы на публикацию в рецензируемом журнале и требование (необходимое для получения награды) доступности широкому кругу специалистов абсолютно реалистичны для достаточного количества школьников. Действительно, в математических школах или на Летней Конференции Турнира Городов школьники пишут достаточно серьезные математические тексты. Кроме того, каждый год в реферируемых журналах публикуется несколько работ школьников (или начатых авторами во время учебы в школе). Если же указанные требования будут явно высказаны, то количество (и качество) таких работ резко возрастет.

Если работа не удовлетворяет этим критериям, то полезны

(1) доклады школьников по работам, не выложенным на `www.arxiv.org` (это аналоги докладов на научных семинарах, за которые не присуждаются премии; возможно, что в будущем такие работы будут доведены до «премиальных»);

(2) награждение *после* конференции в случае публикации работы.

Решать *учебно-исследовательские* задачи и просто учиться полезно многим школьникам, для которых приведенные требования нереалистичны. Для некоторых именно такой путь в науку наиболее естественен. Полезны поощрительные призы за учебно-исследовательские работы, не претендующие на научную новизну (а также за хорошую учебу).

Как подготовить работу и доклад? Классическими рекомендациями являются статьи [4, 5].

В самом начале работы нужно привести ясные формулировки основных результатов, доступные специалисту по данному разделу математики (например, геометрии и топологии), а также ссылки на литературу, достаточную для понимания формулировок *любым математиком*[10)].

См., например, [3, 7, 10–12, 14, 15, 21, 22].

Это требование необходимо, поскольку:

[10)] Впрочем, согласно известному высказыванию Гильберта (которое подтверждается моим собственным опытом), в случае действительно интересного результата можно прямо в тексте привести сведения, необходимые для понимания формулировок *любым математиком*.

– с *ясной формулировки* основных результатов начинается структуризация (т. е. *ясная формулировка* этапов) доказательства, а без нее нельзя считать, что доказательства проверены самим автором;

– отсутствие *ясной формулировки* затрудняет понимание и использование результатов работы другими математиками (даже работающими в данной области).

Награждение *научными* премиями работ, не удовлетворяющих этим требованиям, способствует:

– понижению стандартов достоверности научных результатов,

– распаду математики на отдельные области, представители которых не понимают друг друга.

Проверка работы специалистами в данной конкретной области должна *предшествовать* представлению работы к публикации/премии и ее рецензированию неспециалистами. Перед докладом на конференции нужно:

– обсудить результаты и проверить доказательства со специалистом по близким проблемам (сначала с научным руководителем, потом с независимым советчиком);

– выступить на научном семинаре;

– разослать текст, содержащий ясную формулировку и полные доказательства специалистам по близким проблемам.

После серьезной проверки работу разумно выложить на `www.arxiv.org`, а после сбора замечаний и соответствующей правки текста — представить к публикации. Затем работа может претендовать на награждение *школьной* (*студенческой*) премией (для научных премий уже необходимо ее *принятие к публикации*).

Еще раз нужно предупредить: размещение на `www.arxiv.org`, публикация или награждение некачественной работы наносит огромный вред репутации ее автора.

В каких конференциях школьников участвовать? Конференции-конкурсы высшего уровня в России, с которых проходит отбор на международную конференцию Intel ISEF — *Интел-Юниор* (председатель научного жюри по математике профессор Московского государственного университета им. М. В. Ломоносова А. В. Михалев) и *Балтийский Конкурс* (председатель научного жюри по математике профессор Санкт-Петербургского государственного педагогического университета В. М. Нежинский).[11)] К ним примыкает конференция *Интел-Авангард*[12)]: на ней А. Я. Белов ввел *предварительное прослушивание* школьников математиками, на котором высказываются рекомендации по докладам (и по итогам которого

[11)] См. `http://junior.mephi.ru`, `http://baltic.contedu.ru`.

[12)] См. `www.conference-avangard.ru`

распределяется время докладов).[13)] Хочется надеяться, что будет высоким уровень Московской Математической Конференции Школьников[6)].

Среди *наград для школьников, подготовивших хорошие доклады*, — гранты, а также приглашения (оплачиваемые органами образования или спонсорами) на Летнюю Конференцию Турнира Городов, в летнюю школу «Современная Математика»[14)], на другие конференции школьников.

Примеры исследовательских работ школьников. Некоторыми математиками и учителями накоплен положительный опыт по привлечению сильных школьников к исследовательской работе. Расскажу кратко о своем опыте. Благодаря тому, что в 1991–2003 гг. я был членом жюри Всесоюзной и Всероссийской олимпиады, в 1990–1994 гг. участвовал в подготовке команды СССР и России на Международную олимпиаду, а с 2004 г. являюсь научным руководителем команды Москвы на Всероссийскую олимпиаду, мне удавалось привлекать к исследовательской работе сильных школьников. В результате некоторые из этих школьников подготовили работы, представляющие научный интерес (ссылки приведены ниже; отдельные работы завершены в студенческие годы). Многие из этих школьников входили в команду России на международную конференцию школьников Intel ISEF в 2000–2007 гг.

Примеры хороших работ школьников: [3, 7, 11, 12, 14, 19–22]; некоторые результаты работ [10, 15] были получены авторами в свои школьные годы.[15)] Расскажем подробнее о работах [7, 11].

1. Формулировка критерия Куратовского планарности графов хорошо известна (вместе с необходимыми понятиями она напомнена в [16]). Однако его классическое доказательство сложно и приводится не во всех книгах по теории графов. Более простые доказательства критерия Куратовского содержатся в [23, §5] и [11] (Юрий Макарычев придумал свое доказательство, еще будучи школьником!). В [16] приводится доказательство Макарычева с дальнейшими упрощениями (сделанными А. А. Заславским, В. В. Прасоловым и автором).

2. Число называется *трансцендентным*, если оно не является корнем многочлена с целыми коэффициентами. В университете или даже в старших классах изучается теоретико-множественное доказательство существования трансцендентных чисел [6, гл. 2, §6]. Отыскание *явных* примеров трансцендентных чисел и доказательство их трансцендентности

[13)] Такое предварительное прослушивание проводил М. М. Постников перед семинаром (носящим теперь имя Постникова) мехмата Московского государственного университета.

[14)] См. `www.mccme.ru/dubna`

[15)] Чтобы не обидеть авторов тех хороших работ, ссылки на которые мне недоступны, я ссылаюсь на работы по единственному формальному критерию, который могу четко соблюсти: на работы своих учеников.

более трудно и не всегда входит даже в программу университетского курса. Первый явный пример трансцендентного числа был приведен Жозефом Лиувиллем в 1835 г. [6, гл. 2, §6]: $\lambda = \sum\limits_{n=0}^{\infty} 2^{-n!}$. В 1929 г. Курт Малер доказал трансцендентность числа $\mu = \sum\limits_{n=0}^{\infty} 2^{-2^n}$, не вытекающую из общей теоремы Лиувилля, а также из теорем Туэ, Зигеля и Рота [6, гл. 2, §6]. В работе Малера был получен более общий результат; доказательство не элементарно и длинно. Главный результат заметки А. Каибханова и А. Скопенкова [7] — *короткое элементарное доказательство трансцендентности числа Малера* (основанное на двоичной записи). Видимо, это доказательство является новым.

Список литературы

[1] В. И. Арнольд. *О представлении функций нескольких переменных в виде суперпозиции функций меньшего числа переменных* // Мат. Просвещение, сер. 2, вып. 3, 1958. С. 41–61.
`http://ilib.mccme.ru/djvu/mp2/mp2-3.htm`

[2] A. Cavicchioli, D. Repovš, A. B. Skopenkov. *Open problems on graphs, arising from geometric topology* // Topol. Appl., 1998. Vol. 84. P. 207–226.

[3] М. Гортинский, О. Скрябин. *Критерий вложимости графов в плоскость вдоль прямой*. Представлено к публикации.

[4] P. R. Halmos. *How to talk Mathematics* // Notices Amer. Math. Soc., 1974. Vol. 21 P. 155–158.

[5] P. R. Halmos. *How to write Mathematics* // L'Enseignement Math., 1970. Vol. 16. P. 123–152. Русск. пер.: П. Р. Халмош. *Как писать математические тексты* // УМН, 1971. Т. 26, вып. 5.
`http://www.ega-math.narod.ru/Halmos.htm`

[6] Р. Курант, Г. Роббинс. *Что такое математика*? М.: МЦНМО, 2001.

[7] А. Каибханов, А. Скопенков. *Примеры трансцендентных чисел* // Мат. Просвещение, сер. 3, вып. 10, 2006. С. 176–184.
`http://www.mccme.ru/free-books/matprosb.html`

[8] В. Курлин, А. Скопенков. *Базисные вложения графов в плоскость* // Мат. Образование, №3, 1997. С. 105–113.

[9] П. Кожевников, А. Скопенков. *Узкие деревья на плоскости* // Мат. Образование, №2–3, 1999. С. 126–131.

[10] V. A. Kurlin. *Basic embeddings into products of graphs* // Topol. Appl., 2000. Vol. 102. P. 113–137.

[11] Yu. Makarychev. *A short proof of Kuratowski's graph planarity criterion* // J. of Graph Theory, 1997. Vol. 25. P. 129–131.

[12] Н. Однобоков. *Классификация вложения графов в плоскость с непересекающимися образами*. Представлено к публикации.

[13] G. Polya. *How to Solve it*. Princeton: Princeton University Press, 1945. Рус. перевод: Пойа Д. *Как решать задачу*. М.: Учпедгиз, 1961.

[14] G. Pogudin, P. Verevkin. *On the embeddability of cubic R-graphs into the torus* // Preprint. 2006.

[15] M. Skopenkov. *On approximability by embeddings of cycles in the plane* // Topology and its Applications, 2003. Vol. 134. P. 1–22.

[16] А. Скопенков. *Вокруг критерия Куратовского планарности графов* // Мат. Просвещение, сер. 3, вып. 9, 2005. С. 116–128 и вып. 10, 2006, с. 276–277.
`http://www.mccme.ru/free-books/matprosa.html`
`http://dfgm.math.msu.su/files/skopenkov/kuratow.pdf`

[17] А. Скопенков. *Алгебраическая топология с элементарной точки зрения*. М.: МЦНМО. В печати.
`http://dfgm.math.msu.su/files/skopenkov/obstruct2.ps`

[18] А. Скопенков. 13-*я проблема Гильберта и базисные вложения*
`http://dfgm.math.msu.su/files/skopenkov/hilbert.pdf`

[19] А. Скопенков, А. Таламбуца. *Упаковки правильных многогранников* // Мат. Образование, №3(14), 2000. С. 52–53.

[20] А. Скопенков, А. Таламбуца. *Экстремальные расположения правильных многогранников* // Мат. Просвещение, сер. 3, вып. 8, 2004. С. 53–65.
`http://www.mccme.ru/free-books/matprosa.html`

[21] А. Скопенков и А. Телишев. *И вновь о критерии Куратовского планарности графов* Мат. Просвещение, сер. 3, вып. 11, 2007. С. 159–160.

[22] A. Telishev. *On realizability of graphs on the Klein bottle*. Preprint. 2007.

[23] Thomassen C. *Kuratowski's theorem* // J. Graph. Theory, 1981. Vol. 5. P. 225–242.

А. Б. Скопенков: механико-математический факультет Московского государственного университета им. М. В. Ломоносова, Независимый московский Университет, Московский институт открытого образования
Инфо: `http://dfgm.math.msu.su/people/skopenkov/papersc.ps`
e-mail: `skopenko@mccme.ru`

Тема номера: p-адические числа

Удивительные арифметические свойства биномиальных коэффициентов

Э. Б. Винберг

1. Вступление

Хорошо известные формулы

$$(a+b)^2 = a^2 + 2ab + b^2,$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

являются частными случаями формулы бинома Ньютона

$$(a+b)^n = a^n + C_n^1 a^{n-1}b + C_n^2 a^{n-2}b^2 + \cdots + C_n^{n-1}ab^{n-1} + b^n = \sum_{k=1}^{n} C_n^k a^{n-k}b^k. \quad (1)$$

Коэффициент C_n^k в этой формуле есть «число сочетаний из n по k» — число способов выбрать k предметов из n предметов без учета порядка[1)].

Выбирая k предметов из n предметов по порядку, первый предмет мы можем выбрать n способами, второй — $n-1$ способами, третий — $n-2$ способами и т. д. Таким образом, число упорядоченных выборок k предметов из n предметов равно

$$n(n-1)(n-2)\cdot\ldots\cdot(n-k+1).$$

Если же мы не хотим учитывать порядок, то это число надо разделить на «число перестановок» k предметов — число способов упорядочить k

[1)] Вместо C_n^k используется также обозначение $\binom{n}{k}$.

предметов, которое (по тем же соображениям) равно

$$k(k-1)\cdot\ldots\cdot 2\cdot 1 = k!\,.$$

Окончательно получаем

$$C_n^k = \frac{n(n-1)(n-2)\cdot\ldots\cdot(n-k+1)}{k!}\,. \tag{2}$$

(Обратите внимание на то, что число множителей в числителе и знаменателе одинаково.)

Формуле (2) можно придать вид

$$C_n^k = \frac{n!}{k!(n-k)!}\,,$$

откуда следует, что

$$C_n^k = C_n^{n-k}\,. \tag{3}$$

Впрочем, последнее свойство очевидно и из комбинаторного смысла числа сочетаний: выбрать k предметов из n предметов — это то же, что выбрать оставшиеся $n-k$ предметов.

Числа C_n^k, называемые также *биномиальными коэффициентами*, удобно вычислять при помощи следующего рекуррентного соотношения:

$$C_n^k = C_{n-1}^{k-1} + C_{n-1}^k\,. \tag{4}$$

Для его доказательства выделим один предмет из имеющихся n предметов. Тогда число способов выбрать k предметов, включая выделенный, равно C_{n-1}^{k-1}, а число способов выбрать k предметов, отличных от выделенного, равно C_{n-1}^k, откуда и следует формула (4).

Удобно считать, что

$$C_n^k = 0 \text{ при } k<0 \text{ или } k>n.$$

Тогда формула (4) будет справедлива и при $k = 0, n$.

Биномиальные коэффициенты можно записать в форме *треугольника Паскаля* — бесконечной треугольной таблицы, в n-й строке которой стоят числа

$$C_n^0,\ C_n^1,\ C_n^2,\ \ldots,\ C_n^{n-1},\ C_n^n\,,$$

причем строки таблицы сдвинуты таким образом, что каждое число n-й строки в соответствии с формулой (4) равно сумме двух ближайших к нему чисел $(n-1)$-й строки. Первые 10 строк (от нулевой до девятой) треугольника Паскаля показаны на рис. 1.

Биномиальные коэффициенты обладают рядом удивительных арифметических свойств. Подсчитаем, например, сколько нечетных чисел имеется в каждой строке треугольника Паскаля. Мы получим последовательность чисел

$$1,\ 2,\ 2,\ 4,\ 2,\ 4,\ 4,\ 8,\ 2,\ 4,\ \ldots$$

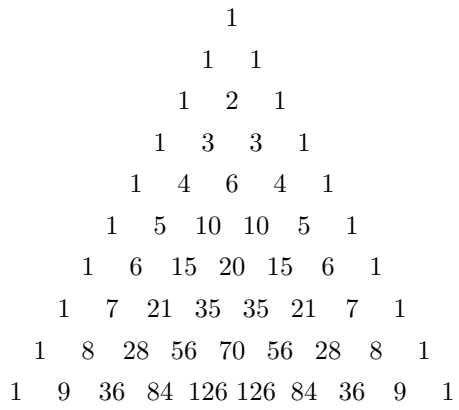


Рис. 1. *Треугольник Паскаля*

Сразу трудно угадать общий закон для членов этой последовательности. Однако видно, что все выписанные числа являются степенями двойки! В следующем разделе мы опишем закон, по которому четные и нечетные числа располагаются в треугольнике Паскаля и, в частности, докажем, что число нечетных чисел в каждой строке действительно является степенью двойки.

2. Биномиальные коэффициенты по модулю p

Пусть p — простое число. Займемся вычислением биномиальных коэффициентов C_n^k по модулю p.

Разделим n и k на p с остатком:

$$n = n'p + n_0, \quad k = k'p + k_0, \quad (0 \leqslant n_0, k_0 < p). \tag{5}$$

Докажем, что

$$C_n^k \equiv C_{n'}^{k'} C_{n_0}^{k_0} \pmod{p}. \tag{6}$$

Среди имеющихся n предметов выделим n' блоков по p предметов в каждом блоке, оставив n_0 предметов вне блоков. Выборку k предметов будем называть *блочной*, если она состоит из k' целых блоков и k_0 предметов вне блоков. Число блочных выборок равно $C_{n'}^{k'} C_{n_0}^{k_0}$. Поэтому нам достаточно доказать, что число остальных выборок делится на p.

Отметим, что, как видно из (2), C_p^l при $0 < l < p$ делится на p.

Рассмотрим выборки, содержащие соответственно l_1, l_2, …, l_s предметов ($0 < l_1, \ldots, l_s < p$) из каких-то фиксированных s блоков ($s > 0$) и, кроме того, целиком какие-то фиксированные блоки и какие-то фиксированные предметы вне блоков. (Общее число выбираемых предметов,

естественно, должно быть равно k.) Число таких выборок равно

$$C_p^{l_1} C_p^{l_2} \cdot \ldots \cdot C_p^{l_s}$$

и согласно предыдущему делится на p^s. Суммируя, получаем, что число всех неблочных выборок делится на p. Тем самым сравнение (6) доказано.

Разделим теперь n' и k' на p с остатком:

$$n' = n''p + n_1, \quad k' = k''p + k_1 \quad (0 \leqslant n_1, k_1 < p).$$

Подставляя в (5), получаем

$$n = n''p^2 + n_1 p + n_0, \quad k = k''p^2 + k_1 p + k_0.$$

Продолжая так дальше, мы в конце концов получим p-ичное представление чисел n и k:

$$n = n_d p^d + n_{d-1} p^{d-1} + \cdots + n_1 p + n_0,$$
$$k = k_d p^d + k_{d-1} p^{d-1} + \cdots + k_1 p + k_0.$$

(Число цифр в p-ичной записи чисел n и k, конечно, не обязано быть одинаковым, но мы можем для удобства сделать его формально одинаковым, приписав спереди к одному из чисел несколько нулей.)

Применив несколько раз сравнение (6), мы получим следующую теорему.

Теорема 1 (Люка́ (Lucas), 1878).

$$C_n^k \equiv C_{n_d}^{k_d} C_{n_{d-1}}^{k_{d-1}} \cdot \ldots \cdot C_{n_1}^{k_1} C_{n_0}^{k_0} \pmod{p}.$$

Следствие. *C_n^k не делится на p тогда и только тогда, когда $k_i \leqslant n_i$ при всех $i = 0, 1, \ldots, d$.*

В частности, число нечетных биномиальных коэффициентов в n-й строке треугольника Паскаля равно числу таких k, в двоичной записи которых единицы стоят лишь там, где они стоят в двоичной записи числа n. Число таких k равно 2^r, где r — число единиц в двоичной записи числа n.

На рис. 2 изображены первые 16 строк треугольника Паскаля по модулю 2. Для большей наглядности нули заменены кружками, а единицы — крестиками.

В следующих трех задачах n_i и k_i $(i = 0, 1, \ldots, d)$ обозначают цифры в двоичной записи чисел n и k.

Задача 1. *Рассмотрим n-ю строку треугольника Паскаля по модулю 2 как двоичную запись некоторого натурального числа P_n. Докажите, что*

$$P_n = F_{i_1} \cdot \ldots \cdot F_{i_s},$$

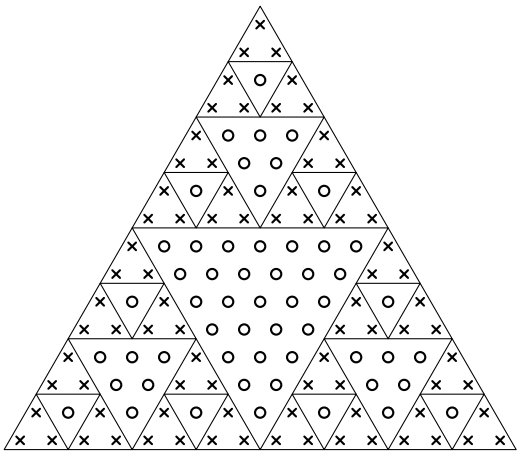


Рис. 2.

где $i_1, \ldots, i_s$ — номера разрядов, в которых в двоичной записи числа n стоят единицы, а $F_i = 2^{2^i} + 1$ — i-е число Ферма.

Например, $P_5 = F_0F_2 = 3 \cdot 17 = 51 = 2^5 + 2^4 + 2 + 1$.

Задача 2. *Докажите, что если биномиальный коэффициент C_n^k нечетен (т. е. $k_i \leqslant n_i$ при всех $i = 0, 1, \ldots, d$), то*

$$C_n^k \equiv \prod_{i=1}^{d} (-1)^{k_{i-1}n_i + k_i n_{i-1}} \pmod 4.$$

Выведите отсюда, что если в двоичной записи числа n нет двух единиц подряд, то все нечетные числа в n-й строке треугольника Паскаля сравнимы с 1 по модулю 4, а в противном случае ровно половина из них сравнима с 1 по модулю 4.

Задача 3. *Докажите, что если биномиальный коэффициент C_n^k четен, то он не делится на 4 тогда и только тогда, когда имеется ровно одно значение i, для которого $k_i > n_i$, и при этом $k_{i+1} < n_{i+1}$.*

3. Делимость биномиальных коэффициентов на степени простых чисел

Мы уже научились определять, делится ли биномиальный коэффициент C_n^k на простое число p. Но, если он делится на p, как узнать, делится ли он на p^2 и, вообще, на какую максимальную степень p он делится? Ответ на этот вопрос дается приводимой ниже теоремой Куммера.

Для любого целого числа N и простого числа p будем обозначать через $\operatorname{ord}_p N$ показатель максимальной степени p, на которую делится N.

Теорема 2 (Куммер (Kummer), 1852). *Показатель* $\operatorname{ord}_p C_n^k$ *равен числу переносов при сложении «столбиком» чисел* k *и* $l = n - k$ *в* p*-ичной записи.*

Доказательство. Будем доказывать теорему индукцией по n. При $n = 0$ утверждение очевидно. При $n > 0$ рассмотрим два случая.

1-й случай. Числа k и l (а значит, и n) делятся на p:

$$n = n'p, \quad k = k'p, \quad l = l'p.$$

Делимость числа C_n^k на степени p определяется теми множителями в выражении (2), которые делятся на p. Число этих множителей в числителе и знаменателе одинаково и равно k'. Если мы оставим только их и сократим полученную дробь на $p^{k'}$, то мы получим $C_{n'}^{k'}$. Следовательно,

$$\operatorname{ord}_p C_n^k = \operatorname{ord}_p C_{n'}^{k'}. \tag{7}$$

С другой стороны, p-ичные записи чисел k' и l' получаются из p-ичных записей чисел k и l отбрасыванием нулей, стоящих в нулевом разряде (и сдвигом остальных разрядов). Поэтому число переносов при сложении k и l такое же, как и при сложении k' и l'. По предположению индукции оно равно $\operatorname{ord}_p C_{n'}^{k'}$, что в силу (7) равно $\operatorname{ord}_p C_n^k$.

2-й случай. Хотя бы одно из чисел k и l не делится на p. Для определенности будем считать, что k не делится на p, т. е. $k_0 > 0$.

Пусть $\operatorname{ord}_p n = s \geqslant 0$. Из формулы (2) следует, что

$$\operatorname{ord}_p C_n^k = \operatorname{ord}_p C_{n-1}^{k-1} + s. \tag{8}$$

С другой стороны, нетрудно видеть, что при сложении k и l в первых s разрядах происходят переносы, а при сложении $k-1$ и l в этих разрядах переносов не происходит; все же остальные переносы происходят в тех же разрядах. Следовательно, число переносов при сложении k и l ровно на s больше, чем при сложении $k - 1$ и l. Учитывая предположение индукции и равенство (8), получаем требуемое утверждение. □

4. «Сокращение» биномиальных коэффициентов на p

Из теоремы Люка следует, что

$$C_{np}^{kp} \equiv C_n^k \pmod{p}.$$

Это сравнение можно улучшить. Разобьем np предметов на n блоков по p предметов в каждом блоке. Выборку из kp предметов назовем блочной (как и в п. 2), если она состоит из k целых блоков. Число блочных выборок

равно C_n^k. Число выборок, содержащих соответственно $l_1, l_2, \ldots, l_s$ предметов ($0 < l_1, \ldots, l_s < p$) из каких-то фиксированных s блоков ($s > 0$) и, кроме того, целиком какие-то фиксированные блоки, равно $C_p^{l_1} C_p^{l_2} \cdot \ldots \cdot C_p^{l_s}$ и, следовательно, делится на p^s. Заметим, что $s > 1$, поскольку общее число выбираемых предметов кратно p. Следовательно, общее число неблочных выборок делится на p^2 и, значит,

$$C_{np}^{kp} \equiv C_n^k \pmod{p^2}.$$

При $p \geqslant 5$ верно еще более сильное сравнение

$$C_{np}^{kp} \equiv C_n^k \pmod{p^3}. \tag{9}$$

Рассуждая, как выше, мы видим, что для его доказательства достаточно рассмотреть случай, когда имеется всего два блока. Именно этот случай составляет предмет следующей теоремы.

Теорема 3 (Волстенхолм (Wolstenholme), 1862). *При* $p \geqslant 5$

$$C_{2p}^{p} \equiv 2 \pmod{p^3} \tag{10}$$

или, что то же самое,

$$C_{2p-1}^{p-1} \equiv 1 \pmod{p^3}. \tag{11}$$

(Легко видеть, что при $p = 2, 3$ сравнение (11) не выполняется.)

Доказательство. Распространим сравнения по модулю степеней p на рациональные числа, знаменатели которых не делятся на p, считая, что такое число делится на p^s, если числитель в его несократимой записи делится на p^s. Все основные свойства сравнений между целыми числами при этом останутся в силе.

Имеем:

$$C_{2p-1}^{p-1} = \frac{(2p-1)(2p-2)\cdot\ldots\cdot(p+1)}{p!} = \left(\frac{2p}{1} - 1\right)\left(\frac{2p}{2} - 1\right)\cdot\ldots\cdot\left(\frac{2p}{p-1} - 1\right).$$

Произведя умножение и выделив члены, содержащие p не более, чем во второй степени, получим сравнение

$$C_{2p-1}^{p-1} \equiv 1 - 2p\sum_{i=1}^{p-1}\frac{1}{i} + 4p^2 \sum_{\substack{i,j=1 \\ i<j}}^{p-1}\frac{1}{ij} \pmod{p^3}. \tag{12}$$

Далее,

$$2\sum_{i=1}^{p-1}\frac{1}{i} = \sum_{i=1}^{p-1}\left(\frac{1}{i} + \frac{1}{p-i}\right) = p\sum_{i=1}^{p-1}\frac{1}{i(p-i)}.$$

Подставляя в (12), получаем:

$$C_{2p-1}^{p-1} \equiv 1 - p^2 \sum_{i=1}^{p-1} \frac{1}{i(p-i)} + 4p^2 \sum_{\substack{i,j=1 \\ i<j}}^{p-1} \frac{1}{ij} \pmod{p^3}.$$

Таким образом, нам достаточно доказать, что

$$\sum_{i=1}^{p-1} \frac{1}{i(p-i)} \equiv \sum_{\substack{i,j=1 \\ i<j}}^{p-1} \frac{1}{ij} \equiv 0 \pmod{p}.$$

Перейдя к полю вычетов

$$\mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\},$$

мы можем переписать предыдущие сравнения в виде равенств

$$\sum_{i=1}^{p-1} \frac{1}{\bar{i}^2} = \sum_{\substack{i,j=1 \\ i<j}}^{p-1} \frac{1}{\bar{i}\,\bar{j}} = 0. \tag{13}$$

Заметим, что $\frac{1}{\bar{1}}, \frac{1}{\bar{2}}, \dots, \frac{1}{\overline{p-1}}$ — это те же элементы $\bar{1}, \dots, \overline{p-1}$ поля $\mathbb{Z}_p$, взятые в каком-то другом порядке. Поэтому

$$\sum_{i=1}^{p-1} \frac{1}{\bar{i}^2} = \sum_{i=1}^{p-1} \bar{i}^2, \quad \sum_{\substack{i,j=1 \\ i<j}}^{p-1} \frac{1}{\bar{i}\,\bar{j}} = \sum_{\substack{i,j=1 \\ i<j}}^{p-1} \bar{i}\,\bar{j}.$$

Известно, что все ненулевые элементы поля $\mathbb{Z}_p$ — это корни многочлена $x^{p-1} - 1$ (малая теорема Ферма). При $p > 3$ по формулам Виета получаем:

$$\sum_{i=1}^{p-1} \bar{i} = 0, \quad \sum_{\substack{i,j=1 \\ i<j}}^{p-1} \bar{i}\,\bar{j} = 0,$$

$$\sum_{i=1}^{p-1} \bar{i}^2 = \left(\sum_{i=1}^{p-1} \bar{i} \right)^2 - 2 \sum_{\substack{i,j=1 \\ i<j}}^{p-1} \bar{i}\,\bar{j} = 0.$$

Тем самым равенства (13), а с ними и теорема Волстенхолма доказаны. □

Примеры. При $p = 5$ имеем

$$C_9^4 = \frac{9 \cdot 8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 3 \cdot 4} = 126 \equiv 1 \pmod{5^3},$$

а при $p = 7$ —

$$C_{13}^6 = \frac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} = 1716 \equiv 1 \pmod{7^3}.$$

Отметим, что по ходу доказательства теоремы мы установили, что (при $p \geqslant 5$)

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

Пример. При $p = 5$ имеем

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{25}{12} \equiv 0 \pmod{5^2},$$
$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} = \frac{205}{144} \equiv 0 \pmod{5}.$$

Возникает естественный вопрос: существуют ли простые числа p, для которых сравнение (11) выполняется по модулю p^4?

Задача 4. *Докажите эквивалентность следующих сравнений:*

1) $C_{2p-1}^{p-1} \equiv 1 \pmod{p^4}$;

2) $\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p^3}$;

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

Простые числа p, для которых выполняются эти сравнения, называются *числами Волстенхолма*. Путем вычислений на компьютерах установлено, что в пределах первого миллиарда имеется ровно два таких числа: 16843 и 2124679. Существуют ли другие числа Волстенхолма, неизвестно.

Сравнение (9) может быть, однако, улучшено, если известно, что n, k, $l = n - k$ или C_n^k делятся на p.

Теорема 4 (Якобсталь (Jacobsthal), 1945). *При* $p \geqslant 5$

$$C_{np}^{kp} : C_n^k \equiv 1 \pmod{p^{3+\operatorname{ord}_p n + \operatorname{ord}_p k + \operatorname{ord}_p l}}$$

или, что то же,

$$C_{np}^{kp} \equiv C_n^k \pmod{p^{3+\operatorname{ord}_p n + \operatorname{ord}_p k + \operatorname{ord}_p l + \operatorname{ord}_p C_n^k}}.$$

Например, при $p \geqslant 5$

$$C_{p^3}^{p^2} \equiv C_{p^2}^{p} \pmod{p^8} \tag{14}$$

(учитывая, что $\operatorname{ord}_p C_{p^2}^p = 1$).

Заметим, что проверить сравнение (14) непосредственным вычислением без помощи компьютера весьма затруднительно даже при $p = 5$.

Задача 5. *Докажите сравнение* (14) *самостоятельно, не опираясь на теорему Якобсталя.*

Список литературы

[1] Granville, A. *Arithmetic properties of binomial coefficients.* I: *Binomial coefficients modulo prime powers* // Canad. Math. Soc. Conference Proc., 1997. Vol. 20. P. 253–275.

[2] Стенли Р. *Перечислительная комбинаторика*. М.: Мир, 1990. (Упражнение 6 к гл. 1, с. 72–73.)

[3] Fuchs D., Tabachnikov S. *Mathematical Omnibus. Thirty lectures on classic mathematics*, 2006. Lecture 2, pp. 24–40.
`http://www.math.psu.edu/tabachni/Books/taba.pdf`

Э. Б. Винберг, механико-математический факультет МГУ

Малая теорема Ферма и ее обобщения

Э. Б. Винберг

1. Три доказательства малой теоремы Ферма

Пусть p — простое число. Как известно, малая теорема Ферма утверждает, что

$$a^{p-1} \equiv 1 \pmod{p} \tag{1}$$

для всякого целого a, не делящегося на p, или, что эквивалентно,

$$a^p \equiv a \pmod{p} \tag{2}$$

для всякого целого a.

Первое доказательство. Наиболее простое, но наименее элементарное доказательство малой теоремы Ферма основано на следствии теоремы Лагранжа из теории групп, утверждающей, что порядок элемента конечной группы делит порядок группы.

Напомним, что порядком конечной группы G называется число ее элементов, а порядком элемента $g \in G$ — наименьший показатель его степени, равной единичному элементу e группы G.

Пусть G — конечная группа порядка n. Из того, что порядок элемента $g \in G$ делит n, следует, что $g^n = e$.

Рассмотрим поле $\mathbb{Z}_p$ вычетов по модулю p. Вычет целого числа a будем обозначать через $\bar{a}$. Ненулевые элементы поля $\mathbb{Z}_p$ образуют группу относительно умножения. Порядок этой группы, очевидно, равен $p-1$. Ее единичным элементом является $\bar{1}$. Следовательно, для любого целого числа a, не делящегося на p, $\bar{a}^{p-1} = \bar{1}$, но это как раз и означает сравнение (1).

Второе доказательство. (Petersen, 1872.) Пусть имеется p предметов, расположенных по кругу, каждый из которых нужно раскрасить в один из a цветов. Число всех раскрасок, очевидно, равно a^p.

Предположим, что некая раскраска переходит в себя при повороте на какой-то угол $\dfrac{2\pi d}{p}$, $0 < d < p$. Будем считать d наименьшим возможным и разделим p на d с остатком:

$$p = qd + r, \quad 0 \leqslant r < p.$$

Ясно, что данная раскраска переходит в себя при повороте на угол $\frac{2\pi qd}{p} = 2\pi - \frac{2\pi r}{p}$ и, следовательно, — и при повороте на угол $\frac{2\pi r}{p}$. В силу выбора d получаем, что $r = 0$, т. е. d делит p. Так как p — простое число, то $d = 1$, т. е. данная раскраска одноцветная.

Число одноцветных раскрасок равно a. Все остальные $a^p - a$ раскрасок разобьем на классы, отнеся к одному классу раскраски, получающиеся друг из друга поворотами. В силу предыдущего каждый класс состоит из p раскрасок. Отсюда и следует сравнение (2).

Третье доказательство. Так как при простом p все биномиальные коэффициенты C_p^k, $0 < k < p$, делятся на p (см. [1]), то в кольце $\mathbb{Z}[x, y]$ многочленов с целыми коэффициентами от переменных x и y имеет место сравнение

$$(x + y)^p \equiv x^p + y^p \pmod{p}. \tag{3}$$

(Два многочлена с целыми коэффициентами считаются сравнимыми по какому-то модулю, если их соответственные коэффициенты сравнимы по этому модулю.)

Подставляя в (3) $x = a$, $y = b$, где a, b — какие-то целые числа, мы получаем, что

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

Следовательно, если $a^p \equiv a \pmod{p}$ и $b^p \equiv b \pmod{p}$, то и $(a + b)^p \equiv a+b \pmod{p}$. Так как $1^p \equiv 1 \pmod{p}$ и любое натуральное число можно получить сложением нескольких единиц, то сравнение (2) верно для всех натуральных a, а значит, и для всех целых a.

2. Теорема Эйлера

Напомним, что для любого натурального числа m через $\varphi(m)$ обозначается количество натуральных чисел, не превосходящих m и взаимно простых с m. Функция φ, называемая *функцией Эйлера*, обладает следующим свойством мультипликативности (вытекающим из китайской теоремы об остатках): если m_1 и m_2 — взаимно простые натуральные числа, то

$$\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2). \tag{4}$$

Если $m = p$ — простое число, то $\varphi(m) = p - 1$; если $m = p^n$, то $\varphi(m) = p^n - p^{n-1}$.

Теорема Эйлера (сравнение Эйлера) утверждает, что

$$a^{\varphi(m)} \equiv 1 \pmod{m} \tag{5}$$

для всякого целого a, взаимно простого с m. Это, очевидно, является обобщением малой теоремы Ферма.

Если $m = m_1 m_2$, где m_1 и m_2 взаимно просты, то для доказательства сравнения (5) достаточно проверить, что

$$a^{\varphi(m)} \equiv 1 \pmod{m_1} \quad \text{и} \quad a^{\varphi(m)} \equiv 1 \pmod{m_2}. \tag{6}$$

Учитывая (4), получаем, что

$$a^{\varphi(m)} = \left(a^{\varphi(m_2)}\right)^{\varphi(m_1)} = \left(a^{\varphi(m_1)}\right)^{\varphi(m_2)}$$

и, значит, сравнения (6) вытекают из теоремы Эйлера для модулей m_1 и m_2. Это рассуждение показывает, что теорему Эйлера достаточно доказать для $m = p^n$, где p — простое число. В этом случае она принимает вид

$$a^{p^n - p^{n-1}} \equiv 1 \pmod{p^n} \tag{7}$$

для всякого целого a, не делящегося на p.

Сравнение (7) эквивалентно сравнению

$$a^{p^n} \equiv a^{p^{n-1}} \pmod{p^n}, \tag{8}$$

причем последнее сравнение, очевидно, верно и при a, кратном p, так как в этом случае обе его части делятся на p^n.

Приведем три доказательства теоремы Эйлера, обобщающие соответствующие доказательства малой теоремы Ферма.

Первое доказательство. Рассмотрим кольцо $\mathbb{Z}_m$ вычетов по модулю m. Вычет целого числа a будем обозначать через $\bar{a}$. Обратимые элементы кольца $\mathbb{Z}_m$ образуют группу относительно умножения. Как известно (и легко доказывается), элемент $\bar{a}$ обратим в $\mathbb{Z}_m$ тогда и только тогда, когда число a взаимно просто с m. Значит, порядок группы обратимых элементов равен $\varphi(m)$. Отсюда, как и в первом доказательстве малой теоремы Ферма, следует сравнение (5).

Второе доказательство. Пусть имеется p^n предметов, расположенных по кругу, каждый из которых нужно раскрасить в один из a цветов. Число всех раскрасок равно a^{p^n}. Как и во втором доказательстве малой теоремы Ферма, можно показать, что если какая-то раскраска переходит в себя при нетривиальном повороте, то она является периодической с периодом, делящим p^{n-1}. Число таких раскрасок равно $a^{p^{n-1}}$ (достаточно задать цвета каких-либо p^{n-1} расположенных подряд предметов).

Оставшиеся $a^{p^n} - a^{p^{n-1}}$ апериодических раскрасок разобьем на классы, отнеся к одному классу раскраски, получаемые друг из друга поворотами. В силу предыдущего каждый класс состоит из p^n раскрасок. Отсюда и следует сравнение (8).

Третье доказательство. Это доказательство сложнее двух предыдущих, но его идеи будут полезны нам в дальнейшем для доказательства обобщения теоремы Эйлера на алгебраические числа.

Для любого целого числа N будем обозначать через $\operatorname{ord}_p N$ показатель наибольшей степени p, на которую делится N. Докажем, что

$$\operatorname{ord}_p C_{p^n}^k = n - \operatorname{ord}_p k \text{ при } 0 < k < p^n. \tag{9}$$

Это частный случай теоремы Куммера, позволяющей найти максимальную степень p, на которую делится любой заданный биномиальный коэффициент (см. [1]), но мы дадим здесь независимое доказательство.

Имеем, прежде всего,

$$\operatorname{ord}_p C_{p^n}^1 = \operatorname{ord}_p p^n = n.$$

Далее, при увеличении k на единицу в формуле

$$C_{p^n}^k = \frac{p^n(p^n-1)\cdot\ldots\cdot(p^n-k+1)}{1\cdot 2\cdot\ldots\cdot k}$$

добавляется по одному множителю в числителе и знаменателе, причем только один из них может делиться на p. Поэтому

$$\operatorname{ord}_p C_{p^n}^{k+1} = \begin{cases} \operatorname{ord}_p C_{p^n}^k, & \text{если } k \text{ и } k+1 \text{ не делятся на } p, \\ \operatorname{ord}_p C_{p^n}^k - \ell, & \text{если } \operatorname{ord}_p(k+1) = \ell > 0, \\ \operatorname{ord}_p C_{p^n}^k + \ell, & \text{если } \operatorname{ord}_p(k) = \ell > 0. \end{cases}$$

Таким образом, при прохождении каждого числа, кратного p, $\operatorname{ord}_p C_{p^n}^k$ уменьшается, но уже на следующем шаге статус-кво восстанавливается. Отсюда и следует (9).

Группируя в формуле бинома Ньютона

$$(x+y)^{p^n} = \sum_{k=0}^{p^n} C_{p^n}^k x^{p^n-k} y^k$$

слагаемые с одинаковыми значениями $\operatorname{ord}_p k$, получаем разложение

$$(x+y)^{p^n} = x^{p^n} + y^{p^n} + \sum_{\ell=1}^{n} p^\ell f_\ell(x^{p^{n-\ell}}, y^{p^{n-\ell}}), \tag{10}$$

где $f_1, \ldots, f_n$ — какие-то многочлены с целыми коэффициентами. Это разложение является обобщением сравнения (3).

Сравнение (3) означает, что

$$(x+y)^p = x^p + y^p + ph(x,y),$$

где $h \in \mathbb{Z}[x,y]$. Возводя это равенство в степень p^{n-1} и пользуясь формулой

бинома Ньютона и равенством (9), получаем сравнение

$$(x+y)^{p^n} \equiv (x^p + y^p)^{p^{n-1}} \pmod{p^n}. \tag{11}$$

Основываясь на разложении (10) и сравнении (11), мы покажем, что если сравнение (8) выполняется для двух целых чисел a и b (для всех степеней p), то оно выполняется и для их суммы. Так как оно, очевидно, выполняется для единицы, то отсюда следует, что оно выполняется для всех целых чисел.

Итак, пусть при всех n верно, что

$$a^{p^n} \equiv a^{p^{n-1}} \pmod{p^n}, \qquad b^{p^n} \equiv b^{p^{n-1}} \pmod{p^n}.$$

Из (11) следует, что

$$(a+b)^{p^n} \equiv (a^p + b^p)^{p^{n-1}} \pmod{p^n}.$$

Записывая разложение (10) для показателя $n-1$ и подставляя $x = a^p$, $y = b^p$, получаем:

$$(a^p + b^p)^{p^{n-1}} = a^{p^n} + b^{p^n} + \sum_{\ell=1}^{n-1} p^\ell g_\ell(a^{p^{n-\ell}}, b^{p^{n-\ell}}),$$

где $g_1, \ldots, g_{n-1}$ — какие-то многочлены с целыми коэффициентами. Так как

$$a^{p^{n-\ell}} \equiv a^{p^{n-\ell-1}} \pmod{p^{n-\ell}}, \qquad b^{p^{n-\ell}} \equiv b^{p^{n-\ell-1}} \pmod{p^{n-\ell}},$$

то

$$p^\ell g_\ell(a^{p^{n-\ell}}, b^{p^{n-\ell}}) \equiv p^\ell g_\ell(a^{p^{n-1-\ell}}, b^{p^{n-1-\ell}}) \pmod{p^n}.$$

Следовательно,

$$(a+b)^{p^n} \equiv a^{p^{n-1}} + b^{p^{n-1}} + \sum_{\ell=1}^{n-1} p^\ell g_\ell(a^{p^{n-1-\ell}}, b^{p^{n-1-\ell}}) = (a+b)^{p^{n-1}} \pmod{p^n},$$

что и требовалось доказать.

Задача 1. *Докажите, что для составного m утверждение малой теоремы Ферма (т. е. сравнение $a^m \equiv a \pmod{m}$ при всех целых a) может быть верно, только если m является произведением не менее трех различных нечетных простых чисел, и что наименьшее составное m, для которого это утверждение верно — это* 561.

3. Теорема Гаусса

В случае $m = p^n$ теорема Эйлера может быть записана в форме сравнения (8). Естественно спросить, что является аналогом этого сравнения в общем случае. Ответ на этот вопрос дается теоремой Гаусса: если

$m = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ — разложение m на простые множители, то

$$a^m - \sum_{i=1}^{s} a^{\frac{m}{p_i}} + \sum_{\substack{i,j=1 \\ i<j}}^{s} a^{\frac{m}{p_i p_j}} - \cdots + (-1)^s a^{\frac{m}{p_1 \cdot \ldots \cdot p_s}} \equiv 0 \pmod{m}. \qquad (12)$$

Например, при $m = 360$ имеем:

$$a^{360} - a^{180} - a^{120} - a^{72} + a^{60} + a^{36} + a^{24} - a^{12} \equiv 0 \pmod{360}. \qquad (13)$$

Сравнение (12) было доказано Гауссом только для простых a; в общем случае оно было доказано сразу несколькими математиками в 1880-е гг. Оно является легким следствием теоремы Эйлера. Не проводя формального доказательства в общем случае, продемонстрируем его на приведенном выше примере.

Для доказательства сравнения (13) достаточно проверить, что его левая часть A делится на 8, 9 и 5. Пользуясь теоремой Эйлера для этих модулей, получаем:

$$\begin{aligned}
A &= \big((a^{45})^8 - (a^{45})^4\big) - \big((a^{15})^8 - (a^{15})^4\big) - \big((a^9)^8 - (a^9)^4\big) + \\
&\quad + \big((a^3)^8 - (a^3)^4\big) \equiv 0 \pmod{8}, \\
A &= \big((a^{40})^9 - (a^{40})^3\big) - \big((a^{20})^9 - (a^{20})^3\big) - \big((a^8)^9 - (a^8)^3\big) + \\
&\quad + \big((a^4)^9 - (a^4)^3\big) \equiv 0 \pmod{9}, \\
A &= \big((a^{72})^5 - a^{72}\big) - \big((a^{36})^5 - a^{36}\big) - \big((a^{24})^5 - a^{24}\big) + \\
&\quad + \big((a^{12})^5 - a^{12}\big) \equiv 0 \pmod{5}.
\end{aligned}$$

Задача 2. *Докажите, что если a не делится на 2 и 5, то десятичная запись числа $a^{90} - a^{40} - a^{10}$ оканчивается на 99.*

4. Малая теорема Ферма для алгебраических чисел

Многочлен от одной переменной называется *нормированным*, если его старший коэффициент равен единице. Корни многочленов с целыми коэффициентами называются *алгебраическими числами*, а корни нормированных многочленов с целыми коэффициентами — *целыми алгебраическими числами*.

Пусть $a_1, \ldots, a_d$ — (вообще говоря, комплексные) корни нормированного многочлена $f \in \mathbb{Z}[x]$ степени d. Из формул Виета следует, что элементарные симметрические функции от $a_1, \ldots, a_d$ с точностью до знака равны коэффициентам многочлена f и, стало быть, являются обычными целыми числами. Более того, пусть $F \in \mathbb{Z}[x_1, \ldots, x_d]$ — произвольный симметрический многочлен с целыми коэффициентами; тогда по основной теореме о симметрических многочленах F представляется в виде многочлена

с целыми коэффициентами от элементарных симметрических функций и, следовательно, $F(a_1, \ldots, a_d) \in \mathbb{Z}$.

Следующая теорема является обобщением малой теоремы Ферма на алгебраические числа.

Теорема 1 (T. Schönemann, 1839). *Пусть $a_1, \ldots, a_d$ — корни нормированного многочлена $f \in \mathbb{Z}[x]$ степени d и p — простое число. Тогда*

$$a_1^p + \cdots + a_d^p \equiv a_1 + \cdots + a_d \pmod{p}. \tag{14}$$

Доказательство. Индукцией по числу переменных, исходя из сравнения (3), легко получить сравнение

$$(x_1 + \cdots + x_d)^p \equiv x_1^p + \cdots + x_d^p \pmod{p} \tag{15}$$

в кольце $\mathbb{Z}[x_1, \ldots, x_d]$. Подставляя в (15) $x_1 = a_1, \ldots, x_d = a_d$ и используя малую теорему Ферма в обычном варианте, получаем

$$a_1^p + \cdots + a_d^p \equiv (a_1 + \cdots + a_d)^p \equiv a_1 + \cdots + a_d \pmod{p},$$

что и требовалось доказать.

В качестве примера рассмотрим квадратный трехчлен $f = x^2 - 2x - 1$. Его корни — это $a_1 = 1 + \sqrt{2}$, $a_2 = 1 - \sqrt{2}$. При $p = 5$ получаем

$$a_1^5 + a_2^5 = 2(1 + 10 \cdot 5 + 5 \cdot 25) = 352 \equiv 2 = a_1 + a_2 \pmod{5}.$$

(Члены, содержащие $\sqrt{2}$, сокращаются.)

Следствие. *В обозначениях теоремы* 1, *если $F \in \mathbb{Z}[x_1, \ldots, x_d]$ — любой симметрический многочлен, то*

$$F(a_1^p, \ldots, a_d^p) \equiv F(a_1, \ldots, a_d) \pmod{p}. \tag{16}$$

Доказательство. Обозначим через $S(x_1^{k_1} \ldots x_d^{k_d})$ сумму всех различных одночленов, получаемых из $x_1^{k_1} \ldots x_d^{k_d}$ перестановками переменных. Например, при $d = 4$

$$S(x_1^2 x_2 x_3) = x_1^2(x_2x_3 + x_2x_4 + x_3x_4) + x_2^2(x_1x_3 + x_1x_4 + x_3x_4) + \\ + x_3^2(x_1x_2 + x_1x_4 + x_2x_4) + x_4^2(x_1x_2 + x_1x_3 + x_2x_3).$$

Ясно, что всякий симметрический многочлен с целыми коэффициентами является целочисленной линейной комбинацией многочленов такого вида. Поэтому достаточно доказать сравнение (16) в случае, когда $F = S(x_1^{k_1} \ldots x_d^{k_d})$.

Итак, пусть $F = S(x_1^{k_1} \ldots x_d^{k_d})$. Обозначим через $y_1, \ldots, y_\ell$ члены многочлена F и через $b_1, \ldots, b_\ell$ — их значения при $x_1 = a_1, \ldots, x_d = a_d$. Ясно, что

элементарные симметрические функции от $y_1, \dots, y_\ell$ — это какие-то симметрические многочлены с целыми коэффициентами от $x_1, \dots, x_d$. Следовательно, элементарные симметрические функции от $b_1, \dots, b_\ell$ являются целыми числами, а это означает, что $b_1, \dots, b_\ell$ суть корни некоторого нормированного многочлена с целыми коэффициентами. По теореме 1

$$b_1^p + \dots + b_\ell^p \equiv b_1 + \dots + b_\ell \pmod{p},$$

но это и есть сравнение (16).

5. Теорема Эйлера для алгебраических чисел

Обобщением теоремы Эйлера на алгебраические числа является

Теорема 2 (C. J. Smyth [2], 1986). *В обозначениях теоремы* 1,

$$a_1^{p^n} + \dots + a_d^{p^n} \equiv a_1^{p^{n-1}} + \dots + a_d^{p^{n-1}} \pmod{p^n}. \tag{17}$$

Следствие. *Если* $F \in \mathbb{Z}[x_1, \dots, x_d]$ *— любой симметрический многочлен, то*

$$F(a_1^{p^n}, \dots, a_d^{p^n}) \equiv F(a_1^{p^{n-1}}, \dots, a_d^{p^{n-1}}) \pmod{p}. \tag{18}$$

Вывод этого следствия дословно повторяет вывод следствия теоремы 1. Для дальнейшего нам важно отметить, что это рассуждение показывает, что если утверждение теоремы 2 верно для каких-то фиксированных p и n (но для всех целочисленных многочленов f), то утверждение следствия верно для тех же p и n.

Доказательство теоремы 2, данное в [2], основано на формулах Ньютона, выражающих рекуррентным образом степенные суммы через элементарные симметрические функции, и довольно хитрой комбинаторной интерпретации степенных сумм корней нормированного целочисленного многочлена в духе приведенного выше второго доказательства теоремы Эйлера. Мы дадим другое доказательство, основанное на идеях приведенного выше третьего доказательства теоремы Эйлера.

Получим вначале следующее обобщение разложения (10) на произвольное число переменных:

$$(x_1 + \dots + x_d)^{p^n} = x_1^{p^n} + \dots + x_d^{p^n} + \sum_{\ell=1}^{n} p^\ell f_\ell(x_1^{p^{n-\ell}}, \dots, x_d^{p^{n-\ell}}), \tag{19}$$

где $f_1, \dots, f_n$ — какие-то многочлены с целыми коэффициентами. Иными словами, докажем, что если не все показатели $k_1, \dots, k_d$ какого-то члена $cx_1^{k_1} \dots x_d^{k_d}$ многочлена $(x_1 + \dots + x_d)^{p^n}$ делятся на $p^{n-\ell}$, то коэффициент c делится на $p^{\ell+1}$. Пусть для определенности k_1 не делится на $p^{n-\ell}$. Тогда, полагая в формуле (10) $x = x_1$, $y = x_2 + \dots + x_d$, мы получаем требуемое.

Можно считать, что f_ℓ не содержит членов, все показатели которых делятся на p: иначе соответствующий член многочлена $p^\ell f_\ell(x_1^{p^{n-\ell}}, \ldots, x_d^{p^{n-\ell}})$ можно было бы отнести к предыдущему слагаемому разложения (19). При этом условии многочлены $f_1, \ldots, f_n$ определены однозначно и, следовательно, являются симметрическими (поскольку симметрическим является многочлен $(x_1 + \cdots + x_d)^{p^n}$).

Так же, как из сравнения (3) следует сравнение (11), из сравнения (15) следует сравнение

$$(x_1 + \cdots + x_d)^{p^n} \equiv (x_1^p + \cdots + x_d^p)^{p^{n-1}} \pmod{p^n}. \tag{20}$$

Запишем разложение (19) для показателя $n-1$:

$$(x_1 + \cdots + x_d)^{p^{n-1}} = x_1^{p^{n-1}} + \cdots + x_d^{p^{n-1}} + \sum_{\ell=1}^{n-1} p^\ell g_\ell(x_1^{p^{n-1-\ell}}, \ldots, x_d^{p^{n-1-\ell}}). \tag{21}$$

Здесь $g_1, \ldots, g_{n-1}$ — какие-то многочлены с целыми коэффициентами, которые, как было сказано выше, можно считать симметрическими. Используя это разложение для правой части сравнения (20), получаем:

$$(x_1 + \cdots + x_d)^{p^n} = x_1^{p^n} + \cdots + x_d^{p^n} + \sum_{\ell=1}^{n-1} p^\ell g_\ell(x_1^{p^{n-\ell}}, \ldots, x_d^{p^{n-\ell}}). \tag{22}$$

Доказательство теоремы 2. Будем доказывать теорему индукцией по n. При $n = 1$ это теорема 1. При $n > 1$ подставим $x_1 = a_1$, …, $x_d = a_d$ в (21) и (22). По обычной теореме Эйлера

$$(a_1 + \cdots + a_d)^{p^n} \equiv (a_1 + \cdots + a_d)^{p^{n-1}} \pmod{p^n}.$$

По предположению индукции

$$g_\ell(a_1^{p^{n-\ell}}, \ldots, a_d^{p^{n-\ell}}) \equiv g_\ell(a_1^{p^{n-1-\ell}}, \ldots, a_d^{p^{n-1-\ell}}) \pmod{p^{n-\ell}}$$

при $\ell = 1, \ldots, n-1$. Следовательно,

$$a_1^{p^n} + \cdots + a_d^{p^n} \equiv a_1^{p^{n-1}} + \cdots + a_d^{p^{n-1}} \pmod{p^n},$$

что и требовалось доказать.

6. Дальнейшие следствия и обобщения

Точно так же, как из обычной теоремы Эйлера выводится сравнение (12), из теоремы 2 выводится сравнение

$$a_1^m + \cdots + a_d^m - \sum_{i=1}^{s} \left(a_1^{\frac{m}{p_i}} + \cdots + a_d^{\frac{m}{p_i}} \right) + \sum_{\substack{i,j=1 \\ i<j}}^{s} \left(a_1^{\frac{m}{p_i p_j}} + \cdots + a_d^{\frac{m}{p_i p_j}} \right) - \cdots +$$

$$+(-1)^s\left(a_1^{\frac{m}{p_1\cdot\ldots\cdot p_s}}+\cdots+a_d^{\frac{m}{p_1\cdot\ldots\cdot p_s}}\right)\equiv 0 \pmod m,$$

где $m=p_1^{k_1}\cdot\ldots\cdot p_s^{k_s}$ — разложение m на простые множители, а $a_1,\ldots,a_d$ те же, что в теореме 2. (На самом деле в [2] сразу доказывается именно это сравнение.)

В своем докладе в Московском математическом обществе (см. также [3]) В. И. Арнольд высказал в качестве гипотезы следующее утверждение: если A — целочисленная квадратная матрица, то

$$\operatorname{tr} A^{p^n}\equiv \operatorname{tr} A^{p^{n-1}} \pmod{p^n}.$$

Это утверждение является немедленным следствием теоремы 2. В самом деле,

$$\operatorname{tr} A^m=a_1^m+\cdots+a_d^m,$$

где $a_1,\ldots,a_d$ — корни характеристического многочлена матрицы A, но последний ввиду целочисленности матрицы A является нормированным многочленом с целыми коэффициентами. Можно также заметить, что гипотеза Арнольда на самом деле эквивалентна теореме 2, так как всякий нормированный многочлен с целыми коэффициентами является характеристическим многочленом некоторой целочисленной матрицы.

А. В. Зарелуа [4] доказал следующее обобщение теоремы 2. Пусть K — некоторое поле алгебраических чисел; A — кольцо его целых чисел и $\mathfrak{p}$ — простой идеал кольца A, содержащий простое число $p\in\mathbb{Z}$ и обладающий свойством

$$a^{p^n}\equiv a^{p^{n-1}} \pmod{\mathfrak{p}^n}$$

для любого $a\in A$ и любого натурального n. Пусть, далее, $a_1,\ldots,a_d$ — корни нормированного многочлена степени d с коэффициентами из A. Тогда

$$a_1^{p^n}+\cdots+a_d^{p^n}\equiv a_1^{p^{n-1}}+\cdots+a_d^{p^{n-1}} \pmod{\mathfrak{p}^n}.$$

Эта теорема может быть доказана дословным повторением приведенного выше доказательства теоремы 2 с заменой сравнений по модулю p^n сравнениями по модулю $\mathfrak{p}^n$ (хотя в работе [4] дано другое доказательство).

Список литературы

[1] Винберг Э. Б. *Удивительные арифметические свойства биномиальных коэффициентов* // Математическое просвещение. Третья серия. Вып. 12. 2008.

[2] Smyth C. J. *A coloring proof of a generalization of Fermat's little theorem* // Amer. Math. Monthly. 1986, 93, no. 6, 469–471.

[3] Arnold V. I. *On the matricial version of Fermat – Euler congruences* // Japanese J. Math. Ser. 3, 2006, 1, 1–24.

[4] Зарелуа А. В. *О матричных аналогах малой теоремы Ферма* // Матем. заметки, 2006, 79, вып. 6, 838–853.

[5] Vinberg E. B. *On some number-theoretic conjectures of V. Arnold* // Japan. J. Math., 2007, 2, 297-302.

Э. Б. Винберг, механико-математический факультет МГУ

Издательство МЦНМО

В. В. Прасолов. **Задачи по алгебре, арифметике и анализу.** 2007. 608 с.

В книгу включены задачи по алгебре, арифметике и анализу, относящиеся к школьной программе, но, в основном, несколько повышенного уровня по сравнению с обычными школьными задачами. Есть также некоторое количество весьма трудных задач, предназначенных для учащихся математических классов. Сборник содержит более 1000 задач с полными решениями.

Для школьников, преподавателей математики, руководителей математических кружков, студентов пединститутов.

А. Шень. **Вероятность: примеры и задачи.** 2007. 64 с.

На примерах излагаются первые понятия теории вероятностей (вероятность события, правила подсчёта вероятностей, условная вероятность, независимость событий, случайная величина, математическое ожидание, дисперсия).

Брошюра рассчитана на школьников и учителей, свободно оперирующих с дробями и процентами.

А. Шень. **Игры и стратегии с точки зрения математики.** 2007. 40 с.

Хотите верьте, хотите нет — но либо в шахматах у белых есть гарантированный выигрыш, либо у чёрных есть гарантированная ничья. В этой брошюре рассказывается, что это значит, почему это верно (хотя и бесполезно в шахматной практике!), какие ещё бывают подобные игры и как их можно математически анализировать.

А. М. Райгородский. **Линейно-алгебраический метод в комбинаторике.** 2007. 136 с.

Современная комбинаторика — это весьма многогранная и активно развивающаяся область математики. В XX веке был разработан ряд мощных методов, позволяющих решать многие трудные задачи комбинаторики. Среди этих методов особое место занимает линейно-алгебраический метод. С его помощью удалось добиться прорыва в таких классических проблемах, как, например, проблема Борсука о разбиении множеств на части меньшего диаметра. В книге излагаются основы метода и описываются наиболее яркие примеры его применения. Для понимания материала достаточно знания элементарных понятий линейной алгебры и математического анализа. Книга будет полезна студентам и аспирантам, интересующимся комбинаторным анализом, а также специалистам в области дискретной математики.

А. В. Акопян, А. А. Заславский. **Геометрические свойства кривых второго порядка.** 2007. 136 с.

Книга посвящена тем свойствам коник (кривых второго порядка), которые формулируются и доказываются на чисто геометрическом языке (проективном или метрическом). Эти свойства находят применение в разнообразных задачах, а их исследование интересно и поучительно. Изложение начинается с элементарных фактов и доведено до весьма нетривиальных результатов, классических и современных. Раздел «Некоторые факты классической геометрии» является содержательным дополнением к традиционному курсу евклидовой планиметрии, расширяющим математический кругозор читателя.

Книга демонстрирует преимущества чисто геометрических методов, сочетающих наглядность и логическую прозрачность. Она содержит значительное количество задач, решение которых тренирует геометрическое мышление и интуицию.

Книга может быть полезна для школьников старших классов, студентов физико-математических специальностей, преподавателей и широкого круга любителей математики.

Локальные и глобальные методы в арифметике

А. А. Панчишкин

1. p-адические числа и сравнения

Идея расширения поля $\mathbb{Q}$ в теории чисел встречается в различных вариантах. Например, вложение $\mathbb{Q} \subset \mathbb{R}$ часто дает полезные необходимые условия существования решений диофантовых уравнений над $\mathbb{Q}$ и над $\mathbb{Z}$. Важное свойство поля $\mathbb{R}$ — его полнота: любая фундаментальная последовательность (последовательность Коши) $\{\alpha_n\}_{n=1}^{\infty}$ в $\mathbb{R}$ имеет предел. Фундаментальность означает, что абсолютная величина разности $\alpha_n - \alpha_m$ стремится к 0, когда n и m стремятся к бесконечности. Кроме того, все элементы поля $\mathbb{R}$ являются пределами фундаментальных последовательностей $\{\alpha_n\}_{n=1}^{\infty}$ с $\alpha_n \in \mathbb{Q}$. Таким образом, можно сказать, что поле $\mathbb{R}$ получается из $\mathbb{Q}$ «присоединением пределов фундаментальных последовательностей». Такая конструкция называется *пополнением*.

Определение предела и фундаментальной последовательности дается в терминах абсолютной величины числа. Абсолютная величина обладает следующими свойствами:

$$\text{а) } |a| \geqslant 0, \text{ причем } |a| = 0 \text{ тогда и только тогда, когда } a = 0; \quad (1)$$

$$\text{б) } |ab| = |a| \cdot |b|; \quad (2)$$

$$\text{в) } |a + b| \leqslant |a| + |b|. \quad (3)$$

Всякая вещественная функция $|\cdot|$ на каком-либо поле K, обладающая этими свойствами, называется (мультипликативным) *нормированием* поля K. Для поля $\mathbb{Q}$, помимо абсолютной величины, существуют и другие нормирования. Так, для любого простого p можно определить так называемое *p-адическое нормирование* $|\cdot|_p$:

$$|a/b|_p = p^{\mathrm{ord}_p b - \mathrm{ord}_p a}, \quad |0|_p = 0,$$

где $\mathrm{ord}_p a$ есть наивысшая степень числа p, делящая целое число a. Согласно теореме Островского, всякое нормирования поля $\mathbb{Q}$ с точностью до постоянного (положительного) множителя есть либо абсолютная величина, либо p-адическое нормирование для некоторого простого p.

Пополнение поля $\mathbb{Q}$ относительно p-адического нормирования называется *полем p-адических чисел* и обозначается через $\mathbb{Q}_p$. Легко видеть, что нормирование (в данном случае p-адическое) однозначно продолжается на пополнение.

Использование вложений поля $\mathbb{Q}$ в его пополнения по всем нормированиям, то есть в $\mathbb{R}$ и в $\mathbb{Q}_p$ для всех простых p, часто значительно упрощает ситуацию в арифметических задачах. Замечательный пример дает *теорема Минковского – Хассе* (см.[1], глава 1): уравнение

$$\sum_{i,j} a_{ij} x_i x_j = 0 \ (a_{ij} \in \mathbb{Q}) \tag{4}$$

имеет нетривиальное решение в рациональных числах в том и только в том случае, когда оно нетривиально разрешимо над $\mathbb{R}$ и над $\mathbb{Q}_p$ для всех простых чисел p. Для нахождения решений уравнений над $\mathbb{Q}_p$ можно эффективно применять такие приемы, взятые из вещественного анализа, как «метод касательных Ньютона», который в p-адическом случае известен как *лемма Гензеля*.

Наиболее простым способом можно ввести p-адические числа как выражения вида

$$\alpha = a_m p^m + a_{m+1} p^{m+1} + \dots, \tag{5}$$

где $a_i \in \{0, 1, \dots . p-1\}$ – цифры (по основанию p), а $m \in \mathbb{Z}$. При этом число α называется целым, если $m \geqslant 0$. Удобно записывать α в виде последовательности цифр, бесконечной влево:

$$\alpha = \begin{cases} \cdots a_{m+1} a_m \overbrace{000\dots0}^{m-1}{}_{(p)}, & \text{если } m \geqslant 0, \\ \cdots a_1 a_0, a_{-1} \cdots a_{m(p)}, & \text{если } m < 0. \end{cases}$$

Эти выражения образуют поле, в котором сложение и умножение выполняются так же, как для рациональных чисел вида $p^m n \, (m \in \mathbb{Z}, n \in \mathbb{N})$, записанных по основанию p (с конечным числом цифр после запятой). На самом деле в этом поле лежат все рациональные числа. Например,

$$-1 = \frac{p-1}{1-p} = (p-1) + (p-1)p + (p-1)p^2 + \cdots = \cdots (p-1)(p-1)_{(p)}.$$

Если $n \in \mathbb{N}$, то выражение для $-n = n \cdot (-1)$ вида (5) получается, если перемножить такие выражения для n и для -1. Если n не делится на p, то выражение для $-\dfrac{1}{n}$ может быть получено следующим образом. По теореме Эйлера $p^{\varphi(n)} - 1 = un$, где $u \in \mathbb{N}$. Положим $\varphi(n) = r$. Тогда

$$-\frac{1}{n} = \frac{u}{1-p^r} \, .$$

Так как $u < un = p^r$, то запись по основанию p числа u имеет вид $a_{r-1}\cdots a_{0(p)}$ (где, быть может, первые несколько цифр равны 0). Следовательно,

$$-\frac{1}{n} = \cdots a_0\overbrace{a_{r-1}\cdots a_0}^{r}\overbrace{a_{r-1}\cdots a_0}^{r}{}_{(p)}.$$

Пользуясь этим, легко получить p-адическое выражение для любого рационального числа. Например, для $p = 5$ имеем

$$\frac{9}{7} = 2 - \frac{5}{7} = 2 + \frac{5\cdot 2232}{1-5^6}.$$

Так как

$$2232 = 3\cdot 5^4 + 2\cdot 5^3 + 4\cdot 5^2 + 1\cdot 5 + 2,$$

то

$$\frac{9}{7} = \cdots\overbrace{032412032412}\,2_{(5)}.$$

Нетрудно проверить, что пополнение поля $\mathbb{Q}$ относительно p-адической метрики $|\cdot|_p$ отождествляется с полем «p-адических разложений» вида (5) (см. [2]). При этом $|\alpha|_p = p^m$, если в выражении (5) для α имеем $a_m \neq 0$.

Разложения (5) p-адических чисел можно рассматривать как аналоги разложения функции f переменной x в окрестности точки a по степеням $(x-a)$, причем p является аналогом $(x-a)$.

Любопытно также сравнить разложения (5), «бесконечные влево», с десятичными разложениями действительных чисел $\alpha \in \mathbb{R}$, «бесконечными вправо»:

$$\alpha = a_m a_{m-1}\cdots a_0, a_{-1}\cdots = \\ = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_0 + a_{-1}10^{-1} + \cdots, \quad (6)$$

где $a_i \in \{0, 1, \cdots, 9\}$. Разложения такого типа по любому основанию приводят к одному и тому же полю $\mathbb{R}$. Их можно рассматривать как аналоги разложения функции f переменной x в окрестности бесконечности по степеням x^{-1}.

Поле $\mathbb{Q}_p$ является *полным метрическим пространством*. Более того, из любой ограниченной по норме последовательности p-адических чисел можно выбрать сходящуюся подпоследовательность. Это легко доказывается с помощью последовательного рассмотрения p-адических цифр справа налево, с учетом того, что у всех членов последовательности число знаков после запятой ограничено фиксированным числом. Иначе говоря, всякий «открытый диск» $U(r) = \{x \in \mathbb{Q}_p \mid |x|_p < r\}$, а также всякий «замкнутый диск» $D(r) = \{x \in \mathbb{Q}_p \mid |x|_p \leqslant r\}$, компактны. При этом и $U(r)$, и $D(r)$ являются открыто-замкнутыми подмножествами в $\mathbb{Q}_p$.

В частности, кольцо целых p-адических чисел

$$\mathbb{Z}_p = D(1) = \{x \in \mathbb{Q}_p \mid \ |x|_p \leqslant 1\} = \left\{x = a_0 + a_1 p + a_2 p^2 + \cdots\right\}$$

— это компактное топологическое кольцо. Оно совпадает с замыканием множества $\mathbb{Z}$ обычных целых чисел в $\mathbb{Q}_p$.

Множество обратимых элементов («единиц») кольца $\mathbb{Z}_p$ — это

$$\mathbb{Z}_p^\times = \mathbb{Z}_p \backslash p\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid \ |x|_p = 1\} = \left\{x = a_0 + a_1 p + a_2 p^2 + \cdots \mid a_0 \neq 0\right\}.$$

Оно является группой по умножению. Для описания этой группы положим $\nu = 1$, если $p > 2$, и $\nu = 2$, если $p = 2$, и рассмотрим подгруппу

$$U_p = \left\{x \in \mathbb{Z}_p^\times \mid x \equiv 1 \pmod{p^\nu}\right\}.$$

Отображение, определяемое степенным рядом

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}\,,$$

задает гомоморфизм аддитивной группы $p^\nu\mathbb{Z}_p$ в мультипликативную группу U_p. На самом деле это изоморфизм, так как существует обратное отображение, задаваемое рядом

$$\log(x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}\,.$$

Можно показать, что

$$\mathbb{Q}_p^\times = \{p^m \mid m \in \mathbb{Z}\} \times \mathbb{Z}_p^\times, \quad \mathbb{Z}_p^\times \cong (\mathbb{Z}/p^\nu\mathbb{Z})^\times \times U_p, \tag{7}$$

где $\nu = 1$, если $p > 2$, $\nu = 2$, если $p = 2$.

1.1. Приложения p-адических чисел к решению сравнений

Возникновение p-адических чисел в работах Гензеля было связано с проблемой решения сравнений по модулю p^n, а применение их к теории квадратичных форм его учеником Хассе привело к элегантной формулировке теории квадратичных форм над рациональными числами, не использующей рассмотрений в кольцах вычетов $\mathbb{Z}/p^n\mathbb{Z}$, работать с которыми затруднительно из-за наличия в них делителей нуля.

Нетрудно видеть, что если $f(x_1, \ldots, x_n) \in \mathbb{Z}_p[x_1, \ldots, x_n]$, то сравнения

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p^n}$$

разрешимы при любом $n \geqslant 1$ тогда и только тогда, когда уравнение

$$f(x_1, \ldots, x_n) = 0$$

разрешимо в целых p-адических числах. Эти решения в $\mathbb{Z}_p$ можно находить с помощью p-адического варианта метода касательных Ньютона.

Теорема 1 (лемма Гензеля). *Пусть $f(x) \in \mathbb{Z}_p[x]$ — многочлен одной переменной x, $f'(x) \in \mathbb{Z}_p[x]$ — его формальная производная и для некоторого $\alpha_0 \in \mathbb{Z}_p$ выполнено начальное условие*

$$|f(\alpha_0)/f'(\alpha_0)^2|_p < 1 \tag{8}$$

Тогда существует единственное такое $\alpha \in \mathbb{Z}_p$, что

$$f(\alpha) = 0, \quad |\alpha - \alpha_0|_p < 1.$$

Доказательство проводится с помощью рассмотрения последовательности

$$\alpha_n = \alpha_{n-1} - \frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}\,.$$

С учетом формального разложения Тейлора многочлена $f(x)$ в точке $x = \alpha_{n-1}$ проверяется, что последовательность фундаментальна, а ее предел α обладает всеми необходимыми свойствами (см. [1], [6]).

Например, если $f(x) = x^{p-1} - 1$, то любое $\alpha_0 \in \{1, 2, \ldots, p-1\}$ удовлетворяет условию $|f(\alpha_0)|_p < 1$, в то время как $f'(\alpha_0) = (p-1)\alpha_0^{p-2} \not\equiv \not\equiv 0 \pmod p$, так что начальное условие (8) выполнено. Корень $\alpha \equiv \alpha_0 \pmod p$ называется представителем Тейхмюллера числа α_0 и обозначается через $\omega(\alpha_0)$. Например, для $p = 5$ имеем

$$\begin{aligned}
&\omega(1) = 1;\\
&\omega(2) = 2 + 1\cdot 5 + 2\cdot 5^2 + 1\cdot 5^3 + 3\cdot 5^4 \cdots;\\
&\omega(3) = 3 + 3\cdot 5 + 2\cdot 5^2 + 3\cdot 5^3 + 1\cdot 5^4 + \cdots;\\
&\omega(4) = 4 + 4\cdot 5 + 4\cdot 5^2 + 4\cdot 5^3 + 4\cdot 5^4 + \cdots = -1;
\end{aligned}$$

Описанный метод применим и к многочленам многих переменных, но уже без единственности находимого решения, (см. [1], [6]).

Еще одно приложение леммы Гензеля связано с описанием квадратов поля $\mathbb{Q}_p$: для произвольного элемента

$$\alpha = p^m \cdot v \ \in \ \mathbb{Q}_p \ \ (m \in \mathbb{Z},\ v \in \mathbb{Z}_p^\times)$$

свойство α быть квадратом в $\mathbb{Q}_p$ равносильно тому, что

а) если $p > 2$, то $m \in 2\mathbb{Z}$, а $\overline{v} \equiv v \pmod p \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}$ (то есть $\left(\frac{\overline{v}}{p}\right) = 1$, где $\left(\frac{\overline{v}}{p}\right)$ — символ Лежандра);

б) если $p = 2$, то $m \in 2\mathbb{Z}$, а $v \equiv 1 \pmod 8$.

Разрешимость уравнения $x^2 = \alpha$ в $\mathbb{Q}_p$ при условиях а) и б) выводится из леммы Гензеля, а необходимость этих условий вытекает из простых рассмотрений по модулю p и по модулю 8. Как следствие мы получаем, что факторгруппа $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$

а) при $p > 2$ изоморфна $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ с системой представителей $\{1, p, v, pv\}$, $\left(\frac{v}{p}\right) = -1$;

б) при $p = 2$ изоморфна $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ с системой представителей $\{\pm 1, \pm 5, \pm 2, \pm 10\}$.

2. Диофантовы системы линейных уравнений и сравнений

2.1. Вычисления с классами вычетов.

С точки зрения алгебры множество $\mathbb{Z}$ целых чисел является коммутативным ассоциативным кольцом с единицей, то есть множеством с двумя коммутативными и ассоциативными операциями (сложение и умножение), связанными друг с другом законом дистрибутивности.

Пусть N — фиксированное натуральное число. Остатки от деления на N подразделяют все целые числа на непересекающиеся классы

$$\bar{a} = a + N\mathbb{Z}, \quad 0 \leqslant a \leqslant N - 1,$$

которые также образуют кольцо

$$\mathbb{Z}/N\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{N-1}\},$$

называемое кольцом вычетов по модулю N. При этом равенство $\bar{a} = \bar{b}$ равносильно сравнению $a \equiv b \pmod N$.

Часто в задачах теории чисел вычисления в кольце $\mathbb{Z}$ можно сводить к вычислениям в кольцах вычетов $\mathbb{Z}/N\mathbb{Z}$. Это доставляет ряд удобств. Например, на многие элементы из $\mathbb{Z}/N\mathbb{Z}$ можно делить, оставаясь в пределах этого кольца (в отличие от целых чисел, где всегда определено только деление на ± 1). Действительно, если число a взаимно просто с N, то есть $(a, N) = 1$, класс $\bar{a}$ обратим, так как в этом случае существуют такие целые числа $x,\ y$, что $ax + Ny = 1$, и поэтому $\bar{a} \cdot \bar{x} = \bar{1}$. Так получаются все обратимые элементы кольца вычетов $\mathbb{Z}/N\mathbb{Z}$. Они образуют группу по умножению, обозначаемую $(\mathbb{Z}/N\mathbb{Z})^\times$. Порядок этой группы обозначается через $\varphi(N)$ (функция Эйлера). Название происходит от обобщения малой теоремы Ферма, принадлежащего Эйлеру:

$$a^{\varphi(N)} \equiv 1 \pmod N \tag{9}$$

для всех таких чисел a, что $(a, N) = 1$, то есть $\bar{a}^{\varphi(N)} = \bar{1}$ для всех обратимых элементов $\bar{a}$ в кольце $\mathbb{Z}/N\mathbb{Z}$.

Доказательство Эйлера, применимое к любой конечной абелевой группе порядка f, показывает, что порядок любого элемента a делит f. А именно, умножение на a является перестановкой элементов группы (в нашем случае группы $(\mathbb{Z}/N\mathbb{Z})^\times$ порядка $f = \varphi(N)$). Произведение всех элементов группы при этой перестановке умножается на a^f. Поэтому $a^f = 1$.

Если число N разложено в произведение $N = N_1 N_2 \cdot \ldots \cdot N_k$ попарно взаимно простых чисел, то имеется разложение

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/N_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/N_k\mathbb{Z} \tag{10}$$

в прямую сумму колец, что эквивалентно китайской теореме об остатках: для любых вычетов $a_i \bmod N_i$, $i = 1, \ldots, k$, найдется такое целое число a, что $a \equiv a_i \pmod{N_i}$ для всех i. Практический поиск числа a можно быстро осуществить, применяя повторно алгоритм Евклида. Положим $M_i = N/N_i$; тогда числа M_i и N_i по условию взаимно просты и, значит, существуют такие целые числа X_i, что $X_i M_i \equiv 1 \pmod{N_i}$. Искомым числом тогда будет

$$a = \sum_{i=1}^{k} a_i X_i M_i. \tag{11}$$

Из разложения (10) вытекает и разложение мультипликативной группы:

$$(\mathbb{Z}/N\mathbb{Z})^\times \cong (\mathbb{Z}/N_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/N_k\mathbb{Z})^\times, \tag{12}$$

из которого, в частности, следует, что $\varphi(N) = \varphi(N_1) \cdot \ldots \cdot \varphi(N_k)$. Поскольку для простого числа p имеем $\varphi(p^a) = p^{a-1}(p-1)$, мы можем найти $\varphi(N)$, исходя из разложения числа N на простые множители.

В специальном случае, когда N — простое число, кольцо вычетов $\mathbb{Z}/N\mathbb{Z}$ является полем: в нем обратим любой элемент, отличный от нуля.

2.2. Системы линейных уравнений с целыми коэффициентами

В этом параграфе все буквы (коэффициенты и неизвестные в уравнениях) означают целые числа.

Из алгоритма Евклида вытекает, что уравнение

$$ax + by = c \tag{13}$$

разрешимо тогда и только тогда, когда c делится на $d = (a, b)$.

Уравнение (13) дает первый пример общей проблемы: для системы алгебраических уравнений с целыми коэффициентами

$$F_1(x_1,\dots,x_n)=0,\ \cdots\ ,F_m(x_1,\dots,x_n)=0 \tag{14}$$

найти все целочисленные (или все рациональные) решения. Для уравнения (13) задача нахождения рациональных решений тривиальна. Если в системе (14) все уравнения линейные, то и для нее все рациональные решения легко находятся последовательным исключением неизвестных (например, по методу Гаусса).

Опишем общий прием нахождения всех целочисленных решений системы целочисленных линейных уравнений

$$Ax=b, \tag{15}$$

где

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n}\\ \dots & \dots & \ddots & \dots\\ a_{m1} & a_{m2} & \cdots & a_{mn}\end{pmatrix}\in M_{m,n}(\mathbb{Z}),\quad x=\begin{pmatrix} x_1\\ \cdots\\ x_n\end{pmatrix},\quad b=\begin{pmatrix} b_1\\ \cdots\\ b_m\end{pmatrix}.$$

Эта задача также сводится к применению алгоритма Евклида.

Элементарным преобразованием над $\mathbb{Z}$ строк матрицы назовем преобразование, при котором к некоторой строке прибавляют другую, умноженную на целое число, а остальные строки не меняют. Проверяется, что применение такого преобразования эквивалентно умножению исходной матрицы слева на некоторую матрицу из $\mathrm{SL}_m(\mathbb{Z})$ (целочисленную матрицу с определителем, равным 1). Аналогичное преобразование столбцов равносильно умножению матрицы справа на некоторую матрицу из $\mathrm{SL}_n(\mathbb{Z})$.

Применение нескольких элементарных преобразований приводит матрицу A к виду UAV с $U\in\mathrm{SL}_m(\mathbb{Z}), V\in\mathrm{SL}_n(\mathbb{Z})$, а целочисленные решения соответствующей системы уравнений

$$UAVy=Ub \tag{16}$$

и исходной системы (15) взаимно однозначно соответствуют друг другу по формуле $x=Vy$.

Действуя, как в алгоритме Евклида, с помощью описанных преобразований и, быть может, умножений каких-то строк на -1 матрицу A можно привести к диагональному виду

$$D=\begin{pmatrix} d_1 & 0 & 0 & \dots & 0\\ 0 & d_2 & 0 & \dots & 0\\ \dots & \dots & \ddots & \dots & 0\\ 0 & 0 & \dots & d_r & \dots\\ \dots & \dots & \dots & \dots & \dots\end{pmatrix} \tag{17}$$

(где на диагонали после выписанных элементов стоят нули). Система уравнений примет тогда вид

$$d_i y_i = c_i \text{ для } i \leqslant r, \quad c_i = 0 \text{ для остальных } i.$$

Эта система легко решается, причем критерий ее совместности (а значит, и совместности исходной системы) над $\mathbb{Z}$ состоит в том, что $d_i \mid c_i$ для всех $i \leqslant r$ и $c_i = 0$ для остальных i.

В частности, отсюда следует, что для совместности над $\mathbb{Z}$ системы (15) необходимо и достаточно, чтобы была разрешима соответствующая система сравнений

$$Ax \equiv b \pmod{p^m}$$

для любого простого p и любого натурального m, а это, в свою очередь, равносильно совместности системы (15) над $\mathbb{Z}_p$ для любого простого p. Критерий такого рода называется принципом Минковского – Хассе, и он часто встречается в задачах диофантовой геометрии.

3. Уравнения второй степени

3.1. Квадратичные формы и квадрики

Для диофантова уравнения

$$f(x_1, x_2, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j + \sum_{i=1}^{n} b_i x_i + c = 0 \tag{18}$$

находить целочисленные решения значительно труднее, чем рациональные, хотя и последняя задача уже нетривиальна.

Известный пример — рациональная параметризация окружности $x^2 + y^2 = 1$ по формулам универсальной подстановки

$$x = \frac{2t}{1+t^2}\,,\ y = \frac{1-t^2}{1+t^2} \quad \left(x = \cos\varphi,\ y = \sin\varphi,\ t = \operatorname{tg}\left(\frac{\varphi}{2}\right)\right). \tag{19}$$

Полагая $t = u/v$, получаем отсюда следующее описание всех примитивных пифагорейских троек (X, Y, Z), то есть натуральных решений уравнения $X^2 + Y^2 = Z^2$ с $(X,\ Y,\ Z) = 1$:

$$X = 2uv,\ Y = u^2 - v^2,\ Z = u^2 + v^2,$$

где $u > v > 0$ — взаимно простые натуральные числа противоположной четности.

При отыскании рациональных решений уравнения (18) удобно перейти к квадратичной форме

$$F(X_0, X_1, \cdots, X_n) = \sum_{i,j=0}^{n} f_{ij} X_i X_j = \\ = \sum_{i,j=1}^{n} f_{ij} X_i X_j + 2\sum_{i=1}^{n} f_{i0} X_i X_0 + f_{00} X_0^2, \qquad (20)$$

где $f_{ij} = f_{ji} = a_{ij}$ для $1 \leqslant i < j \leqslant n$, $f_{0i} = f_{i0} = b_i/2$ для $1 \leqslant i \leqslant n$ и $f_{00} = c$. Для этого надо заменить «неоднородные координаты» $x_1, \ldots, x_n$ на «однородные» $X_0, \ldots, X_n$ по формулам $x_i = X_i/X_0$ $(i = 1, 2, \ldots, n)$. Квадратичная форма F является однородным многочленом второй степени, который удобно записывать в матричной форме

$$F(X) = X^t A_F X, \quad X^t = (X_0, X_1, \ldots, X_n),$$

где $A_F = (f_{ij})$ — матрица коэффициентов. Если существует ненулевое рациональное решение уравнения $F(X) = 0$, то говорят, что форма F представляет нуль над полем $\mathbb{Q}$.

Рассмотрим квадрику

$$Q_F = \{(X_0 : X_1 : \cdots : X_n) \in \mathbb{CP}^n \mid F(X_0, X_1, \ldots, X_n) = 0\}$$

в комплексном проективном пространстве $\mathbb{CP}^n$. Ненулевое рациональное решение X^0 уравнения $F(X) = 0$ определяет точку на квадрике Q_F. Остальные рациональные точки (рациональные решения) легко найти: они совпадают с точками пересечения квадрики Q_F со всевозможными прямыми, выходящими из X^0 в направлении векторов с рациональными координатами. Пусть Y^0 — какая-либо рациональная точка. Проективная прямая, проходящая через X^0 и Y^0, состоит из точек $uX^0 + vY^0$. Уравнение $F(uX^0 + vY^0) = 0$ сводится к уравнению

$$u\sum_{i=1}^{n} \frac{\partial F}{\partial X_i}(X^0) Y_i^0 + vF(Y^0) = 0.$$

Если точка X^0 не является вершиной квадрики, то есть если $\dfrac{\partial F}{\partial X_i}(X^0) \neq 0$ хотя бы для одного i, то для любого Y^0 находится точка пересечения квадрики Q_F с этой прямой:

$$v = -u\sum_{i=1}^{n} \frac{\partial F}{\partial X_i}(X^0) Y_i^0 / F(Y^0). \qquad (21)$$

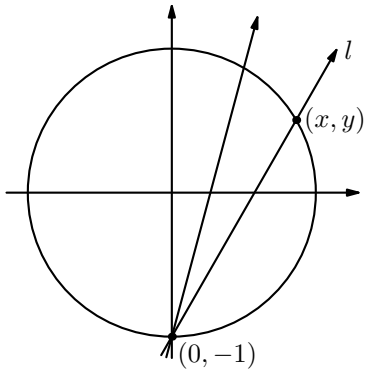


Рис. 1.

(Если $F(Y^0) = 0$, то Y^0 уже на Q_F.)

Примером рассмотренной конструкции, записанным в неоднородных координатах, являются формулы (19). Чтобы найти все пары (x, y) рациональных чисел, для которых $x^2 + y^2 = 1$, рассмотрим прямую l, проходящую через точки $(0, -1)$ и (x, y) (рис. 1). Эта прямая имеет угловой коэффициент $t = \dfrac{y+1}{x}$, который может быть любым рациональным числом. Находя точку пересечения этой прямой с окружностью, получаем формулы (19).

При нахождении рациональных решений уравнения

$$F(X_0, X_1, \ldots, X_n) = 0 \tag{22}$$

(с квадратичной формой F из (20)) можно считать, что форма F диагональна: метод Лагранжа выделения полных квадратов дает замену переменных $X = CY$ с невырожденной рациональной матрицей C, приводящую форму F к диагональному виду.

Для однородных уравнений типа (22) нет существенной разницы между их целочисленными и рациональными решениями: после умножения на подходящее целое число любое рациональное решение становится целочисленным, и его можно считать примитивным, то есть имеющим взаимно простые в совокупности координаты. Наиболее фундаментальным фактом теории квадратичных форм над полем рациональных чисел является следующий результат.

3.2. Принцип Минковского – Хассе для квадратичных форм

Теорема 2. *Невырожденная рациональная квадратичная форма $F(x_1, x_2, \ldots, x_n)$ представляет нуль над полем рациональных чисел тогда*

и только тогда, когда она представляет нуль над полем $\mathbb{R}$ *вещественных чисел (то есть является неопределенной) и над полем* $\mathbb{Q}_p$ *p-адических чисел для любого простого* p.

(См. [1], глава 1. Конечно, утверждение «только тогда» тривиально.)

Приведем красивое доказательство этой теоремы для ключевого случая $n = 3$, рассмотренного Лежандром ([1]).

Путем линейной замены переменных с рациональными коэффициентами приведем форму F к диагональному виду. Пусть

$$F = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 \qquad (a_1a_2a_3 \neq 0).$$

Неопределенность формы F означает, что не все коэффициенты a_1, a_2, a_3 одного знака. Умножив форму при необходимости на -1, мы придем к случаю, когда два коэффициента положительны, а один отрицателен. Кроме того, мы можем считать эти числа целыми, свободными от квадратов и взаимно простыми в совокупности, так как их можно сократить на наибольший общий делитель. Далее, если, например, a_1 и a_2 имеют общий простой делитель p, то, умножив форму на p и взяв px и py за новые переменные, мы получим форму с коэффициентами a_1/p, a_2/p и pa_3. Повторяя этот процесс несколько раз, мы заменим нашу форму формой вида

$$F = ax^2 + by^2 - cz^2, \tag{23}$$

в которой a, b, c — попарно взаимно простые свободные от квадратов натуральные числа.

Пусть теперь p — какой-нибудь простой делитель числа c, и пусть (x_0, y_0, z_0) — ненулевое решение уравнения $F = 0$ над полем $\mathbb{Q}_p$. Можно считать, что x_0, y_0, z_0 — целые p-адические числа, не делящиеся одновременно на p. Рассматривая равенство

$$ax_0^2 + by_0^2 - cz_0^2 = 0$$

по модулю p^2, мы видим, что x_0 и y_0 не могут одновременно делиться на p (так как тогда и z_0 делилось бы на p). Пусть для определенности y_0 не делится на p. Тогда можно считать, что $y_0 = 1$. При этом условии мы получаем разложение на множители

$$F \equiv a(x + x_0y)(x - x_0y) \pmod{p}.$$

Аналогичные разложения имеют место по модулю простых p, делящих a и b. Таким образом, для любого простого $p \mid abc$ существуют такие целочисленные линейные формы $L^{(p)}$, $M^{(p)}$ от x, y, z, что

$$F \equiv L^{(p)}M^{(p)} \pmod{p}.$$

Теперь с помощью китайской теоремы об остатках найдем такие целочисленные линейные формы L, M, что

$$L \equiv L^{(p)} \pmod{p}, \quad M \equiv M^{(p)} \pmod{p}$$

для всех $p \mid abc$, и мы получим

$$F \equiv LM \pmod{abc}. \tag{24}$$

Будем придавать переменным x, y, z целые значения, удовлетворяющие условиям

$$0 \leqslant x < \sqrt{bc}, \quad 0 \leqslant y < \sqrt{ac}, \quad 0 \leqslant z < \sqrt{ab}. \tag{25}$$

Если исключить из рассмотрения тривиальный случай $a = b = c = 1$, то не все числа $\sqrt{bc}$, $\sqrt{ac}$, $\sqrt{ab}$ целые и число троек (x, y, z), удовлетворяющих условиям (25), строго больше, чем $\sqrt{bc}\sqrt{ac}\sqrt{ab} = abc$. Следовательно, для каких-то двух различных троек форма L принимает одно и то же значение по модулю abc, откуда в силу линейности формы L получаем

$$L(x_0, y_0, z_0) \equiv 0 \pmod{abc} \tag{26}$$

для некоторых $|x_0| < \sqrt{bc}$, $|y_0| < \sqrt{ac}$, $|z_0| < \sqrt{ab}$. Поэтому

$$ax_0^2 + by_0^2 - cz_0^2 \equiv 0 \pmod{abc} \tag{27}$$

и имеют место неравенства

$$-abc < ax_0^2 + by_0^2 - cz_0^2 < 2abc.$$

Таким образом,

$$ax_0^2 + by_0^2 - cz_0^2 = 0 \text{ или } abc.$$

В первом случае теорема доказана. Во втором случае доказательство следует из равенства

$$a(x_0z_0 + by_0)^2 + b(y_0z_0 - ax_0)^2 - c(z_0^2 + ab)^2 = 0.$$

В формулировке Лежандра диофантово уравнение $ax^2 + by^2 - cz^2 = 0$ рассмотренного выше вида имеет нетривиальное целочисленное решение в том и только в том случае, когда классы вычетов

$$bc \,(\mathrm{mod}\, a), \quad ac \,(\mathrm{mod}\, b), \quad -ab \,(\mathrm{mod}\, c)$$

являются квадратами.

Можно доказать, что рациональная квадратичная форма ранга $\geqslant 5$ всегда представляет нуль над $\mathbb{Q}$.

В общем случае существуют эффективные методы (основанные на принципе Минковского – Хассе) выяснения того, представляет ли нуль данная рациональная квадратичная форма. Эти методы используют символ Гильберта.

3.3. Символ Гильберта

В этом пункте мы допускаем значение $p = \infty$, считая, что $\mathbb{Q}_\infty = \mathbb{R}$ и $|\cdot|_\infty = |\cdot|$.

Символ Гильберта (символ норменного вычета) $(a,b)_p$ для $a, b \in \mathbb{Q}_p^\times$ определяется равенством

$$(a,b)_p = \begin{cases} 1, \text{ если уравнение } ax^2 + by^2 = 1 \text{ имеет решение в } \mathbb{Q}_p, \\ -1 \text{ в противном случае.} \end{cases}$$

Ясно, что $(a,b)_p$ не меняется при умножении a и b на квадраты любых элементов из $\mathbb{Q}_p^\times$, то есть зависит только от классов a и b по модулю подгруппы квадратов в $\mathbb{Q}_p^\times$.

Заметим, что если квадратичная форма $ax^2 + by^2$ представляет нуль в поле $\mathbb{Q}_p$, то она разлагается на линейные множители и, следовательно, принимает все значения в $\mathbb{Q}_p$. В частности, в этом случае $(a,b)_p = 1$.

Иногда бывает полезна несимметричная форма определения символа Гильберта. Именно, $(a,b)_p = 1$ тогда и только тогда, когда уравнение

$$z^2 - by^2 = a \tag{28}$$

имеет решение в $\mathbb{Q}_p$. Действительно, пусть $z_0^2 - by_0^2 = a$. Если $z_0 \neq 0$, то $(1/z_0, y_0/z_0)$ — решение уравнения $ax^2+by^2 = 1$. Если же $z_0 = 0$, то $(1, y_0)$ — нетривиальный нуль формы $ax^2 + by^2$ и $(a,b)_p = 1$ согласно сказанному выше. Обратно, пусть (x_0, y_0) — решение уравнения $ax^2 + by^2 = 1$. Если $x_0 \neq 0$, то $(y_0/x_0, 1/x_0)$ — решение уравнения (28). Если же $x_0 = 0$, то $(y_0, 1)$ — нетривиальный нуль формы $z^2 - by^2$ и, следовательно, уравнение (28) также имеет решение.

Если b не является квадратом, то равенство (28) выражает тот факт, что a является нормой элемента $z + y\sqrt{b}$ квадратичного расширения $\mathbb{Q}_p(\sqrt{b})$ поля $\mathbb{Q}_p$ (см. [1], [6]). Отсюда, в частности, следует, что при фиксированном b все a, для которых $(a,b)_p = 1$, образуют подгруппу в группе $\mathbb{Q}_p^\times$ (содержащую подгруппу квадратов). Нетрудно показать, что это подгруппа индекса 2.

Локальные свойства символа Гильберта:

$$\text{(а) } (a,b)_p = (b,a)_p; \tag{29}$$

$$\text{(б) } (a_1a_2, b)_p = (a_1,b)_p(a_2,b)_p, \quad (a, b_1b_2)_p = (a,b_1)_p(a,b_2)_p; \tag{30}$$

$$\text{(в) если } (a,b)_p = 1 \text{ для всех } b, \text{ то } a \in \mathbb{Q}_p^{\times 2}; \tag{31}$$

$$\text{(г) } (a, 1-a)_p = 1 \text{ для всех } a; \tag{32}$$

$$\text{(д) если } p \neq 2, \infty \text{ и } |a|_p = |b|_p = 1, \text{ то } (a,b)_p = 1. \tag{33}$$

Свойства (а) и (б) тривиальны. Свойства (в) и (г) вытекают из описанной выше интерпретации символа Гильберта в терминах норм элементов поля $\mathbb{Q}_p(\sqrt{b})$. Свойство (д) выводится при помощи леммы Гензеля из того факта, что при любых целых a и b, не делящихся на p, сравнение $ax^2 + by^2 \equiv 1 \pmod p$ имеет решение. (Для доказательства последнего факта надо представить сравнение в виде $ax^2 \equiv 1 - by^2 \pmod p$ и посмотреть, сколько значений принимают левая и правая части при различных x и y.)

Вычисление символа Гильберта позволяет полностью решить вопрос о представлении нуля квадратичными формами над $\mathbb{Q}_p$ и, тем самым (с помощью теоремы Минковского – Хассе) — над $\mathbb{Q}$. В частности, из определения символа Гильберта и теоремы Минковского – Хассе следует, что форма

$$ax^2 + by^2 + cz^2 \quad (a, b, c \in \mathbb{Q}^\times), \tag{34}$$

представляет нуль над полем $\mathbb{Q}$ тогда и только тогда, когда $(-a/c, -b/c)_p = 1$ для всех p (включая $p = \infty$). Этот критерий является весьма эффективным, так как для почти всех p имеем $|a|_p = |b|_p = 1$, и в этом случае согласно свойству (д) $(a, b)_p = 1$, если только $p \neq 2, \infty$.

Очевидно, что $(a, b)_\infty = -1$, если a и b отрицательны, и $(a, b)_\infty = 1$ во всех остальных случаях. Выпишем теперь таблицы значений символа Гильберта для простых p.

Табл. 1. *Символ Гильберта для $p > 2$. Здесь v обозначает такое число $v \in \mathbb{Z}$, что $\left(\frac{v}{p}\right) = -1$; $\varepsilon = 1$, если $-1 \in \mathbb{Q}_p^{\times 2}$ (то есть если $p \equiv 1 \pmod 4$), и $\varepsilon = -1$ в противном случае.*

a / b	1	v	p	pv
1	$+1$	$+1$	$+1$	$+1$
v	$+1$	$+1$	-1	-1
p	$+1$	-1	ε	$-\varepsilon$
pv	$+1$	-1	$-\varepsilon$	ε

Отметим, в частности, что если a — целое число, не делящееся на p, то

$$(a, p)_p = \left(\frac{a}{p}\right). \tag{35}$$

Табл. 2. *Символ Гильберта в случае* $p = 2$.

a / b	1	5	-1	-5	2	10	-2	-10
1	$+1$	$+1$	$+1$	$+1$	$+1$	$+1$	$+1$	$+1$
5	$+1$	$+1$	$+1$	$+1$	-1	-1	-1	-1
-1	$+1$	$+1$	-1	-1	$+1$	$+1$	-1	-1
-5	$+1$	$+1$	-1	-1	-1	-1	$+1$	$+1$
2	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1
10	$+1$	-1	$+1$	-1	-1	$+1$	-1	$+1$
-2	$+1$	-1	-1	$+1$	$+1$	-1	-1	$+1$
-10	$+1$	-1	-1	$+1$	-1	$+1$	$+1$	-1

В частности, если a и b — нечетные целые числа, то

$$(a, b)_2 = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}. \tag{36}$$

Глобальное свойство символа Гильберта (*формула произведения*). Пусть $a, b \in \mathbb{Q}^\times$. Тогда $(a, b)_p = 1$ для почти всех p и

$$\prod_p (a, b)_p = 1, \tag{37}$$

где произведение берется по всем p, включая ∞.

Формула (37) равносильна квадратичному закону взаимности. Действительно, ввиду мультипликативности символов Гильберта (свойство (б) выше) достаточно проверить ее для случаев, когда a и b — простые числа или -1. Предоставляя читателю рассмотрение остальных случаев, рассмотрим случай, когда a и b — различные нечетные простые числа. Так как в этом случае $(a, b)_p = 1$ для всех $p \neq a, b, 2$, то с учетом (35) и (36) формула произведения принимает вид

$$(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}} \left(\frac{b}{a}\right)\left(\frac{a}{b}\right) = 1,$$

но это и есть квадратичный закон взаимности.

Отметим также следующее глобальное свойство нормирований $|\cdot|_p$, аналогичное свойству (37) и вытекающее непосредственно из их определения.

Формула произведения для нормирований. Пусть $a \in \mathbb{Q}^\times$. Тогда $|a|_p = 1$ для почти всех p и

$$\prod_p |a|_p = 1, \tag{38}$$

где произведение берется по всем p, включая ∞.

4. Кубические уравнения и эллиптические кривые

4.1. Проблема существования рационального решения

Для рациональных кубических форм $F(X, Y, Z)$ от трех переменных уже не известно никакого общего алгоритма, позволяющего установить существование нетривиального рационального решения уравнения $F = 0$, хотя изучено большое число конкретных уравнений, например уравнений вида

$$aX^3 + bY^3 + cZ^3 = 0.$$

Оказывается, для кубических форм перестает, вообще говоря, выполняться принцип Минковского – Хассе: например, уравнение $3X^3 + 4Y^3 + 5Z^3 = 0$ не имеет нетривиальных решений в рациональных числах, хотя имеет нетривиальные решения в поле вещественных чисел и во всех полях p-адических чисел (см. [1, гл. I, §7.6], где приведен план доказательства этого факта).

4.2. Сложение точек на кубической кривой

Кубическая форма $F(X, Y, Z)$ с комплексными коэффициентами задает кривую $\mathcal{C}$ на комплексной проективной плоскости $\mathbb{C}P^2$:

$$\mathcal{C} = \{(X : Y : Z) \in \mathbb{C}P^2 \mid F(X, Y, Z) = 0\}. \tag{39}$$

Форма F называется невырожденной, если частные производные $\dfrac{\partial F}{\partial X}$, $\dfrac{\partial F}{\partial Y}$, $\dfrac{\partial F}{\partial Z}$ не обращаются одновременно в нуль ни в какой точке $(X, Y, Z) \neq \neq (0, 0, 0)$. Геометрически это означает, что кривая $\mathcal{C}$ гладкая (не имеет особенностей).

Всякая прямая проективной плоскости пересекает гладкую кубическую кривую $\mathcal{C}$ ровно в трех точках, если считать точку касания с кратностью 2, а точку касания, являющуюся точкой перегиба кривой $\mathcal{C}$ — с кратностью 3.

Существует красивый геометрический способ определить сложение точек гладкой кубической кривой $\mathcal{C}$, превращающее ее в абелеву группу («метод секущих и касательных»), см. [8], [5], [13]. А именно, фиксируем точку $O \in \mathcal{C}$ (см. рис. 2). Если $P, Q \in \mathcal{C}$ — различные точки, то проведем через них прямую. Она пересечет $\mathcal{C}$ в однозначно определенной третьей точке R. Затем проведем прямую через R и O. Точку ее пересечения с $\mathcal{C}$ назовем суммой $P + Q$ точек P и Q. Аналогично определяется точка $2P$, но вместо секущей PQ следует взять касательную, проходящую через точку P (рис. 3).

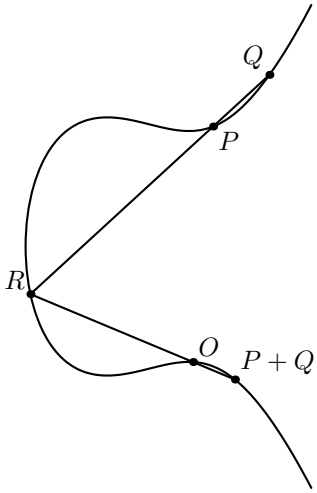


Рис. 2.

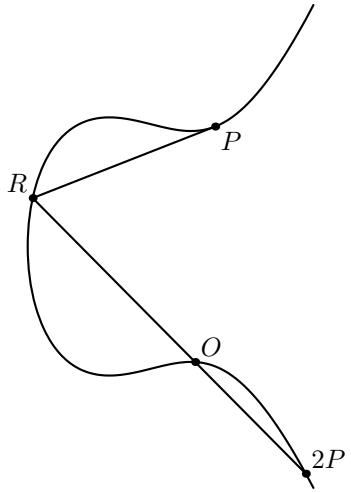


Рис. 3.

Коммутативность определенной таким образом операции сложения очевидна. Ее ассоциативность есть красивая теорема, обобщающая теорему Паскаля о шестиугольнике, вписанном в окружность (см., например, [5]). Роль нуля, как легко видеть, играет точка O. Точка, противоположная P, находится следующим образом. Проведем через точку O касательную. Она пересечет кривую $\mathcal{C}$ в некоторой точке O'. Теперь проведем прямую через O' и P. Третья точка ее пересечения с $\mathcal{C}$ и будет точкой, противоположной P.

Кубическая форма F называется неприводимой, если она не разлагается в произведение квадратичной и линейной форм. Геометрически это означает, что соответствующая кубическая кривая $\mathcal{C}$ не распадается на конику и прямую или на три прямые. Известно (см., например, [5]), что с помощью невырожденной линейной замены координат (над полем комплексных чисел) всякую неприводимую кубическую форму можно

привести к вейерштрассовой нормальной форме

$$Y^2Z - X^3 - aXZ^2 - bZ^3 \quad (a, b \in \mathbb{C}). \tag{40}$$

(см. также [8, т. 1, гл. 1, §6, следствие 3, с. 31]). Уравнение соответствующей кривой $\mathcal{C}$ в неоднородных координатах $x = X/Z$, $y = Y/Z$ примет тогда вид

$$y^2 = x^3 + ax + b, \tag{41}$$

Условие гладкости кривой (41) означает, что многочлен x^3+ax+b не имеет кратных корней, то есть его дискриминант $D = -4a^3 - 27b^2$ отличен от нуля.

Кривая (41) имеет единственную бесконечно удаленную точку $O = (0 : 1 : 0)$, являющуюся точкой перегиба. Если взять эту точку в качестве фиксированной точки при определении операции сложения, то легко найти явные выражения для координат суммы точек. А именно, сумма точек (x_1, y_1) и (x_2, y_2) при $x_1 \neq x_2$ есть точка с координатами

$$x_3 = -x_1 - x_2 + \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2, \quad y_3 = \frac{y_1 - y_2}{x_1 - x_2}(x_1 - x_3) - y_1. \tag{42}$$

Если $x_1 = x_2$, но $y_1 \neq y_2$, то $y_1 = -y_2$ и суммой данных точек является точка O; иными словами, точка $(x_1, -x_2)$ противоположна точке (x_1, x_2). Наконец, если $x_1 = x_2$ и $y_1 = y_2$, то

$$x_3 = -2x_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)^2, \quad y_3 = \frac{3x_1^2 + a}{2y_1}(x_1 - x_3) - y_1. \tag{43}$$

4.3. Строение группы рациональных точек на кубической кривой

Предположим теперь, что кубическая форма $F(X, Y, Z)$ имеет рациональные коэффициенты. Если кривая $\mathcal{C}$, задаваемая уравнением $F = 0$, гладкая и имеет хотя бы одну рациональную точку, то она называется эллиптической кривой (над $\mathbb{Q}$). Метод секущих и касательных дает возможность «размножать» рациональные точки эллиптических кривых.

Более точно, если в качестве фиксированной точки O при определении операции сложения взята рациональная точка, то легко видеть, что сумма рациональных точек будет рациональна и точка, противоположная рациональной, также рациональна. Иными словами, рациональные точки кривой $\mathcal{C}$ образуют подгруппу в группе всех ее точек. Обозначим эту подгруппу через $\mathcal{C}(\mathbb{Q})$. Имеет место

Теорема 3 (теорема Морделла). *Абелева группа $\mathcal{C}(\mathbb{Q})$ конечно порождена.*

(См. [10], и приложение Ю. И. Манина к [3]).

Согласно теореме о строении конечнопорожденных абелевых групп, имеется разложение

$$\mathcal{C}(\mathbb{Q}) = \Delta \oplus \mathbb{Z}^r,$$

где Δ — конечная подгруппа, а $\mathbb{Z}^r$ — прямая сумма бесконечных циклических групп. Подгруппа Δ называется группой кручения, а ее элементы — точками кручения кривой $\mathcal{C}$. Число r называется рангом кривой $\mathcal{C}$ (над $\mathbb{Q}$).

О группе кручения Δ уже давно было кое-что известно. Так, Нагелль и позднее Лутц получили следующий интересный результат, дающий одновременно метод для явного определения точек кручения конкретных кривых: если $P = (x_P, y_P)$ — рациональная точка кручения на кривой, заданной уравнением $y^2 = x^3 + ax + b$, то ее координаты x_P и y_P являются целыми числами, причем либо $y_P = 0$, либо y_P^2 есть делитель дискриминанта $D = -4a^3 - 27b^2$ данной кривой.

Б. Мазур доказал в 1976 г., что группа Δ может быть изоморфна лишь одной из пятнадцати групп

$$\mathbb{Z}/m\mathbb{Z}\ (m \leqslant 10, m = 12),\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}\ (n \leqslant 4), \tag{44}$$

причем все возможности реализуются (см. [14], глава 6).

Вычисление ранга r остается открытой проблемой.

Приведение неприводимой кубической формы $F(X, Y, Z)$ к вейерштрассовой нормальной форме над полем рациональных чисел, вообще говоря, невозможно. Однако если соответствующая кубическая кривая $\mathcal{C}$ имеет хотя бы одну рациональную точку, то она изоморфна над $\mathbb{Q}$ некоторой кривой вида (41)(см. [8, §3, п.1] и [7, гл. III, §2, с. 113]). Изоморфизм задается рациональными функциями с рациональными коэффициентами и, в частности, переводит рациональные точки в рациональные (см. [8, §3, п.1]. Так как явный вид этого изоморфизма может быть достаточно легко найден, то, если известна одна рациональная точка кривой $\mathcal{C}$, нахождение всех остальных рациональных точек сводится к нахождению рациональных точек кривой вида (41).

Примеры. 1) Пусть кривая $\mathcal{C}$ задается уравнением

$$y^2 + y = x^3 - x,$$

целочисленные решения которого описывают все случаи, когда произведение двух последовательных целых чисел равно произведению некоторых других трех последовательных чисел. В этом примере группа Δ тривиальна и группа $\mathcal{C}(\mathbb{Q})$ (с бесконечно удаленной точкой в качестве нуля) является бесконечной циклической группой (то есть $r = 1$), причем в качестве ее образующей можно взять точку $P = (0, 0)$. Точки вида mP указаны на рис. 4.

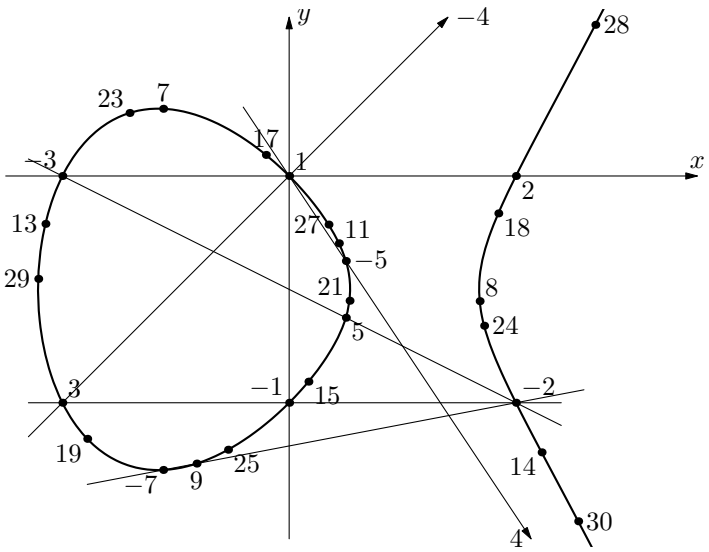


Рис. 4.

2) Пусть кривая $\mathcal{C}$ задается уравнением

$$y^2 + y = x^3 - 7x + 6.$$

Тогда $\mathcal{C}(\mathbb{Q}) = \mathbb{Z}^3$, причем в качестве свободных образующих этой группы можно взять точки $(1,0), (2,0), (0,2)$, см. [11].

3) Рассмотрим кривую $\mathcal{C} : y^2 = x^3 + 877x$. Можно показать, что образующая по модулю кручения группы $\mathcal{C}(\mathbb{Q})$ имеет x-координату

$$x = \frac{37549452812716219310550406994209279234620 1}{62159877768715054254632207806972380441 00}\,.$$

Этот пример дает определенное представление о трудностях нахождения рациональных точек бесконечного порядка на кубических кривых.

Для кубических кривых, имеющих особенности, описанный метод неприменим. Пусть, к примеру,

$$\mathcal{C} : \ y^2 = x^2 + x^3 \tag{45}$$

— кривая, изображенная на рис. 5. Тогда любая прямая, проходящая через точку $(0,0)$, имеет еще лишь одну общую точку с кривой $\mathcal{C}$. А именно, прямая $y = tx$ пересекает $\mathcal{C}$ в точке $(t^2-1, t(t^2-1))$. Поэтому, хотя и нельзя определить сложение точек, как в случае гладких кривых, мы находим все рациональные точки на $\mathcal{C}$ с помощью рациональной параметризации $x = t^2 - 1,\ y = t(t^2 - 1)$.

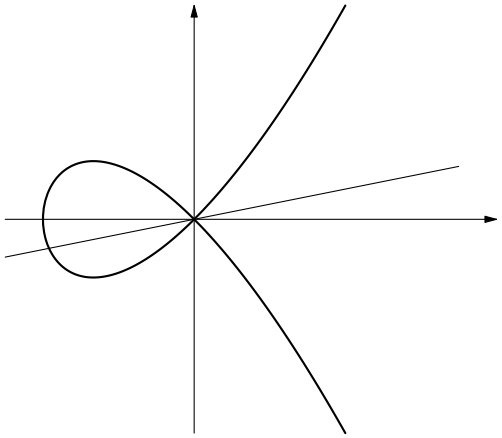


Рис. 5.

4.4. Кубические сравнения по простому модулю

Пусть p — простое число и $F(X,Y,Z)$ — невырожденная целочисленная кубическая форма. Решение сравнения $F \equiv 0 \pmod p$ равносильно решению уравнения $\overline{F} = 0$, где $\overline{F}$ обозначает кубическую форму над полем $\mathbb{Z}/p\mathbb{Z}$, полученную из F рассмотрением ее коэффициентов по модулю p.

Предположим, что форма F невырождена по модулю p. Это означает, что форма F и ее частные производные $\dfrac{\partial\overline{F}}{\partial X}$, $\dfrac{\partial\overline{F}}{\partial Y}$, $\dfrac{\partial\overline{F}}{\partial Z}$ не имеют общих нетривиальных нулей ни в каком конечном расширении поля $\mathbb{Z}/p\mathbb{Z}$.

Как и в случае поля рациональных чисел, если известно одно решение уравнения $\overline{F} = 0$ над $\mathbb{Z}/p\mathbb{Z}$, $p \neq 2,3$, то простые алгебро-геометрические идеи позволяют свести нахождение всех остальных решений к нахождению решений уравнения вида

$$y^2 = x^3 + ax + b,\ \ a,b \in \mathbb{Z}/p\mathbb{Z}. \tag{46}$$

Ясно, что число решений этого уравнения не превосходит $2p$, так как для каждого значения $x \in \mathbb{Z}/p\mathbb{Z}$ найдутся не больше двух значений $y \in \mathbb{Z}/p\mathbb{Z}$, таких, что (x,y) удовлетворяет уравнению. Однако лишь половина элементов из $(\mathbb{F}_p)^\times$ являются квадратами, поэтому можно ожидать, что число решений вдвое меньше (предположив, что значения x^3+ax+b разбросаны случайно в поле $\mathbb{Z}/p\mathbb{Z}$).

Более точно, пусть $\chi(x) = \left(\frac{x}{p}\right)$ при $x \neq 0$ и $\chi(0) = 0$. Тогда число решений уравнения $y^2 = u$ в $\mathbb{Z}/p\mathbb{Z}$ равно $1 + \chi(u)$ и мы получаем следующую формулу для числа точек кривой $\mathcal{C}$, заданной уравнением (46), над полем

$\mathbb{Z}/p\mathbb{Z}$ (с учетом бесконечно удаленной точки $(0:1:0)$):

$$\begin{aligned}\#\,\mathcal{C}(\mathbb{Z}/p\mathbb{Z}) &= 1+\sum_{x\in\mathbb{Z}/p\mathbb{Z}}(1+\chi(x^3+ax+b))\\ &= p+1+\sum_{x\in\mathbb{Z}/p\mathbb{Z}}\chi(x^3+ax+b).\end{aligned}$$

Коблиц сравнивает взятие суммы в этой формуле со случайным блужданием, при котором делается шаг вперед, если $\chi(x^3+ax+b)=1$, и шаг назад, если $\chi(x^3+ax+b)=-1$. Из теории вероятностей известно, что расстояние от исходной точки после p шагов при случайном блуждании будет иметь порядок $\sqrt{p}$. И действительно, это так: сумма всегда ограничена величиной $2\sqrt{p}$.

Теорема 4 (теорема Хассе). *Пусть* $N_p=\#\,\mathcal{C}(\mathbb{Z}/p\mathbb{Z})$. *Тогда*

$$|N_p-(p+1)|\leqslant 2\sqrt{p}.$$

Элементарное доказательство этого факта было дано Ю. И. Маниным в 1956 г.

4.5. От сравнений к рациональным точкам: гипотеза Бёрча и Суиннертона–Дайера

Знаменитый пример, связывающий локальную и глобальную информацию, дается гипотезой Бёрча и Суиннертона–Дайера для кубических кривых. Эта гипотеза принадлежит к числу семи проблем тысячелетия института Клея, за решение каждой из которых предложен приз в миллион долларов!

Пусть $\mathcal{C}$ — эллиптическая кривая, заданная уравнением

$$y^2=x^3+ax+b$$

с $a,b\in\mathbb{Z}$. Для $p\nmid\Delta=-16(4a^3+27b^2)$ положим $a_p=p+1-\#\mathcal{C}(\mathbb{Z}/p\mathbb{Z})$. Пусть

$$L(\mathcal{C},s)=\prod_{p\nmid\Delta}\frac{1}{1-a_pp^{-s}+p^{1-2s}}=\sum_{n=1}^{\infty}c_nn^{-s},\tag{47}$$

где c_n — какие-то целые числа. Из теоремы 4 следует, что последний ряд сходится абсолютно при $\operatorname{Re}(s)>\dfrac{3}{2}$.

Теорема 5 (Брёй, Конрад, Дайамонд, Тэйлор, Уайлс). *Функция $L(\mathcal{C},s)$ продолжается до аналитической функции на всей комплексной плоскости.*

Гипотеза 6 (Бёрча и Суиннертона–Дайера). *Разложение Тэйлора функции* $L(\mathcal{C}, s)$ *в* $s = 1$ *имеет вид*

$$L(\mathcal{C}, s) = c(s-1)^r + \text{члены высшей степени}, \tag{48}$$

где $c \neq 0$, *а* r *— ранг кривой* $\mathcal{C}$ *над* $\mathbb{Q}$.

(См. изложение в [14], главы 32–34, и в [15].)

Специальный случай гипотезы БСД утверждает, что $L(\mathcal{C}, 1) = 0$ тогда и только тогда, когда группа $\mathcal{C}(\mathbb{Q})$ бесконечна.

В статье [15] обсуждается история следующего результата:

Теорема 7 (Гросс, Колывагин, Загир и др.). *Предположим, что*

$$L(\mathcal{C}, s) = c(s-1)^r + \text{ члены высшей степени}$$

с $c \neq 0$ *и* $r \leqslant 1$. *Тогда гипотеза БСД справедлива для* $\mathcal{C}$, *то есть* r *— ранг кривой* $\mathcal{C}$ *над* $\mathbb{Q}$.

Джон Тэйт сделал доклад о гипотезе БСД для института Клея. Этот доклад можно посмотреть в интернете по адресу
`http://www.msri.org/publications/ln/hosted/cmi/2000/cmiparis/index-tate.html`

Отметим также, что гипотеза БСД допускает «экспериментальную» проверку. Для этого можно приближенно вычислять показатель r в разложении (48). Для вычислений с эллиптическими кривыми можно использовать компьютерную систему PARI (см. [9]). Например, для кривой $y^2+y = x^3-7x+6$ из примера 2) на с. 75 ранг равен 3. Приближенное вычисление показателя в формуле (48) дает значение 3.000011487248732705286325574.

* * * * * *

Статья основана на материалах лекций автора в Институте Фурье (Гренобль, Франция), в Эколь Нормаль (Лион, Франция), а также на материалах спецкурсов на мехмате МГУ в 1979–1991 и в 2001.

Искренне благодарю Эрнеста Борисовича Винберга за адаптирование первоначальной версии статьи для сборника «Математическое просвещение», посвященного p-адическим числам и их приложениям.

Список литературы

[1] Боревич З. И., Шафаревич И. Р. *Теория чисел*. Изд. 3е, доп. М.: Наука, 1985.

[2] Коблиц Н. *p-адические числа, p-адический анализ и дзета функции*. М.: Мир, 1982.

[3] Мамфорд Д. *Абелевы многообразия*. М.: Мир, 1971.

[4] Острик В. В., Цфасман М. А. *Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые*. М.: МЦНМО, 2005.

[5] Прасолов В. В., Соловьев Ю. П. *Эллиптические функции и алгебраические уравнения* М.: Факториал, 1997.

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

[7] Степанов С. А. *Арифметика алгебраических кривых*. М.: Наука, 1991.

[8] Шафаревич И. Р. *Основы алгебраической геометрии*. Тт. 1–2. Изд. 2е. М.: Наука, 1988.

[9] Batut C., Belabas K., Bernardi H., Cohen H., Olivier M. *The PARI/GP number theory system*.
`http://pari.math.u-bordeaux.fr`

[10] Cassels J.W.S. *Diophantine equations with special reference to elliptic curves* // J. Lond. Math. Soc. Vol. 41, 1966. P. 193–291.

[11] Buhler J. P., Gross B. H., Zagier D. B. *On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank* 3 // Mathematics of Computation. Vol. 44, no. 170., 1985. P. 473–481.

[12] Manin Yu. I., *Selected papers of Yu. I. Manin*, World Scientific Series in 20th Century Mathematics, 3. World Scientific Publishing Co., Inc., River Edge, NJ, 1996. xii+600 pp.

[13] Manin Yu.I. and Panchishkin A.A., *Introduction to Modern Number Theory*, Encyclopaedia of Mathematical Sciences, vol. 49 (2nd ed.), Springer-Verlag, 2005, 514 p. (Русск. пер. М.: МЦНМО, 2008.)

[14] Stein W. *An Explicit Approach to Number Theory*.
`http://modular.fas.harvard.edu/edu/Fall2001/124/lectures/lectures_all/lectures.pdf`

[15] Wiles A. *The Birch and Swinnerton-Dyer Conjecture*.
`http://www.claymath.org/millennium/Birch_and_Swinnerton-Dyer_Conjecture/birchswin.pdf`

А. А. Панчишкин: Institut Fourier,Université de Grenoble I, France

Издательство МЦНМО

Д. Мамфорд. **Красная книга о многообразиях и схемах.** Пер. с англ. С. М. Львовского. 2007. 296 с.

На этой книге было воспитано не одно поколение алгебраических геометров. Ее автор — не только один из крупнейших математиков XX века, но и блестящий педагог, книги которого неоднократно выходили в русских переводах и всегда пользовались заслуженной популярностью.

В книге успешно решена неразрешимая на первый взгляд задача: дать одновременно краткое и содержательное введение в алгебраическую геометрию на языке схем. Для каждого из абстрактных понятий, вводимых в книге, Д. Мамфорд приводит геометрические мотивировки и, более того, помогает читателю выработать геометрическую интуицию, необходимую для обращения с такими непростыми для объяснения «на пальцах» понятиями, как плоскостность или нормальность.

Для студентов, аспирантов и научных работников физико-математических специальностей.

С. В. Матвеев. **Алгоритмическая топология и классификация трехмерных многообразий.** 2007. 456 с.

В книге изложены основы алгоритмической и компьютерной топологии трехмерных многообразий, включая теорию сложности, теорию нормальных поверхностей и алгоритмическую классификацию большого числа трехмерных многообразий. В частности, это дает полную классификацию классических узлов.

Книга адресована широкому кругу специалистов в области математики и тех ее приложений, где появляются трехмерные многообразия. Тщательность изложения и обилие иллюстраций делают книгу доступной студентам математических факультетов.

Г. А. Маргулис. **Дискретные подгруппы полупростых групп Ли.** Пер. с англ. 2007. 464 с.

Книга посвящена дискретным подгруппам конечного кообъема в полупростых группах Ли. Рассматриваются вопросы строения, классификации и описания дискретных подгрупп групп Ли. Результаты допускают применение в теории алгебраических групп над глобальными полями.

Для студентов, аспирантов и научных сотрудников математических специальностей.

В. И. Арнольд, Б. А. Хесин. **Топологические методы в гидродинамике.** Пер. с англ. 2007. 392 с.

Данная книга — это первая монография, в которой топологические, теоретико-групповые и геометрические задачи идеальной гидродинамики и магнитогидродинамики рассматриваются с единой точки зрения. Необходимый подготовительный материал из гидродинамики и чистой математики излагается с большим количеством примеров и рисунков.

Книга предназначена для студентов, аспирантов и специалистов по чистой или прикладной математике, работающих в таких областях, как гидродинамика, группы Ли, динамические системы и дифференциальная геометрия.

Наш семинар: математические сюжеты

Заметки об исключительных изоморфизмах

В. В. Доценко

Эрнесту Борисовичу Винбергу к юбилею, с уважением и восхищением

Введение

Предметом предлагаемого читателю текста является некоторая разновидность «математической зоологии». А именно, я приведу довольно простые и элегантные конструкции некоторых «исключительных изоморфизмов» (так традиционно называются изоморфизмы между двумя группами из известных серий групп, сами по себе не образующие серию), и опишу ситуации, в которых простой конструкции не известно, в надежде, что кому-то из читателей удастся заполнить имеющиеся тут пробелы.

Я признателен всем моим друзьям и коллегам, с кем я обсуждал в разные моменты вопросы, затрагиваемые здесь. Особо я хочу поблагодарить М. Финкельберга, который сообщил эффектное (и, возможно, совершенно новое) доказательство изоморфизма $PSL_2(\mathbb{F}_9) \simeq A_6$, и М. Вялого, который предложил красивый путь доказательства изоморфизма $Sp_4(\mathbb{F}_2) \simeq S_6$, вдохновивший меня на доказательство изоморфизма $GL_4(\mathbb{F}_2) \simeq A_8$. Столь изящное рассуждение не имело шанса быть совершенно новым: как выяснилось в ходе написания этого текста, мы переоткрыли результаты статьи [4], и опубликованное здесь доказательство по существу не отличается от приведённого в той статье. После того, как первая версия текста

была представлена в редакцию, Э. Б. Винберг сообщил мне ряд комментариев и уточнений, которые сделали некоторые доказательства и структуру текста в целом значительно более прозрачными, за что я ему чрезвычайно признателен.

Серии конечных групп, которым мы уделяем тут наибольшее внимание, суть симметрические группы S_n, знакопеременные группы A_n и проективные группы симметрий $PGL_n(\Bbbk)$ и $PSL_n(\Bbbk)$, в случае, когда $\Bbbk = \mathbb{F}_q$ — конечное поле из q элементов. Группы S_n и A_n хорошо известны всем, кто имел дело с понятием группы. Что касается проективных групп, они могут быть известны не всем читателям, и мы напомним их определение.

Определение 1. Общая (соответственно, специальная) линейная группа $GL_n(\Bbbk)$ (соответственно, $SL_n(\Bbbk)$) — это группа всех обратимых матриц с элементами из поля $\Bbbk$ (соответственно, всех матриц с коэффициентами из поля $\Bbbk$ и с определителем 1).

Будучи интересными сами по себе, такие группы не имеют шанса быть изоморфными симметрическим и знакопеременным группам, потому что обычно имеют нетривиальный центр (элементы, которые перестановочны со всеми элементами группы).

Упражнение. Проверьте, что центр каждой из этих групп состоит из скалярных матриц (т. е. матриц, кратных единичной).

Определение 2. Проективная общая линейная группа $PGL_n(\Bbbk)$ — это факторгруппа группы $GL_n(\Bbbk)$ по ее центру. Проективная специальная линейная группа $PSL_n(\Bbbk)$ — это образ группы $SL_n(\Bbbk)$ в $PGL_n(\Bbbk)$ при гомоморфизме факторизации.

Геометрический смысл этих групп такой. Каждая из них действует на n-мерном векторном пространстве над полем $\Bbbk$. Если рассматривать точки этого пространства с точностью до одновременного умножения всех их координат на ненулевое число, т. е. перейти к множеству прямых, проходящих через начало координат, мы получим $(n-1)$-мерное проективное пространство над полем $\Bbbk$. Наши группы, будучи факторгруппами по подгруппе, которая сохраняет все прямые, которые проходят через начало координат, действуют на этом проективном пространстве автоморфизмами. Это будет очень существенно для нас.

Приведем для использования в дальнейшем несколько стандартных фактов. Все они не очень сложно доказываются, и мы предлагаем читателю доказать их самостоятельно или обратиться к стандартным учебникам ([2], [3], [5]) за доказательствами.

Порядки линейных и проективных групп читатель легко вычислит в качестве упражнения, доказав тем самым следующее предложение.

Предложение 1.

$$\#GL_n(\mathbb{F}_q) = (q^n-1)(q^n-q)\cdot\ldots\cdot(q^n-q^{n-1}),$$
$$\#SL_n(\mathbb{F}_q) = \frac{1}{q-1}(q^n-1)(q^n-q)\cdot\ldots\cdot(q^n-q^{n-1}),$$
$$\#PGL_n(\mathbb{F}_q) = \frac{1}{q-1}(q^n-1)(q^n-q)\cdot\ldots\cdot(q^n-q^{n-1}),$$
$$\#PSL_n(\mathbb{F}_q) = \frac{1}{(q-1)\,(n,q-1)}(q^n-1)(q^n-q)\cdot\ldots\cdot(q^n-q^{n-1})$$

Следующее предложение (тоже предлагаемое в качестве упражнения) тоже не очень сложно и довольно стандартно.

Предложение 2.

1. *Группы A_n просты*[1)] *при $n \geqslant 5$.*
2. *Нормальные подгруппы группы S_n при $n \geqslant 5$ суть $\{e\}$, A_n и S_n.*
3. *Группы $PSL_n(\mathbb{F}_q)$ просты при $n \geqslant 3$ и при $n = 2$, $q > 3$.*
4. *Нормальная подгруппа группы $PGL_n(\mathbb{F}_q)$ либо равна $\{e\}$, либо содержит $PSL_n(\mathbb{F}_q)$ во всех случаях кроме $n = 2$, $q = 2, 3$.*

Это предложение демонстрирует дополнительную причину интересоваться изоморфизмами между данными группами. Классификация конечных простых групп является одним из центральных вопросов теории групп, и для двух бесконечных списков простых групп хотелось бы знать, насколько эти списки пересекаются.

Схема доказательств в большинстве обсуждаемых нами случаев одна и та же. Чтобы доказать, что две группы G и H изоморфны, мы сначала строим гомоморфизм $\varphi\colon G \to H$. Далее мы проверяем инъективность или сюръективность этого гомоморфизма и привлекаем знания о порядках наших групп, чтобы установить, что построенный гомоморфизм в действительности является изоморфизмом.

От геометрии к алгебре

В этом разделе мы для построения гомоморфизмов используем естественное действие проективных групп на соответствующих пространствах, находя подходящие геометрические объекты, на которых эти группы действуют.

В простейших примерах естественное действие проективных преобразований приводит к успеху. Напомним, что преобразование из $PGL_2(\Bbbk)$,

[1)] Т. е. не имеют нетривиальных нормальных подгрупп.

которое сохраняет все точки проективной прямой (их в случае конечного поля $1 + \#\Bbbk$), тождественно, и потому естественный гомоморфизм из $PGL_2(\mathbb{F}_q)$ в S_{q+1} инъективен.

Предложение 3.

$$PGL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2) = GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) \simeq S_3,$$
$$PGL_2(\mathbb{F}_3) \simeq S_4,$$
$$PSL_2(\mathbb{F}_3) \simeq A_4,$$
$$PSL_2(\mathbb{F}_4) = PGL_2(\mathbb{F}_4) \simeq A_5.$$

Доказательство. Центр группы матриц над полем $\mathbb{F}_2$ тривиален, а определитель обратимой матрицы может быть равен только единице, так что

$$PGL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2) = GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2).$$

Порядок группы $GL_2(\mathbb{F}_2)$ равен 6, так что естественный гомоморфизм в S_3 является изоморфизмом.

Порядок группы $PGL_2(\mathbb{F}_3)$ равен 24, и потому гомоморфизм в S_4 является изоморфизмом. В случае группы $PSL_2(\mathbb{F}_3)$ можно использовать то, что у S_4 только одна подгруппа индекса 2, или найти в $PSL_2(\mathbb{F}_3)$ цикл длины 3, или рассуждать каким-либо иным способом.

Порядок группы $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4)$ равен 60. Поэтому образ этой группы при естественном гомоморфизме в S_5 — подгруппа индекса 2 (которая обязательно нормальна). Чтобы доказать, что эта подгруппа есть A_5, можно рассуждать разными способами. Теоретико-групповой подход говорит, что пересечение этой подгруппы с A_5 — нормальная подгруппа, и предложение 2 позволяет этим завершить доказательство. Геометрический подход подсказывает более простое рассуждение. Проективное преобразование может перевести любые три точки в любые три. Возьмем три точки A, B и C и циклически переставим их проективным преобразованием. Это даст нам в образе гомоморфизма либо тройной цикл (ABC) (а потому все тройные циклы в силу нормальности подгруппы и все четные подстановки, поскольку A_n порождается тройными циклами), либо перестановку с цикловым типом $(ABC)(DE)$, квадрат которой — тройной цикл.

Следующее рассуждение является несколько более тонким.

Предложение 4.

$$PGL_2(\mathbb{F}_5) \simeq S_5,$$
$$PSL_2(\mathbb{F}_5) \simeq A_5.$$

Доказательство. Порядок группы $PGL_2(\mathbb{F}_5)$ равен 120. Действие на точках проективной прямой дает гомоморфизм из $PGL_2(\mathbb{F}_5)$ в S_6. Дальнейшее наше рассуждение не использует геометрию и является чисто

теоретико-групповым. Мы докажем, что вообще любая подгруппа $H \subset$ $\subset S_6$ порядка 120 изоморфна S_5. А именно, рассмотрим множество смежных классов S_6/H. Действие S_6 сдвигами на множестве смежных классов приводит к гомоморфизму $\alpha\colon S_6 \to S_6$ (поскольку смежных классов ровно 6). Попробуем выяснить, каково ядро этого гомоморфизма. Это нормальная подгруппа. Нормальные подгруппы в S_6 суть $\{e\}$, A_6 и S_6. Действие группы на смежных классах по подгруппе транзитивно, поэтому два последних варианта отпадают. Значит, α является изоморфизмом. Осталось заметить, что при действии на смежных классах по подгруппе стабилизатор точки изоморфен этой подгруппе. Стабилизатор же точки для обычного действия S_6 на 6-элементном множестве есть S_5. Значит, исходная подгруппа H изоморфна S_5. Отметим, что эта подгруппа S_5 не сопряжена стандартному вложению S_5, поскольку ее действие транзитивно (и потому не имеет неподвижных точек).

Утверждение о группе $PSL_2(\mathbb{F}_5)$ проще всего доказать с помощью предложения 2: в S_5 ровно одна подгруппа индекса 2.

Предложение 5. $PSL_2(\mathbb{F}_9) \simeq A_6$.

Доказательство. Порядок группы $PSL_2(\mathbb{F}_9)$ равен 360. Поэтому достаточно построить нетривиальный гомоморфизм этой группы в S_6 (он будет инъективен в силу простоты групп PSL, а единственной подгруппой индекса 2 в S_6 является A_6). Мы сделаем это, предъявив подгруппу $H \subset PSL_2(\mathbb{F}_9)$ индекса 6 (тогда гомоморфизм возникнет из действия на смежных классах по этой подгруппе). Подгруппа индекса 6 в A_6 изоморфна A_5 (это доказывается аналогично тому, что подгруппа индекса 6 в S_6 изоморфна S_5; см. доказательство предложения 4), так что мы и будем искать подгруппу A_5. Хорошо известно, что A_5 изоморфна группе вращений додекаэдра, поэтому она действует на двумерной сфере в $\mathbb{R}^3$. Теперь главное — правильно эту сферу интерпретировать. Легко понять, что группа вращений додекаэдра вкладывается в группу симметрий сферы, понимаемой как сфера Римана (комплексная проективная прямая), то есть в $PSL_2(\mathbb{C})$. Можно проверить, что это вложение определено над $\mathbb{Q}(\sqrt[5]{1}) = \mathbb{Q}(\sqrt{5}, i)$, и потому можно рассмотреть его по модулю 3, что приведет к вложению $A_5 = PSL_2(\mathbb{F}_5)$ в $PSL_2(\mathbb{F}_9)$, поскольку $\mathbb{F}_9 = \mathbb{F}_3(i)$, а $\sqrt{5} \equiv \sqrt{-1} = i \pmod 3$.

Задача*. Можно ли придумать аналогичное рассуждение, которое использует изоморфизм A_5 и $PSL_2(\mathbb{F}_4)$?

Задача*. Можно ли, используя двумерные комплексные представления групп $SL_2(\mathbb{F}_q)$, доказать изоморфизм $PSL_2(\mathbb{F}_4) \simeq PSL_2(\mathbb{F}_5)$ напрямую?

Замечание 1. Доказанные ранее утверждения могут навести читателя на мысль, что имеет место и изоморфизм $PGL_2(\mathbb{F}_9) \simeq S_6$. Это неверно (попробуйте понять, почему).

Интермедия: внешний автоморфизм S_6, простые группы небольших порядков и всё такое

В этом разделе мы извлечем из обсуждавшихся доказательств (да-да, именно из доказательств, а не из доказанного) следствия, которые могут быть интересны любителям теории групп. Во втором из них полезны знания из университетского курса алгебры (теоремы Силова).

Следствие 1. *У группы S_6 существует внешний (не внутренний, то есть не задаваемый сопряжением никаким элементом) автоморфизм.*

Доказательство. Таким автоморфизмом является отображение α из доказательства предложения 4. В самом деле, прообраз стандартного вложения S_5 является подгруппой без общей неподвижной точки, и потому этот автоморфизм не может быть внутренним.

Построенный нами внешний автоморфизм сам по себе является исключительным. Чтобы продемонстрировать это, мы докажем следующее утверждение.

Предложение 6. *При $n \neq 6$ любой автоморфизм группы S_n является внутренним.*

Доказательство. Ясно, что автоморфизм переводит сопряженные элементы в сопряженные элементы. Наше доказательство будет состоять из двух частей. Чтобы доказать, что автоморфизм является внутренним, мы проверим, что транспозиции переходят в транспозиции, после чего убедимся, что автоморфизм, переводящий транспозиции в транспозиции, обязательно внутренний.

Всякая транспозиция является инволюцией (в квадрате равна единице), поэтому класс сопряженности транспозиции переходит в класс сопряженности произведения нескольких непересекающихся транспозиций. Пусть этих транспозиций $k \leqslant n/2$. Вычислим число элементов в соответствующем классе (здесь и далее можно считать, что $n \geqslant 4$, чтобы в S_n были нетривиальные инволюции). Это число равно индексу централизатора такого элемента, т. е. $\dfrac{n!}{k!2^k(n-2k)!}$, что, очевидно, не меньше (а при $k > 1$ — больше), чем $\dfrac{n!}{(2k)!(n-2k)!} = C_n^{2k}$. Число транспозиций равно C_n^2. Поскольку числа сочетаний при фиксированном n возрастают до середины строки, C_n^2 не меньше, чем C_n^{2k}, только если $2k$ равно одному из чисел

$2, n-2, n-1, n$. Если $2k = 2$, то всё доказано. В остальных случаях $n > 4$, а количества элементов в соответствующем классе сопряженности равны, соответственно,

$$\frac{n!}{2 \cdot 4 \cdot \ldots \cdot (n-2) \cdot 2}, \quad \frac{n!}{2 \cdot 4 \cdot \ldots \cdot (n-1)} \text{ и } \frac{n!}{2 \cdot 4 \cdot \ldots \cdot n}.$$

Первое число больше $\frac{n(n-1)}{2}$ при $n > 4$, второе число не меньше $n(n-2)$, что больше $\frac{n(n-1)}{2}$ при $n > 3$, и, наконец, третье число не меньше $(n-1)\times$ $\times(n-3)$, что больше $\frac{n(n-1)}{2}$ при $n > 6$ и не равно $\frac{n(n-1)}{2}$ при $n = 5$. Поэтому при $n \neq 6$ любой автоморфизм переводит транспозиции в транспозиции.

Пусть теперь известно, что транспозиции переходят в транспозиции. Докажем, что в этом случае автоморфизм обязательно является внутренним. Будем последовательно подправлять его, умножая на внутренние автоморфизмы, так, что в результате получится тождественный автоморфизм. Можно с самого начала считать, что транспозиция (12) остается на месте. Далее, транспозиция (23) переходит в транспозицию, которая не коммутирует с (12), и потому есть либо $(1k)$, либо $(2k)$, где $k \geqslant 3$. Такую транспозицию сопряжением с помощью элемента, который коммутирует с (12), можно перевести в (23) — так что можно домножить наш автоморфизм на подходящий внутренний, так что в итоге и (12), и (23) остаются на месте. Далее, если мы уже добились того, что транспозиции (12), (23), $\ldots$, $(k{-}1\ k)$ остаются на месте, то транспозиция $(k\ k{+}1)$ должна переходить в транспозицию (kl) или $(k{+}1\ l)$ (поскольку она коммутирует со всеми из них, кроме последней), и сопряжением перестановкой, которая коммутирует со всеми перечисленными транспозициями, такую транспозицию можно перевести в $(k\ k{+}1)$, так что в итоге и эта транспозиция будет оставаться на месте. Всевозможные транспозиции $(k\ k{+}1)$ порождают S_n, так что если все они неподвижны при автоморфизме, то этот автоморфизм тождественный.

Замечание 2. Из структуры доказательства немедленно следует, что любой внешний автоморфизм S_6 переводит каждую транспозицию в произведение трех непересекающихся транспозиций (это единственный класс сопряженности нужной мощности, который состоит из инволюций). Мы используем это ниже. Немедленное же следствие этого факта состоит в том, что группа внешних автоморфизмов S_6 состоит из двух элементов. В самом деле, любые два внешних автоморфизма S_6 переводят класс сопряженности транспозиций в один и тот же класс сопряженности, и потому отличаются на автоморфизм, который переводит транспозиции в транспозиции, а значит, является внутренним.

Задача*. Постройте три существенно различных (не отличающихся на внутренний автоморфизм) внешних автоморфизма A_6, и три неизоморфных группы, которые содержат A_6 в качестве подгруппы индекса 2.

Следствие 2. *Простая группа порядка* 60 *единственна с точностью до изоморфизма.*

Доказательство. Рассмотрим действие нашей группы на множестве ее силовских 5-подгрупп с помощью сопряжения. Теоремы Силова гласят, что число этих подгрупп сравнимо с единицей по модулю 5 и является делителем порядка группы. Значит, это число делит 12. Если силовская подгруппа единственна, то она нормальна, что противоречит простоте нашей группы. Значит, в нашей группе шесть силовских 5-подгрупп (других делителей 12, сравнимых с единицей по модулю 5, нет). Отсюда следует, что наша группа гомоморфно отображается в S_6. Более того, в силу простоты нашей группы этот гомоморфизм инъективен, а его образ лежит в A_6 (инъективность следует из того, что ядро было бы нормальной подгруппой, а если образ не лежит в A_6, то ядро гомоморфизма вычисления четности образа было бы нормальной подгруппой). Дальнейшее доказательство аналогично приведенному выше (подгруппа в A_6 индекса 6 изоморфна A_5).

Неабелевых простых групп порядка меньше 60 не существует. Следующий возможный порядок неабелевой простой группы равен 168. Среди проективных групп есть сразу две группы такого порядка: $PSL_2(\mathbb{F}_7)$ и $PSL_3(\mathbb{F}_2)$. Оказывается, что эти группы изоморфны. Мы приводим набросок доказательства, опуская технические проверки. Подробное доказательство см., например, в [1].

Предложение 7. $PSL_2(\mathbb{F}_7) \simeq PSL_3(\mathbb{F}_2)$.

Эскиз доказательства. Как известно, двумерная проективная геометрия над полем из двух элементов с точностью до проективной двойственности задается отношением инцидентности. Именно, если мы знаем для множества из 14 элементов (точек и прямых в двумерном проективном пространстве), какие пары элементов этого множества *инцидентны*[2)], то мы восстановим геометрию с точностью до, возможно, проективной двойственности (т. е. прямые окажутся точками, и наоборот). В частности, группа проективных преобразований $PGL_3(\mathbb{F}_2) = PSL_3(\mathbb{F}_2)$ является подгруппой индекса 2 в группе всех перестановок подмножеств проективной плоскости, которые сохраняют инцидентность.

Предъявим совершенно аналогичную картину «с точки зрения группы $PSL_2(\mathbb{F}_7)$». В качестве 14-элементного множества точек и прямых мы

[2)] Т. е. один из которых содержится в другом.

рассмотрим множество всех максимальных по включению подгрупп в $PSL_2(\mathbb{F}_7)$, которые состоят из инволюций (элементов, которые в квадрате равны e). Мы предоставляем читателю убедиться в том, что таких подгрупп ровно 14. Среди них есть две, которые содержат инволюцию $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, а именно

$$\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 2 & 4 \end{pmatrix}, \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}\right\}$$

и

$$\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}\right\},$$

остальные получаются из этих с помощью сопряжениями матрицами $\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$. Две подгруппы называются инцидентными, если их пересечение отлично от $\{e\}$. Можно проверить[3)], что отношение инцидентности на этих подгруппах изоморфно отношению инцидентности на точках и прямых проективной плоскости над $\mathbb{F}_2$. Поэтому группа $PSL_2(\mathbb{F}_7)$ (которая действует на нашем множестве подгрупп сопряжениями) изоморфна подгруппе индекса 2 в группе всех перестановок подмножеств проективной плоскости, которые сохраняют инцидентность. Поскольку группы $PSL_2(\mathbb{F}_7)$ и $PSL_3(\mathbb{F}_2)$ просты, две построенные подгруппы обязательно должны совпадать.

Замечание 3. Приведем набросок другого варианта доказательства[4)]. Рассмотрим множество всех четверок точек проективной прямой над $\mathbb{F}_7$, двойное отношение которых равно 3 (или 5, если перечислять их в другом порядке). Таких четверок точек ровно 28 (проверьте!). Если не отличать четверку точек от «дополнительной» четверки (вспомните, что проективная прямая над $\mathbb{F}_7$ состоит из 8 точек), то такие классы четверок образуют 14-элементное множество. На этом множестве отношение инцидентности вводится аналогично приведённому выше отношению инцидентности на подгруппах, и далее доказательство аналогично.

Задача*. Двумерная проективная геометрия над полем из двух элементов возникает также при изучении умножения в алгебре октав (чисел Грейвса – Кэли). Есть ли какая-то разумная связь группы $PSL_2(\mathbb{F}_7)$ с октавами?

Задача*. Докажите, что любая группа порядка 168 изоморфна $PSL_2(\mathbb{F}_7)$.

Замечание 4. Подсчет порядков показывает, что количества элементов в группах $PSL_4(\mathbb{F}_2)$ и $PSL_3(\mathbb{F}_4)$ одинаковы. Можно предположить,

[3)] Говорить «легко проверить» тут было бы чрезмерным издевательством над читателем.

[4)] Это доказательство автор узнал от Э. Б. Винберга.

что, как и выше, удастся связать теоретико-групповые конструкции для $PSL_3(\mathbb{F}_4)$ с проективной геометрией над $\mathbb{F}_2$, и использовать это для доказательства изоморфизма. Оказывается, что эти две группы неизоморфны. Попробуйте это доказать. Один из путей состоит в том, чтобы изучить классы сопряженности инволюций в этих группах. Может быть, Вы придумаете другой путь?

От алгебры к геометрии

В этом разделе наша стратегия радикально изменится. Если до этого мы изучали геометрию действий проективных групп и обнаруживали объекты, на которых эти группы действуют, то теперь мы стартуем с действий симметрических и знакопеременных групп, и обнаружим действие этих групп на геометрических объектах. Следующее предложение является первым нетривиальным примером такой ситуации.

Предложение 8. $S_6 \simeq Sp_4(\mathbb{F}_2)$. *Здесь $Sp_4(\Bbbk)$ обозначает группу линейных преобразований четырехмерного пространства над полем $\Bbbk$, которые сохраняют кососимметричную билинейную форму*

$$\langle (x_0, x_1, x_2, x_3), (y_0, y_1, y_2, y_3) \rangle = x_0y_1 - x_1y_0 + x_2y_3 - x_3y_2.$$

Доказательство. Рассмотрим 16-элементное множество, элементами которого являются все двухэлементные подмножества шестиэлементного множества и его пустое подмножество. Определим на этом множестве «сложение»: сумма пустого множества с любым элементом A снова равна A, сумма $A + A$ всегда равна пустому множеству, если два непустых подмножества не пересекаются, то их сумма равна дополнению к их объединению, если же они пересекаются по одному элементу, то их сумма равна их симметрической разности (разности их объединения и пересечения). Можно проверить, что это «сложение» ассоциативно, и тем самым на нашем множестве задается структура четырехмерного векторного пространства над полем из двух элементов.

Определим билинейную форму на нашем векторном пространстве формулой $(A, B) = \#A \cap B$ (это число надо понимать как элемент $\mathbb{F}_2$, т. е. нас интересует лишь его четность; проверку того, что это действительно билинейная форма, мы оставляем читателю). Легко видеть, что в базисе $\{1, 2\}$, $\{2, 3\}$, $\{4, 5\}$, $\{5, 6\}$ эта форма имеет вид, указанный в формулировке предложения. Кроме того, действие симметрической группы, очевидно, сохраняет эту форму, и потому мы имеет гомоморфизм $S_6 \to Sp_4(\mathbb{F}_2)$. Нетрудно проверить, что порядок группы $Sp_4(\mathbb{F}_2)$ равен 6!, так что надо лишь проверить, что этот гомоморфизм не имеет ядра. Но нетрудно видеть, что его образ состоит из более чем двух элементов, а нетривиальные нормальные подгруппы S_6 суть A_6 и S_6.

Замечание 5. Нетривиальный способ интерпретировать использованную в доказательстве конструкцию, который помимо прочего приводит к ясному доказательству ассоциативности суммы подмножеств, состоит в том, чтобы понимать эту конструкцию как частный случай следующей общей конструкции. Пусть M — конечное множество. На множестве $\mathcal{P}(M)$ всех его подмножеств имеется естественная структура абелевой группы, задаваемая вычислением симметрической разности. Ясно, что каждый элемент этой группы имеет порядок 2, так что $\mathcal{P}(M)$ — не только абелева группа, но и векторное пространство над $\mathbb{F}_2$. Подмножество $\{\varnothing, M\}$ является подпространством, и мы можем образовать соответствующее факторпространство. Оно состоит из смежных классов $\{A, M \setminus A\}$. Если в множестве M четное число элементов, то подпространство $\mathcal{P}^+(M) \subset \mathcal{P}(M)$, состоящее из всех подмножеств, в которых четное число элементов, содержит подпространство, по которому мы факторизуем. Обозначим через V образ $\mathcal{P}^+(M)$ в факторпространстве.

В случае, если множество M шестиэлементно, пространство V четырехмерно, и естественно отождествляется с построенным выше четырехмерным пространством. В самом деле, выбирая в каждом смежном классе то из множеств, в котором меньше элементов, мы можем сопоставить каждому элементу $v \in V$ подмножество множества M, которое либо пусто, либо двухэлементно. Симплектическая форма, как нетрудно видеть, определена на всём $\mathcal{P}(M)$, и ее ограничение на $\mathcal{P}^+(M)$ опускается на V после факторизации.

Теорема 1. $GL_4(\mathbb{F}_2) \simeq A_8$.

Эскиз доказательства. Здесь мы тоже ограничимся наброском доказательства, оставляя некоторые детали в качестве (весьма полезного) упражнения.

Из замечания 2 мы знаем, что внешний автоморфизм S_6 переводит класс сопряженности транспозиции в класс сопряженности произведения трех непересекающихся транспозиций (далее мы называем перестановку, которая является произведением r непересекающихся транспозиций, r-инволюцией). Выше мы научились сопоставлять транспозициям в S_6 (то есть двухэлементным подмножествам шестиэлементного множества) ненулевые элементы 4-мерного векторного пространства над $\mathbb{F}_2$. Перенесем с помощью внешнего автоморфизма это сопоставление на 3-инволюции. Мы построим действие A_8 на этих объектах, которое и задаст гомоморфизм $A_8 \to GL_4(\mathbb{F}_2)$. Для начала заменим 3-инволюции в S_6 на 4-инволюции в S_8 с помощью гомоморфизма $\imath\colon S_6 \to A_8$, заданного правилом

$$\imath(\sigma) = \begin{cases} \sigma, & \text{если } \sigma \in A_6, \\ \sigma \cdot (7\ 8) & \text{иначе.} \end{cases}$$

Теперь группа A_8 могла бы действовать на этих перестановках сопряжением, завершая доказательство. Увы, это действие не подходит: оно не согласовано со структурой векторного пространства (и потому не задает гомоморфизм в $GL_4(\mathbb{F}_2)$). В действительности всё устроено чуть сложнее (но весьма изящно).

Вспомним доказательство теоремы Кэли (которая гласит, что каждая конечная группа изоморфна подгруппе симметрической группы). Именно, это доказательство нумерует элементы данной группы, и каждому элементу сопоставляет перестановку элементов группы, задаваемую правым сдвигом на этот элемент. Простое наблюдение, которое будет для нас очень важным, заключается в том, что 4-инволюции можно понимать как образы элементов векторного пространства $\mathbb{F}_2^3$ при вложении Кэли этого векторного пространства в S_8. (В самом деле, эти образы имеют порядок 2 и не имеют неподвижных точек, и потому обязаны быть 4-инволюциями.) Всевозможные образы вложений Кэли этого векторного пространства (отвечающие разным нумерациям элементов) образуют множество, на котором A_8 (и даже S_8) естественно действует. Сформулируем в виде упражнений несколько свойств этого действия.

Упражнение. 1. Для любого вложения Кэли $\mathbb{F}_2^3 \hookrightarrow S_8$ каждая транспозиция $(i\ j) \subset S_8$ входит сомножителем ровно в один элемент образа.

2. Нормализатор такой подгруппы изоморфен полупрямому произведению $GL_3(\mathbb{F}_2) \ltimes \mathbb{F}_2^3$ и целиком содержится в A_8.

3. Действие S_8 на разных вложениях Кэли с помощью сопряжений имеет одну орбиту, действие A_8 — две орбиты.

4. Любые две подгруппы из одной A_8-орбиты пересекаются лишь по единичному элементу.

Выберем представителей двух A_8-орбит на множестве вложений Кэли. Обозначим эти подгруппы через G_+ и G_-. Будем называть подгруппы, сопряженные с G_+, четными, а подгруппы, сопряженные с G_-, нечетными.

Ровно один элемент $g \subset G_+$ содержит транспозицию (7 8) в качестве сомножителя. Сопоставляя подгруппе элемент g, мы получаем биекцию между множеством четных подгрупп и множеством 4-транспозиций, которые получаются из 3-транспозиций S_6 с помощью гомоморфизма $\imath$. Аналогичное верно для нечетных подгрупп.

С помощью этой биекции мы получаем на множестве четных подгрупп структуру векторного пространства над $\mathbb{F}_2$. Ключевое (и наиболее нетривиальное) утверждение, которое осталось доказать, таково.

Предложение 9. *Действие A_8 с помощью сопряжений на этом векторном пространстве линейно.*

Доказательство. Скажем, что четная подгруппа H инцидентна нечетной подгруппе K, если пересечение H и K содержит более одного элемента. Отношение инцидентности важно по той причине, что подгруппа, являющаяся суммой H и K относительно нашей структуры векторного пространства, является единственной подгруппой, которая инцидентна всем подгруппам, инцидентным и H, и K. Из этого немедленно следует наше предложение, поскольку мы определили сумму векторов нашего пространства в чисто теоретико-групповых терминах — а значит, это определение стабильно относительно действия сопряжениями.

Желательное нам утверждение составляет содержание следующего упражнения.

Упражнение. 1. Подгруппа H инцидентна подгруппе K если и только если отвечающие им 4-инволюции коммутируют.

2. Пусть s и t — две различных 3-инволюции в S_6. Существует единственная 3-инволюция, отличная от s и t, которая коммутирует со всеми 3-инволюциями, которые коммутируют и с s, и с t. Это в точности инволюция, являющаяся суммой s и t относительно существующей на 3-инволюциях структуры векторного пространства над $\mathbb{F}_2$.

Замечание 6. Выше мы построили отображение S_6 в группу линейных преобразований четырехмерного пространства над полем из двух элементов. Построенный сейчас гомоморфизм A_8 в $GL_4(\mathbb{F}_2)$ расширяет этот гомоморфизм с подгруппы $\imath(S_6)$ на всю группу.

Список литературы

[1] О'Мира О. *Лекции о линейных группах* // Автоморфизмы классических групп. М.: Мир, 1976.

[2] Винберг Э. Б. *Курс алгебры*. М.: Факториал, 2002.

[3] Lang S. *Algebra*. Rev. 3rd ed. Springer, 2002.

[4] Murray J., *The alternating group A_8 and the general linear group $GL_4(2)$* // Math. Proc. of the Royal Irish Academy, 1999. Vol. 99A, no. 2. P. 123–132.

[5] Каргаполов М. И., Мерзляков К. И. *Основы теории групп*. М.: Наука, 1977.

В. В. Доценко: Trinity College, Dublin

Издательство МЦНМО

Дж. Кингман. **Пуассоновские процессы.** Под ред. А.М. Вершика. 2007. 136 с.

Книга признанного мирового специалиста в области теории вероятностей, математической статистики и их приложений Дж. Кингмана представляет собой систематическое изложение классической теории пуассоновских процессов в произвольных пространствах. Книга предназначена как для начинающих изучение теории случайных процессов, так и для специалистов, поскольку сочетает ясное и красивое изложение основ теории с представлением новых идей, связанных прежде всего с разнообразными приложениями пуассоновских процессов к геометрии, теории массового обслуживания, экологии, генетике, астрономии и др.

М. Я. Кельберт, Ю. М. Сухов. **Вероятность и статистика в примерах и задачах.** Том I. Основные понятия теории вероятностей и математической статистики. 2007. 456 с.

Для освоения теории вероятностей и математической статистики тренировка в решении задач и выработка интуиции важны не меньше, чем изучение доказательств теорем; большое разнообразие задач по этому предмету затрудняет студентам переход от лекций к экзаменационным задачам, а от них — к практике.

Ввиду того, что предмет этой книги критически важен и для современных приложений (финансовая математика, менеджмент, телекоммуникации, обработка сигналов, биоинформатика), так и для приложений классических (актуарная математика, социология, инженерия), авторы собрали большое количество упражнений, снабженных полными решениями. Эти решения адаптированы к нуждам и умениям учащихся. Для удобства усвоения текста авторы приводят в книге целый ряд основных математических фактов; кроме того, текст снабжен историческими отступлениями.

В. И. Арнольд. **Экспериментальное наблюдение математических фактов**. 2006. 120 с.

Книга содержит записи курсов лекций, прочитаных академиком В. И. Арнольдом в 2005 г., в Дубне, на летней школе «Современная математика». В книге рассказывается о нескольких новых направлениях математических исследований, основанных на численных экспериментах.

Игорь Фёдорович Шарыгин. К 70-летию со дня рождения. Сост. А. А. Заславский, В. Ю. Протасов, Д. И. Шарыгин. 2007. 304 с.

В книге собраны различные материалы, связанные с жизнью и деятельностью выдающегося педагога и учёного, популяризатора науки Игоря Фёдоровича Шарыгина (1937–2004), его статьи и воспоминания о нём.

Отдельная часть книги содержит задачи и подробные решения геометрических олимпиад им. И. Ф. Шарыгина, проводимых с 2005 года.

Книга предназначена для всех интересующихся вопросами математического образования, школьных учителей и руководителей кружков.

Ж.-П. Серр. **Собрание сочинений. Том III.** (Совместно с НМУ) 2007. 540 с.

Жан-Пьер Серр — один из величайших математиков нашего времени, чьи работы на протяжении последнего полувека преобразили современную математику, в особенности алгебраическую топологию, алгебраическую геометрию, теорию алгебр и групп Ли, теорию чисел.

Собрание сочинений выпускается к 75-летию ученого. В 3-й том настоящего издания включены работы 1961–68 гг.

На сколько частей делят плоскость n прямых?

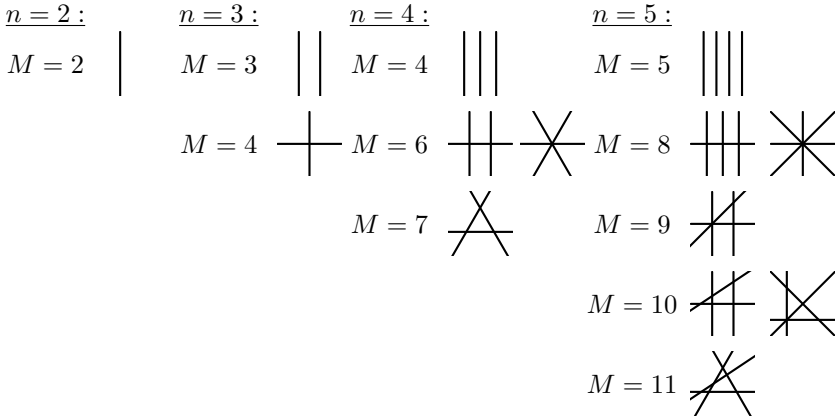
В. И. Арнольд*

Рассмотрим n различных прямых на вещественной проективной плоскости. Они делят ее на (выпуклые) части. Спрашивается, сколько частей может получиться (при всевозможных расположениях данного числа прямых)?

При малых n ответы ясны, возможное количество частей M дается следующей таблицей:

n	1	2	3	4	5
M	1	2	3	4	5
			4	6	8
				7	9
					10
					11

Считая одну из прямых бесконечно удаленной, мы получим $n-1$ прямую в $\mathbb{R}^2$. Значения M из таблицы доставляются следующими рисунками $n-1$ прямой:



Аналогичным образом исследуется и число компонент дополнения к набору прямых на аффинной плоскости $\mathbb{R}^2$: это та же задача, так как

*частично поддержано РФФИ, грант 05–01–00104.

можно одну из n прямых объявить бесконечно удаленной и исследовать дополнение к $n-1$ прямой на аффинной плоскости (совпадающее с дополнением к n прямым на проективной).

Мы замечаем, глядя на предыдущие примеры, что наименьшее число частей дополнения к n прямым в $\mathbb{R}P^2$ есть $M=n$, а наибольшее есть

$$M=1+(1+2+3+\cdots+(n-1))=1+n(n-1)/2.$$

Но промежуточные числа между этими пределами достигаются не все, а только некоторые. Начиная с некоторого места, все достаточно большие значения M достигаются, но начало списка достижимых значений содержит пробелы, дыры.

Целью настоящей работы является описание этих дыр. Вот первая дыра.

Теорема 1. *Значение $M=2(n-1)$ достижимо, а ни одно из значений M в интервале*

$$n<M<2(n-1)$$

не достижимо.

Ни при каком выборе n прямых в $\mathbb{R}P^2$ дополнение к их объединению не может состоять из такого числа M связных компонент.

Доказательство. Обозначим через k наибольшее число прямых, проходящих через одну точку (среди наших n прямых).

Лемма 1. *Если $k=n$, то $M=n$.*

Доказательство. Будем считать одну из этих n прямых бесконечно удаленной. Тогда остальные прямые параллельны. Они делят дополнительную к первой прямой аффинную плоскость $\mathbb{R}^2$ на n частей, так как их $n-1$ штука.

Лемма 2. *Если $k=n-1$, то $M=2(n-1)$.*

Доказательство. Будем считать оставшуюся, n-ую, прямую бесконечно удаленной. Дополнение к ней есть $\mathbb{R}^2$. Набор из $n-1$ проходящих через одну точку прямых делит плоскость $\mathbb{R}^2$ на $2(n-1)$ часть, что и требовалось доказать.

Лемма 3. *Если $k\leqslant n-1$, то $M\geqslant 2(n-1)$.*

Доказательство. Заметим, что при $n>1$ имеем $k\geqslant 2$ (так как в $\mathbb{R}P^2$ любые две прямые пересекаются).

Выберем одну из k проходящих через одну точку прямых за бесконечно удаленную. Дополнение к ней представляет собой аффинную плоскость $\mathbb{R}^2$, содержащую $k-1$ параллельную прямую выбранного пучка и еще $n-k\geqslant 1$ остальных прямых.

Указанные параллельные прямые делят плоскость $\mathbb{R}P^2$ на k частей. Добавляя по одной остальные прямые, мы будем, шаг за шагом, увеличивать число частей. При этом, если добавляемая s-я прямая пересекается с уже имеющимися прямыми в x_s точках, то она делится ими на x_s отрезков, каждый из которых делит одну из бывших до проведения s-й прямой частей на две. Поэтому число частей дополнения увеличивается при проведении s-й прямой ровно на x_s.

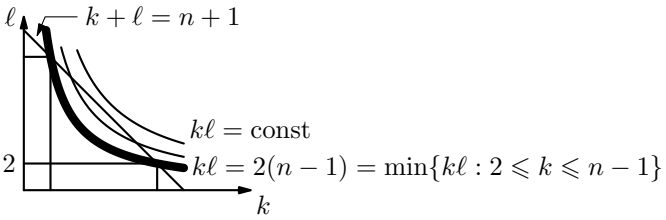
Заметим теперь, что $x_s \geqslant k$ (так как добавляемая прямая пересекает все k параллельных прямых исходного пучка в k разных своих точках). Поэтому общее число добавляемых частей есть

$$x_1 + \cdots + x_{n-k} \geqslant k(n-k).$$

Добавляя эти части к k частям, имевшимся до проведения $n-k$ «дополнительных» прямых, мы получаем вывод:

$$M \geqslant k + k(n-k) = k(n-k+1). \tag{1}$$

Сумма обоих сомножителей в правой части равна $n+1$. Произведение двух положительных сомножителей, сумма которых равна $n+1$, тем больше, чем больше меньший сомножитель:



Если $2 \leqslant k \leqslant n-1$, то $\min\limits_{k+\ell=n+1}(k,\ell) \geqslant 2$, так что $M \geqslant 2(n-2+1) = 2(n-1)$, что и доказывает лемму 3.

Из лемм 1, 2 и 3 следует теорема 1 (так как любое число $k \leqslant n$ либо равно n, либо равно $n-1$, либо меньше $n-1$).

Первая дыра описана. Опишем вторую дыру. Пусть $n \geqslant 3$.

Теорема 2. *Значение $M = 3n-6$ достижимо, а ни одно из значений M в интервале*

$$2(n-1) < M < 3(n-2)$$

не достижимо.

Ни при каком выборе $n > 2$ прямых в $\mathbb{R}P^2$ дополнение к ним не может состоять из такого числа M связных компонент.

Доказательство. Как и выше, будем обозначать через k максимальное число пересекающихся в одной точке прямых (из данных n) и будем

называть одну из них бесконечно удаленной. Будем рассматривать остальные прямые в дополнительной к выбранной прямой аффинной плоскости $\mathbb{R}^2$ как составляющие пучок из $k-1$ параллельных друг другу прямых и дополнительный набор из $n-k$ остальных прямых, не параллельных этим $k-1$ прямым пучка.

Если $k = n-1$, то $M = 2(n-1)$ по лемме 2. Если же $k \leqslant n-2$, то из соотношения (1) в доказательстве леммы 3 мы находим

$$M \geqslant k(n-k+1) \geqslant (n-2)((n+1)-(n-2)) = 3(n-2),$$

при условии, что $k \geqslant 3$ (при котором $\min\limits_{k+\ell=n+1}(k,\ell) \geqslant 3$).

Таким образом, утверждение теоремы доказано для всех таких расположений n прямых, что $k > 2$.

В оставшемся случае, когда $k = 2$, мы тоже докажем сейчас, что $M \geqslant$ $\geqslant 3(n-2)$.

Если $k = 2$, т. е. никакие три прямые не проходят через общую точку, то все наши n прямых делят плоскость на максимально возможное при n прямых (и достижимое для n прямых общего положения) число частей, равное

$$M = 1 + n(n-1)/2.$$

Лемма. *Имеет место неравенство*

$$n(n-1)/2 + 1 \geqslant 3(n-2).$$

Доказательство. Это неравенство имеет вид

$$n^2 - n - 6(n-2) + 2 \geqslant 0,$$

т. е.

$$n^2 - 7n + 14 \geqslant 0,$$

что и выполняется, поскольку дискриминант квадратного трехчлена, стоящего в левой части,

$$49 - 4 \cdot 14 < 0,$$

отрцателен.

Следовательно, лемма доказана, и в случае $k = 2$ неравенство $M \geqslant$ $\geqslant 3(n-2)$ тоже выполняется.

Теорема 2 доказана, мы описали вторую дыру. Она появляется впервые при $n = 6$ (когда в определяющем дыру интервале есть целые точки: $3(n-2) - 2(n-1) > 1$ при $n > 5$).

Дальнейшие дыры мы изучим теперь в предположении, что число прямых n достаточно велико (по сравнению с номером дыры).

Теорема 3. *Предположим, что наибольшее число из n прямых, проходящих через одну точку, равно k. Тогда эти прямые делят плоскость* $\mathbb{R}P^2$ *на M частей, где число M принадлежит интервалу*

$$k(n+1-k) \leqslant M \leqslant k(n+1-k) + r(r-1)/2, \quad \text{где } r = n-k$$

(*причем все числа M из этого интервала достигаются при надлежащем выборе n прямых, если число прямых n достаточно велико*).

Доказательство. Выберем пучок из k прямых. Прямые этого пучка делят плоскость $\mathbb{R}P^2$ на k частей. Оставшиеся $n-k=r$ прямых добавляют к k число частей

$$M' = x_1 + x_2 + \cdots + x_{n-k},$$

где x_s есть число точек s-й из добавляемых прямых, по которым ее пересекают предыдущие прямые.

Среди этих предыдущих прямых имеются k прямых выбранного пучка (и $s-1$ добавляемая прямая). Точки пересечения с прямыми пучка все различны (так как единственная общая точка двух прямых пучка есть избранная вначале точка пересечения k прямых пучка, поэтому больше никакие из наших n прямых через эту точку не проходят).

Следовательно, $x_s \geqslant k$, $M' \geqslant k(n-k)$, $M \geqslant k(n-k+1)$. Первое неравенство теоремы 3 доказано.

С другой стороны, $x_s \leqslant k + (s-1)$. Следовательно,

$$M' \leqslant k(n-k) + (0+1+\cdots+n-k-1) = k(n-k) + \frac{r(r-1)}{2},$$
$$M \leqslant k(n+1-k) + r(r-1)/2.$$

Этим доказано второе неравенство теоремы 3.

Все значения M из описанного обоими неравенствами интервала достигаются (при достаточно больших n) по следующей причине.

Наибольшее число частей доставляет выбор дополнительных r прямых общего положения. Для них все точки пересечения (с прямыми пучка и друг с другом) различны, что и дает $k(n+1-k) + r(r-1)/2$ частей.

Если n достаточно велико по сравнению с r (например, если $n \geqslant r(r-1)/2$), то можно выбрать дополнительные прямые так, чтобы любые выбранные точки их попарного пересечения друг с другом лежали на прямых пучка (так что $x_s = k$ для соответствующих s).

Действительно, можно, например, начать с r прямых общего положения в аффинной плоскости $\mathbb{R}^2$ и провести параллельные друг другу и не параллельные ни одной из этих прямых прямые через любое количество $r(r-1)/2 - S$ точек их попарного пересечения. Включив эти параллельные прямые вместе с бесконечно удаленной прямой в пучок из $k = n - r$ параллельных прямых, мы получим набор прямых, для которого $x_s = k$

при всех значениях s, кроме S выбранных, для которых $x_s = k+1$. В этом случае $M' = kr + S$, $M = k(n-k+1) + S$, и теорема 3 доказана.

Теорема 4. *Предположим, что наибольшее число из n прямых, проходящих через одну точку, равно $k > 2$. Тогда эти прямые делят плоскость $\mathbb{R}P^2$ на M частей, где $M \geqslant n(n-1)/(2(k-1))$.*

Здесь важно, что числитель растет с числом прямых n как n^2, а знаменатель от числа прямых n не зависит. Из-за этого правая часть становится большей любой линейной функции от n при достаточно больших n (когда k фиксировано).

Для доказательства теоремы 4 упорядочим как-либо заданные n прямых. Назовем «событием» пересечение какой-либо прямой с прямой с меньшим номером. Число событий равно, таким образом, $0+1+2+\cdots+$ $+(n-1) = n(n-1)/2$ (независимо от того, сколько различных точек пересечения имеется).

Назовем «разделением» деление какой-либо прямой (скажем, s-й) на части прямыми с меньшими номерами. Обозначим через x_s число разделений s-й прямой. Эти x_s точек разделяют указанную проективную прямую на x_s частей.

Добавляя прямые по одной, мы каждый раз увеличиваем число компонент дополнения к прямым на число частей x_s, добавляемых s-й прямой (делящей на две части своими x_s отрезками каждую из ровно x_s уже существовавших пересекаемых ею компонент).

Поэтому общее число компонент дополнения в проективной плоскости $\mathbb{R}P^2$ к объединению n прямых составляет

$$M = \sum_{s=1}^{n} x_s,$$

считая формально $x_s = 1$: хотя первую прямую «предыдущие» прямые не делят, нужно учесть единственную компоненту дополнения к одной прямой на *проективной* плоскости.

В каждой точке разделения происходит самое большее $k-1$ событие (пересечение s-й прямой с предыдущими), так как больше k прямых нашего набора ни через одну точку не проходят. Поэтому *число всех событий не превосходит произведения* $M(k-1)$. А так как оно равно $n(n-1)/2$, то мы заключаем, что

$$n(n-1)/2 \leqslant M(k-1), \quad \text{т. е. } M \geqslant \frac{n(n-1)}{2(k-1)},$$

что и доказывает теорему 4.

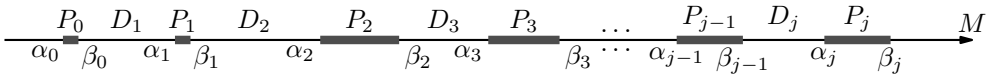
Для исследования «стабильных» дыр (j-я стабильная дыра D_j будет исследоваться при числе прямых n, превосходящем некоторую зависящую

от j постоянную), введем следующие обозначения:

$$\alpha_j = (n-j)(j+1), \quad \beta_j = (n-j)(j+1) + j(j-1)/2.$$

При достаточно большом n первые члены этих двух последовательностей расположены в следующем порядке:

$$(\alpha_0 = \beta_0) < (\alpha_1 = \beta_1) < \alpha_2 < \beta_2 < \alpha_3 < \beta_3 < \cdots < \alpha_{j-1} < \beta_{j-1} < \alpha_j.$$



Обозначим через P_0, P_1, ..., замкнутые интервалы

$$P_0 = [\alpha_0 \leqslant M \leqslant \beta_0], \quad P_1 = [\alpha_1 \leqslant M \leqslant \beta_1], \quad \ldots, P_j = [\alpha_j \leqslant M \leqslant \beta_j],$$

и через D_1, D_2, ..., D_j дополнительные открытые интервалы

$$D_1 =]\beta_0 < M < \alpha_1[, \quad D_2 =]\beta_1 < M < \alpha_2[, \quad \ldots, D_j =]\beta_{j-1} < M < \alpha_j[.$$

Стабильная дыра D_j описывается следующим образом.

Теорема 5. *Если число прямых n достаточно велико, то число M компонент дополнения к ним в проективной плоскости $\mathbb{R}P^2$ не может принимать значений из интервала D_j: невозможны все значения M, для которых*

$$\beta_{j-1} = j(n+1-j) + (j-1)(j-2)/2 < M < (j+1)(n-j) = \alpha_j.$$

Доказательство. Обозначим наибольшее число из n прямых, проходящих через одну точку, через k. Мы докажем, что M не может попасть в интервал D_j ни при каком k, но это доказательство будет основано на разных соображениях в следующих трех случаях:

I. $k > n - j$;

II. $j + 1 \leqslant k \leqslant n - j$;

III. $k \leqslant j$.

При этом мы будем предполагать, что $n - j \geqslant j + 1$ (что выполнено, если n достаточно велико).

Случай I. Предположим, что k принимает одно из значений $\{n, n-1, \ldots, n-j+1\}$, например, $k = n - r$.

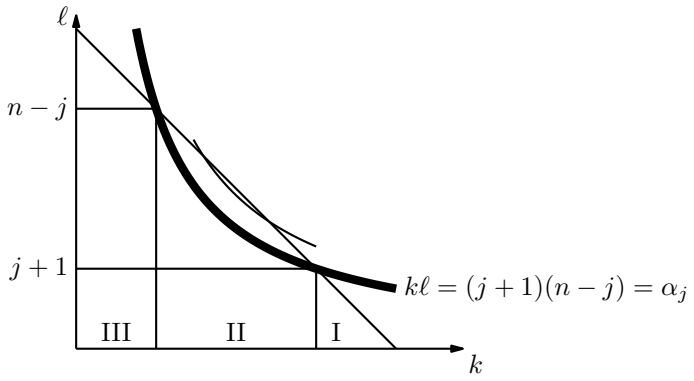
Согласно теореме 3, число M лежит в интервале

$$\alpha_r = (n-r)(r+1) \leqslant M \leqslant (n-r)(r+1) + r(r-1)/2 = \beta_r,$$

т. е. $M \in P_r$, $0 \leqslant r \leqslant j - 1$.

Все эти r отрезков с интервалом D_j не пересекаются, так что в случае I теорема 5 доказана.

Случай II. Предположим, что $j+1 \leqslant k \leqslant n-j$. Тогда $\ell = n+1-k$ также удовлетворяет неравенствам $j+1 \leqslant \ell \leqslant n-j$. В этом случае $\min\limits_{k+\ell=n+1}(k,\ell) \geqslant j+1$:



Поэтому, опять согласно теореме 3,

$$M \geqslant (n-j)(j+1) = \alpha_j.$$

В интервале D_j, однако, $M < \alpha_j$. Тем самым теорема 5 доказана и в случае II.

Случай III. Предположим, что $2 < k \leqslant j$. Согласно теореме 4,

$$M \geqslant \frac{n(n-1)}{2(k-1)} \geqslant \frac{n(n-1)}{2(j-1)}.$$

Правая часть этого неравенства превосходит число α_j, если n достаточно велико. Действительно, $\dfrac{n(n-1)}{2(j-1)} > (n-j)(j+1)$ при достаточно больших n, поскольку тогда

$$\frac{n(n-1)}{n-j} > 2(j^2-1).$$

Например,

$$\frac{n(n-1)}{n-j} \geqslant n,$$

так что условие $n > 2(j^2-1)$ достаточно для неравенства $M > \alpha_j$, исключающего принадлежность точки M интервалу D_j (между β_{j-1} и α_j).

В единственном оставшемся неразобранным случае $k=2$ наши n прямых общего положения делят проективную плоскость $\mathbb{R}P^2$ на $M = 1 + {} + n(n-1)/2$ частей.

Это число M больше предела $\alpha_j = (n-j)(j+1)$, так как при $j+1 < n/2$ (что мы предполагали) выполнены неравенства

$$\alpha_j < \frac{n(n-1)}{2} < M$$

для $j > 0$.

Стало быть, теорема 5 доказана и при $k = 2$, а следовательно она доказана при всех k (случай $k = 1$ при $n > 1$ не реализуется, так как любые две прямые на проективной плоскости пересекаются).

Таким образом, теорема 5 доказана полностью, так что (при достаточно большом числе прямых n) существуют все стабильные дыры

$$D_1, D_2, \ldots, D_j, \ldots$$

в последовательности чисел компонент M, на которые n прямых делят вещественную проективную плоскость.

Замечание 1. Я не знаю, будут ли нестабильные дыры (при меньших n, чем указано выше) задаваться теми же формулами ($\beta_{j-1} < M < \alpha_j$), что стабильные. Вначале (при малых j) нестабильность не сказывается.

Первый неясный случай — третья дыра для $n = 9$. В этом случае формулы дают $\alpha_3 = 24$, $\beta_2 = 22$.

Девять прямых могут делить проективную плоскость и на 22 области, и на 24 области. Могут ли они делить ее на 23 области (или же $M = 23$ составляет для $n = 9$ третью дыру) неизвестно. Такое расположение прямых если и возможно, то лишь в том случае, когда никакие 4 из этих 9 прямых не проходят через одну точку (случай $k = 3$ в доказательстве теоремы 5).

Замечание 2. Источником настоящей работы послужило осуществленное в Беркли А. Б. Гивенталем издание перевода «Геометрии» А. П. Киселёва на американский язык. Просматривая в апреле 2007 года в Калифорнии этот перевод, я не смог сразу решить одну из задач этой книги (все задачи которой я успешно решил в детстве).

Эта задача была такой: сколько прямых делят плоскость $\mathbb{R}^2$ на пять выпуклых частей?

Гивенталь, которого я спросил, как формулировал этот вопрос в исходной книге Киселёв, сознался, что никак: задача добавлена переводчиком (усовершенствовавшим Киселёва и в других местах).

Каждая математическая задача допускает «русскую» версию, которая не может быть упрощена (без потери сущности задачи) и «французскую», которая не может быть обобщена (так как она сформулирована уже в столь общем виде, чтобы он содержал все возможные обобщения).

Приехав в Беркли из Парижа, я решил сформулировать французскую версию вопроса Гивенталя, а для этого заменил 5 областей любым их числом M — от чего и произошла настоящая работа.

Получившуюся общую задачу я так и не решил: следовало бы описать все дыры при всех значениях n, а я даже третью дыру вычислил явно только при $n \geqslant 14$ (когда она становится стабильной). Читая в Беркли, Стенфорде, Сан-Хосе и Санта-Кларе лекции местным школьникам (которых героические руководители здешних математических кружков московского образца выучили лучше меня решать трудные задачи), я надеялся, что они справятся с описанием нестабильных дыр, но всё еще этого пока не дождался.

Не решен, по-видимому, вопрос, могут ли 9 прямых делить проективную плоскость на 23 части.

18 июля 2007 года

В. И. Арнольд: Математический институт им. Стеклова РАН
Москва, 119991, Улица Губкина, д. 8

Степени простых чисел в составе пифагоровых троек

Е. А. Горин

Устанавливается, что вопрос о пифагоровых тройках, в состав которых входят две степени простых, непосредственно связан с известными нерешенными классическими проблемами теории чисел. Хотя некоторые свойства множества таких троек удается довольно легко выяснить, уже́ вопрос о бесконечности этого множества остается открытым.

Введение

1. Пифагорова тройка — это (упорядоченный) набор $\{x, y, z\}$ натуральных чисел, для которых

$$x^2 + y^2 = z^2. \tag{1}$$

Тройка $\{x, y, z\}$ называется *примитивной*, если $\gcd(x, y, z) = 1$. Здесь и далее через $\gcd(a, b, \ldots)$ обозначается наибольший общий делитель набора $\{a, b, \ldots\}$ целых (в частности, натуральных) чисел.

В дальнейшем, если противное явно не оговаривается, имеются в виду примитивные тройки. Из соотношения (1) тогда следует, что одно из чисел x, y является четным, а другое — нечетным. Для определенности и для удобства в дальнейшем, если противное не оговаривается явно, *четным считается* x. Заметим, что для примитивных троек z всегда является нечетным.

Пифагоровы тройки — один из древнейших объектов математики, так что было бы наивным надеяться сказать о них что–нибудь особенно оригинальное. Однако наша цель в другом: мы хотим показать, что входящий в заглавие (немного странный) вопрос тесно связан с целым рядом нетривиальных классических проблем теории чисел.

Пифагоровы тройки при сделанных предположениях допускают следующую исчерпывающую параметризацию:

$$\begin{cases} x = 2ab, \\ y = a^2 - b^2, \\ z = a^2 + b^2, \end{cases} \tag{2}$$

где a и b — натуральные числа различной четности, причем $a > b$ и $\gcd(a, b) = 1$. Формулы (2) иногда называют *формулами индусов* (см., например, [1, с.10]), и мы будем использовать эту терминологию.

Отметим, что сформулированная задача о пифагоровых тройках со степенями простых разбивается на несколько других, существенно различных по степени сложности.

Действительно, используя формулы (2), совсем легко убедиться, что *все три* компоненты являются степенями простых только в случае тройки $\{4, 3, 5\}$, известной (по меньшей мере) со времен строительства египетских пирамид. На самом деле, кроме этой тройки, нет других, в которых x и y — степени простых.

Довольно легко разбирается другой крайний случай, когда речь идет о наличии *хотя бы одной* степени простого в составе пифагоровой тройки. Множество таких троек само естественно разбивается на три класса, каждый из которых бесконечен, причем исследование одного из этих классов (z — степень простого) не так тривиально, как исследование двух других.

Более интересны два оставшихся случая, когда среди компонент присутствуют в точности две степени простых.

Случай, когда степенями простых являются x и z, напрямую связан с простыми Ферма. В этом смысле «самая большая» из известных троек такого типа соответствует соотношению

$$2^{18} + (2^{16} - 1)^2 = (2^{16} + 1)^2.$$

Наиболее интересен тот случай, когда степенями простых являются y и z. Отметим (это легко получается из (2)), что в этом (но и не только в этом, см. ниже) случае $2z = 1 + y^2$ и $x = z - 1$. Поэтому в приведенных далее списках достаточно указать только y или только z и, с другой стороны, легко дописать x. Довольно простые и не очень скучные вычисления позволяют предъявить многочисленные примеры такого типа. В частности, к пифагоровым тройкам приводят следующие пары *простых*:

y	3	5	11	19	29	59	61	71	79	101
z	5	13	61	181	421	1741	1861	2521	3121	5101

В следующих парах встречаются квадраты простых:

y	7	3^2	5^2	41	7^2	11^2
z	5^2	41	313	29^2	1201	7321

Во втором списке квадраты не встречаются парами, и это не случайно (так не бывает). Оказывается, показатели степеней простых сами непременно имеют вид 2^k (как в случае чисел Ферма), причем степень выше

2–й в качестве z встречается лишь однажды, а именно в тройке, где

$$y = 239 \text{ и } z = 13^4.$$

Отмечу здесь еще одну, на первый взгляд экзотическую, тройку, для которой

$$y = 3^8 \text{ и } z = (3^{16} + 1)/2 \text{ (это число простое).}$$

Вероятно, множество подобных троек бесконечно, однако в дальнейшем я приведу, кроме данного, лишь несколько примеров на эту тему, так как объем вычислений для проверки простоты стремительно возрастает, тогда как мои возможности ограничены, и никакой общей теоремы на эту тему я не знаю[1)].

Я не знаю, конечно или нет множество всех пифагоровых троек с двумя простыми или с простым и степенью простого (другие возможности, как будет показано, исключены).

Бо̀льшая часть доказательств носит чисто арифметический характер, а другая в основном использует лишь классические результаты элементарной теории чисел (теории сравнений), восходящие к Эйлеру. Заинтересованный читатель найдет их доказательства во всех учебниках, названных в списке литературы. Замечу, что и сборник «Математическое просвещение» многократно писал (и продолжает писать) об этих материях.

Исключение составляют два утверждения о диофантовых уравнениях, которые я также использую, привожу ссылки, но не привожу доказательств. В оправдание отмечу, что отчасти их применение лишь упрощает окончательные формулировки и, с другой стороны, хотя формулировки этих утверждений элементарные, элементарных и коротких доказательств, кажется, до сих пор нет (такое случается часто, когда речь идет о диофантовых уравнениях).

2. В основном мы будем использовать стандартные обозначения:
$\mathbb{C}$ — поле комплексных чисел;
$\mathbb{R}$ — поле вещественных чисел;
$\mathbb{Q}$ — поле рациональных чисел;
$\mathbb{Z}$ — кольцо (группа) целых чисел;
$\mathbb{N}$ — натуральный ряд чисел,
а также
$\mathbb{P}$ — множество простых чисел;
$\mathbb{P}^\times$ — множество натуральных степеней простых чисел.

Кроме того, значок $\square$ будет символизировать конец доказательства, а иногда — примера или какого–нибудь иного рассуждения.

[1)] Список примеров заметно расширил М. Н. Вялый. В конце статьи мы кратко обсудим, как и зачем это делать.

3. С конца 80-х годов я пользовался поддержкой, советами и многочисленными консультациями по конкретным вопросам теории чисел (и другим) Л. Л. Степановой, к которой я всегда испытывал чувство симпатии и глубокого уважения. Несколько (довольно скептических) замечаний она успела сделать и по поводу первоначального варианта данного сочинения[2)].

Различные задачи, связанные с пифагоровыми тройками, обычно предлагает своим студентам Е. И. Деза, и мысль рассмотреть тройки со степенями простых посетила меня, когда по служебной необходимости я слушал отчеты ее подопечных.

Часть из детально описанных здесь результатов были сформулированы на Тульской конференции [2], и я признателен В. Н. Чубарикову, который посоветовал мне не стесняться объявить такой доклад.

Я благодарен Е. И. Деза и Б. Н. Кукушкину, которые указали мне на необходимость уточнить некоторые рассуждения. Наконец, вклад М. Н. Вялого в улучшение текста заметно превысил даже те стандарты, которые были приняты в прежние времена.

§1. Простейшие случаи

1. Для удобства ссылок мы сформулируем следующие два очевидных утверждения в виде лемм.

Лемма 1. *Если в пифагоровой тройке x — степень простого, то*

$$x = 2^{\alpha+1}, \;\; y = 4^{\alpha} - 1, \;\; z = 4^{\alpha} + 1, \tag{3}$$

где α — натуральное число.

Доказательство. Ясно, что в формуле (2) в этом случае $a = 2^{\alpha}$, $b = 2^{\beta}$, где $0 \leqslant \beta < \alpha$. Если $\beta > 0$, то y окажется четным. □

Лемма 2. *Если в пифагоровой тройке y — степень простого, то*

$$x = 2b(b+1), \;\; y = 2b + 1, \;\; z = (b+1)^2 + b^2, \tag{4}$$

в частности, $z = x + 1$ и $2z = y^2 + 1$.

Доказательство. Действительно, в этом случае $a - b = 1$. □

Заметим, что в этих двух случаях очевидно, что когда одна из компонент пифагоровой тройки — степень простого, *две другие компоненты определяются однозначно.* Оказывается, это верно и тогда, когда степенью простого является z-компонента, однако в этом случае доказательство не так тривиально (см. ниже).

[2)] Лидия Леонидовна Степанова (1941–2004) работала доцентом кафедры теории чисел Московского педагогического гос. университета.

2. Следующая лемма «отсекает» еще один из тривиальных случаев.

Лемма 3. *Если в пифагоровой тройке $x \in \mathbb{P}^\times$ и $y \in \mathbb{P}^\times$, то $x = 4$, $y = 3$. В частности, все три компоненты — степени простых только для тройки $\{4, 3, 5\}$.*

Доказательство. Мы воспользуемся леммой 1. Так как $3 \mid (4^\alpha - 1)$, то из формулы (3) вытекает, что в условиях данной леммы

$$(2^\alpha - 1) \cdot (2^\alpha + 1) = 3^\beta$$

с некоторым натуральным β. При $\alpha > 1$ оба стоящих слева сомножителя были бы *натуральными* степенями числа 3. Но тогда число 3 оказалось бы делителем их разности, а это не так. Поэтому $\alpha = 1$. □

§2. Случай, когда z — степень простого

1. По формуле (2), в этом случае z представляется в виде суммы двух квадратов, и мы сначала напомним, когда это происходит.

Для простых z вопрос о такой представимости начал рассматривать Ферма, который угадал точный ответ. Доказательство нашел Эйлер. Он же начал рассматривать составные числа. Окончательное решение давно помещают в каждый учебник теории чисел, см., в частности, [3–7] из списка литературы.

Представление $c = a^2 + b^2$ натурального числа c называется *собственным,* если $\gcd(a, b) = 1$. По смыслу нашей задачи (неприводимость) и ввиду формул (2) нам интересны как раз такие представления. Используя комплексную символику, представление $c = a^2 + b^2$ можно переписать в виде $c = |a + ib|^2$, и такая запись может оказаться полезной. Например, из нее легко получается, что вместе с c при натуральном n собственное представление имеет c^n, а при нечетном c такое представление имеет $2c = |(1 + i)(a + ib)|^2$. Эти факты можно рассматривать как пояснение к формулировке следующей ниже леммы 4.

Имея представление $c = a^2 + b^2$, мы можем получить еще несколько представлений, меняя местами a и b и меняя их знаки. Говоря о единственности, мы всегда будем иметь в виду *единственность этого класса эквивалентности*.

Приведем для ясности несколько простых числовых примеров. Числа 3 и 4 не представляются в виде суммы двух квадратов, числа 5 и 10 представляются однозначно (в указанном выше смысле). Число 65 — минимальное из имеющих два собственных представления (и не имеющее других). Число 50 имеет два представления, из которых одно собственное, а второе нет. Число 20 собственных представлений не имеет, однако $20 = 2^2 + 4^2$.

Основная теорема состоит в том, что *простое нечетное p тогда и только тогда имеет (непременно собственное) представление, когда $p \equiv 1 \pmod 4$, причем представление единственно.*

В общем случае ответ несколько более сложен, однако есть ситуация, когда формулировка почти не меняется:

Лемма 4. *Пусть p — нечетное простое число, n — натуральное число и число c имеет вид p^n или $2p^n$. В таком случае условие $p \equiv 1 \pmod 4$ остается критерием представимости c в виде суммы двух квадратов. Кроме того, если условие $p \equiv 1 \pmod 4$ выполняется, то существует единственное собственное представление.*

2. Из леммы 4 сразу вытекает, что z-компонента (неприводимой) пифагоровой тройки тогда и только тогда принадлежит множеству $\mathbb{P}^\times$, когда для соответствующего простого p имеем $p \equiv 1 \pmod 4$. При этом в представлении $z = a^2+b^2$ по формуле (2) компоненты a и b однозначно определяются по z. Следовательно, однозначно определяются две другие компоненты тройки — числа x и y.

Сопоставляя это со сказанным выше, мы получаем, что *если в пифагоровой тройке какая-то из компонент — степень простого числа, то две другие компоненты однозначно определяются по этой компоненте.*

§3. Тройки с $\mathbb{P}^\times$-компонентами x, z

1. Число вида $2^m + 1$ с натуральным m может оказаться простым только в том случае, когда m не имеет нетривиальных нечетных делителей, т.е. $m = 2^n$, так что число имеет вид

$$f_n = 2^{2^n} + 1$$

(числа Ферма). Простые такого вида называются простыми Ферма. Согласно теореме Гаусса, простые Ферма играют центральную роль при описании случаев, когда правильный многоугольник может быть построен циркулем и линейкой.

При $n = 0, 1, 2, 3, 4$ числа f_n являются простыми, но число $f_5 = 2^{32} + 1$, как заметил Эйлер, делится на простое число 641 (дополнительный множитель также является простым числом). Не известно ни одного простого Ферма с $n > 4$, зато относительно многих чисел Ферма с $n \geqslant 5$ доказано, что они являются составными, в частности, это так, если $5 \leqslant n \leqslant 32$, и сейчас считается правдоподобным, что простых Ферма с $n \geqslant 5$ нет[3)].

[3)] С развитием вычислительной техники появляются новые сведения и о числах Ферма. Свежую информацию по этому поводу, разумеется, можно найти в Интернете, см., например, страницу, которую поддерживает Вильфрид Келлер (Wilfrid Keller) `http://www.prothsearch.net/fermat.html`

2. Простые Ферма естественно появляются при описании пифагоровых троек, указанных в заглавии данного параграфа. Нам будет удобно начать со следующей элементарной леммы.

Лемма 5. *Пусть k, l, m — натуральные числа. Если*

$$2^k + 1 = (2^l + 1)^m \tag{5}$$

и $m > 1$, то $k = 3$, $l = 1$ и $m = 2$.

Доказательство. Из условий (5) и $m > 1$ вытекает, что $k > m \cdot l \geqslant 2l$. Раскрывая правую часть в (5) по формуле бинома, мы получим, что

$$2^{k-l} = m + n \cdot 2^l,$$

где $n \in \mathbb{N}$. Отсюда следует, что $2^l \mid m$. В частности, m — четное число, так что $(2^l + 1)^m = t^2$, где $t \in \mathbb{N}$. По формуле (5), имеются такие $k_1, k_2 \in \mathbb{N}$, что

$$t - 1 = 2^{k_1},\ t + 1 = 2^{k_2} \ \text{ и } \ k_1 + k_2 = k.$$

Очевидно, что $2^{k_1 - 1}(2^{k_2 - k_1} - 1) = 1$, откуда вытекает, что $k = 3$ и доказательство легко завершается. □

Теорема 1. *В (неприводимой) пифагоровой тройке $\{x, y, z\}$ компоненты x и z тогда и только тогда обе принадлежат к $\mathbb{P}^\times$, когда z — простое Ферма, причем $z > 3$.*

Доказательство. Предположим сначала, что z — простое Ферма и $z > 3$. Тогда, в частности, $z = 2^{2l} + 1$, где $l \in \mathbb{N}$. По лемме 4, простое число z имеет в точности одно собственное представление в виде суммы квадратов. Поэтому в формулах (2) будет $a = 2^l$, $b = 1$, так что $x = 2^{l+1}$.

Докажем обратное утверждение. По условию, $z = p^m$, где p — простое число и m — натуральное. Мы должны убедиться, что p — простое Ферма и что $m = 1$.

В соответствии с леммой 1 имеем представление $x = 2^{k+1}$, $z = 2^{2k} + 1$ с некоторым натуральным k. Так как $(p - 1) \mid (p^m - 1)$, то $p = 2^l + 1$ с некоторым натуральным l, и это означает, что p — простое Ферма. Далее,

$$2^{2k} + 1 = z = (2^l + 1)^m.$$

Так как степень двойки слева четная, то из леммы 5 вытекает, что $m = 1$.□

Из сказанного выше следует, что в данный момент мы в состоянии предъявить только четыре тройки данного типа. Не исключено, что других таких троек нет (а если есть, то заведомо их компоненты — фантастически большие числа). Поэтому тройки последнего типа, которыми мы займемся ниже, имеют особенный интерес.

§4. Тройки с $\mathbb{P}^\times$-компонентами y, z

1. Так как в рассматриваемом случае $y \in \mathbb{P}^\times$, то, по лемме 2,

$$2z = 1 + y^2. \tag{6}$$

Легко видеть, что каждое целочисленное решение уравнения (6) имеет нечетные компоненты и что мы получим пифагорову тройку, добавляя к y, z число $x = z - 1$.

Таким образом, дело свелось к вопросу о разрешимости в степенях простых очень простого (с виду) уравнения (6). Хотя вопрос о разрешимости этого уравнения *в целых числах* тривиален, целочисленная разрешимость уравнения

$$2v^l = 1 + u^k, \tag{7}$$

в зависимости от выбора k, l уже́ представляет большой интерес. Для наших целей достаточно четных k и простых u, v, однако не лишено смысла попытаться рассмотреть более общую ситуацию.

Замечание. Уравнение (7) — частный случай *диофантова уравнения* вида $f(u, v) = 0$, где f — полином с целочисленными коэффициентами. Основная проблема относительно таких уравнений — это проблема конечности числа целочисленных решений[4)]. Проблема разрешимости, а также проблема поиска нетривиальных решений могут существенно различаться по сложности для внешне очень похожих уравнений. Многочисленные примеры на эту тему имеются, в частности, в популярной когда-то брошюре [9].

Первые существенные результаты на эту тему в общем случае получил в 1909 г. А. Туэ, а окончательное решение проблемы конечности для таких уравнений через 20 лет нашел К. Зигель. Отметим популярную статью [10], из которой среди прочего легко понять, как действовал Туэ. Формулировка теоремы Зигеля предполагает знакомство с целым рядом дополнительных понятий, и мы от нее воздержимся.

Вместе с тем, для (невырожденных) двучленных диофантовых уравнений $au^k + bv^l = c$, включающих уравнение (7), ответ на один из основных вопросов в принципе описывается очень просто: если $k, l \geqslant 2$, причем хотя бы одно из этих неравенств строгое, то множество решений конечно, тогда как в других случаях реализуются и сравнительно просто распознаются все три возможности (решений нет, множество решений конечно или бесконечно).

[4)] Сравнительно недавно была решена заметно более сложная проблема конечности числа *рациональных* решений. Отметим очень интересную (но далеко не элементарную) статью [8] на эту тему.

Однако, вообще говоря, поиск конструктивных априорных оценок решений и, тем более, поиск всех решений, как правило, даже в самых простых (по виду) случаях — сложная задача. Дополнительное условие простоты (компонент) решений может как упростить, так и усложнить задачу.

2. Теперь мы приступим непосредственно к вопросу о разрешимости в степенях простых уравнения (6). В конце концов мы убедимся, что в случае разрешимости степени простых далеко не произвольны. Вначале мы рассмотрим некоторые частные случаи уравнения (7).

В следующей лемме $k, l, u \in \mathbb{N}$ и $q \in \mathbb{P}$.

Лемма 6. *Предположим, что $q \geqslant 3$ и что k — нечетное число. Если $2q^l = 1 + u^k$, то $k = 1$.*

Доказательство. Допустим, что $k \geqslant 3$, и покажем, что это приводит к противоречию. Не ограничивая общности, мы можем (и будем) считать, что $k \in \mathbb{P}$.

Так как k — нечетное число, то $(u+1) \mid (u^k+1)$. Кроме того, u — нечетное число, причем $u > 1$. Поэтому $u = 2q^t - 1$, где $t \in \mathbb{N}$. Далее, $2q^l \geqslant 1 + u^3 > (1+u)^2$, откуда легко следует, что $l > 2t$.

Имеем

$$\begin{aligned} 2q^l &= 1 + (-1 + 2q^t)^k \\ &= k \cdot (2q^t) - \frac{k(k-1)}{2} \cdot (2q^t)^2 + \dots, \end{aligned}$$

так что

$$q^{l-t} = k - \frac{k(k-1)}{2} \cdot (2q^t) + \dots.$$

Из этой формулы сразу вытекает, что $q \mid k$. Так как k — простое число, то $k = q$. Заменяя в этой формуле k на q и вспоминая, что $l > 2t$, мы получаем противоречие: левая часть и все слагаемые справа, кроме первого, делятся на q^{t+1}. □

Замечание. В последней лемме снять предварительное условие $q \in \mathbb{P}$ нельзя. Действительно, при произвольном целом k уравнение $2v = 1 + u^k$ разрешимо в натуральных числах: в качестве u годится любое нечетное число. Например, $2 \cdot 14 = 1 + 3^3$. □

Из леммы 6, в частности, вытекает, что разрешимость уравнения (7) в простых u, v влечет за собой тот факт, что фигурирующий там показатель *k не имеет нетривиальных нечетных делителей*, т. е. это число представляется в виде 2^n с целым $n \geqslant 0$. Оказывается, аналогичный факт имеет место и в отношении показателя l.

Следующая лемма — это теорема Штёрмера (C. Störmer), установленная им еще в 1895 г. Признаюсь, что первоначально, еще не зная об этой теореме, я собирался поместить (не очень короткое) доказательство аналогичного утверждения, но с дополнительным условием простоты переменной v. Однако затем я нашел работу Лунгрена [11], в которой среди прочего содержатся далеко идущие обобщения этого факта и детальные ссылки на многие предшествующие работы[5)]. Кроме того, я вспомнил один тезис П. Халмоша и решил ему последовать[6)].

Лемма 7. *Пусть $l \geqslant 3$ — нечетное натуральное число. Тогда уравнение $2v^l = 1 + u^2$ не имеет натуральных решений $\{u, v\}$, для которых $v > 1$.*

3. Соединяя леммы 6 и 7, мы получаем ту информацию о степенях простых в пифагоровых тройках, о которой сказано во введении. Однако, если иметь в виду замечание на с. 112, то ясно, что в первую очередь имеет смысл более тщательно разобраться с проблемой разрешимости в натуральных числах $\{u, v\}$ двух конкретных уравнений:

$$2v^2 = 1 + u^4 \text{ и } 2v^4 = 1 + u^2.$$

Первое из этих уравнений существенно проще второго (причем проще и ответ на вопрос, и путь к нему).

Лемма 8. *Уравнение $2v^2 = 1 + u^4$ не имеет никаких натуральных решений, кроме тривиального $u = v = 1$.*

Доказательство. Положим $w = v^2 - 1$. Тогда w, u, v — неотрицательные целые числа, и выполняется равенство $w^2 + u^4 = v^4$. Вместе с тем, хорошо известно, что последнее уравнение не имеет натуральных решений (см., например, [14, с.81]). Поэтому $w = 0$. □

Следующая лемма, касающаяся второго уравнения — это теорема Лунгрена, доказанная им в 1942 г. Первоначальное доказательство было весьма сложным. Различные обобщения и подробные ссылки на предшествующие результаты можно найти в его статье [12]. Кстати, неоднократно предпринимались попытки найти простое и короткое доказательство, однако достигнутый прогресс лишь отчасти решает эту задачу.

[5)] Кстати, фотокопии журнала Mathematica Scandinavica, в котором содержится данная и ряд других работ Лунгрена, свободно доступны в Интернете.

[6)] В своем хорошо известном (специалистам) задачнике по гильбертовым пространствам (с. 68 русского перевода) он пишет в связи со спектральной теоремой: «Мощные общие теоремы затем и существуют, чтобы их использовали, и упрямое пренебрежение ими приводит к потере понимания по меньшей мере так же часто, как и к достижению его.» Другое дело, что, используя такое средство, полезно узнать, откуда оно взялось, т. е. в какой-то момент проверить доказательство или придумать новое.

Лемма 9. *Уравнение* $2v^4 = 1+u^2$, *кроме тривиального, имеет в точности одно решение:* $u = 239, v = 13$.

Из сказанного выше вытекает следующая теорема, которая в качестве следствия дает (общее, но не полное) описание степеней простых, которые могут появляться в пифагоровой тройке в качестве y и z.

Теорема 2. *При натуральных* $k \geqslant 2$ *и* l *уравнение* $2q^l = 1 + u^k$ *относительно* $3 \leqslant q \in \mathbb{P}$ *и* $u \in \mathbb{N}$ *может иметь решения только в следующих случаях*: $l = 4$, $k = 2$; $l = 2$, $k = 2$; $l = 1$, $k = 2^n$ *с натуральным* n.

По поводу теоремы 2 имеет смысл сделать несколько замечаний. Во-первых, при $l = 4$, $k = 2$ в соответствии с леммой 9 (т. е. теоремой Лунгрена) имеется в точности одно решение $q = 13$, $u = 239$, даже без предварительного предположения $q \in \mathbb{P}$. Тот факт, что в теореме Лунгрена обе компоненты оказались простыми числами можно, по-моему, отнести к разряду чудес, и это действительно делает пифагорову тройку с $y = 239$, $z = 13^4$ по-своему исключительной.

Во-вторых, в §5 мы предъявим (хорошо известный) алгоритм, позволяющий выписывать по возрастанию компоненты *всех* натуральных решений уравнения $2v^2 = 1+u^2$. Среди этих пар встречаются пары простых (и это помогает составить короткую из таблиц, указанных во введении), однако не известно, конечно или нет множество таких пар (см. по этому поводу, например, [13, с.83]; этот популярный источник заметно устарел, но проблема, по-моему, остается). Кстати, на этом пути довольно быстро появляется пара Лунгрена.

Наконец, третий случай в теореме 2 приводит к поиску таких простых нечетных p и неотрицательных целых n, что $(p^{2^n} + 1)/2$ — снова простое, и это напоминает классическую проблему о простых Ферма. Некоторые из таких чисел для $n = 1$ собраны в верхней строке первой из таблиц во введении. Кроме того, есть и «большие» пары, например, $y = 3^8$, $z = (3^{16} + 1)/2$ (также упомянутая во введении). Однако, хотя по сравнению с проблемой о простых Ферма возможности вроде бы расширяются (можно менять не только n, но и p), я не знаю, бесконечно ли это множество.

§5. Комментарии и вычисления

1. Нам осталось более детально прокомментировать второй и третий случаи в теореме 2. В этом пункте мы разберем второй случай, т. е. уравнение

$$u^2 - 2v^2 = -1. \tag{8}$$

Наряду с уравнением (8) имеет смысл рассматривать так называемое *уравнение Пелля*[7)]

$$u^2 - 2v^2 = 1. \tag{9}$$

Существует несколько подходов к описанию множества всех решений диофантовых уравнений (8) и (9), и мы вкратце опишем некоторые из них (детали можно найти в учебниках, перечисленных в списке литературы; там же указаны некоторые дополнительные источники).

Обозначим через $\mathbb{Q}(\sqrt{2})$ поле, которое получается в результате присоединения к полю $\mathbb{Q}$ числа $\sqrt{2}$. Таким образом, каждый элемент $\lambda \in \mathbb{Q}(\sqrt{2})$ однозначно представляется в виде $\lambda = \alpha + \beta\sqrt{2}$, где $\alpha, \beta \in \mathbb{Q}$. В частности, $\mathbb{Q}(\sqrt{2})$ естественно наделяется структурой двумерного векторного пространства над полем $\mathbb{Q}$ с базисом $\{1, \sqrt{2}\}$.

Каждому элементу $\lambda = \alpha + \beta\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ сопоставим $\mathbb{Q}$-линейный оператор T_λ умножения на λ. Заметим, что в базисе $\{1, \sqrt{2}\}$ оператору T_λ отвечает матрица

$$\begin{pmatrix} \alpha & 2\beta \\ \beta & \alpha \end{pmatrix}$$

с детерминантом $\det(T_\lambda) = \alpha^2 - 2\beta^2$. В (алгебраической) теории чисел это рациональное число часто называют *нормой* числа λ и обозначают $\|\lambda\|$. Мы будем использовать промежуточное обозначение. Именно, имея в виду, что соответствие $\lambda \to T_\lambda$ — изоморфизм полей, мы будем писать $\det(\lambda)$ вместо $\det(T_\lambda)$. Одно из основных свойств детерминанта влечет за собой соотношение

$$\det(\lambda_1 \cdot \lambda_2) = \det(\lambda_1) \cdot \det(\lambda_2),$$

справедливое для каждой пары чисел $\lambda_1, \lambda_2 \in \mathbb{Q}(\sqrt{2})$.

Обозначим через $\mathbb{Z}(\sqrt{2})$ совокупность всех тех $\lambda = \alpha + \beta\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, для которых $\alpha, \beta \in \mathbb{Z}$. Очевидно, что $\mathbb{Z}(\sqrt{2})$ составляет подкольцо в $\mathbb{Q}(\sqrt{2})$.

Если $\lambda \in \mathbb{Z}(\sqrt{2})$, то $\det(\lambda) \in \mathbb{Z}$. Так как $\det(1) = 1$, то для обратимых (относительно умножения) элементов $\lambda \in \mathbb{Z}(\sqrt{2})$ число $\det(\lambda)$ будет обратимым элементом кольца $\mathbb{Z}$, так что в этом случае $\det(\lambda) = \pm 1$. Правило составления обратной матрицы показывает, что обратное тоже верно: если $\lambda \in \mathbb{Z}(\sqrt{2})$ и $\det(\lambda) = \pm 1$, то λ — обратимый элемент кольца $\mathbb{Z}(\sqrt{2})$.

Так как $\det(\alpha+\beta\sqrt{2}) = \alpha^2-2\beta^2$, то описание решений уравнения Пелля равносильно описанию группы тех обратимых элементов $\lambda \in \mathbb{Z}(\sqrt{2})$, для которых $\det(\lambda) = 1$. Особенно просто выглядит описание тех обратимых

[7)] Это уравнение точнее было бы называть уравнением Эйлера, уравнением Ферма или даже (в соответствии с легендой) уравнением Архимеда. Однако Эйлер в своих исследованиях назвал его по имени английского математика, который как раз этим уравнением никогда не занимался, и традиция называть уравнение (9) уравнением Пелля нарушается не часто. Напротив, иногда уравнением Пелля называют и уравнение (8).

$\lambda = \alpha + \beta\sqrt{2}$, для которых $\alpha, \beta > 0$. Оказывается, что среди них имеется $\lambda_1 = \alpha_1 + \beta_1\sqrt{2}$ с наименьшим значением $\alpha + \beta\sqrt{2}$, и все остальные (вместе с этим в качестве первого члена) составляют последовательность, которая формируется по правилу

$$\alpha_n + \beta_n\sqrt{2} = (\alpha_1 + \beta_1\sqrt{2})^n, \;\; n = 1, 2, 3, \ldots .$$

Легко убедиться, что $\alpha_1 = 3, \beta_1 = 2$. Детальное (причем вполне элементарное) обсуждение этого факта можно найти, например, в [3, с. 340].

Пара $\{1, 1\}$ служит (минимальным) положительным решением уравнения (8). Это эквивалентно тому, что $\det(\mu_1) = -1$, где $\mu_1 = 1 + \sqrt{2}$. Заметим, что $\mu_1^2 = \lambda_1$. Все остальные натуральные решения уравнения (8) получаются из $\mu_1 \cdot \lambda_1^n = \mu_1^{2n+1}$, где $n \in \mathbb{N}$.

Замечание. Аналогично можно размножать решения уравнения $u^2 - 2v^2 = m$ с $m \in \mathbb{Z}$. Однако у такого уравнения натуральные решения существуют не при каждом m. Например, при $m = 2$, как легко видеть, решения есть, тогда как при $m = 3$ решений нет. □

Детальное изучение таких уравнений — предмет академической науки, с которым можно познакомиться по первым главам монографии [15], однако без предварительной алгебраической подготовки сознательное чтение этой монографии практически невозможно.

Еще один способ найти натуральные решения уравнений (8) и (9) дает разложение числа $\sqrt{2}$ в цепную дробь. Прочесть о цепных дробях можно во всех учебниках, включенных в список литературы. Более подробную информацию можно найти, например, в [16] и [17].

Если не прибегать к оборотам вроде «выражение вида» (фактически превращающих вводимое понятие в первичное), первая сложность появляется, когда возникает желание дать корректное определение (бесконечной) цепной дроби[8)]. Мы не будем давать общего определения, но поясним всё на примере упомянутого выше разложения.

Ясно, что

$$\sqrt{2} = 1 + \frac{1}{1+\sqrt{2}} = 1 + \frac{1}{2 + \dfrac{1}{1+\sqrt{2}}} = 1 + \frac{1}{2 + \dfrac{1}{2 + \dfrac{1}{1+\sqrt{2}}}} \tag{10}$$

и т. д. Вычеркивая в заключенных между знаками равенства выражениях

[8)] Кстати, ситуация здесь практически не отличается от той, которая имеет место, когда начинают рассматривать, например, бесконечные ряды. Довольно часто, особенно в тех вузах, где математика имеет как бы вспомогательный характер (не говоря уже́ о школе) определение ряда фактически не дается. Быть может, как раз в таких случаях этот вульгаризм («выражение вида») можно считать оправданным, однако тогда не стоит удивляться, почему именно *хорошие* студенты долго привыкают к рядам. Кстати, подобно рядам, цепные дроби можно «составлять» не только из чисел.

последнее $1/(1+\sqrt{2})$, мы получим последовательность «многоэтажных» дробей, которые в результате естественного приведения (не надо, например, в самом начале заменять $1/2$ на $3/6$) превращается в последовательность несократимых дробей

$$1 = 1/1,\ 3/2,\ 7/5,\ 17/12, \ldots.$$

Члены этой последовательности очень хорошо (с разных сторон) приближаются к $\sqrt{2}$ и называются *подходящими дробями* цепной дроби. Между элементами (числителями и знаменателями) подходящих дробей имеются простые рекуррентные соотношения (ниже они указаны). Это позволяет в данном случае бесконечную цепную дробь понимать как *последовательность всех ее подходящих дробей,* и на этом пути можно корректно ввести и общее понятие. Тот факт, что построенная цепная дробь представляет число $\sqrt{2}$ теперь можно (красиво) записать в виде

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ldots}}}$$

Положим дополнительно $u_0 = 1, v_0 = 0$ и обозначим через u_n и v_n при натуральных n соответственно последовательность числителей и знаменателей подходящих дробей.

Оказывается, при четных n пары $\{u_n, v_n\}$ будут давать (указанную выше) последовательность решений уравнения Пелля, а при нечетных — уравнения (8).

Рекуррентные соотношения между элементами пар можно записывать по-разному, в частности, так:

$$\begin{cases} v_{n+1} = u_n + v_n, \\ u_{n+1} = v_n + v_{n+1}. \end{cases}$$

Так как $u_0 = 1, v_0 = 0, u_1 = 1, v_1 = 1$, то мы без хлопот можем найти и рассмотреть первый десяток пар (так как обе последовательности экспоненциально возрастают, то затем возникают большие числа),

n	0	1	2	3	4	5	6	7	8	9
u_n	1	1	3	7	17	41	99	239	577	1393
v_n	0	1	2	5	12	29	70	169	408	985

Так как при четных n числа v_n четные, то легко убедиться, что, кроме $\{3, 2\}$, уравнение Пелля не имеет решений, v-компонента которых — степень простого.

С другой стороны, даже из приведенной краткой таблицы видно, что уравнение (8) вначале имеет решения, обе компоненты которых — простые

числа. Вместе с тем, бесконечно ли множество таких решений, кажется, никто не знает.

Пара Лунгрена — это $\{u_7, v_7\}$. Используя теорему Лунгрена (лемма 9) и простые соображения типа леммы 8, легко убедиться, что за исключением чисел 0 и 1 в самом начале строк $\{u_n\}$ и $\{v_n\}$ *в этих строках, кроме* $v_7 = 13^2$*, нет других квадратов.* При нечетных n это уже установлено. Поэтому остается проверить, что уравнения

$$x^4 - 2y^2 = 1 \text{ и } x^2 - 2y^4 = 1$$

не имеют натуральных решений. Эта проверка не требует особой фантазии, и мы ее опустим, тем более, что этот факт имеет лишь косвенное отношение к нашей теме. Заметим только, что в конечном счете второе уравнение сводится к первому.

2. Нам осталось обсудить последнюю возможность из указанных в теореме 2. В этом пункте мы сформулируем некоторые общие определения и результаты и приведем основанные на них примеры. Затем мы приведем дальнейшие примеры, требующие «нечеловеческих» вычислений. Кстати, каждый, кто имеет доступ к продвинутой вычислительной технике, сможет расширить список таких примеров.

Пусть $a, b \in \mathbb{N}$, причем $\gcd(a, b) = 1$. Рассмотрим арифметическую прогрессию $A \stackrel{\text{def}}{=} \{ak + b \mid k \in \mathbb{N}\}$. При $t > 0$ обозначим через $\pi_A(t)$ количество простых чисел $p < t$, попадающих в арифметическую прогрессию A.

Классическая теорема Дирихле устанавливает, что $\pi_A(t) \to \infty$ при $t \to \infty$. Другими словами, прогрессия A содержит бесконечное множество простых. Представление о том, как рассуждал Дирихле, можно получить по очень красивому (простому, но не элементарному) описанию этой темы в [18].

В дальнейшем теорема Дирихле уточнялась и обобщалась. Эти уточнения и обобщения опирались на изучение так называемой ζ-функции Римана как аналитической функции в комплексной плоскости[9)].

Здесь (и в дальнейшем) нам потребуется функция Эйлера $\varphi = \varphi(n)$ натурального аргумента, значение которой равно количеству таких m, где $1 \leqslant m \leqslant n$, что $\gcd(m, n) = 1$. По определению, $\varphi(1) = 1$. Легко показать,

[9)] ζ-функцию как функцию вещественного переменного знал Эйлер, а Дирихле использовал в своем доказательстве теоремы об арифметической прогрессии. Заслуга Римана в данном случае в том, что он первым начал изучать ζ-функцию как аналитическую функцию комплексного переменного, поняв среди прочего значение ее поведения в комплексной плоскости для точного описания распределения простых чисел. Заметим, кстати, что Риман слушал лекции Дирихле и что в своем единственном мемуаре по теории чисел он ссылается на Гаусса и Дирихле, но почему-то не ссылается на П. Л. Чебышева (с написанными по-французски работами которого он мог быть знаком) и на Мёбиуса.

что $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ и что $\varphi(xy) = \varphi(x)\varphi(y)$, если $\gcd(x,y) = 1$, и это позволяет легко находить значения φ при небольших значениях аргумента. С алгебраической точки зрения, $\varphi(n)$ — это количество обратимых (по умножению) элементов кольца $\mathbb{Z}/(n)$ классов вычетов по модулю n.

Указанные обобщения описаны, например, в [19]. Результат состоит в том, что имеет место эквивалентность:

$$\pi_A(t) \sim \frac{1}{\varphi(a)} \cdot \frac{t}{\log t},$$

где $\log t$ обозначает натуральный логарифм.

При $n \in \mathbb{N}$ и $3 \leqslant p \in \mathbb{P}$ положим

$$g_p^n \stackrel{\text{def}}{=} (p^{2^n} + 1)/2.$$

Удобно представлять себе $G = \{g_p^n\}$ как бесконечную вправо и вверх матрицу, *столбцы* C_p которой занумерованы простыми числами и идут снизу вверх, а *строки* S_n — натуральными и идут слева направо.

С точки зрения нашей исходной проблемы наибольший интерес представляет вопрос о бесконечности подмножества простых среди элементов матрицы G. Ответа на этот вопрос я не знаю. По аналогии с числами Ферма представляет интерес не только специальный вопрос о бесконечности подмножества простых в столбцах C_p, но и вопрос о бесконечности подмножества составных в них. Некоторая (довольно скудная) информация по этому поводу имеется (и приводится немного ниже). Следующий пример показывает, что, применяя теорему Дирихле, на остающийся (самый неинтересный) вопрос о составных в строках матрицы G легко дать положительный ответ.

Пример. Пусть b — четное положительное число, $m \in \mathbb{N}$ и $a = 1 + b^m$. Рассмотрим прогрессию $A = \{ak + b \mid k = 1, 2, \ldots\}$. Так как $\gcd(a,b) = 1$, то, по теореме Дирихле, A содержит бесконечное подмножество простых. Далее, если $q = ak + b$, то $q^m \equiv b^m \equiv -1 \pmod{a}$, т.е. $a \mid (q^m + 1)$. Так как $a > 2$ то, в частности (при $m = 2^n$) получается, что *каждая строка* S_n *матрицы* G *содержит бесконечное подмножество составных чисел.* □

В обзоре [20] автор отмечает, что еще в 1877 г. Пепэн (T. Pepin) установил, что число Ферма $f > 3$ тогда и только тогда является простым, когда

$$3^{(f-1)/2} \equiv -1 \pmod{f}.$$

Доказательство этого факта дано, например, в [6, с.47].

Если $f = 2^m + 1$, то $(f-1)/2 = 2^{m-1}$. Поэтому из теоремы Пепэна сразу вытекает следующее сравнительно содержательное утверждение: множество $F \cup C_3$, где F — множество чисел Ферма, содержит бесконечное подмножество составных чисел.

На самом деле число 3 в теореме Пепэна, а потому и в последнем утверждении легко заменить многими другими (см. ниже).

Пусть $m \geqslant 2$ — натуральное число. Следующая теорема (см., например, [6, с.16]) при $m \in \mathbb{P}$ была найдена Ферма (Малая теорема Ферма), а в общем случае — Эйлером. Именно, если $\gcd(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod{m}$. Легко привести примеры, когда $a^k \equiv 1 \pmod{m}$ для $k < \varphi(m)$. Если d — наименьшее натуральное k с этим свойством, то говорят, что a принадлежит показателю d по модулю m. Легко убедиться, что $d \mid k$ для всех остальных k с указанным свойством. В частности, $d \mid \varphi(m)$.

Теперь мы приведем обобщение теоремы Пепэна. В отличие от исходного случая удобно вместо критерия дать два простых утверждения, с формальной точки зрения различающихся по степени общности. Вместе с тем, мы почти не отступаем от доказательства, приведенного в [6].

Лемма 10. *Пусть $f \geqslant 3$ — число Ферма. Если при некотором $a \in \mathbb{Z}$ выполняется сравнение*

$$a^{(f-1)/2} \equiv -1 \pmod{f}, \tag{11}$$

то f — простое число.

Доказательство. Пусть q — простой делитель числа f. Мы должны убедиться, что $q = f$. Неравенство $q \leqslant f$ очевидно.

Из сравнения (11) вытекает, что аналогичное сравнение выполняется при замене модуля f на q (с сохранением самого сравнения), так как $q \mid f$.

Пусть $f = 2^m + 1$ и пусть d — показатель, которому принадлежит a по модулю q. Тогда $d \mid 2^m$, поскольку

$$a^{f-1} \equiv 1 \pmod{q},$$

так что $d = 2^\mu$ с некоторым $\mu \in \mathbb{N}$, причем $\mu \leqslant m$. Вместе с тем из (11) вытекает, что

$$a^{(f-1)/2} \equiv -1 \pmod{q},$$

так что $d > (f-1)/2$. Поэтому $\mu > m-1$. Следовательно, $\mu = m$ и $d = f-1$. Но тогда $(f-1) \mid (q-1)$, так как $\varphi(q) = q-1$. Следовательно, $f \leqslant q$. □

Для справедливости обратного (к лемме 10) утверждения относительно a придется сделать некоторое дополнительное (по существу, формальное) предположение.

Пусть $3 \leqslant p \in \mathbb{P}$. Тогда $\mathbb{Z}/(p)$ — конечное поле, так что группа его обратимых элементов — циклическая группа порядка $p-1$. Классическая формулировка (существование первообразного корня) и доказательство этого факта имеется, например, в [5, с.95], в приведенной здесь форме теорема доказана, например, в [21, с.12] (кстати, доказательство становится существенно более прозрачным, если считать известными основные свойства

φ-функции Эйлера). Количество элементов, которые могут служить образующими в циклической группе обратимых элементов поля $\mathbb{Z}/(p)$ равно $\varphi(p-1)$. В частности, если f — простое Ферма, то получается, что образующими могут служить $(f-1)/2$ элемента.

Пусть $\lambda = \lambda_p$ — нетривиальный гомоморфизм (мультипликативной) группы обратимых элементов поля $\mathbb{Z}/(p)$ в мультипликативную группу $\{\pm 1\}$ и пусть g — (какая-нибудь) образующая исходной группы. Тогда $\lambda_p(g) = -1$, так как в противном случае гомоморфизм будет тривиальным. Поэтому $\lambda_p(g^k) = (-1)^k$. Обычно продолжают λ_p на всё поле $\mathbb{Z}/(p)$, полагая $\lambda_p(0) = 0$. Результат сквозного гомоморфизма $\mathbb{Z} \to \mathbb{Z}/(p) \to \{-1, 0, 1\}$ (это числовая полугруппа по умножению) называется символом Лежандра и имеет классическое обозначение, похожее на обозначение биномиального коэффициента,

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } p \nmid a \text{ и сравнение } x^2 \equiv a \pmod p \text{ имеет решение,} \\ 0, & \text{если } p \mid a, \\ -1, & \text{если сравнение } x^2 \equiv a \pmod p \text{ не имеет решения.} \end{cases}$$

Довольно часто удобнее использовать для символа Лежандра обозначение «в строчку»: (a/p). Среди чисел a, для которых $1 \leqslant a < p$, в точности половина, т. е. $(p-1)/2$ удовлетворяют условию $(a/p) = 1$ (квадратичные вычеты). Отсюда следует, что для простых Ферма f равенство $(a/f) = -1$ выполняется тогда и только тогда, когда a служит образующей в группе обратимых элементов. Число 3 годится для всех простых Ферма (и с этим связана теорема Пепэна). При $f = 5$ появляется еще $a = 2$, а при $f = 17$ возникает множество

$$\{3, 5, 6, 7, 10, 11, 12, 14\}. \tag{12}$$

Вычислять значение символа Лежандра, исходя только из приведенного определения, — унылое занятие. Однако во всех учебниках теории чисел описаны различные способы для сравнительно небольших p и a сделать это довольно быстро (надо ввести символ Якоби и применять квадратичный закон взаимности — один из самых красивых фактов элементарной теории чисел).

Следующий факт (доказательство которого также есть во всех учебниках) был предсказан Лежандром и строго доказан Эйлером: при простом $p \geqslant 3$

$$a^{(p-1)/2} \equiv (a/p) \pmod p.$$

Из сказанного сразу вытекает следующая лемма, включающая вторую часть теоремы Пепэна.

Лемма 11. *Если f — простое Ферма и $(a/f) = -1$, то*

$$a^{(f-1)/2} \equiv -1 \pmod{f}.$$

Пример. Данный пример представляет собой частную, но более деликатную версию примера со с. 120. Рассмотрим арифметическую прогрессию, члены которой имеют вид $q = 17k + l$, где $k = 0, 1, 2, \ldots$, а l — какой-нибудь элемент строки (12). По теореме Эйлера, $17 \mid (q^8 + 1)$ для всех таких b. По теореме Дирихле, при каждом фиксированном l среди них встречается бесконечное подмножество простых, и для всех таких простых число $(q^8 + 1)/2$ составное. Минимальное простое, которое не попадает в эту категорию — число 13 (т.е. $13^8 + 1$ не делится на 17; более того, оказывается, что число $(13^8 + 1)/2$ простое.). □

Отмечу, что ряд других фактов, известных для чисел Ферма, с небольшими модификациями или почти дословно переносится на числа g_p^n.

Делитель 641 для числа $2^{32} + 1$ Эйлер получил не «в слепую»: сначала он доказал, что каждый простой делитель числа f_n имеет вид $k \cdot 2^{n+2} + 1$ (по поводу доказательства см., например, [6, с.47]). Делитель 641 появляется при $k = 5$.

Аналогичное утверждение *сохраняется* (вместе с доказательством) *при переходе к числам g_p^n, однако в выражении для делителя $n+2$ следует поменять на $n + 1$.* Кстати, как в этом утверждении, так и в упомянутой теореме Эйлера, предположение о простоте делителя, как легко видеть, не существенно.

Далее, как и в случае чисел Ферма, числа, *стоящие в столбцах матрицы G попарно взаимно просты.* Снова доказательство, приведенное в [6, с.47–48]), сохраняется. Конечно, в отношении строк матрицы G это не верно.

3. Теперь я приведу результаты вычислений, проделанных практически «голыми руками», т. е. с использованием калькулятора. Они собраны в таблицу 1, которая аналогична начальному участку указанной выше матрицы G, однако в левом столбце вместо чисел n стоят $m = 2^n$, а вместо самих элементов g_p^n — та информация о простоте, которая у меня появилась. Буква p символизирует простоту соответствующего элемента, c — ее отсутствие, а крестик $\times$ означает, что проверить простоту соответствующего числа на калькуляторе не удалось.

В частности, неоднократно упомянутое число $(3^{16} + 1)/2$ простое. Для заполнения нижней строки и левой половины следующей за ней не требуется даже калькулятора. Кроме того, имеется еще 6 клеток таблицы, которым отвечают числа с делителем 17. Действительно, $19^4 \equiv -1 \pmod{17}$, а строчка (12) показывает, что $a^8 \equiv -1 \pmod{17}$ при $a = 3, 5, 7, 11$ и 23

Табл. 1.

16	p	c	×	×	×	×	×	×
8	c	c	c	c	p	c	c	c
4	p	p	p	p	p	p	c	p
2	p	p	c	p	c	c	p	c
	3	5	7	11	13	17	19	23

(ибо $23 = 6 + 17$). В последнем случае имеем

$$23^8 + 1 = 78\,310\,985\,282 = 2 \cdot 17 \cdot 3697 \cdot 623009.$$

М. Н. Вялый, используя программу Maple, заметно расширил эту таблицу. В таблице 2 собрана часть результатов этих вычислений. В левом столбце указан показатель степени $m = 2, 4, 8, \ldots$, а в строках — те простые $p < 100$, для которых $(p^m + 1)/2$ — также простое.

Табл. 2.

64	3										
32	3										
16	3	29	41	73							
8	13	43	47	53							
4	3	5	7	11	13	17	23	29	61	71	73
2	3	5	11	19	29	59	61	71	79		

Заинтересованный читатель сможет повторить эти вычисления (это не лишено смысла). Использование таких программ, как Maple, Mathematica, PARI и им подобных позволит значительно расширить и эту таблицу. Такое расширение имеет не только спортивный интерес, оно позволит сформулировать правдоподобные гипотезы, от чего пока, вероятно, стоит воздержаться.

Список литературы

[1] Хинчин А.Я. *Великая теорема Ферма.* М.–Л., ОНТИ ГТТИ, 1934.

[2] Горин Е.А. *Пифагоровы тройки, включающие степени простых.* Тезисы 4-й межд. конф. «Совр. проблемы теории чисел и ее прил.», Тула, 10–15 сент. 2001 г., с. 47–48.

[3] Айерленд К., Роузен М. *Классическое введение в современную теорию чисел.* М., Мир, 1987 (пер. с англ.).

[4] Бухштаб А.А. *Теория чисел.* М., Просвещение, 1966.

[5] Виноградов И.М. *Основы теории чисел.* М., Гостехиздат, 1953.

[6] Трост Э. *Простые числа.* М., Физматгиз, 1959 (пер. с нем.).

[7] Чандрасекхаран К. *Введение в аналитическую теорию чисел.* М., Мир, 1974 (пер. с англ.).

[8] McMullen C.T. *From dynamics on surfaces to rational points on curves.* Bull. of the Am. Math.Soc., 2000. Vol. 37, no 2. P. 119–140.

[9] Серпинский В. *О решении уравнений в целых числах.* М., Физматгиз, 1961 (пер. с польского).

[10] Гельфонд А.О. *О проблеме приближения алгебраических чисел рациональными.* Мат. просвещение, сер. 2, вып.2, (1957), с. 35–50.

[11] Ljunggren W. *On the Diophantine equation* $Cx^2 + D = 2y^n$. Math. Scand., 1966. Vol. 18. P. 69–86.
См. также `http://www.mscand.dk/article.php?id=1772`

[12] Ljunggren W. *On the Diophantine equation* $Ax^4 - By^2 = C$ $(C = 1, 4)$. Math. Scand., 1967. Vol. 21. P. 149–158.
См. также `http://www.mscand.dk/article.php?id=1845`

[13] Серпинский В. *Что мы знаем и чего не знаем о простых числах.* М.–Л., Физматгиз, 1963 (пер. с польского).

[14] Степанова Л.Л. *Избранные главы элементарной теории чисел.* М., Прометей, 2001.

[15] Боревич З.И., Шафаревич И.Р. *Теория чисел.* М., Наука, 1972.

[16] Хинчин А.Я. *Цепные дроби.* М.–Л., Гостехиздат, 1949.

[17] Ленг С. *Введение в теорию диофантовых приближений.* М., Мир, 1970 (пер. с англ.).

[18] Дэвенпорт Г. *Мультипликативная теория чисел.* М., Наука, 1971 (пер. с англ.).

[19] Гельфонд А.О. *Аналитический метод оценки числа простых чисел в натуральном ряде и арифметической прогрессии.* (Приложение редактора перевода к книге [6]).

[20] Рибенбойм П. *Рекорды простых чисел.* Успехи мат.наук, 1987. Т. 42, вып. 5. С. 119–176 (сокр. пер. с англ.).

[21] Серр Ж.–П. *Курс арифметики.* М., Мир, 1972 (пер. с фр.).

Горин Евгений Алексеевич, проф. кафедры мат. анализа МПГУ.
e-mail: `evgeny.gorin@mtu-net.ru`

Издательство МЦНМО

Р. Л. Добрушин. **Избранные работы по математической физике.** Под ред. Р. А. Минлоса, Ю. М. Сухова и С. Б. Шлосмана. 2007. 720 с.

Сборник содержит избранные статьи Роланда Львовича Добрушина (1929–1995) — выдающегося математика, одного из создателей современной математической статистической физики. Эти статьи были опубликованы в основном в зарубежных журналах, которые в настоящее время малодоступны современному читателю. Сборник дополнен комментариями, в которых прослеживается современное развитие идей, изложенных в публикуемых работах.

М. А. Акивис, Б. А. Розенфельд. **Эли Картан (1869–1951).** 2007. 328 с.

Книга посвящена описанию жизни и творчества великого французского математика Эли Картана, работы которого оказали огромное влияние на развитие математики в XX веке.

Р. Э. Клима, Дж. К. Ходж. **Математика выборов.** 2007. 224 с.

Вопрос о том, являются ли те или иные выборы демократичными, соответствуют ли результаты выборов воле народа, имеет много разных аспектов. В книге американских преподавателей Дж. К. Ходжа и Р. Э. Клима в научной форме, живо и наглядно обсуждаются проблемы математической теории выборов и референдумов.

Книга написана в форме учебника и рассчитана прежде всего на студентов. Для ее понимания вполне достаточно школьных знаний по математике. Книга предназначена для политологов, социологов и юристов.

Всероссийские олимпиады школьников по математике 1993–2006: Окружной и финальный этапы. Под ред. Н.Х.Агаханова. 2007. 472 с.

В книге приведены задачи заключительных (четвертого и пятого) этапов Всероссийских математических олимпиад школьников 1993–2006 годов с ответами и полными решениями.

Все приведенные задачи являются авторскими. Многие из них одновременно красивы и трудны, что отражает признанный в мире высокий уровень российской олимпиадной школы. Часть задач уже стала олимпиадной классикой.

Книга предназначена для подготовки к математическим соревнованиям высокого уровня. Она будет интересна педагогам, руководителям кружков и факультативов, школьникам старших классов. Для удобства работы приведен тематический рубрикатор.

Московские математические регаты. Сост. А. Д. Блинков, Е. С. Горская, В. М. Гуровиц. 2007. 360 с.

Математическая регата — ежегодное соревнование для школьных команд, В данном сборнике представлены материалы всех московских математических регат по 2005–06 уч. год. Приведены также правила проведения регаты, описана технология ее проведения и особенности подготовки. В приложение включены материалы школьных математических регат и регат, проведенных на всероссийских фестивалях.

Книжка адресована учителям средней школы, методистам, школьникам и может быть интересна всем любителям математики.

Геометрические олимпиады им. И. Ф. Шарыгина. Сост. А. А. Заславский, В. Ю. Протасов, Д. И. Шарыгин. 2007. 152 с.

В книге собраны задачи геометрических олимпиад им. И. Ф. Шарыгина (2005–2007) с подробными решениями. В приложении приведены две статьи И. Ф. Шарыгина и воспоминания о нем.

Пособие предназначено для школьников, учителей математики и руководителей кружков. Книга будет интересна всем любителям красивых геометрических задач.

В поисках утраченной алгебры: в направлении Гаусса* (подборка задач)

П. Ю. Козлов А. Б. Скопенков†

Listeners are prepared to accept unstated (but hinted) generalizations much more than they are able... to decode a precisely stated abstraction and to re-invent the special cases that motivated it in the first place.

P. Halmos, How to talk mathematics

Введение

Теорема Гаусса. [1] *Калькулятор (вычисляющий числа с абсолютной точностью) имеет кнопки*

$$1, \quad +, \quad -, \quad \times, \quad : \quad \text{и} \quad \sqrt{}$$

(и неограниченную память). На этом калькуляторе можно вычислить число $\cos\frac{2\pi}{n}$ *тогда и только тогда, когда* $n = 2^\alpha p_1 \cdot \ldots \cdot p_l$, *где* $p_1, \ldots, p_l$ — *различные простые числа вида* $2^{2^s}+1$.

*Полный обновляемый текст находится по адресу: `www.mccme.ru/circles/oim/materials/construc.pdf`

†Частично поддержан Российским Фондом Фундаментальных Исследований, Гранты номер 05-01-00993, 07-01-00648a и 06-01-72551-NCNILa, Грантами Президента РФ НШ-4578.2006.1 и МД-4729.2007.1, а также стипендией П. Делиня, основанной на его Премии Бальзана 2004 года.

[1] Переформулировка теоремы Гаусса в терминах построимости циркулем и линейкой правильных многоугольников приводится ниже (см. отступление) и не используется в остальном тексте. История этой знаменитой теоремы приводится в [6]. Строго говоря, теорема Гаусса не дает настоящего решения проблемы построимости правильных многоугольников, поскольку неизвестно, какие числа вида $2^{2^s}+1$ являются простыми. Однако теорема Гаусса дает, например, полиномиальный алгоритм выяснения построимости правильного n-угольника (n задано десятичной записью).

В этой заметке предлагается набросок *элементарного доказательства приведенной теоремы*. Оно не использует терминов «группа Галуа» (даже понятия «группа») и «поле» (доказательство невозможности использует квадратичные расширения только *множества рациональных чисел*). Несмотря на отсутствие этих *терминов*, *идеи* приводимых доказательств являются *отправными* для теории Галуа,[2)] которая (вместе с теорией групп) появилась в опыте *группировки* корней многочлена, с помощью которой их можно выразить через радикалы.[3)]

Нам кажется, что именно с *новых идей*, а не с *немотивированных определений*, полезно *начинать* изучение любой теории. Как правило, такие идеи наиболее ярко выражаются доказательствами, подобными приведенным здесь. Более подробно это обсуждается в философском отступлении, которое содержится в полном тексте заметки (см. примечание к заглавию статьи).

Приводимые доказательства *известны в математическом фольклоре*, однако авторам не удалось найти их в явном виде в литературе (кроме второго доказательства невозможности в теореме Гаусса [3]).

Элементарное доказательство *возможности* для $n = 17$ приводится в [6,9,13,15,16]. Для общего случая оно намечено в [4,6], где ясности доказательства немного мешает построение общей теории вместо доказательства конкретного результата.[4)]

Невозможность в теореме Гаусса не доказана явно в [4]. Однако первое доказательство невозможности в настоящей заметке (серия D) основано на идеях из [4] и поэтому его можно принять за рассуждение Гаусса. Элементарное изложение идеи неэлементарного доказательства невозможности приводится в [8]. Доказательства невозможности в теореме Гаусса являются алгебраическим выражением этой идеи «разбиения решений на пары». Простое доказательство *невозможности* из [3, гл. 5] намечено в серии E (отличие приводимого изложения в том, что необходимые понятия не вводятся немотивированно впрок, а естественно появляются в процессе размышления над проблемой). Еще одно доказательство невозможности, возникшее в ходе обсуждений с А. Я. Канелем-Беловым, приводится в приложении в полном тексте. По сути все доказательства очень близки.

Перед доказательствами невозможности в теореме Гаусса некоторые их идеи демонстрируются по одной и на простейших примерах (серия C). Эти

[2)] Конечно, *отправные* идеи любой теории не исчерпывают *всех* ее идей.

[3)] Вульгарно, но ярко, эти идеи можно выразить девизом *группируй и властвуй* или *объединяй и властвуй*.

[4)] Авторы лишь потому позволяют себе данное замечание по поводу изложения в [4], что преклоняются перед величием Гаусса, начавшего путь в науку с труднейших разделов чистой математики, а затем много занимавшегося приложениями и превратившего один из разделов географии в раздел математики.

примеры дают решение классических задач древности об удвоении куба и трисекции угла, ждавших своего решения два тысячелетия. Приводимое изложение основано на [10, 12]; оно немного более коротко и ясно за счет того, что не используется термин «поле». Ср. [5, §4.19].

Приводимые серии задач (в частности, доказательства возможности и невозможности) независимы друг от друга. В доказательствах используется определение построимости из второго отступления и эквивалентность теоремы Гаусса аналогичной теореме для *комплексного* калькулятора (задача А4).

Доказательства представлены в виде циклов задач (большинство задач снабжены указаниями или решениями). Решение задач потребует от многих читателей усилий (впрочем, опытный математик, не знакомый с теорией Галуа, с легкостью восстановит решения по приведенным указаниям или даже без них). Однако эти усилия будут сполна оправданы тем, что вслед за великими математиками в процессе изучения интересной проблемы читатель познакомится с некоторыми основными идеями алгебры. Надеюсь, это поможет читателю совершить собственные настолько же полезные открытия (не обязательно в математике)!

Общее замечание к формулировкам задач: если условие задачи является утверждением, то в задаче требуется это утверждение доказать.

Предварительная версия этой заметки представлялась А. Беловым-Канелем, П. Дергачом и авторами в виде цикла задач на Летней Конференции Турнира Городов в августе 2007 г. Сокращенный английский перевод (выполненный П. Дергачом и А. Скопенковым) доступен в интернете[5)].

В этой заметке использованы материалы занятий со школьниками по элементарному доказательству теоремы Гаусса, которые вели А. С. Голованов, А. И. Ефимов и второй автор. Аналогичные занятия вели А. Я. Белов-Канель, И. И. Богданов, Г. Р. Челноков и, возможно, другие. Мы благодарим их всех, а также Э. Б. Винберга, М. Н. Вялого, П. А. Дергача, А. А. Казначеева и В. В. Прасолова за полезные обсуждения.

Отступление: связь с построениями циркулем и линейкой

А1. Используя отрезки длины a, b и c, можно построить циркулем и линейкой отрезки длины $a+b$, $a-b$, ab/c, $\sqrt{ab}$.

Вещественное число называется *построимым*, если его можно получить на нашем калькуляторе (т. е. получить из 1 при помощи сложения,

[5)] См. www.mccme.ru/circles/oim/materials/constreng.pdf

вычитания, умножения, деления и извлечения квадратного корня из положительного числа). Например, числа

$$1+\sqrt{2},\quad \sqrt[4]{2}=\sqrt{\sqrt{2}},\quad \sqrt{2\sqrt{3}},\quad \sqrt{2}+\sqrt{3},\quad \sqrt{1+\sqrt{2}},\quad \frac{1}{1+\sqrt{2}}\quad \text{и}\quad \cos 3^\circ$$

построимы. Про последние два числа это не совсем очевидно.

А2. Любое построимое число можно построить циркулем и линейкой (далее слова «циркулем и линейкой» опускаются).

Этот простой (вытекающий из А1) результат был известен еще древним грекам. Он показывает, что из *выразимости* числа $\cos(2\pi/n)$ в теореме Гаусса вытекает *построимость* правильного n-угольника.

А3. *Основная теорема теории геометрических построений.* Обратное тоже верно: если отрезок длины a можно построить циркулем и линейкой, то число a построимо.

Этот несложный результат [9,14] (доказанный лишь в 19-м веке) показывает, что из *невыразимости* в теореме Гаусса вытекает *непостроимость* соответствующих n-угольников.

Для его доказательства рассмотрите все возможные случаи появления новых объектов (точек, прямых, окружностей). Покажите, что координаты всех построенных точек и коэффициенты уравнений всех проведённых прямых и окружностей являются построимыми. См. детали в [9,10,12,14].

Определение *комплексно построимого* комплексного числа аналогично определению построимого вещественного числа, только квадратные корни извлекаются из произвольных уже выраженных чисел и комплексно построимыми считаются оба значения квадратного корня.

А4. Комплексное число комплексно построимо тогда и только тогда, когда его вещественная и мнимая части (вещественно) построимы.

Указание: Если $\sqrt{a+bi}=u+vi$, то u,v выражаются через a и b с помощью арифметических операций и квадратных радикалов.

По поводу невыразимости вещественных чисел через вещественные (положительные) значения корней произвольной целой степени (из положительных чисел) см. [2].

А5. Если правильный mn-угольник построим, то и правильный m-угольник построим.

А6. Правильные 3-угольник и 5-угольник построимы.

А7. Правильный 120-угольник построим. Или, эквивалентно, угол 3° построим.

Указание: Если не получается, то см. следующие задачи.

А8. Если правильный n-угольник построим, то и правильный $2n$-угольник построим.

Указание: Получается делением угла пополам или применением формулы половинного угла.

А9. Пусть правильные m- и n-угольники построимы, причем числа m и n взаимно просты. Тогда правильный mn-угольник построим.

Указание: Так как m и n взаимно просты, то существуют целые a, b такие, что $am + bn = 1$.

Доказательство возможности в теореме Гаусса

Нетрудно доказать возможность в теореме Гаусса для $n \leqslant 16$.

Доказательство возможности в теореме Гаусса для $n = 5$. Видимо, приводимый способ сложнее придуманного Вами. Зато из него будет видно, что делать в общем случае. Достаточно выразить число $\varepsilon = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$. Сразу это сделать трудно, поэтому сначала построим некоторые многочлены от ε. Мы знаем, что $\varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 = -1$. Поэтому

$$(\varepsilon + \varepsilon^4)(\varepsilon^2 + \varepsilon^3) = \varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 = -1.$$

Обозначим

$$A_0 := \varepsilon + \varepsilon^4 \text{ и } A_1 := \varepsilon^2 + \varepsilon^3.$$

Тогда по теореме Виета числа A_0 и A_1 являются корнями уравнения $t^2 + t - 1 = 0$. Поэтому можно выразить A_0 (и A_1). Поскольку $\varepsilon \cdot \varepsilon^4 = 1$, то по теореме Виета числа ε и ε^4 являются корнями уравнения $t^2 - A_0 t + 1 = 0$. Поэтому можно выразить ε (и ε^4).

В1. Если число $2^m + 1$ простое, то m — степень двойки.

Идея доказательства построимости в теореме Гаусса. Достаточно выразить число $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ для простого $n = 2^m + 1$ (тогда m обязано быть степенью двойки).

Сначала хорошо бы разбить сумму

$$\varepsilon + \varepsilon^2 + \cdots + \varepsilon^{n-1} = -1$$

на два слагаемых A_0 и A_1, *произведение* которых построимо (иными словами, *сгруппировать* хитрым образом корни уравнения $1 + \varepsilon + \varepsilon^2 + \cdots + \varepsilon^{n-1} = 0$). Тогда A_0 и A_1 построимы по теореме Виета. Затем хорошо бы разбить сумму A_0 на два слагаемых $A_0 = A_{00} + A_{01}$, произведение которых построимо, и аналогично разбить $A_1 = A_{10} + A_{11}$. И так далее, пока не построим $A_{0\ldots0} = \varepsilon$.

Однако придумать нужные группировки корней уравнения $1+\varepsilon+\varepsilon^2+\dots+\varepsilon^{n-1}=0$ совершенно нетривиально и возможно не для всех n. Как это можно придумать, описано в [7]. Здесь приведем лишь ответ, который очень прост.

Теорема о первообразном корне. Для любого простого p существует число g, для которого остатки от деления на p чисел $g^1, g^2, g^3, \dots, g^{p-1}=1$ различны.

Как строить нужные группировки, видно из задач B3a, B4a и B4c ниже.

B2. *Доказательство теоремы о первообразном корне.* Пусть p простое и a не делится на p.

(a) $p-1$ делится на наименьшее $k>0$, для которого $a^k \equiv 1 \pmod p$.

Указание: используйте малую теорему Ферма.

(b) Для любых целых n и a сравнение $x^n \equiv a \pmod p$ имеет не более n решений.

(c) Если $p-1$ делится на d, то сравнение $x^d \equiv 1 \pmod p$ имеет ровно d решений.

(d) Докажите теорему о первообразном корне для $p=2^m+1$. (Только этот частный случай нужен для теоремы Гаусса.)

(e)* Докажите теорему о первообразном корне для $p=2^m\cdot 3^n+1$.

(f)* Докажите теорему о первообразном корне для *произвольного* простого p.

(g)* Верно ли, что число 3 является первообразным корнем по модулю любого простого числа вида $p=2^m+1$?

Начиная с этого момента $p=2^m+1\geqslant 5$ — простое число и g — (любой) первообразный корень по модулю p.

B3. (a) Положим

$$A_0 := \varepsilon^{g^2}+\varepsilon^{g^4}+\varepsilon^{g^6}+\dots+\varepsilon^{g^{2^m}} \quad \text{и} \quad A_1 := \varepsilon^{g^1}+\varepsilon^{g^3}+\varepsilon^{g^5}+\dots+\varepsilon^{g^{2^m-1}}.$$

Докажите, что $A_0A_1=-\dfrac{p-1}{4}$. (Следующие задачи являются подсказками.)

(b) $g^k+g^l \equiv 0 \pmod p$ тогда и только тогда, когда $k-l \equiv \dfrac{p-1}{2} \pmod{p-1}$.

(c) $A_0A_1=\sum\limits_{s=1}^{2^m}\varepsilon^s\alpha(s)$, где $\alpha(s)$ равно числу решений (k,l) (в вычетах по модулю $p-1$) сравнения $g^{2k}+g^{2l+1}\equiv s \pmod p$.

(d) $\alpha(s)=\alpha(gs)$.

(e) $\alpha(s)$ не зависит от $s=1,\dots,2^m$.

B4. (a) Положим

$$A_{00} := \varepsilon^{g^4} + \varepsilon^{g^8} + \varepsilon^{g^{12}} + \cdots + \varepsilon^{g^{2^m}} \quad \text{и} \quad A_{01} := \varepsilon^{g^2} + \varepsilon^{g^6} + \varepsilon^{g^{10}} + \cdots + \varepsilon^{g^{2^m-2}}.$$

Докажите, что $A_{00}A_{01} = sA_0 + tA_1$ для некоторых целых чисел s и t $(s + t = \dfrac{p-1}{8})$. (Следующая задача является подсказкой.)

(b) Сравнение $g^{4k} + g^{4l+2} \equiv 1 \pmod p$ имеет столько же решений (k, l) (в вычетах по модулю $p - 1$), сколько сравнение $g^{4k} + g^{4l+2} \equiv g^2 \pmod p$.

(c) Положим

$$A_{11} := \varepsilon^{g^1} + \varepsilon^{g^5} + \varepsilon^{g^9} + \cdots + \varepsilon^{g^{2^m-3}} \quad \text{и} \quad A_{10} := \varepsilon^{g^3} + \varepsilon^{g^7} + \varepsilon^{g^{11}} + \cdots + \varepsilon^{g^{2^m-1}}.$$

Докажите, что $A_{10}A_{11} = uA_0 + vA_1$ для некоторых целых чисел u и v $(u + v = \dfrac{p-1}{8})$.

(d) Закончите доказательство возможности в теореме Гаусса.

B5. Найдите явно выражение через квадратные радикалы числа

(a) A_0 из задачи B3a. (b) $\cos\dfrac{2\pi}{17}$. (c)* $\cos\dfrac{2\pi}{257}$. (d)* $\cos\dfrac{2\pi}{65537}$.

При помощи приведенного метода и компьютера эту задачу можно решить быстро, несмотря на следующую историю [11]. «Один слишком навязчивый аспирант довел своего руководителя до того, что тот сказал ему: „Идите и разработайте построение правильного многоугольника с 65 537 сторонами“. Аспирант удалился, чтобы вернуться через 20 лет с соответствующим построением (которое хранится в архивах в Геттингене).»

Замечание. Построимость можно доказывать по тому же плану без использования комплексных чисел. Приведем указание для случая правильного 17-угольника. Положим $a_k = \cos(2\pi k/17)$. Тогда $a_k = a_{17-k}$, $2a_ka_l = a_{k+l} + a_{k-l}$ и $a_1 + a_2 + a_3 + \cdots + a_8 = -1/2$. Сначала выразите $a_1 + a_2 + a_4 + a_8$ и $a_3 + a_5 + a_6 + a_7$. Затем выразите $a_1 + a_4$, $a_2 + a_8$, $a_3 + a_5$ и $a_6 + a_7$. Наконец, выразите a_1.

Указания и решения к доказательству возможности

Указание к B1. Если n нечетно, то $2^{kn} + 1$ делится на $2^k + 1$.

Указание к B2b. Докажем более общее утверждение: *многочлен степени n не может иметь более n корней в множестве $\mathbb{Z}/p\mathbb{Z}$ вычетов по модулю p (в котором имеются операции сложения и умножения по модулю p)*. Здесь многочленом называется бесконечный упорядоченный набор $(a_0, \ldots, a_n, \ldots)$ вычетов по модулю p, в котором лишь конечное число элементов отлично от нуля. Обычно многочлен записывается в виде $a_0 + {+}a_1x{+}\cdots{+}a_kx^k$ (если $a_{k+1} = a_{k+2} = \cdots = 0$). Эта запись дает отображение

$\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Будьте осторожны: разным многочленам может соответствовать одно и то же отображение. *Корнем* многочлена $a_0+a_1x+\cdots+a_kx^k$ называется такой вычет x_0 по модулю p, что $a_0 + a_1x_0 + \cdots + a_kx_0^k = 0$.

Пусть многочлен $P(x)$ степени n имеет различные корни $x_1, \ldots, x_n$, x_{n+1} в множестве вычетов $\mathbb{Z}/p\mathbb{Z}$. Представьте его в виде

$$P(x) = b_n(x-x_1)\cdot\ldots\cdot(x-x_n)+b_{n-1}(x-x_1)\cdot\ldots\cdot(x-x_{n-1})+\cdots+b_1(x-x_1)+b_0$$

(«*интерполяция Ньютона*»). Последовательно подставляя в сравнение $P(x) \equiv 0 \pmod p$ вычеты $x_1, \ldots, x_n, x_{n+1}$, получим $b_0 \equiv b_1 \equiv \cdots \equiv b_{n-1} \equiv \equiv b_n \equiv 0 \pmod p$.

То же самое решение можно записать и так. Пусть P — многочлен. Тогда $P - P(a) = (x - a)Q$ для некоторого многочлена Q степени меньше $\deg P$. Поэтому если $P(a) = 0$, то $P = (x-a)Q$ для некоторого многочлена Q степени меньше $\deg P$. Теперь требуемое в задаче утверждение доказывается индукцией по степени многочлена P с использованием простоты числа p.

Первое указание к B2c. Заметьте, что многочлен $x^{p-1} - 1$ имеет ровно $p-1$ корень в множестве вычетов $\mathbb{Z}/p\mathbb{Z}$ и делится на x^d-1. Докажите, что если многочлен степени a имеет ровно a корней и делится на многочлен степени b, то этот многочлен степени b имеет ровно b корней.

Второе указание к B2c. Если $p = kd$, то для любого a сравнение $y^k \equiv \equiv a \pmod p$ имеет не более k решений.

Указание к B2d. Если первообразного корня нет, то по 2a сравнение $x^{2^{m-1}} \equiv 1 \pmod p$ имеет $p - 1 = 2^m > 2^{m-1}$ решений.

Указание к B2e,f. Аналогично B2d.

Замечание к B2f. Из существования первообразного корня легко вывести, что для $p-1 = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ количество первообразных корней равно $(p-1)(1-\frac{1}{p_1}) \cdot \ldots \cdot (1-\frac{1}{p_k}) = \varphi(p-1)$.

Указание к B3c. Раскройте скобки и сгруппируйте равные слагаемые.

Указание к B3d. Если (a, b) — решение сравнения $g^{2k} + g^{2l+1} \equiv s \pmod p$, то $(b + 1, a)$ — решение сравнения $g^{2k} + g^{2l+1} \equiv gs \pmod p$. Если (a, b) — решение сравнения $g^{2k} + g^{2l+1} \equiv gs \pmod p$, то $(b, a - 1)$ — решение сравнения $g^{2k} + g^{2l+1} \equiv s \pmod p$.

Указание к B5c. (Написано с использованием решения задачи 4d из `http://www.turgor.ru/lktg/2007/5/index.php`, представленного Е. Лукьянцом, учеником ФМЛ 239 г. Санкт-Петербурга, и В. Соколовым, учеником гимназии №261 г. Санкт-Петербурга.) Положим

$$\overline{i_0 \ldots i_x} := i_0 2^0 + \cdots + i_x 2^x \quad \text{и} \quad A_{i_0 \ldots i_x} := \sum_{s=1}^{2^{m-x-1}} \varepsilon^{g^{-\overline{i_0 \ldots i_x}+s2^{x+1}}}.$$

Тогда $A_{i_0\dots i_x 0} + A_{i_0\dots i_x 1} = A_{i_0\dots i_x}$. При $x < m$ имеем

$$A_{i_0\dots i_x 0} A_{i_0\dots i_x 1} = \sum_{s=0}^{2^m} \alpha(s)\varepsilon^s = \sum_{(j_0\dots j_x)} b_{j_0\dots j_x} A_{j_0\dots j_x} \quad \text{для некоторых } b_{j_0\dots j_x} \in \mathbb{Z}.$$

Здесь в первом равенстве $\alpha(s)$ равно числу решений (k, l) (в вычетах по модулю $p-1$) сравнения

$$g^{-\overline{i_0\dots i_x}+k2^{x+1}} + g^{-\overline{i_0\dots i_x}+l2^{x+1}+2^x} \equiv s \pmod p.$$

По B3b $\alpha(0) = 0$ при $x < m$. Аналогично B3c $\alpha(s) = \alpha(sg^{2^x})$. Отсюда вытекает второе равенство.

Подготовка к доказательству невозможности в теореме Гаусса

C1. Не существует рациональных чисел a, b, c, d, для которых $\sqrt[3]{2} =$
(a) $a + \sqrt{b}$; (b) $a - \sqrt{b}$; (c) $\dfrac{1}{a+\sqrt{b}}$; (d) $a + \sqrt{b} + \sqrt{c}$; (e) $a + \sqrt{b} + \\ + \sqrt{c} + \sqrt{bc}$; (f) $a + \sqrt{b + \sqrt{c}}$; (g) $a + \sqrt{b} + \sqrt{c} + \sqrt{d}$.

Указание к C1c. Домножьте на сопряженное.

C2. Пусть нажатие кнопок «1» и четырех арифметических действий на калькуляторе из теоремы Гаусса бесплатны, а за извлечение корня нужно платить копейку.

(a) *Число A можно получить за r копеек тогда и только тогда, когда существуют такие $a_1, \dots, a_{r-1} \in \mathbb{R}$, что*

$$\mathbb{Q} = Q_1 \subset Q_2 \subset Q_3 \subset \dots \subset Q_{r-1} \subset Q_r \ni A, \quad \text{где } a_k \in Q_k,\ \sqrt{a_k} \notin Q_k,$$

а $Q_{k+1} = Q_k[\sqrt{a_k}] := \{\alpha + \beta\sqrt{a_k} \mid \alpha, \beta \in Q_k\}$ для любого $k = 1, \dots, r-1$.

Указание: Это утверждение легко доказывается индукцией по количеству операций калькулятора, необходимых для получения числа, с применением домножения на сопряженное.

Такая последовательность называется *цепочкой квадратичных расширений* (это единый термин, термин «квадратичное расширение» мы не используем).

Итак, число A построимо тогда и только тогда, когда для некоторого r существует цепочка квадратичных расширений длины r, последнее множество которой содержит A.

Доказательство невозможности, основанное на рассмотрении аналогичных цепочек, называется в математической логике и программировании *индукцией по глубине формулы*.

(b) Оторвем у (комплексного аналога) калькулятора из теоремы Гаусса кнопку «:», но разрешим использовать все рациональные числа. Тогда

множество чисел, которые можно реализовать на калькуляторе, не изменится.

Указание: Следует из предыдущего.

(c) $\sqrt[3]{2}$ непостроимо. (Значит, удвоение куба циркулем и линейкой невозможно.)

Доказательство непостроимости числа $\sqrt[3]{2}$. Предположим, что $\sqrt[3]{2}$ построимо. Тогда существует такая цепочка квадратичных расширений

$$\mathbb{Q} = Q_1 \subset Q_2 \subset Q_3 \subset \ldots \subset Q_{r-1} \subset Q_r, \quad \text{что} \quad \sqrt[3]{2} \in Q_r \setminus Q_{r-1}.$$

Поскольку $\sqrt[3]{2} \notin \mathbb{Q}$, то $r \geqslant 2$. Значит,

$$\sqrt[3]{2} = \alpha + \beta\sqrt{a}, \quad \text{где} \quad \alpha, \beta, a \in Q_{r-1}, \quad \sqrt{a} \notin Q_{r-1} \quad \text{и} \quad \beta \neq 0.$$

Отсюда

$$2 = (\sqrt[3]{2})^3 = (\alpha^3 + 3\alpha\beta^2 a) + (3\alpha^2\beta + \beta^3 a)\sqrt{a} = u + v\sqrt{a}.$$

Поскольку $2 \in \mathbb{Q} \subset Q_{r-1}$, то $2 - u \in Q_{r-1}$. Так как

$$v\sqrt{a} = 2 - u \quad \text{и} \quad v \in Q_{r-1}, \quad \text{то} \quad 0 = v = 3\alpha^2\beta + \beta^3 a.$$

Так как $3\alpha^2 + \beta^2 a > 0$, получаем $\beta = 0$ — противоречие! □

C3. (a) Число $\cos(2\pi/9)$ является корнем уравнения $8x^3 - 6x + 1 = 0$.

(b) Не существует рациональных чисел a и b, для которых $\cos(2\pi/9) = a + \sqrt{b}$.

(c) Не существует рациональных чисел a, b, c, для которых $\cos(2\pi/9) = a + \sqrt{b + \sqrt{c}}$.

(d) Число $\cos(2\pi/9)$ не построимо (значит, трисекция угла $\pi/3$ циркулем и линейкой невозможна и правильный 9-угольник не построим).

(e) *Теорема.* Корни кубического уравнения с рациональными коэффициентами построимы тогда и только тогда, когда один из них рационален.

Указания к C3. (a) Выразите $\cos 3\alpha$ через $\cos\alpha$.

(b) Если $\cos(2\pi/9) = a + \sqrt{b}$, то число $a - \sqrt{b}$ тоже является корнем уравнения $8x^3 - 6x + 1 = 0$. Тогда по теореме Виета третий корень равен $-(a + \sqrt{b}) - (a - \sqrt{b}) = -2a \in \mathbb{Q}$.

(d) Следует из (a) и (e).

(e) См. следующую лемму.

C4. *Лемма о сопряжении.* В цепочке квадратичных расширений положим $a = a_k$ и определим отображение сопряжения $\overline{\cdot}\colon Q_k[\sqrt{a}] \to Q_k[\sqrt{a}]$ формулой $\overline{x + y\sqrt{a}} = x - y\sqrt{a}$. Тогда

(a) Это определение корректно.

(b) $\overline{z + w} = \overline{z} + \overline{w}$, $\quad \overline{zw} = \overline{z}\,\overline{w} \quad$ и $\quad \overline{z} = z \Leftrightarrow z = x + 0\sqrt{a} \in Q_{k-1}$.

(c) Если $z \in Q_k[\sqrt{a}]$ — корень многочлена P с рациональными коэффициентами, то $P(\overline{z}) = 0$.

(Сравните с леммой о комплексных корнях многочлена с вещественными коэффициентами.)

Доказательство теоремы С3е *о кубических уравнениях для уравнений, все три корня которых вещественны (этот частный случай достаточен для непостроимости правильного* 9*-угольника).* Часть «тогда» очевидна. Чтобы доказать часть «только тогда», предположим, что хотя бы один из корней построим. Для каждого из построимых корней z рассмотрим минимальную цепочку расширений

$$\mathbb{Q} = Q_1 \subset Q_2 \subset Q_3 \subset \ldots \subset Q_{r-1} \subset Q_r, \quad \text{для которой} \quad z_1 \in Q_r \setminus Q_{r-1}.$$

Возьмем корень $z = z_1$ с наименьшей длиной минимальной цепочки l.

Если кубическое уравнение не имеет рациональных корней, то $l \geqslant 2$. Значит,

$$z_1 = \alpha + \beta\sqrt{a}, \quad \text{где} \quad \alpha, \beta \in Q_{l-1}, \quad \sqrt{a} \notin Q_{l-1} \qquad \text{и} \quad \beta \neq 0.$$

Тогда число $z_2 := \overline{z}_1 = \alpha - \beta\sqrt{a}$ также является корнем кубического уравнения (по лемме о сопряжении). Поскольку

$$\beta \neq 0, \text{ то } \alpha - \beta\sqrt{a} \neq \alpha + \beta\sqrt{a}, \text{ т. е. } z_2 \neq z_1.$$

Обозначим z_3 третий корень кубического уравнения (возможно, $z_3 \in \{z_1, z_2\}$). По формуле Виета

$$z_1+z_2+z_3 = (\alpha+\beta\sqrt{a})+(\alpha-\beta\sqrt{a})+z_3 = 2\alpha+z_3 \in \mathbb{Q}, \quad \text{поэтому} \quad z_3 \in Q_{l-1}.$$

Следовательно, для корня z_3 существует цепочка меньшей длины, чем для z_1. Противоречие. □

С5. *Эта задача не используется при доказательстве теоремы Гаусса.*

(a)* Корни многочлена 4-ой степени с рациональными коэффициентами построимы тогда и только тогда, когда его *кубическая резольвента* [9, 14] имеет рациональный корень.

(b) Любое построимое число является алгебраическим, т. е. корнем некоторого многочлена с целыми коэффициентами. (Из этого и доказанной в 1883 г. Линдеманом трансцендентности числа π, влекущей трансцендентность числа $\sqrt{\pi}$, вытекает, что задача о квадратуре круга неразрешима циркулем и линейкой.)

(c) (Г. Челноков) Лешин калькулятор получается из комплексного гауссова добавлением кнопки извлечения кубического корня из комплексных чисел (которая дает все три значения корня). Гришин калькулятор получается из комплексного гауссова добавлением кнопки нахождения по комплексному числу a всех трех комплексных корней уравнения $a = \dfrac{3x - 4x^3}{1 - 3x^2}$. Будет ли множество «Лешиных» чисел совпадать с множеством «Гришиных»?

(d) (Г. Челноков) Если неприводимый над $\mathbb{Q}$ многочлен раскладывается над $\mathbb{Q}[\sqrt[4]{2}]$ ровно на четыре множителя (неприводимых над $\mathbb{Q}[\sqrt[4]{2}]$), то степень этого многочлена делится на 8.

Указание к C5b. Пусть $a{=}a_1$ и $b{=}b_1$ — построимые числа, а P и Q — многочлены с рациональными коэффициентами минимальной степени, корнями которых являются соответственно a и b. Пусть $a_2, \dots, a_m$ — все остальные комплексные корни многочлена P, а $b_2, \dots, b_n$ — все остальные комплексные корни многочлена Q. Заметим, что

$a+b$ — корень многочлена $P(x-b_1)\cdot\ldots\cdot P(x-b_n)$,

$a-b$ — корень многочлена $P(x+b_1)\cdot\ldots\cdot P(x+b_n)$,

ab — корень многочлена $P(\frac{x}{b_1})\cdot\ldots\cdot P(\frac{x}{b_n})$,

$\frac{a}{b}$ — корень многочлена $P(xb_1)\cdot\ldots\cdot P(xb_n)$,

$\sqrt{a}$ — корень многочлена $P(x^2)$.

Осталось доказать следующее вспомогательное утверждение.

Лемма. Пусть $R(x,y)$ — многочлен от двух переменных с рациональными коэффициентами, а $b_1, b_2, \dots, b_n$ — все комплексные корни многочлена Q с рациональными коэффициентами. Тогда многочлен от одной переменной $R(x,b_1)R(x,b_2)\cdot\ldots\cdot R(x,b_n)$ также имеет рациональные коэффициенты.

Первое доказательство невозможности в теореме Гаусса

Это доказательство наиболее похоже на доказательство возможности.

D1. Число $\cos(2\pi/7)$ не построимо (значит, правильный 7-угольник не построим).

D2. Пусть $n = 4k{+}3$ простое. Обозначим $f_s = \varepsilon^s{+}\varepsilon^{-s}$. Назовем *рангом* построимого числа наименьшую длину минимальной цепочки квадратичных расширений, последнее множество которой содержит данное число.

(a) Для любого k число $f_1^k + f_2^k + \dots + f_{(p-1)/2}^k$ рационально.

(b) После раскрытия скобок и приведения подобных в выражении $(x-f_1)(x-f_2)\cdot\ldots\cdot(x-f_{(p-1)/2})$ получается многочлен с рациональными коэффициентами.

(c) Ранги чисел $\varepsilon, \varepsilon^2, \dots, \varepsilon^{p-1}$ одинаковы.

(d) Ранги чисел $f_1, \dots, f_{(p-1)/2}$ одинаковы.

(e) Число $\cos(2\pi/n)$ не построимо.

D3. Обозначим $\varepsilon = \cos(2\pi/13) + i\sin(2\pi/13)$, $g = 2$ — первообразный корень по модулю 13,

$A_0 = \varepsilon^{g^0}{+}\varepsilon^{g^3}{+}\varepsilon^{g^6}{+}\varepsilon^{g^9}$, $A_1 = \varepsilon^{g^1}{+}\varepsilon^{g^4}{+}\varepsilon^{g^7}{+}\varepsilon^{g^{10}}$ и $A_2 = \varepsilon^{g^2}{+}\varepsilon^{g^5}{+}\varepsilon^{g^8}{+}\varepsilon^{g^{11}}$.

(a) $A_0^2 = 4 + A_1 + 2A_2$, $A_1^2 = 4 + A_2 + 2A_0$ и $A_2^2 = 4 + A_0 + 2A_1$.

(b) Числа A_0, A_1, A_2 являются корнями неприводимого кубического уравнения с рациональными коэффициентами.

(c) Числа A_0, A_1, A_2 имеют одинаковый ранг.

(d) Число $\cos(2\pi/13)$ не построимо.

D4. Число $\cos(2\pi/p)$ не построимо для

(a) $p = 3 \cdot 2^k + 1$ простого.

(b) p простого, $p \neq 2^m + 1$.

(c) $p = 289$.

(d) числа p, не являющегоеся произведением степени двойки и различных простых чисел вида $2^m + 1$.

Решение D1. Рассмотрим комплексное число

$$\varepsilon = \cos(2\pi/7) + i\sin(2\pi/7).$$

Так как $\varepsilon \neq 1$, то число ε удовлетворяет уравнению 6-ой степени

$$\varepsilon^6 + \varepsilon^5 + \varepsilon^4 + \varepsilon^3 + \varepsilon^2 + \varepsilon + 1 = 0.$$

Разделим обе части уравнения на ε^3. Положим

$$f := \varepsilon + \varepsilon^{-1}, \quad \text{тогда } \varepsilon^2 + \varepsilon^{-2} = f^2 - 2 \text{ и } \varepsilon^3 + \varepsilon^{-3} = f(\varepsilon^2 + \varepsilon^{-2} - 1).$$

Получим кубическое уравнение

$$f(f^2 - 3) + (f^2 - 2) + f + 1 = 0, \quad \text{то есть} \quad f^3 + f^2 - 2f - 1 = 0.$$

Кандидаты на рациональные корни этого уравнения $f = \pm 1$ отвергаются проверкой. Согласно теореме С3е о кубических уравнениях число $f = \varepsilon + \varepsilon^{-1}$ не построимо. Поэтому и ε не построимо (поясните).

Указания к D2. (a) Индукция по k.

(b) Следует из пункта (a) и из того, что любой симметрический многочлен от переменных $f_1, f_2, \ldots, f_{(p-1)/2}$ рационально выражается через многочлены вида $f_1^k + f_2^k + \cdots + f_{(p-1)/2}^k$.

(c) Так как для любых $s, t \in \{1, 2, \ldots, p-1\}$ существует такое k, что $\varepsilon^s = (\varepsilon^t)^k$, то ранги чисел $\varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-1}$ одинаковы.

(d) Так как $\varepsilon^s + \varepsilon^{-s}$ рационально выражается через $\varepsilon + \varepsilon^{-1}$, то для любых $s, t \in \{1, 2, \ldots, p-1\}$ число $\varepsilon^s + \varepsilon^{-s}$ рационально выражается через $\varepsilon^t + \varepsilon^{-t}$ (аналогично приведенному решению задачи D1). Поэтому ранги чисел $f_1, \ldots, f_{(p-1)/2}$ одинаковы.

(Заметим, что $\operatorname{rk}(\varepsilon + \varepsilon^{-1}) = \operatorname{rk}\varepsilon - 1$.)

(e) Пусть $r := \operatorname{rk} f_s$. Значит, для некоторой цепочки квадратичных расширений

$$f_s = \alpha_s + \beta_s\sqrt{a}, \quad \text{где } \alpha_s, \beta_s, a \in Q_{r-1},\ \sqrt{a} \notin Q_{r-1} \text{ и } \beta_s \neq 0.$$

Тогда число $\overline{f}_s = \alpha_s - \beta_s\sqrt{a}$ также является корнем рассматриваемого многочлена (по лемме о сопряжении). Поскольку

$$\beta_s \neq 0, \quad \text{то} \quad \alpha_s - \beta_s\sqrt{a} \neq \alpha_s + \beta_s\sqrt{a}, \quad \text{т. е.} \quad \overline{f}_s \neq f_s.$$

Итак, корни $f_1, \dots, f_{(p-1)/2}$ разбиваются на пары сопряженных. Значит, $(p-1)/2$ четно — противоречие.

Указания к D3. (a) Докажем первую фомулу (остальные доказываются аналогично). Заметим, что $g^6 = -1$. Поэтому

$$A_0^2 = ((\varepsilon^{g^0} + \varepsilon^{-g^0}) + (\varepsilon^{g^3} + \varepsilon^{-g^3}))^2 =$$
$$= 2 + \varepsilon^{g^1} + \varepsilon^{-g^1} + 2 + \varepsilon^{g^4} + \varepsilon^{-g^4} + 2(\varepsilon^{g^0} + \varepsilon^{g^6})(\varepsilon^{g^3} + \varepsilon^{g^9}) = 4 + A_1 + 2A_2.$$

Последнее равенство верно, поскольку

$$(\varepsilon^{g^0} + \varepsilon^{g^6})(\varepsilon^{g^3} + \varepsilon^{g^9}) = \varepsilon^{g^0+g^3} + \varepsilon^{g^3+g^6} + \varepsilon^{g^6+g^9} + \varepsilon^{g^9+g^0} =$$
$$= \varepsilon^{g^0+g^3} A_0 = \varepsilon^{g^8} A_0 = A_2.$$

(В обеих формулах предпоследние равенства верны, поскольку $g = 2$.)

(b) Докажите, что $A_0 + A_1 + A_2$, $A_0^2 + A_1^2 + A_2^2$, $A_0^3 + A_1^3 + A_2^3$ рациональны.

(c) Пользуясь пунктом (a) и тем, что $A_0 + A_1 + A_2 = -1$, докажите, что любое A_i рационально выражается через любое A_j.

(d) Решение получается из пунктов (b) и (c) аналогично решению задачи D2e.

Вот идея другого решения, не использующего пункт (c). Пусть число A_0 имеет ранг r. Сопряжем его относительно Q_{r-1}. Полученное число будет одним из чисел A_i (поясните). Теперь легко понять, что числа A_i разбиваются на пары сопряженных, т. е. их четное число, что неверно.

Указания к D4. (a) Аналогично задаче D3.

(b) Предположите, что для $p = 2^k r + 1$ число $\cos\dfrac{2\pi}{p}$ построимо (где $r > 1$ — нечетное число). Выведите из этого, что числа

$$A_i = \varepsilon^{g^i} + \varepsilon^{g^{r+i}} + \dots + \varepsilon^{g^{(2^k-1)r+i}}, \quad 0 \leqslant i \leqslant r-1$$

имеют одинаковый ранг и являются корнями мнгочлена степени r с рациональными коэффициентами.

(c) Рассмотрите числа

$$A_0 = \varepsilon^{g^0} + \varepsilon^{g^{17}} + \dots + \varepsilon^{g^{272}},$$
$$A_1 = \varepsilon^{g^1} + \varepsilon^{g^{18}} + \dots + \varepsilon^{g^{273}},$$
$$A_{16} = \varepsilon^{g^{16}} + \varepsilon^{g^{33}} + \dots + \varepsilon^{g^{288}}.$$

Второе доказательство невозможности в теореме Гаусса

Идея этого доказательства выражается понятиями поля и размерности поля.

E1. *Полем* (числовым) называется подмножество множества $\mathbb{C}$ комплексных чисел, замкнутое относительно сложения, вычитания, умножения и деления.

(a) Следующие множества являются полями: $\mathbb{Q}$, множество построимых чисел, множество вещественных чисел, $\mathbb{Q}[\sqrt{2}] := \{\alpha + \beta\sqrt{2} \mid \alpha, \beta \in \mathbb{Q}\}$, каждое Q_k в цепочке квадратичных расширений и

$$\mathbb{Q}[\varepsilon] := \{\alpha_0 + \alpha_1\varepsilon + \alpha_2\varepsilon^2 + \cdots + \alpha_{12}\varepsilon^{12} \mid \alpha_i \in \mathbb{Q}\}, \quad \text{где } \varepsilon = \cos\frac{2\pi}{13} + i\sin\frac{2\pi}{13}\,.$$

(b) Любое поле содержит поле $\mathbb{Q}$.

(c) Любое поле, содержащее $\sqrt{2}$, содержит $\mathbb{Q}[\sqrt{2}]$.

(d) Любое поле, содержащее ε, содержит $\mathbb{Q}[\varepsilon]$.

E2. *Размерностью* $\dim F$ поля F называется наименьшее k, для которого существуют такие $b_2, b_3 \ldots, b_k \in F$, что

$$F = \{\alpha_1 + \alpha_2 b_2 + \alpha_3 b_3 + \cdots + \alpha_k b_k \mid \alpha_i \in \mathbb{Q}\},$$

если такое k существует.

(a) $\dim \mathbb{Q} = 1$.

(b) $\dim \mathbb{Q}[\sqrt{2}] = 2$.

(c) В цепочке квадратичных расширений

$$\dim Q_k = 2 \dim Q_{k-1} \quad \text{при } k \geqslant 1.$$

(d) В цепочке квадратичных расширений $\dim Q_k = 2^{k-1}$.

(e)* Если $G \subset F$ — поля, то $\dim F$ делится на $\dim G$.

E3. (a) $\dim \mathbb{Q}[\cos\frac{2\pi}{13} + i\sin\frac{2\pi}{13}] \leqslant 12$.

(b) Если $\dim \mathbb{Q}[\cos\frac{2\pi}{13} + i\sin\frac{2\pi}{13}] < 12$, то $P(\varepsilon) = 0$ для некоторого многочлена P с рациональными коэффициентами степени меньше 12.

(c) Многочлен $\Phi(x) := x^{12} + x^{11} + \cdots + x + 1$ неприводим над $\mathbb{Q}$.

Указание: если не получается, то используйте лемму Гаусса и признак Эйзенштейна (см. ниже).

(d) $\dim \mathbb{Q}[\cos\frac{2\pi}{13} + i\sin\frac{2\pi}{13}] = 12$.

(e) Число $\cos(2\pi/13)$ не построимо.

E4. (a) *Лемма Гаусса.* Если многочлен с целыми коэффициентами неприводим над $\mathbb{Z}$, то он неприводим и над $\mathbb{Q}$ [14].

(b) *Признак Эйзенштейна.* Пусть p простое. Если для многочлена с целыми коэффициентами старший коэффициент не делится на p, остальные делятся на p, а свободный член не делится на p^2, то этот многочлен неприводим над $\mathbb{Z}$ [14].

E5. (a) $\dim \mathbb{Q}[\cos\frac{2\pi}{289} + i\sin\frac{2\pi}{289}] = 272$.

(b) Выведите из предыдущих пунктов, что число $\cos(2\pi/289)$ не построимо.

(c) Докажите невозможность в теореме Гаусса.

Указание к E2. (c) Докажите, что

$$Q_k = \{\alpha_1 + \alpha_2 b \mid \alpha_1, \alpha_2 \in Q_{k-1}\} \quad \text{для любого } b \in Q_k - Q_{k-1}.$$

(d) Следует из (a) и (c).

(e) *Размерностью* $\dim(F : G)$ поля F над полем G называется наименьшее k, для которого существуют такие $b_1, b_2, \dots, b_k \in F$, что

$$F = \{\alpha_1 b_1 + \alpha_2 b_2 + \alpha_3 b_3 + \dots + \alpha_k b_k \mid \alpha_i \in G\},$$

если такое k существует. Докажите, что $\dim F = \dim G \dim(F : G)$.

Указания к E3. (a) $1 + \varepsilon + \varepsilon^2 \dots + \varepsilon^{12} = 0$.

(b) По определению размерности существуют такие

$$b_1, \dots, b_{11} \in \mathbb{Q}[\cos\frac{2\pi}{13} + i\sin\frac{2\pi}{13}] \text{ и } \alpha_{kl} \in \mathbb{Q}, \text{ что}$$
$$\varepsilon^{j-1} = \alpha_{j,1} b_1 + \alpha_{j,2} b_2 + \dots + \alpha_{j,11} b_{11} \text{ для } j = 1, 2, \dots, 12.$$

Поэтому существуют такие рациональные $a_0, a_1, \dots, a_{12}$, не все равные 0, что $a_0 + a_1\varepsilon + \dots + a_{11}\varepsilon^{11} = 0$. Для доказательства последнего утверждения подставьте выражения для ε^i в последнее равенство, приравняйте к нулю коэффициенты при $b_1, \dots, b_{11}$ и докажите, что полученная система уравнений имеет нетривиальное рациональное решение.

(c) Примените признак Эйзенштейна к многочлену $((x+1)^{13} - 1)/x$ и лемму Гаусса.

(d) Следует из (a), (b) и (c).

(e) Следует из (d) и E2d.

Указание к E4b. Предположите противное и воспользуйтесь методом неопределенных коэффициентов.

Указание к E5a. Аналогично решению задачи E3d. Докажите неприводимость многочлена $\Phi(x) = 1 + x^{17} + x^{34} + x^{51} + \dots + x^{272}$ и воспользуйтесь ей.

Список литературы

[1] Алексеев В. Б. *Теорема Абеля*. М: Наука, 1976.

[2] Ван дер Варден Б. Л. *Алгебра*. М.: Наука, 1976.

[3] Винберг Э. Б. *Алгебра многочленов*. М.: Просвещение, 1980.

[4] Гаусс К. Ф. *Арифметические исследования* // Труды по теории чисел. М.: Изд-во АН СССР, 1959. С. 9–580.

[5] Гашков С. Б. *Современная элементарная алгебра в задачах и упражнениях*. М.: МЦНМО, 2006.

[6] Гиндикин С. *Дебют Гаусса* // Квант, №1, 1972. С. 2–11.

[7] Канель А. Я. *О построениях*. Готовится к печати.

[8] Кириллов А. А. *О правильных многоугольниках, функции Эйлера и числах Ферма* // Квант, №7, 1977. С. 2–9. Квант, №6, 1994. С. 15–18.

[9] Колосов В. А. *Теоремы и задачи алгебры, теории чисел и комбинаторики*. М: Гелиос, 2001.

[10] Курант Р., Роббинс Г. *Что такое математика*? М.: МЦНМО, 2004.

[11] Литлвуд Дж. *Математическая смесь*. М.: Наука, 1978.

[12] Манин Ю.И. *О разрешимости задач на построение с помощью циркуля и линейки* // Энциклопедия элементарной математики. Книга четвертая (геометрия). Под редакцией П. С. Александрова, А. И. Маркушевича и А. Я. Хинчина М.: Физматгиз, 1963.

[13] Постников М. М. *Теория Галуа*. М.: Гос. изд-во физ.-мат. л-ры, 1963.

[14] Прасолов В. В. *Многочлены*. М: МЦНМО, 1999, 2001, 2003.

[15] Прасолов В. В., Соловьев Ю. П. *Эллиптические функции и алгебраические уравнения*. М.: Факториал, 1997.

[16] Чеботарев Н. Н. *Основы теории Галуа*. Часть 1. Л., М.: Гостехиздат, 1934.

[17] Эдвардс Г. *Последняя теорема Ферма. Генетическое введение в алгебраическую теорию чисел*. М.: Мир, 1980.

П. Ю. Козлов: механико-математический факультет Московского государственного университета им. М. В. Ломоносова

А. Б. Скопенков: механико-математический факультет Московского государственного университета им. М. В. Ломоносова, Независимый московский Университет, Московский институт открытого образования
e-mail: `skopenko@mccme.ru`

«Математический омнибус»

Издательство МЦНМО готовит перевод книги С. Л. Табачникова и Д. Б. Фукса «Математический омнибус». Книга состоит из 30 сюжетов, посвященных различным разделам математики. В этот выпуск «Математического просвещения» включен перевод одной из глав книги. Приведем также оглавление книги.

Двадцать семь прямых

С. Л. Табачников Д. Б. Фукс

1. Введение

Некоторые поверхности степени 2 (однополостный гиперболоид) целиком состоят из прямых линий; более того, они *дважды линейчаты*.

Если мы придерживаемся алгебраического подхода к геометрии, то после поверхностей степени 2 следующим этапом должны быть поверхности степени 3. Но тогда как геометрия поверхностей (и, естественно, кривых) второй степени была хорошо понята греками тысячи лет назад, систематическое изучение поверхностей (и кривых) третьей степени началось лишь в XIX веке.

Ныне имеются книги, посвященные «кубической геометрии» (отметим "The non-singular cubic surfaces" B. Segre [4] и «Кубические формы» Ю. И. Манина [1]). Кубическая геометрия весьма отличается от классической «квадратичной геометрии». В частности, кубические поверхности, вообще говоря, не линейчаты. Но всё же они содержат обширные, хотя и конечные, семейства прямых. (Кстати, поверхности степени выше трех обычно не содержат прямых.) Геометры XIX века, в частности Салмон и Кэли, нашли ответ на естественный вопрос:

Сколько прямых содержит поверхность степени 3?

Ответ: двадцать семь.

2. «Сколько?» — удачный ли это вопрос?

Он имеет смысл в *алгебраической геометрии*, т. е. в геометрии кривых и поверхностей, заданных алгебраическими (полиномиальными) уравнениями. Такие кривые и поверхности имеют *степень*, которая равна степени полинома.

Например, сколько общих точек имеют две прямые на плоскости? Следует ответить — одну, хотя может быть и 0 (если прямые параллельны) или бесконечность (если они совпадают). В первом случае можно сказать,

Глава из книги «Математический омнибус». Публикуется с любезного разрешения авторов. Перевод Б. Р. Френкина.

что общая точка «бесконечно удалена», и всё же учесть ее. Поэтому ответ равен 1 или ∞.

Рассмотрим теперь кривую степени два. Это может быть эллипс, гипербола, парабола или что-нибудь более вырожденное, вроде пары прямых. Можно сказать, что кривая степени 2 имеет с прямой 2, 1, 0 или бесконечно много общих точек. Но случаи 1 и 0 спорны. Наличие только одной общей точки означает, что имеется либо касательная, т. е. две совпавшие точки, либо прямая, параллельная асимптоте гиперболы или оси параболы; в последних случаях «вторая точка» бесконечно удалена. Отсутствие общей точки означает, что на самом деле общие точки — комплексные (имеют комплексные координаты, удовлетворяющие уравнениям прямой и кривой) или бесконечно удаленные (это происходит, если наша прямая — асимптота гиперболы). Но если мы учитываем каждую точку нужное количество раз и не отбрасываем комплексные и бесконечно удаленные точки, то наш ответ: 2 или бесконечность.

Аналогично, кривые степеней m и n должны иметь mn или бесконечно много общих точек (теорема Безу).

Неформально говоря, если задача из алгебраической геометрии имеет конечное число решений, то количество решений зависит лишь от степеней соответствующих кривых и поверхностей. Разумеется, это перестает выполняться, если нас интересуют лишь *вещественные* решения. Что хуже, в некоторых задачах не могут все решения быть вещественными. Например, известно, что кривая третьей степени, не содержащая прямой, имеет ровно 9 точек перегиба. Но вещественны из них не более трех. Кривая третьей степени с тремя вещественными точками перегиба показана на рис. 1. Для удобства читателя мы показали асимптоту кривой и отметили точки перегиба стрелками.

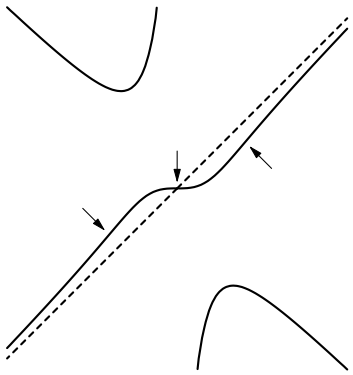


Рис. 1. *Кривая $x^3 = xy^2 + y$ с отмеченными точками перегиба*

3. Основной результат

Теорема 1. *Поверхность степени* 3 *содержит* 27 *или бесконечно много прямых.*

4. Вспомогательная задача: двойные касательные

Двойная касательная к кривой или поверхности — это прямая, касательная к ней в двух различных точках. Точка касания учитывается как две или больше точек пересечения прямой с кривой или поверхностью. Поэтому кривые и поверхности степени ниже четырех никогда не имеют двойных касательных, не содержащихся в них.

Важное наблюдение. Двойная касательная к поверхности степени 3 содержится в этой поверхности.

Рассмотрим теперь кривые степени 4 на плоскости.

Вопрос. Сколько двойных касательных имеет кривая степени 4?
Ответ: 28.

Не станем приводить полное доказательство этого факта. Ограничимся построением кривой степени 4 с 28 *вещественными*, *конечными*, *различными* двойными касательными. Рассмотрим многочлен

$$p(x, y) = (4x^2 + y^2 - 1)(x^2 + 4y^2 - 1).$$

Его степень равна 4. Уравнение $p(x, y) = 0$ определяет на плоскости «эллиптический крест» (см. рис. 2, слева). Крест делит плоскость на 6 областей. Функция $p(x, y)$ положительна во внешней (неограниченной) области и в центральной области, а в лепестках отрицательна. Возьмем очень малое положительное ε и рассмотрим кривую $p(x, y)+\varepsilon = 0$, также степени 4.

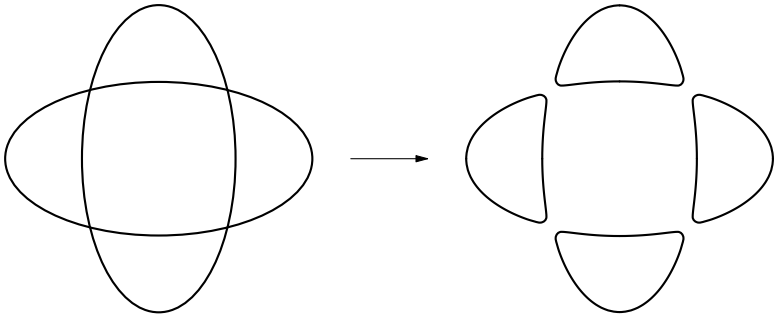


Рис. 2. *Построение кривой*

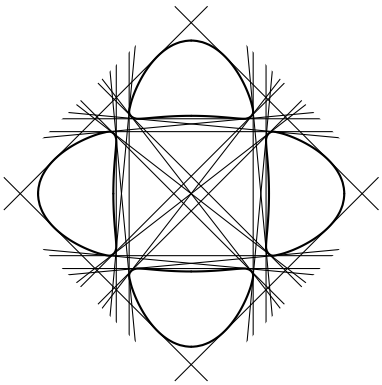


Рис. 3. *28 двойных касательных*

Она состоит из четырех овалов внутри лепестков предыдущего креста[1)]. Эти овалы очень близки к границам лепестков.

Каждые два овала имеют (не менее чем, но в действительности ровно) 4 общих касательных: две внешних и две внутренних. При этом овалы не выпуклы (их форма близка к форме лепестков), и к каждому из них имеется двойная касательная. Итого:

$$\binom{4}{2} \cdot 4 + 4 = 28.$$

5. Поверхности степени 3 и кривые степени 4

Пусть S — поверхность степени 3, заданная уравнением

$$p_3(x, y, z) + p_2(x, y, z) + p_1(x, y, z) + c = 0,$$

где p_1, p_2, p_3 — однородные многочлены степени 1, 2, 3 соответственно. Предположим, что $0 = (0, 0, 0) \in S$, то есть $c = 0$. Рассмотрим некоторую прямую, проходящую через 0; она состоит из точек с пропорциональными координатами, скажем

$$x = \alpha t,\ y = \beta t,\ z = \gamma t \quad (\alpha, \beta, \gamma) \neq (0, 0, 0). \tag{1}$$

Эта прямая пересекает S в нуле и еще двух точках. Если эти две точки совпадают, пометим нашу прямую. Таким образом, каждая помеченная прямая пересекает S в нуле, касается S в некоторой точке T и не имеет с

[1)] Термин «овал» часто обозначает замкнутую строго выпуклую гладкую кривую. В вещественной алгебраической геометрии овал алгебраической кривой — это ее компонента, ограничивающая топологический круг.

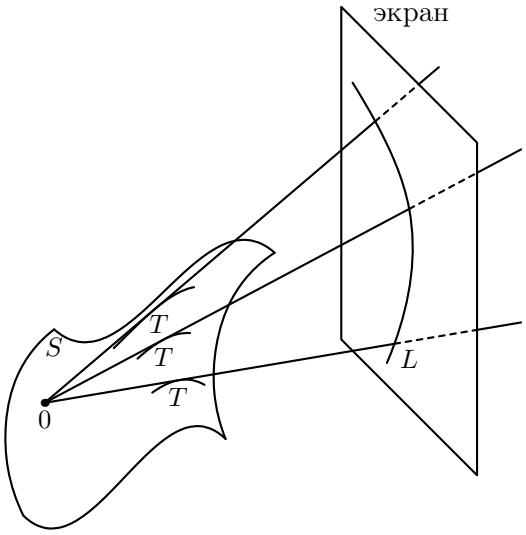


Рис. 4. *Проекция поверхности на экран*

S общих точек, кроме 0 и T. Рассмотрим пересечения помеченных прямых с некоторым экраном. Получаем на экране кривую, которую обозначим L (рис. 4).

Таким образом, если $P \in L$, то прямая, проходящая через 0 и P, касается S в некоторой точке $T(P) \in S$. Заметим, что если l — прямая, касательная к L в точке P, то плоскость, содержащая 0 и l, касается S в точке $T(P)$.

Теперь покажем, что кривая L имеет степень 4. Чтобы найти пересечение прямой (1) с S, подставим (1) в уравнение для S:

$$p_3(\alpha,\beta,\gamma)t^3 + p_2(\alpha,\beta,\gamma)t^2 + p_1(\alpha,\beta,\gamma)t = 0.$$

Одно из решений этого уравнения равно 0, а два других совпадают тогда и только тогда, когда

$$D(\alpha,\beta,\gamma) = p_2(\alpha,\beta,\gamma)^2 - 4p_3(\alpha,\beta,\gamma)p_1(\alpha,\beta,\gamma) = 0.$$

Пересечение прямой (1) и плоскости $z = 1$ отвечает значению $t = \gamma^{-1}$ (если $\gamma = 0$, то пересечения нет; это имеет место для «бесконечно удаленных» точек на L, количество которых равно 4). Это пересечение имеет координаты $(x, y, 1)$, где $x = \alpha/\gamma,\ y = \beta/\gamma$. Уравнение $D(\alpha,\beta,\gamma) = 0$ можно записать в виде $D(x, y, 1)\gamma^4 = 0$, то есть $D(x, y, 1) = 0$. Это уравнение имеет степень 4.

Пусть теперь l — одна из 28 двойных касательных к L, а P_1, P_2 — ее точки касания. Плоскость p, содержащая 0 и l, касается S в точках $T(P_1)$

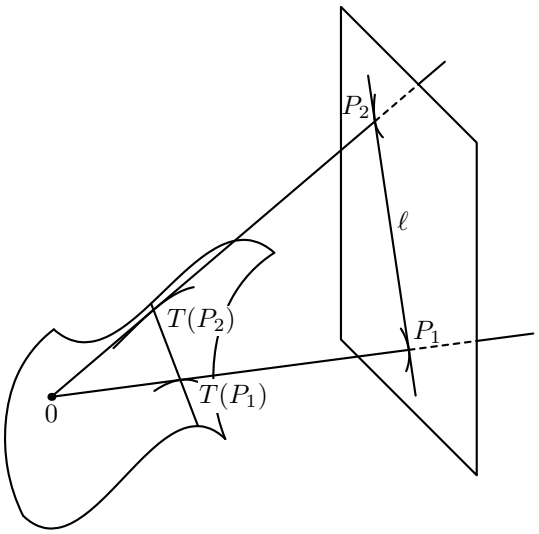


Рис. 5. *От двойных касательных — к прямым на поверхности*

и $T(P_2)$ (см. рис. 5). Следовательно, прямая, проходящая через $T(P_1)$ и $T(P_2)$, касается S в этих точках. Это возможно, лишь если она содержится в S (см. Важное наблюдение в разделе 4). Это доказывает нашу теорему за вычетом последнего, и довольно неожиданного, вопроса.

6. Двадцать восемь или двадцать семь?

Казалось бы, мы построили 28 прямых, лежащих в S. Покажем, что одна из них — мираж.

Кто может поручиться, что если $P = (x, y, 1) \in L$, то $T(P) \neq 0$? Равенство $T(P) = 0$ верно в том и только том случае, если прямая (1) имеет тройное пересечение с S. Это означает, что уравнение

$$p_3(x, y, 1)t^3 + p_2(x, y, 1)t^2 + p_1(x, y, 1)t = 0$$

имеет три совпадающих решения: $t_1 = t_2 = t_3 = 0$; последнее происходит тогда и только тогда, когда $p_2(x, y, 1) = 0$ и $p_1(x, y, 1) = 0$. Эти два уравнения описывают прямую и кривую степени 2 в плоскости с координатами x, y; поэтому имеется два решения. Геометрически это означает, что существуют две прямых, пересекающих S лишь в нуле: все три точки пересечения сливаются. Эти две прямые порождают касательную плоскость p_0 к S в нуле; они пересекают плоскость $z = 1$ в двух точках кривой L, а плоскость p_0 пересекает плоскость $z = 1$ по прямой, касательной к L в этих двух точках. Эта двойная касательная к L не соответствует никакой

прямой на S. Таким образом, мы получаем «только» $28-1=27$ прямых на S.

7. Все эти прямые могут быть вещественными

Рассмотрим поверхность

$$4(x^3+y^3+z^3)=(x+y+z)^4+3(x+y+z). \tag{2}$$

Она показана на рис. 6; вертикальная ось на этом рисунке — «диагональ» $x=y=z$.

Теорема 2. *Поверхность* (2) *содержит* 27 *вещественных прямых.*

Все 27 прямых, лежащих на поверхности (2), показаны на рис. 7 — можете их пересчитать. Этот рисунок, однако, выглядит довольно беспорядочным; тем не менее, приведенное ниже доказательство теоремы 2 может пролить некоторый свет на конструкцию прямых и их поведение.

Доказательство. Девять из прямых очевидны:

$$(\mathbf{1})\ \begin{cases} x=0 \\ y=-z \end{cases} \qquad (\mathbf{2})\ \begin{cases} y=0 \\ z=-x \end{cases} \qquad (\mathbf{3})\ \begin{cases} z=0 \\ x=-y \end{cases}$$

$$(\mathbf{4})\ \begin{cases} x=1 \\ y=-z \end{cases} \qquad (\mathbf{5})\ \begin{cases} y=1 \\ z=-x \end{cases} \qquad (\mathbf{6})\ \begin{cases} z=1 \\ x=-y \end{cases}$$

$$(\mathbf{7})\ \begin{cases} x=-1 \\ y=-z \end{cases} \qquad (\mathbf{8})\ \begin{cases} y=-1 \\ z=-x \end{cases} \qquad (\mathbf{9})\ \begin{cases} z=-1 \\ x=-y \end{cases}$$

(каждая из этих систем уравнений имеет следствием $x^3+y^3+z^3=x+y+z=(x+y+z)^3$). Эти прямые лежат в трех параллельных плоскостях: $x+y+z=0$, $x+y+z=1$, $x+y+z=-1$; в первой из этих плоскостей прямые пересекаются в точке (0,0,0), а в двух других образуют равносторонние треугольники.

Остальные 18 прямых обозначим, для удобства в дальнейшем, буквами **a**, **b**, ..., **r**. Шесть из этих прямых имеют простые уравнения:

$$(\mathbf{f})\ \begin{cases} x=0 \\ y=z+1 \end{cases} \qquad (\mathbf{j})\ \begin{cases} y=0 \\ z=x+1 \end{cases} \qquad (\mathbf{b})\ \begin{cases} z=0 \\ x=y+1 \end{cases}$$

$$(\mathbf{g})\ \begin{cases} x=0 \\ y=z-1 \end{cases} \qquad (\mathbf{k})\ \begin{cases} y=0 \\ z=x-1 \end{cases} \qquad (\mathbf{c})\ \begin{cases} z=0 \\ x=y-1 \end{cases}$$

(Чтобы найти эти уравнения, рассмотрим пересечения поверхности (2) с плоскостями $x=0$, $y=0$ и $z=0$. Например, подставим $x=0$ в уравнение (2): $4(y^3+z^3)=(y+z)^3+3(y+z)$, откуда $3x^3+3y^3=3yz(y+z)+3(y+z)$, поэтому либо $y+z=0$, либо $y^2-yz+z^2=yz+1$, т. е. $(y-z)^2=1$,

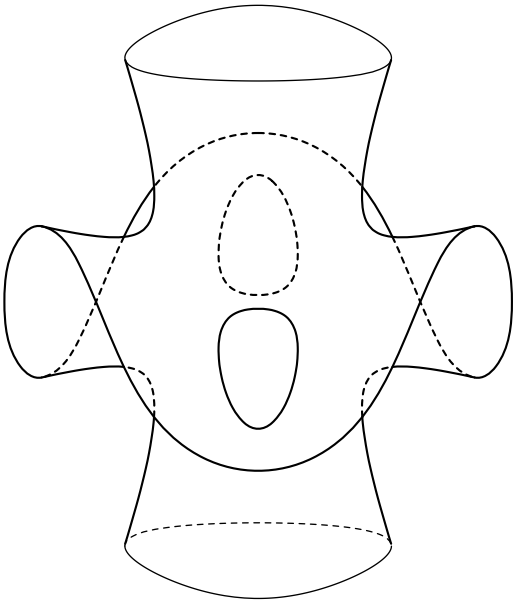


Рис. 6. *Кубическая поверхность* (2)

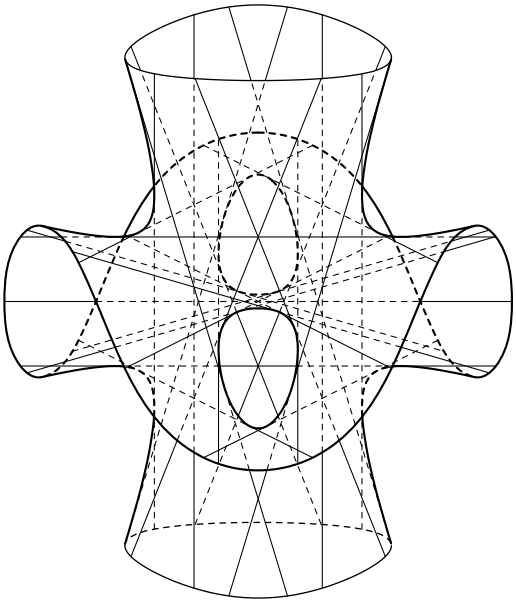


Рис. 7. *Поверхность с 27 прямыми*

$y-z=\pm 1$. Одно из трех полученных уравнений задает прямую (1), а два других совпадают с (**f**) и (**g**). Случаи $y=0$, $z=0$ аналогичны.)

Уравнения оставшихся 12 прямых включают «золотое сечение» $\varphi = \dfrac{1+\sqrt{5}}{2}$. Они имеют вид

$$(\mathbf{a})\ \begin{cases} x=\varphi(y+z) \\ y=z+\varphi \end{cases} \qquad (\mathbf{e})\ \begin{cases} y=\varphi(z+x) \\ z=x+\varphi \end{cases} \qquad (\mathbf{i})\ \begin{cases} z=\varphi(x+y) \\ x=y+\varphi \end{cases}$$

$$(\mathbf{l})\ \begin{cases} x=\varphi(y+z) \\ y=z-\varphi \end{cases} \qquad (\mathbf{d})\ \begin{cases} y=\varphi(z+x) \\ z=x-\varphi \end{cases} \qquad (\mathbf{h})\ \begin{cases} z=\varphi(x+y) \\ x=y-\varphi \end{cases}$$

и

$$(\mathbf{o})\ \begin{cases} x=-\varphi^{-1}(y+z) \\ y=z+\varphi^{-1} \end{cases} \qquad (\mathbf{q})\ \begin{cases} y=-\varphi^{-1}(z+x) \\ z=x+\varphi^{-1} \end{cases} \qquad (\mathbf{m})\ \begin{cases} z=-\varphi^{-1}(x+y) \\ x=y+\varphi^{-1} \end{cases}$$

$$(\mathbf{p})\ \begin{cases} x=-\varphi^{-1}(y+z) \\ y=z-\varphi^{-1} \end{cases} \qquad (\mathbf{r})\ \begin{cases} y=-\varphi^{-1}(z+x) \\ z=x-\varphi^{-1} \end{cases} \qquad (\mathbf{n})\ \begin{cases} z=-\varphi^{-1}(x+y) \\ x=y-\varphi^{-1} \end{cases}$$

(предоставляем читателю подставить эти 12 равенств в уравнение (2) и проверить, что полученные прямые лежат на поверхности).

Диаграммы на рис. 8, 9 показывают сечения нашей поверхности 12 различными плоскостями вида $x+y+z=\text{const}$ (с центрами в точках вида $x=y=z$). Показаны также следы прямых (**a**) — (**r**). Можно видеть, что в каждой из областей $x+y+z>1$ и $x+y+z<1$ поверхность состоит из «центральной трубы» и трех «крыльев». В области $-1\leqslant x+y+z\leqslant 1$ эти крылья сливаются с трубой; в этой области содержатся 9 прямых (**1**)–(**9**). Среди остальных 18 прямых шесть (три пары параллельных (**m**)–(**r**)) лежат на крыльях, а 12 (шесть пар параллельных (**a**)–(**l**)) — на центральной трубе. Конфигурация этих прямых показана на рис. 10. □

8. Некоторые другие поверхности

Существуют и другие кубические поверхности с обширными семействами вещественных прямых. Кратко обсудим некоторые из них.

Рассмотрим семейство поверхностей

$$x^3+y^3+z^3-1=\alpha(x+y+z-1)^3. \tag{3}$$

Теорема 3. *Если* $\alpha>\dfrac{1}{4}$ *и* $\alpha\neq 1$, *то поверхность* (3) *содержит* 27 *вещественных прямых.*

Доказательство. Три прямых очевидны: $\{x=1,\ y=-z\}$ и еще две, получаемые перестановкой переменных x, y, z. Еще четыре имеют вид $\{x=u, y+z=0\}$, $\{x=1, y+uz=0\}$, где u — одно из решений квадратного

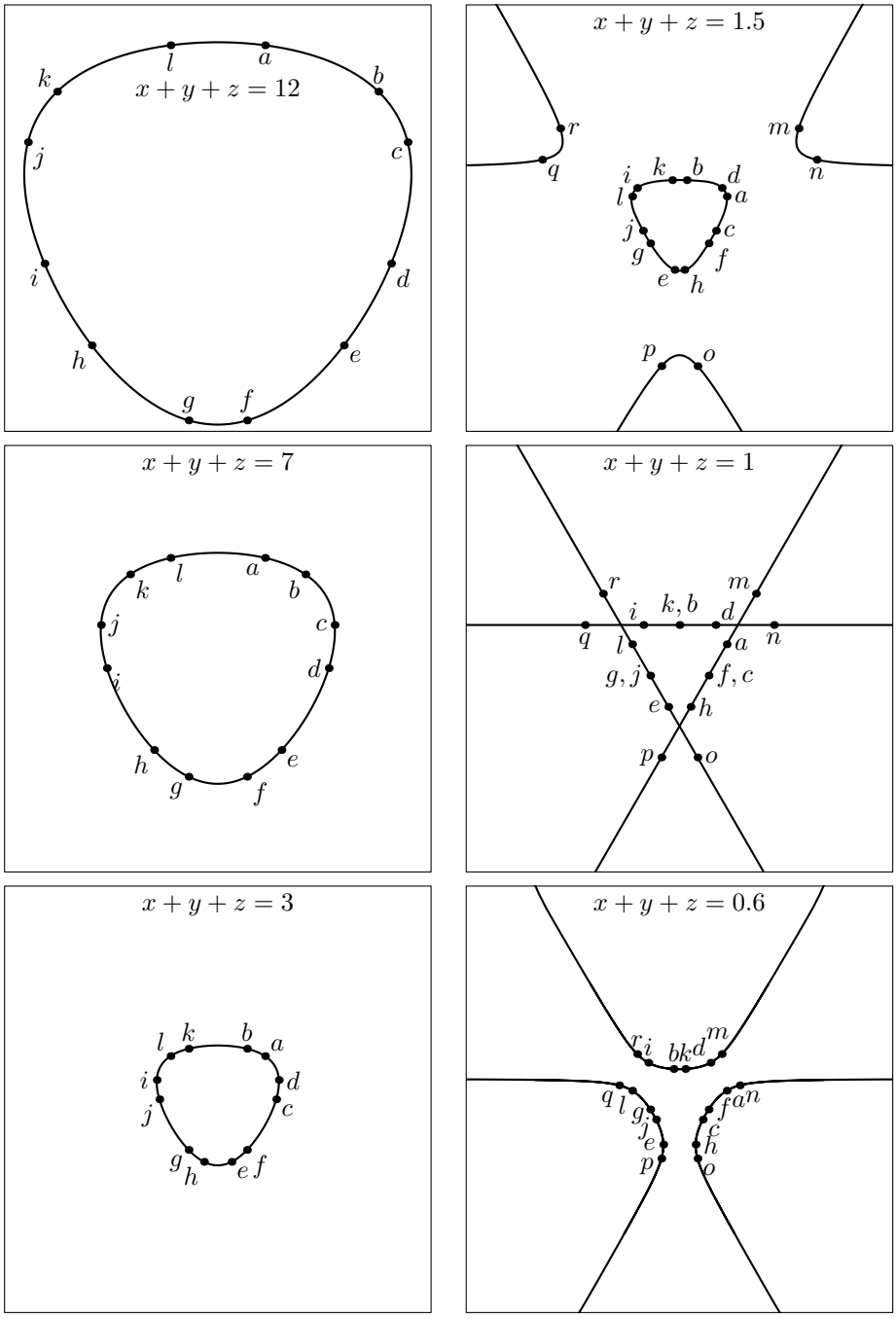


Рис. 8. *Сечения поверхности* (2)

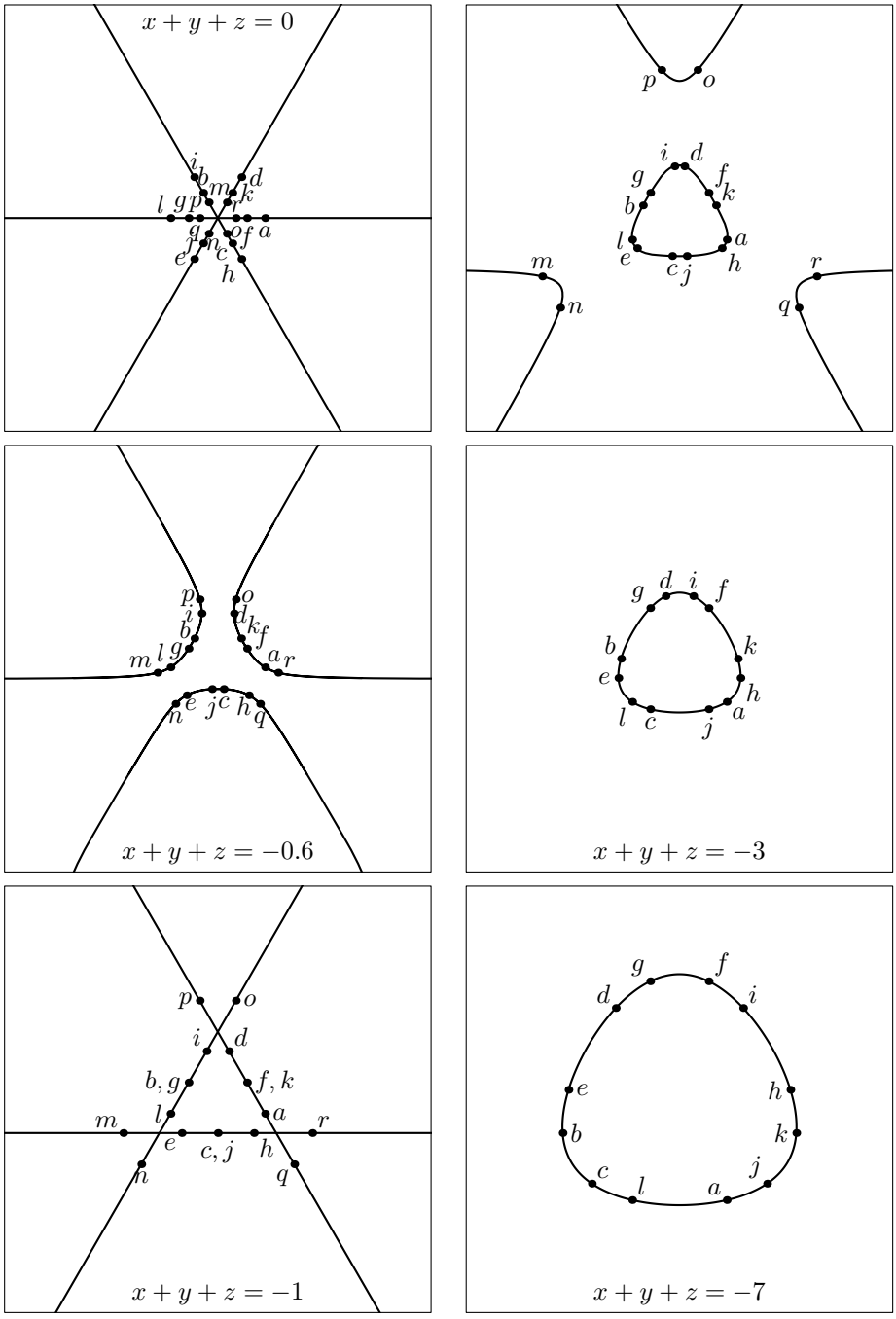


Рис. 9. *Сечения поверхности* (2)*, продолжение*

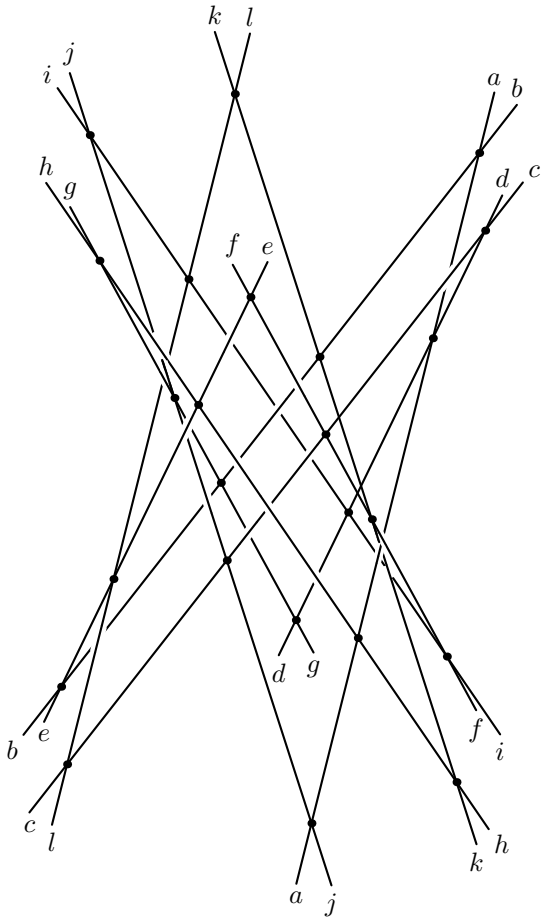


Рис. 10. *Прямые на трубе*

уравнения

$$(\alpha - 1)(u - 1)^2 = 3u,$$

и еще восемь вновь получаются перестановкой x, y, z. Наконец, еще четыре имеют вид $\{x + v^2(y + z) = 0\}$, $\{y - z = 2v - v^3(y + z)\}$, где v — одно из четырех решений уравнения

$$(4\alpha - 1)(v^2 - 1)^2 = 3v^2,$$

а перестановка переменных x, y, z опять дает еще восемь прямых. Всего получается 27. □

В случае $\alpha = 1/4$ уравнение (3) задает поверхность с «особыми точками» $(1, 1, 1)$, $(1, -1, -1)$, $(-1, 1, -1)$, $(-1, -1, 1)$ (в окрестности каждой из

этих точек поверхность похожа на конус). На этой поверхности имеется лишь 9 прямых: $\{x = 1, y = z\}$, $\{x = 1, y = -z\}$, $\{x = -1, y = -z\}$, и можно получить еще шесть, меняя местами x, y, z.

Случай $\alpha = 1$ особенно интересен. Чтобы придать этой поверхности более привлекательный вид, следует выбрать (непрямоугольную) систему координат, в которой точки (0,0,0), (1,0,0), (0,1,0), (0,0,1) (принадлежащие поверхности) являются вершинами правильного тетраэдра. Тогда все симметрии пространства, отображающие тетраэдр в себя, отображают и поверхность в себя. Предоставляем читателю найти уравнения прямых на этой поверхности (см. упражнение 1).

9. Конфигурация 27 прямых

Легко видеть из рис. 8, 9 и особенно 10, что между 27 прямыми имеется много пересечений. На самом деле эти пересечения подчинены очень строгим правилам, одинаковым для всех кубических поверхностей. Как обычно, не будем различать пересекающиеся и параллельные прямые и потому будем говорить не о пересекающихся, а о компланарных прямых. Первое их свойство очевидно.

Теорема 4. *Если какие-то две прямые на нашей поверхности компланарны, то на поверхности существует еще ровно одна прямая, принадлежащая той же плоскости.*

Доказательство. Пересечение кубической поверхности с плоскостью является кубической кривой на плоскости, т. е. определяется уравнением степени 3. Если это пересечение содержит две различные прямые, то уравнение кривой делится на уравнения прямых, и после деления мы получаем уравнение степени 1, которое определяет третью прямую. □

Следующая теорема полностью описывает свойства компланарности рассматриваемых прямых.

Теорема 5. *Пусть ℓ_1 — любая из 27 прямых на кубической поверхности S.*

(1) *Существует ровно 10 прямых на S, компланарных с ℓ_1; обозначим их $\ell_2, \dots, \ell_{11}$. Из этих 10 прямых можно составить 5 пар взаимно компланарных прямых ℓ_2, ℓ_3; ℓ_4, ℓ_5; $\dots$; ℓ_{10}, ℓ_{11}. Никакие другие две прямые среди $\ell_2, \dots, \ell_{11}$ не компланарны.*

(2) *Каждая из остальных 16 прямых $\ell_{12}, \dots, \ell_{27}$ компланарна ровно с одной прямой из каждой пары в (1). Для любых двух прямых среди $\ell_{12}, \dots, \ell_{27}$ количество прямых среди $\ell_2, \dots, \ell_{11}$, компланарных с обеими, нечетно.*

(3) *Две прямые среди* $\ell_{12}, \dots, \ell_{27}$ *компланарны тогда и только тогда, когда существует ровно одна прямая среди* $\ell_2, \dots, \ell_{11}$, *компланарная с обеими* (*т. е. в данном случае нечетное количество из утверждения* (2) *равно* 1).

Замечательно, что все эти утверждения справедливы независимо от того, какую из 27 прямых взять в качестве ℓ_1.

Мы не будем доказывать эту теорему, но для поверхности из раздела 7 ее можно проверить с помощью диаграмм (рис. 7, 9, 10) и/или уравнений. Например, прямая **a** компланарна с каждой из прямых

$$(\mathbf{1}), \mathbf{l};\ (\mathbf{5}), \mathbf{h};\ (\mathbf{9}), \mathbf{d};\ \mathbf{b}, \mathbf{r};\ \mathbf{j}, \mathbf{n}.$$

Здесь показаны также пять пар взаимно компланарных прямых. Любая из остальных прямых компланарна с одной прямой из каждой пары. Например:

прямая **c** компланарна с **l**, (**5**), **d**, **b**, **j**;

прямая **f** компланарна с **1**, (**5**), **9**, **r**, **n**;

прямая **m** компланарна с **l**, (**5**), **d**, **r**, **n**.

Пятерки прямых, компланарных с **c** и **f**, содержат лишь одну общую прямую (**5**), и прямые **c** и **f** компланарны. Напротив, пятерки прямых, компланарных с **c** и **m**, содержат три общих прямых **l**, (**5**) и **d**, и прямые **c** и **m** не компланарны.

Некоторые другие свойства рассматриваемых прямых вытекают из теоремы 5. Предоставляем их читателю в качестве упражнений.

10. Заключение. Другие перечислительные проблемы в алгебраической геометрии

Проблемы подсчета количества алгебраических кривых данной степени (скажем, прямых), пересекающих некоторые другие кривые и/или касательных еще к каким-то кривым, стали ныне весьма популярными ввиду их значения в современной теоретической физике (конкретнее, в квантовой теории поля, см. [2, 3]). Здесь мы кратко обсудим одну из таких проблем, которая интересна неожиданным ответом и драматической двухсотлетней историей.

Вопрос. Даны 5 коник (= эллипсов, гипербол, парабол). Сколько коник касательны ко всем им?

(Почему 5? Потому что для 4 коник количество общих касательных коник бесконечно, а для типичного семейства из 6 коник вообще не существует общих касательных коник.)

Эта проблема была впервые рассмотрена Штейнером. В начале XIX века он опубликовал свой результат: существует 7736 таких коник. Однако

этот ответ многим казался сомнительным. Через несколько десятилетий после работы Штейнера де Жонкьер повторил его выкладки и получил иной результат. Но репутация Штейнера в среде математиков была столь высока, что де Жонкьер не решился опубликовать свою работу. В конце концов правильный ответ был найден в 1864 г. Шалем: существуют 3264 коники, касательные к 5 данным коникам.

Шаль, однако, учитывал комплексные коники, и осталось неясным, сколько из них могут быть вещественными. В 1997 г. Ронга, Тоньоли и Вуст нашли семейство из 5 эллипсов, для которого все 3264 касательных коники вещественны. А в 2005 г. Вельшингер доказал, что для семейства из 5 вещественных коник с попарно непересекающимися внутренностями не менее 32 из 3264 касательных коник вещественны.

11. Упражнения

Упражнение 1. Найдите уравнения всех прямых на поверхности

$$x^3 + y^3 + z^3 - 1 = (x + y + z - 1)^3.$$

Указания. (a) Существует лишь 24 прямых на этой поверхности; остальные 3 оказываются бесконечно удаленными.

(b) Через каждую вершину тетраэдра, описанного в разделе 8, проходят ровно три прямых; они параллельны трем сторонам грани, противоположной этой вершине. Это дает 12 прямых.

(c) Уравнения остальных 12 прямых содержат золотое сечение.

Упражнение 2. Найдите прямые на поверхности

$$xyz + \beta(x^2 + y^2 + z^2) = \gamma.$$

Упражнение 3. Среди 27 прямых на кубической поверхности имеется ровно 45 компланарных троек прямых.

Замечание. Некоторые компланарные тройки из раздела 7 состоят из прямых, которые проходят через одну точку (таких троек семь) или попарно параллельны (таких троек две). Следует рассматривать эти свойства как случайные, на произвольной кубической поверхности такого не происходит.

Упражнение 4. Максимальное количество попарно некомпланарных прямых равно 6. Существует ровно 72 таких шестерки.

Упражнение 5. Количество перестановок 27 прямых, которые переводят компланарные прямые в компланарные, равно $51830 = 2^7 \cdot 3^4 \cdot 5$. (Эти перестановки образуют группу, известную в теории групп как E_6.)

Список литературы

[1] Манин Ю. И. *Кубические формы: алгебра, геометрия, арифметика*. М.: Наука, Физматлит. 1972.

[2] D. Cox, S. Katz. *Mirror symmetry and algebraic geometry*. Amer. Math. Soc., Providence, RI, 1999.

[3] S. Katz. *Enumerative geometry and string theory*. Amer. Math. Soc., Providence, RI, 2006.

[4] B. Segre. *The non-singular cubic surfaces*. Oxford University Press, Oxford, 1942.

С. Л. Табачников: Pennsylvania State University
Д. Б. Фукс: University of California, Davis

a-Диаметры и турановские графы

С. Б. Гашков

1. Введение

Назовем *a-диаметром* произвольную пару точек множества, расстояние между которыми не меньше aD, где D — диаметр этого множества (максимальное расстояние между его точками). Максимальное число a-диаметров у n-элементного плоского множества обозначим $N_2(a, n)$. Предыдущее определение очевидно можно ввести и пространственном случае (тогда в обозначениях появляется индекс 3).

Задача о вычислении максимального числа a-диаметров была поставлена П. Эрдёшем [1] (и впоследствии им же решена). Так как она совершенно элементарна, то представляет интерес даже для школьников, и не случайно, что ее формулировка появилась в задачнике [2]. Однако решения этой задачи там нет, вероятно потому что работы Эрдёша и соавторов, содержащие ее решение, оказались неизвестными И. М. Яглому в момент написания книги [2].

Автор настоящей заметки около двадцати лет назад придумал ее решение (как выяснилось впоследствии, в основном совпадающее с решением Эрдёша, что не удивительно), которое кажется небесполезным вместе со связанными с ним другими интересными задачами предложить вниманию читателя[1)].

Для формулировки теоремы понадобится одно определение, а для доказательства — одна лемма (на самом деле это известная теорема Турана).

Определим $k_2(a)$ как наибольшее число точек в плоском множестве, в котором любая пара точек образует a-диаметр. Аналогичное определение можно ввести и для трехмерного (и вообще d-мерного) пространства. Для краткости индекс, указывающий размерность, далее опускается.

[1)] Я узнал о существовании четырех работ Эрдёша с соавторами, посвященными этой задаче, от А. Ф. Сидоренко, который тогда еще был в Москве, и хотя он любезно дал мне посмотреть эти работы, я не догадался записать их адреса, и поэтому сейчас не знаю, как сделать на них ссылку в библиографии.

2. Теорема Эрдёша об оценке максимального числа a-диаметров

Теорема 1 (Эрдёш – Шош – Туран). *Для любого a, $0 < a < 1$, и $n = k(a)q + r$, где $0 \leqslant r < k(a)$ и q — целое число, справедливо равенство*

$$N(a,n) = \frac{k(a)-1}{2k(a)}(n^2 - r^2) + \frac{r(r-1)}{2}.$$

Для доказательства нижней оценки достаточно указать n-элементное множество с $N(a,n)$ диаметрами. Обозначим $K(a)$ какое-нибудь $k(a)$-элементное множество, в котором любая пара точек образует a-диаметр. Существование такого множества вытекает из определения $k(a)$, из него также следует существование положительного ϵ, такого что расстояние между любыми двумя точками из множества $K(a)$ больше $ad + (a+1)\epsilon$, где d — диаметр $K(a)$. Пусть $n = k(a)q + r$, $0 \leqslant r < k(a)$. Опишем окружности радиуса $\epsilon/2$ с центрами в точках множества $K(a)$. Внутри каждой из первых r окружностей выберем по $q+1$ точке (полученные множества точек обозначим $M_1, \ldots, M_r$), а внутри каждой из остальных $k(a) - r$ окружностей выберем по q точек (полученные множества точек обозначим $M_{r+1}, \ldots, M_{k(a)}$). Объединение M указанных множеств M_i содержит $(q+1)r + q(k(a) - r) = qk(a) + r = n$ точек. Для любых двух точек x, y из полученного множества расстояние между ними в силу неравенства треугольник не больше $d + \epsilon$, поэтому диаметр этого множества не больше $d + \epsilon$. Если x, y взяты из разных множеств M_i, то согласно неравенству треугольника расстояние между x и y больше $ad + (a+1)\epsilon - \epsilon = a(d + \epsilon)$, поэтому любая пара точек из разных множеств M_i образует a-диаметр множества M. Так как число пар точек, принадлежащих одному множеству M_i, равно $(q+1)q/2$ для $q+1$-элементных множеств, и равно $q(q-1)/2$ для остальных $k(a)-r$ множеств, а общее число пар точек равно $n(n-1)/2$, то число a-диаметров не меньше

$$n(n-1)/2 - r(q+1)q/2 - (k(a)-r)q(q-1)/2 = \\ = \frac{k-1}{2k}(n^2 - r^2) + \frac{r(r-1)}{2}.$$

Нижняя оценка доказана.

Для доказательства верхней оценки в произвольном n-элементном множестве отрезки, являющиеся a-диаметрами, покрасим в белый цвет, а остальные отрезки — в черный. Из определения $k(a)$ следует, что в этом множестве не существует $k(a)+1$-элементного подмножества, все отрезки которого белого цвета.

Применяя следующую далее теорему Турана получаем верхнюю оценку.

3. Теорема Турана об экстремальных графах

Эта теорема является одной из первых теорем теории экстремальных графов (этой теории уже посвящены целые книги, например книга Б. Боллобаша *Extremal graph theory*, но на русском языке, кажется, их переводов не появлялось). Доказанная в 1941 году теорема Турана [3] довольно популярна в литературе, связанной с теорией графов, у нее известно много доказательств, есть она и в некоторых книгах на русском языке, например в [4–6] (в последней, правда, без доказательства). Но общеизвестной, пожалуй, ее считать нельзя (да и доказательства в [4,5] написаны так, что их непросто воспринять, не вникая в контекст), поэтому представляется разумным дать ее здесь с доказательством (которое, как недавно стало понятно автору, весьма близко к доказательству из [7], и доказательству самого Турана).

Теорема 2 (Туран). *Отрезки, соединяющие пары точек n-элементного множества, покрашены в белый и черный цвета так, что среди любых его $k+1$ точек найдется хотя бы одна пара, соединенная белым отрезком. Тогда черных отрезков у этого множества не больше*

$$\frac{k-1}{2k}(n^2-r^2)+\frac{r(r-1)}{2},$$

где $n=kq+r$, $0\leqslant r<k$, q — целое число, причем для любых n,k эта оценка достигается.

Для доказательства применим индукцию по n. База индукции ($n\leqslant k$) очевидна. Шаг индукции. Выберем максимальное подмножество, в котором все отрезки между точками черные. Если в нем менее k точек, добавим к нему несколько точек, чтобы получилось k-точечное множество K. Остальные точки образуют $(n-k)$-точечное множество L. Применяя к нему предположение индукции, получаем что в нем не более $\frac{k-1}{2k}((n-k)^2-r^2)+\frac{r(r-1)}{2}$ черных отрезков. Для каждой точки x из L во множество K выходит не более $k-1$ черных отрезков (потому, что в противном случае, добавляя x к выбранному максимальному подмножеству, получаем большее подмножество, в котором все отрезки черные), поэтому общее число черных отрезков не больше

$$\frac{k-1}{2k}((n-k)^2-r^2)+\frac{r(r-1)}{2}+(n-k)(k-1)+\frac{k(k-1)}{2}=$$
$$=\frac{k-1}{2k}(n^2-r^2)+\frac{r(r-1)}{2}.$$

Покажем, что оценка теоремы всегда достигается. Действительно, разобьем n точек на r групп по $q+1$ точке и $k-r$ групп по q точек. Точки из разных групп соединим черными отрезками, а точки из одной

группы — белыми (получается k-дольный граф, если использовать терминологию теории графов; это единственный такой граф, у которого доли различаются по количеству вершин не более чем на 1). Очевидно, среди любых $k+1$ точки найдется пара точек, лежащие в одной группе и соединенные поэтому белым отрезком. Общее число белых отрезков равно $r(q+1)q/2+(k-r)q(q-1)/2 = (n(q-1)+r(q+1))/2$, поэтому общее число черных отрезков равно

$$n(n-1)/2 - (n(q-1)+r(q+1))/2 = \frac{k-1}{2k}(n^2-r^2) + \frac{r(r-1)}{2}.$$

На самом деле экстремальный турановский граф всегда определяется однозначно. Это мы предоставляем доказать читателю самостоятельно.

В книге [8] доказательство теоремы Турана опущено, «как не содержащее вероятностных аспектов». С того времени найдены и такие доказательства, см. [9], где эта теорема выводится из следующей теоремы Каро и Уэя.

Обозначим d_v степень вершины v в данном графе (в нашей терминологии это число *белых* отрезков, выходящих из точки v), и через k — максимальный размер *независимого множества вершин* в этом графе (в независимом множестве никакие две точки не соединяются ребром; в нашей в нашей терминологии это означает, что что среди любых его $k+1$ точек найдется хотя бы одна пара, соединенная белым отрезком, и найдется множество из k точек, соединенных только черными отрезками). Тогда справедлива

Теорема 3 (Каро – Уэй). *Имеет место неравенство*

$$k \geqslant \sum_v \frac{1}{d_v+1}.$$

Еще три доказательства теоремы Турана имеются в [10].

Частным случаем теоремы Турана (на самом деле открытом в 1907 г. Мантелем [11]) является следующая теорема, предлагавшаяся в качестве задачи в 1969 г. на Всесоюзной олимпиаде школьников при $n = 20$.

Теорема 4 (Мантель). *В компании из n человек среди любых трех найдется хотя бы одна пара незнакомых. Тогда число пар знакомых не больше $n^2/4$.*

Теорему эту несложно доказать по индукции (повторяя в этом частном случае доказательство общей теоремы), но у нее есть красивое и более короткое доказательство, предложенное болгарскими математиками Хаджиивановым и Неновым.

Вот оно. Пусть наибольшее число знакомых у одного человека равно a. Рассмотрим этого человека и всех незнакомых с ним. Очевидно в этой

компании $n-a$ человек, а остальные a человек не знакомы друг с другом (так как знакомы с одним человеком). Каждый из первой компании имеет не более a знакомых, поэтому общее число пар знакомых не более $a(n-a)$ (так как знакомых, не принадлежащих этой компании, быть не может). Остается заметить, что $a(n-a) \leqslant n^2/4$.

Подобным же методом можно доказать более общее утверждение, являющееся некоторым ослаблением теоремы Турана (но при n кратном k совпадающей с ней).

Теорема 5. *Пусть в компании из n человек среди любых $(k+1)$ из них найдется хотя бы одна пара незнакомых. Тогда число пар знакомых не больше*

$$\frac{k-1}{2k}n^2.$$

Действительно, применим индукцию по k. База индукции ($k=2$) уже доказана. Выполним шаг индукции. Пусть наибольшее число знакомых у одного человека равно a. Рассмотрим этого человека и всех незнакомых с ним. Очевидно в этой компании $n-a$ человек, а для остальных a человек верно следующее: среди любых k из них найдутся двое незнакомых. Поэтому согласно предположению индукции общее число знакомых пар во второй компании не больше $\dfrac{k-2}{2(k-1)}a^2$. Каждый из первой компании имеет не более a знакомых, поэтому общее число пар знакомых не более

$$a(n-a)+\frac{k-2}{2k-2}a^2 \;=\; \frac{2k-2}{k}\frac{ka}{2k-2}\left(n-\frac{ka}{2k-2}\right) \;\leqslant\; \frac{2k-2}{k}\frac{n^2}{4} \;=\; \frac{k-1}{2k}n^2.$$

В книге [6] в виде задачи (но без решения) приведено некоторое усиление теоремы Мантеля. В частном случае $n=8$ эта задача предлагалась автором в 1983 году на Московской олимпиаде в следующем виде.

Теорема 6. *В пространстве выбрано n точек, никакие 4 из них не лежат в одной плоскости. Проведен $\lfloor n^2/4 \rfloor + 1$ отрезок, у каждого из которых оба конца являются выбранными точками. Доказать, что эти отрезки образуют не менее $\lfloor n/2 \rfloor$ треугольников, причем большего количества треугольников может и не получиться. Если же проведен $\lfloor n^2/4 \rfloor$ отрезок, то треугольников может не быть вообще.*

Здесь $\lfloor x \rfloor = \max\{n : n \leqslant x, n \in \mathbb{N}\}$ — функция *целая часть снизу*.

Доказательство читатель может найти в сборнике задач московских олимпиад [13].

4. Отступление в сторону: проблема Турана

Туран поставил следующую проблему, решение которой было бы обобщением его теоремы. Нужно найти $T(n,k,l)$ — наименьшее число l-элементных подмножеств в данном n-элементном множестве E_n таких, что

любое k-элементное подмножество E_n обязательно содержит хотя бы одно из этих l-элементных подмножеств (сейчас числа $T(n,k,l)$ называются, разумеется, *числами Турана*). В случае $l=2$ получается в точности теорема Турана.

Если произвольному l-элементному подмножеству M множества E_n сопоставить множество $S_k(M)$ всех k-элементных подмножеств множества E_n, содержащих M, то задача Турана превращается в частный случай общей *задачи о покрытии*, точнее задачи о нахождении минимального покрытия данного множества подмножествами из заданной системы его подмножеств. В качестве этого множества нужно взять множество $P_k(E_n)$ всех k-элементных подмножеств E_n, а в качестве данной системы его подмножеств — все определенные выше множества $S_k(M)$.

Любую конкретно заданную задачу о покрытии можно решить тривиальным переборным алгоритмом. Но такие алгоритмы требуют экспоненциального (относительно мощности заданной системы подмножеств) числа используемых в них элементарных операций. Существование алгоритма с полиномиальным числом операций для произвольной задачи о покрытии (и даже многих ее частных случаев) проблематично — этот вопрос равносилен так называемой *проблеме об NP-полноте.*(К этой же проблеме сводится вопрос о существовании полиномиального алгоритма находящего максимальное независимое подмножество в любом заданном графе; примером задачи о нахождении максимального независимого множества является известная задача о расстановке максимального числа не угрожающих друг другу ферзей на шахматной доске.) Проблема об NP-полноте видимо еще долго будет ждать своего решения. Поэтому не удивительно, что вопрос Турана о вычислении точного значения $T(n,k,l)$ в общем случае тоже пока остается без ответа. Несколько частных случаев, в которых ответ известен (часть из них была найдена Катоной, Неметцем, Симановичем, а остальные — А. Ф. Сидоренко), перечислены в [12]. Сам Туран предположил, что $T(2n,5,3)=2\binom{n}{3}$, но кажется и эта очень естественная гипотеза пока не доказана. Верхние и нижние оценки для $T(n,k,l)$ приведены в [8]. Наиболее простую из них, а именно

$$T(n,k,l)\geqslant \binom{n}{l}\Big/\binom{k}{l},$$

читатель может попробовать доказать самостоятельно.

В [8] введены также еще три комбинаторных числа, определения которых похожи на определение чисел Турана $T(n,k,l)$. Например, *число Эрдёша – Ханани* $M(n,k,l)$, в каком-то смысле двойственное к числу Турана $T(n,k,l)$. Действительно, $T(n,k,l)$ можно определить как минимальное число l-множеств, покрывающих все k-множества, а $M(n,k,l)$ определяется как минимальное число k-множеств, покрывающих все l-множества

(это значит, что каждое l-множество содержится хотя бы в одном из выбранных k-множеств). Тот, кто знает, что такое *n-мерный двоичный куб* (иногда называемый *булеаном*), обе эти задачи легко сможет сформулировать в терминах минимальных покрытий множества всех вершин k-слоя n-мерного куба вершинами l-го слоя и наоборот.

Читатель легко сам докажет, что

$$M(n,k,l) \geqslant \binom{n}{l} / \binom{k}{l}.$$

Равенство здесь возможно тогда и только тогда, когда существует такая система k-множеств, в которой любые два множества не имеют общего l-множества (т. е. имеют пересечение мощности меньшей l), и каждое l-множество содержится в одном (и только в одном) k-множестве. Такие системы множеств известны под названием *тактических конфигураций* и активно изучаются в конструктивной комбинаторике. В частном случае $k = 3$, $l = 2$ общие тактические конфигурации превращаются в так называемые *тройки Штейнера* (названные в честь знаменитого геометра).

С задачей Эрдёша – Ханани о вычислении $M(n,k,l)$ дела обстоят, по-видимому, лучше, чем с задачей Турана. В 1985 г. Рёдль доказал гипотезу Эрдёша – Ханани о том, что

$$\lim_{n\to\infty} \frac{M(n,k,l)}{\binom{n}{l}/\binom{k}{l}} = 1.$$

Здесь пора закончить слишком затянувшееся отступление и вернуться к основной теме.

5. Еще одна задача Эрдёша

Для конкретного применения теоремы Эрдёша – Турана – Шош надо уметь вычислять в явном виде функцию $k_d(a)$. Эта задача очевидно сводится к вычислению функции $m_d(n)$, определение которой дается ниже в частном случае $d = 2$ (в общем случае оно дается аналогично).

Обозначим $m(M)$ минимальное расстояние между точками n-элементного множества M, а через $m_2(n)$ обозначим максимальное значение $m(M)$, которое может быть у n-точечного плоского множества M единичного диаметра. Аналогичная величина для трехмерных множеств обозначается $m_3(n)$.

Читателю предлагается самому проверить, что $k_d(a) = n$ если и только если $m_d(n+1) \leqslant a < m_d(n)$.

Очевидно, что $m_2(2) = m_2(3) = 1, m_3(2) = m_3(3) = m_3(4) = 1$.

Чуть менее очевидно, что $m_2(4) = 1/\sqrt{2}$. Единственная экстремальная конфигурация в этом случае есть есть просто квадрат с единичной диагональю. Действительно, если выпуклая оболочка есть треугольник

(возможно вырождающийся в отрезок), то одна из его сторон видна из четвертой точки (лежащей внутри его) под углом не меньшим $2\pi/3$, поэтому согласно теореме косинусов квадрат длины этой стороны не меньше $2m(M)^2 + 2m(M)^2 \cos 2\pi/3 = 3m(M)^2$, откуда имеем, что $m(M) \leqslant 1/\sqrt{3} < < 1/\sqrt{2}$, и, если наконец M совпадает с множеством вершин выпуклого четырехугольника, то наибольший из его углов тупой или прямой, поэтому согласно теореме косинусов квадрат длины лежащей против него диагонали не меньше $2m(M)^2$, откуда имеем, что $m(M) \leqslant 1/\sqrt{2}$, причем равенство возможно лишь когда все углы четырехугольника прямые и все его стороны равны, т. е. он является квадратом.

Покажем, что $m_2(5) = \dfrac{2}{1+\sqrt{5}}$, и единственная экстремальная конфигурация есть правильный пятиугольник с единичной диагональю.

Действительно, если конфигурация образует выпуклый пятиугольник $ABCDE$ (возможно вырожденный), то производя, если нужно, перестановку в обозначениях, можно считать, что угол ABC не меньше $3\pi/5$ (так как если все углы пятиугольника меньше $3\pi/5$, то их сумма меньше 3π, а это невозможно). Тогда согласно теореме косинусов $1 \geqslant |AC|^2 \geqslant \geqslant 2m(M)^2 + 2m(M)^2 \cos 3\pi/5$, откуда (после некоторых вычислений) имеем, что $m(M) \leqslant \dfrac{2}{1+\sqrt{5}}$, причем равенство возможно лишь когда все углы и все стороны у пятиугольника равны, т. е. он правильный. Если выпуклая оболочка множества M есть четырехугольник или треугольник (возможно вырождающийся в отрезок), то одна из точек M лежит внутри или на границе треугольника (возможно вырожденного), образованного тремя другими точками M, а в этом случае, как уже было показано выше, $m(M) \leqslant 1/\sqrt{3} < \dfrac{2}{1+\sqrt{5}}$.

Эрдёш и Бейтмен [14] доказали, что

$$m_2(6) = \frac{1}{\sin 2\pi/5}, \quad m_2(7) = \frac{1}{2}.$$

Читатель легко сможет догадаться, какие конфигурации являются здесь экстремальными, но доказать это так просто не удается.

Известный немецкий логик Шютте в [15] доказал d-мерные теоремы, частным случаем которых является

Теорема 7. *Справедливы равенства*

$$m_3(5) = \frac{1}{2}\sqrt{\frac{7}{3}}, \quad m_3(6) = \frac{1}{\sqrt{2}}.$$

Докажем первое равенство. Пусть диаметр множества A, B, C, D, E равен 1. Возможны два случая (без учета вырожденных): одна точка (например E)лежит в тетраэдре с вершинами в других точках или $ABCDE$ — выпуклый шестигранник, являющийся объединением двух тетраэдров с

общей гранью ($ABCD$ и $EBCD$). В первом случае одно из ребер, скажем AB, видно из E под углом φ, $\cos\varphi \leqslant -1/3$ согласно следующей далее лемме 1. Если предположить, что AE и BE больше $\frac{1}{2}\sqrt{\frac{3}{2}}$, то из теоремы косинусов следует противоречие:

$$1 \geqslant |AB|^2 = |AE|^2 + |BE|^2 - 2|AE| \cdot |BE| \cos\varphi > \frac{3}{4} + \frac{3}{4} \cdot \frac{1}{3} = 1$$

Поэтому в этом случае $m(ABCDE) \leqslant \min\{AE, BE\} \leqslant \frac{1}{2}\sqrt{\frac{3}{2}}$. Во втором случае прямая AE пересекает треугольник BCD в некоторой точке K. Согласно следующей далее второй лемме этот треугольник можно накрыть кругом радиуса $1/\sqrt{3}$, поэтому круги с этим радиусом и центрами в B, C, D накрывают этот треугольник, а значит и точку K, поэтому можно считать, что $BK \leqslant 1/\sqrt{3}$. Поэтому в треугольнике AEB высота $BL \leqslant BK \leqslant 1/\sqrt{3}$. Можно считать, что L лежит на отрезке AE (иначе выберем в этом треугольнике меньшую высоту и сменим обозначения). Так как $AE \leqslant 1$, то можно считать, что $AL \leqslant 1/2$. Тогда из теоремы Пифагора следует, что

$$|AB|^2 = |BL|^2 + |AL|^2 \leqslant \frac{1}{3} + \frac{1}{4} = \frac{7}{12}.$$

Поэтому $m(ABCDE) \leqslant AB \leqslant \frac{1}{2}\sqrt{\frac{7}{3}}$.

Если выбрать A, B, C, D, E так, что $BC = CD = BD = AE = 1$, $AE \perp BCD$, $AE \cap BCD = K$, $BK = CK = DK = 1/\sqrt{3}$, то

$$m(ABCDE) = EB = EC = ED = AB = AC = AD = \frac{1}{2}\sqrt{\frac{7}{3}}.$$

Нужная далее следующая лемма предлагалась автором в качестве задачи в 1982 г. на Всесоюзной олимпиаде.

Лемма 1. *Для любой внутренней точки тетраэдра одно из его ребер видно под углом, косинус которого не больше* $-1/3$.

Ее доказательство можно найти в сборнике задач всесоюзных олимпиад [16].

Мы приведем другой вариант доказательства. Пусть e_1, e_2, e_3, e_4 — единичные вектора, направленные из данной точки в вершины тетраэдра. Прямая, проходящая через e_4, пересекает трехгранный угол, образованный векторами e_1, e_2, e_3, поэтому для некоторых $x_i \geqslant 0$ имеем $x_1e_1 + \ldots + x_4e_4 = 0$. Возводя это равенство скалярно в квадрат и предполагая, что косинусы всех попарных углов между этими векторами больше $-1/3$, имеем

$$0 = \sum_{i=1}^{4} x_i^2 + 2 \sum_{1 \leqslant i < j \leqslant 4} x_i x_i (e_i, e_j) > \sum_{i=1}^{4} x_i^2 - \frac{2}{3} \sum_{1 \leqslant i < j \leqslant 4} x_i x_i = \\ = \frac{1}{3} \sum_{1 \leqslant i < j \leqslant 4} (x_i - x_j)^2 \geqslant 0.$$

Лемма доказана.

Система векторов, ведущих из центра правильного тетраэдра (в d-мерном пространстве — правильного симплекса) в его вершины, оказывается, называется *фреймом Мерседес-Бенц.* (см. [17]).

Лемма 2. *Справедливо неравенство $R \leqslant D/\sqrt{3}$, где под R понимается радиус наименьшего круга, накрывающего треугольник диаметра D.*

Действительно, диаметр — это наибольшая сторона, а угол против нее не больше 60°. Следовательно она видна из центра описанного круга под углом не больше 120°. Лемма доказана.

Второе равенство легко вытекает из не очень просто доказываемой теоремы Шютте о том, что множество $\{M_1, \ldots, M_n\}$ точек в трехмерном пространстве, такое, что все углы $M_i M_j M_k$ острые, существует лишь при $n = 3, 4, 5$. Действительно, если множество M состоит из шести точек, то согласно указанной теореме в нем найдется тупоугольный или прямоугольный треугольник, тогда квадрат его наибольшей стороны по теореме косинусов не меньше $2m(M)^2$, откуда имеем, что $m(M) \leqslant 1/\sqrt{2}$. Интересно, что равенство здесь достигается на двух различных конфигурациях. Одна из них — это правильный октаэдр с единичной диагональю, а вторая — правильная треугольная призма с квадратными боковыми гранями. За доказательством упомянутой теоремы Шютте читатель отсылается к книге [2], задача 32.

Читателю предлагается самому доказать, что $m_2(n)$ и $m_3(n)$ монотонно убывают (после указанных выше точных значений при малых n.) Точные формулы для этих последовательностей, кажется, неизвестны.

В [2] можно найти доказательство неравенств $\frac{1}{2\sqrt{n}} \leqslant m_2(n) \leqslant \frac{2}{\sqrt{n}}$, а в книге [18] — доказательство следующей теоремы более точной теоремы

Теорема 8 (Фейеш-Тот). *Справедливо равенство*

$$\lim_{n \to \infty} m_2(n) \sqrt{n} = \sqrt{\frac{\pi}{2\sqrt{3}}}.$$

Известно, что существует $\lim_{n \to \infty} m_3(n) \sqrt[3]{n}$.

Читатель теперь легко сам докажет, что

$k_2(a) = 3$ при $\frac{1}{\sqrt{2}} \leqslant a < 1$,

$k_2(a) = 4$ при $\frac{2}{1+\sqrt{5}} \leqslant a < \frac{1}{\sqrt{2}}$,

$k_2(a) = 5$ при $\dfrac{1}{\sin 2\pi/5} \leqslant a < \dfrac{2}{1+\sqrt{5}}$,
$k_2(a) = 6$ при $\dfrac{1}{2} \leqslant a < \dfrac{1}{\sin 2\pi/5}$,
$k_2(a) \geqslant 7$ при $a < \dfrac{1}{2}$,
$k_3(a) = 4$ при $\dfrac{1}{2}\sqrt{\dfrac{7}{3}} \leqslant a < 1$,
$k_3(a) = 5$ при $\dfrac{1}{\sqrt{2}} \leqslant a < \dfrac{1}{2}\sqrt{\dfrac{7}{3}}$,
$k_3(a) \geqslant 6$ при $a < \dfrac{1}{\sqrt{2}}$.

6. Задача Винце

Довольно близка к задаче Эрдёша следующая задача (по-видимому, предложенная Эрдёшем Винце). Найти $d(n)$ — максимальное значение $m(M)$, которое может быть у выпуклого n-угольника единичного диаметра.

Очевидно $d(3) = 1$.

Чуть менее очевидно, что $d(4) = 1/\sqrt{2}$.

Винце [19] доказал, что справедлива

Теорема 9. *Для n, не равного степени двойки, $d(n) = 2\sin\dfrac{\pi}{2n}$.*

Читатель легко сам докажет эту теорему, если воспользуется теоремой Рейнхардта (см. [20]). Для n, равного степени двойки, кажется, ответ неизвестен. Винце доказал, что для $n = 8$

$$d(8) > 2\sin\frac{\pi}{16}.$$

Обобщениями этой теоремы на многомерные пространства, видимо, никто не занимался.

7. О возможных обобщениях на произвольные метрические пространства

Функции $k_d(a)$ и $m_d(n)$ можно определить конечно не только для d-мерного евклидова пространства, но и для любого метрического пространства вообще, и тем самым обобщить теорему Эрдёша-Шош-Турана на произвольное *метрическое пространство*. Для некоторых пространств при этом задача о вычислении $k(a)$ и $m(n)$ оказывается совсем несложной. Например, если метрика в d-мерном действительном пространстве определяется равенством

$$\rho(x, y) = \max_i |x_i - y_i|, \quad x = (x_1, \ldots, x_d), y = (y_1, \ldots, y_d),$$

(иногда эту метрику называют *манхеттенской* или *метрикой городских улиц*), то

$$m(n) = \frac{1}{\lceil n^{1/d} \rceil - 1},$$

где $\lceil x \rceil = \min\{n : n \geqslant x, n \in \mathbb{N}\}$ — функция *целая часть сверху*. Читатель легко докажет этот факт самостоятельно.

В двумерном пространстве с метрикой

$$\rho(x, y) = |x_1 - y_1| + |x_2 - y_2|$$

функция $m(n)$ остается такой же. Однако уже в трехмерном пространстве все не так очевидно.

Задача о вычислении функции $m(n)$ для произвольного метрического пространства довольно близка к известной в теории приближений (поставленной в пятидесятые годы А. Н. Колмогоровым) задаче о вычислении *ϵ-емкости* компактных множеств. В теории приближений эта задача рассматривается в функциональных пространствах, которые в наиболее интересных случаях бесконечномерны. В конечномерных пространствах эта задача близка к известной с двадцатых годов задаче *о плотнейшей упаковке шаров* в пространстве (см. [18], [21]), задаче об упаковке кругов на сфере (см. [18]) и различным задачам о расположении точек на сфере (см., например, [17]). В дискретных пространствах с *метрикой Хэмминга* задача о плотнейшей упаковке шаров играет важную роль в *теории кодирования* с исправлением ошибок (см., например, [21]).

8. Задача Хопфа о диаметрах конечного множества

Рассмотрим частный случай задачи вычисления $N_d(a, n)$ при $a = 1$, который однако не покрывался доказательством теоремы Эрдёша – Шош – Турана. Это просто задача о максимальном числе диаметров у данного n-точечного множества.

Справедлива следующая

Теорема 10 (Хопф – Панвиц). *Максимальное число диаметров в n-угольнике (и в любом n-точечном множестве) равно n.*

В качестве задачи эта теорема предлагалась в 1965 году на международной олимпиаде. Одно из ее решений можно прочесть в сборнике задач международных олимпиад [23].

Эта теорема вытекает также из следующей теоремы, предлагавшейся в виде задачи в 1962 году на одной из венгерских олимпиад (почему вытекает, читатель легко сообразит сам).

Теорема 11. *Если в n-угольнике выбрано m попарно пересекающихся сторон или диагоналей, то $m \leqslant n$.*

В книге [24] приведено четыре (!) доказательства этой теоремы.

Далее предлагается еще одно доказательство, разбитое на задачи, оставленные читателю для самостоятельного решения.

Для произвольной фигуры M обозначим $b_M(\varphi)$ *длину проекции* этой фигуры на прямую, выходящую под углом φ из начала координат. Функция $b_M(\varphi)$ очевидно определена на отрезке от нуля до π и ее можно периодически продолжить на всю числовую ось с периодом π.

Шириной плоской фигуры называется минимальная ширина бесконечной полосы с параллельными прямыми краями, накрывающей эту фигуру.

Задача 1. Докажите, что минимум функции $b_M(\varphi)$ равен ширине фигуры M.

Здесь уместно сказать, что фигура, называется *фигурой постоянной ширины*, если для любой прямой минимальная ширина содержащей эту фигуру полосы с краями, параллельными этой прямой, не зависит от этой прямой. У этих фигур есть много интересных свойств (см. например [25]). Легко доказать (но это далее не понадобится), что диаметр фигуры постоянной ширины равен ее ширине.

Задача 2. Докажите, что если M — n-угольник, то функция $b_M(\varphi)$ непрерывна и имеет на отрезке от нуля до π поровну локальных максимумов и минимумов, причем и тех и других не более n.

Задача 3. Выведите из предыдущей задачи теорему Хопфа – Панвица.

Для $d = 3$ аналог теоремы Хопфа – Панвица имеет следующий вид $N_3(1, n) = 2n - 2$ и был доказан независимо в 1957 г. Грюнбаумом, Хеппешем и Страшевичем. Это довольно сложное доказательство можно прочесть в [2]. В многомерном случае, кажется, известны только верхние и нижние оценки, полученные Эрдёшем (см. [2]).

В заключение отметим, что есть еще много других задач о диаметрах точечных множеств, например связанных с *проблемой Борсука*. Заинтересовавшийся этим читатель может обратится к статье [26] и брошюре [27] и указанной в них литературе.

Список литературы

[1] Эрдёш П. *Aufgabe* 250. Elemente der Mathematik 10, 1955.

[2] Шклярский Д.О., Ченцов Н.Н., Яглом И.М. *Геометрические оценки и задачи из комбинаторной геометрии*. М.: Наука, 1974.

[3] Turan P. *On an extremal problem in graph theory* // Mat.Fiz.Lapok, 48 : 436–452.

[4] Оре О. *Теория графов* (любое издание).

[5] Зыков А.А. *Основы теории графов.* М.: Вузовская книга, 2004.

[6] Харари Ф. *Теория графов.* М.: Мир, 1973.

[7] Дистель Р. *Теория графов.* Новосибирск, изд. Института математики, 2002.

[8] Эрдёш П., Спенсер Дж. *Вероятностные методы в комбинаторике.* М.: Мир, 1976.

[9] Алон Н., Спенсер Дж. *Вероятностный метод.* М.: Бином. Лаборатория знаний, 2007.

[10] Айгнер М., Циглер Г. *Доказательства из книги.* М.: Мир, 2006.

[11] Mantel W. Wisk. Opgaven 10 (1907), стр.60.

[12] Баранов В.И., Стечкин Б.С. *Экстремальные комбинаторные задачи и их приложения.* М.: Физматлит, 2004.

[13] Гальперин Г.А., Толпыго А.К. *Московские математические олимпиады.* М.: Просвещение, 1986.

[14] Эрдёш П., Бейтман П. *Геометрические экстремумы, подсказанные одной леммой Безиковича* // Amer. Math. Monthly, 58(5), 1951, стр. 306–314.

[15] Шютте К. *Минимальный диаметр конечных точечных множеств с заданным минимальным расстоянием между двумя точками* // Math. Annalen, 150 (1963), стр. 91–98.

[16] Васильев Н.Б., Егоров А.А. *Задачи Всесоюзных математических олимпиад.* М.: Наука, 1988.

[17] Истомина М.Н., Певный А.Б. *О расположении точек на сфере и фрейме Мерседес-Бенц* // Математическое просвещение, вып.11, 2007, 105-112, МЦНМО.

[18] Фейеш Тот Л. *Расположения на плоскости, на сфере и в пространстве.* М.: Физматгиз, 1958.

[19] S.Vincze *On a geometrical extremum problem* // Acta Scientiarum mathematicarum (Szeged) 12A, 1950, p. 136-142.

[20] Гашков С.Б. *Неравенства для выпуклых многоугольников и многоугольники Рейнхардта* // Математическое просвещение, вып. 11, 2007, 91-103, МЦНМО.

[21] Конвей Дж., Слоэн Н. *Упаковки шаров, решетки и группы.* М.: Мир, 1990.

[22] Хопф Х., Панвиц Е. *Aufgabe* 167 // Jahresbericht Deutch. Math. Vereinigung 43, 1934, стр. 114.

[23] Морозова Е.А., Петраков И.С., Скворцов В.А. *Международные математические олимпиады.* М.: Просвещение, 1976.

[24] *Венгерские математические олимпиады.* М.: «Мир», 1976.

[25] Яглом И.М., Болтянский В.Г. *Выпуклые фигуры.* М.-Л. Гостехиздат, 1951.

[26] Скопенков А.Б. *n-мерный куб, многочлены и решение проблемы Борсука* // Математическое просвещение, вып. 3, 1999, 184-188, МЦНМО.

[27] Райгородский А.М. *Проблема Борсука.* Изд. МЦНМО, 2006.

С. Б. Гашков: механико-математический факультет МГУ
e-mail: gashkov@lsili.ru

Издательство МЦНМО

29-й Турнир им. М. В. Ломоносова 1 октября 2006 года. Задания. Решения. Комментарии. Сост. А.К.Кулыгин. 2007. 156 с.

Приводятся условия и решения заданий Турнира с подробными комментариями (математика, физика, химия, астрономия и науки о Земле, биология, история, лингвистика, литература, математические игры). Авторы постарались написать не просто сборник задач и решений, а интересную научно-популярную брошюру для широкого круга читателей. Существенная часть материала изложена на уровне, доступном для школьников 7-го класса.

Для участников Турнира, школьников, учителей, родителей, руководителей школьных кружков, организаторов олимпиад.

XII Турнир математических боев им. А.П. Савина. 2007. 120 с.

Книга подготовлена по материалам XII летнего Турнира математических боев им. А. П. Савина, заключительного этапа конкурса «Математика 6–8», проводимого журналом «Квант».

Здесь собраны условия и решения задач математической регаты, математических боев, командной и личной олимпиады. Решения задач специально отделены от условий, чтобы читатель мог самостоятельно порешать понравившиеся ему задачи. В приложении приведены списки победителей Турнира.

Книга рассчитана на широкий круг читателей, интересующихся олимпиадными задачами по математике: школьников 6–9 классов, а также школьных учителей и руководителей математических кружков.

Летняя математическая олимпиадная школа СУНЦ МГУ 2005. 2006. 92 с.

Книга является сборником материалов Летней математической олимпиадной школы СУНЦ МГУ, проведенной в июне 2005 года. В качестве материалов представлены подробные содержания лекций и полная задачная база, использованная на семинарских занятиях.

Для школьников, студентов, преподавателей и руководителей кружков, а также всех, кто испытывает удовольствие от красивых математических сюжетов и интересных задач.

Московские учебно-тренировочные сборы по информатике. Весна–2006. Под ред. В. М. Гуровица. 2007. 194 с.

Книга предназначена для школьников, учителей информатики, студентов и просто любителей решать задачи по программированию. В ней приведены материалы весенних Московских учебно-тренировочных сборов по информатике 2006 года: задачи практических туров, планы лекций и материалы избранных лекций и семинаров. Ко всем задачам прилагаются тесты для автоматической проверки их решений, которые можно найти на сайте `www.olympiads.rumoscowsbory`

А. И. Козко, В. Г. Чирский. **Задачи с параметром и другие сложные задачи.** 2007. 296 с.

Книга посвящена решению задач с параметрами. Помимо стандартных сведений в ней приведены оригинальные методы и приемы решения различных сложных задач. Кроме того, в книге рассмотрены задачи, связанные с методом математической индукции, и задачи по стереометрии. Большинство разбираемых авторами задач взято из вариантов вступительных экзаменов в МГУ. Во второй части книги приведены варианты вступительных экзаменов 2003–2006 гг.

Для учащихся старших классов, преподавателей математики и абитуриентов.

Теоремы Штейнера и Понселе в геометриях Евклида и Лобачевского

П. В. Бибиков

1. Одно неравенство для многоугольника Лобачевского

В статье [4] приводится много красивых неравенств, связывающих разные характеристики выпуклого евклидова n-угольника. В этом разделе мы докажем одно аналогичное неравенство для случая n-угольника на плоскости Лобачевского.

Определение. *Радиусом Бляшке выпуклого n-угольника* назовем максимальный радиус лежащего в нем круга, который будем называть *кругом Бляшке*. Обозначим этот радиус через $r_n(M)$.

Теорема 1. *На плоскости Лобачевского для любого выпуклого n-угольника M выполнено неравенство*

$$r_n(M) \leqslant \ln \operatorname{ctg} \frac{\pi}{2n}. \tag{1}$$

Доказательство. Рассмотрим для начала произвольный выпуклый n-угольник $A_1A_2\dots A_n$ в модели Клейна. Докажем, что его радиус Бляшке не превосходит радиуса Бляшке некоторого вырожденного n-угольника (т. е. n-угольника, все вершины которого лежат на абсолюте). Без ограничения общности можно считать, что центр круга Бляшке совпадает с центром граничного круга. Проведем прямые OA_k, пересекающие абсолют в точках A'_k (рис. 1). Тогда очевидно, что радиус Бляшке многоугольника $A_1A_2\dots A_n$ не превосходит радиуса Бляшке вырожденного многоугольника $A'_1A'_2\dots A'_n$. Таким образом, достаточно найти максимальный радиус Бляшке для *вырожденного* n-угольника.

Опять-таки, можно считать, что центр круга Бляшке совпадает с центром граничного круга. В таком случае евклидова длина R_n и неевклидова длина r_n радиуса Бляшке многоугольника $A'_1\dots A'_n$ связаны соотношением

$$R_n = \operatorname{th} \frac{r_n}{2}.$$

Из этой формулы видно, что величина r_n максимальна тогда и только тогда, когда максимальна величина R_n. Учитывая, что с точки зрения

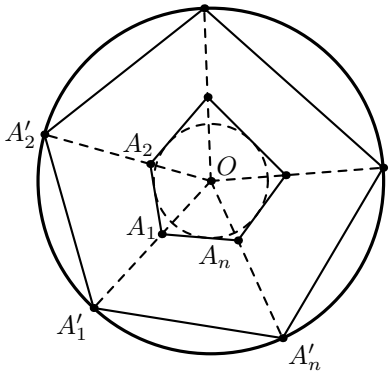


Рис. 1.

геометрии Евклида многоугольник $A_1' \dots A_n'$ вписан в окружность (абсолют) радиуса 1, с помощью неравенства, приведенного в статье [4], получаем:

$$R_n \leqslant \cos \frac{\pi}{n},$$

а значит,

$$r_n \leqslant \ln \operatorname{ctg} \frac{\pi}{2n},$$

что и требовалось.

Заметим, что если многоугольник $A_1' \dots A_n'$ является правильным (с точки зрения геометрии Евклида), то неравенство (1) обращается в равенство.

Рассмотрим более подробно эту ситуацию. Пусть $A_1' \dots A_n'$ — правильный (с точки зрения евклидовой геометрии) n-угольник, описанный вокруг неевклидовой окружности ω. При доказательстве теоремы 1 мы специально расположили многоугольник $A_1' \dots A_n'$ так, чтобы ω была также и евклидовой окружностью. Теперь же мы, наоборот, расположим многоугольник $A_1' \dots A_n'$ совершенно произвольно, тогда ω будет изображаться некоторым эллипсом.

Давайте теперь рассмотрим аналогичную картинку в модели Пуанкаре в круге. Как известно, прямыми в ней являются дуги окружностей, перпендикулярных граничной окружности. Дорисуем дуги $A_i'A_{i+1}'$ до окружностей, а саму граничную окружность сотрем. Легко видеть, что найдется окружность, касающаяся всех полученных окружностей.

Упражнение. Докажите это.

А теперь нарисуем эти две картинки рядом: то, что получилось в модели Пуанкаре в круге, и то, что получилось в модели Клейна (рис. 2 и 3).

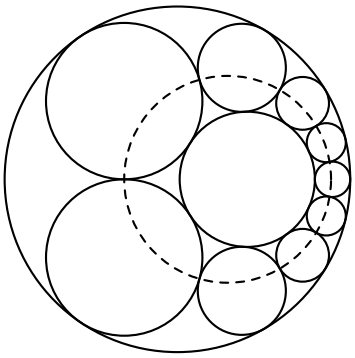


Рис. 2.

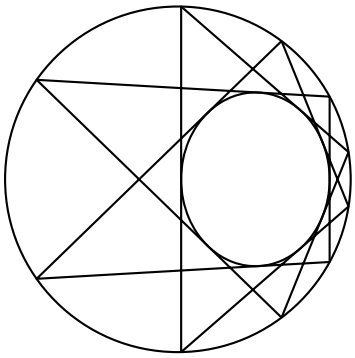


Рис. 3.

Посмотрим сначала на них, а потом на название статьи. Узнаете? Да это же поризмы Штейнера и Понселе!

2. Теоремы Штейнера и Понселе

Сначала напомним классические результаты Штейнера и Понселе.

Теорема 2 (Штейнер). *Возьмем на плоскости кольцо (т. е. две окружности, одна из которых расположена строго внутри другой) и начнем вписывать в него окружности C_1, C_2, ..., каждая из которых касается предыдущей. Тогда если получившаяся цепочка окружностей замкнется (т.е. найдется такое натуральное n, что $C_k = C_{n+k}$ для всех $k \geqslant 1$), то при любом другом выборе начальной окружности C_1' соответствующая цепочка окружностей C_1', C_2', ... тоже замкнется, причем количество окружностей в цепочках будет одинаковым.*

Классическое доказательство этой теоремы проводится применением инверсии: с ее помощью исходное кольцо можно привести к концентрическому, а для него утверждение теоремы очевидно. Однако такое доказательство не дает ответа на следующий естественный вопрос: для какого кольца существует замкнутая цепочка окружностей? Понятно, что любое кольцо однозначно с точностью до движений плоскости определяется тремя параметрами: радиусами a и b внешней и внутренней окружностей соответственно, а также расстоянием c между их центрами. Поэтому существование замкнутой цепочки из n окружностей определяет некоторое соотношение между величинами a, b, c и n. А именно, верна следующая

Теорема 3. *Для данного кольца цепочка из n окружностей замкнется тогда и только тогда, когда выполняется соотношение*

$$\cos^2 \frac{\pi}{n} = \frac{4ab}{(a+b)^2 - c^2}\,. \tag{2}$$

Доказательство. Пусть O_1 и O_2 — центры соответственно внешней и внутренней окружностей кольца. Проведем через точку O_2 диаметр RS внешней окружности, пересекающий окружность внутреннюю в точках P и Q.

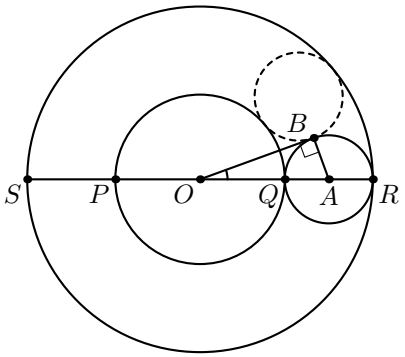


Рис. 4.

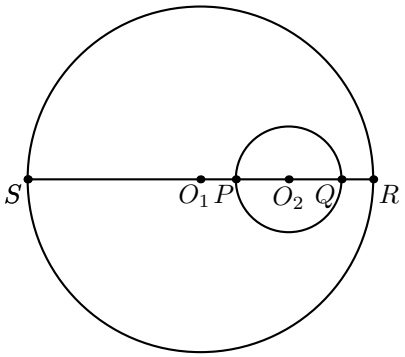


Рис. 5.

Сначала рассмотрим случай $c = 0$, т.е. случай концентрического кольца с центром в точке $O = O_1 = O_2$ (рис. 4). Тогда, радиус вписанных в кольцо окружностей равен $\dfrac{a-b}{2}$. Пусть A — центр одной из таких окружностей, а B — точка ее касания со следующей окружностью кольца. Так как треугольник OBA прямоугольный, $\angle AOB = \dfrac{\pi}{n}$ и $OA = \dfrac{a+b}{2}$, то

$$\sin \frac{\pi}{n} = \frac{a-b}{a+b}.$$

Эта формула тривиально преобразуется в формулу (2). Нам будет удобно записать ее в следующем виде:

$$[PQ, RS] = \frac{1}{\sin^2 \pi/n}\,.$$

(Здесь $[PQ, RS] = \dfrac{RP}{RQ} : \dfrac{SP}{SQ}$ — стандартное двойное отношение.)

Рассмотрим теперь общий случай (рис. 5). Мы уже отмечали, что любое кольцо инверсией можно перевести в концентрическое. Осталось заметить, что при инверсии двойное отношение $[PQ, RS]$ не изменится! Нам остается только выразить величины RP, RQ, SP и SQ через a, b и c и подставить все в предыдущую формулу.

Упражнение. Завершите доказательство, проделав необходимые вычисления.

Упражнение. Докажите, что если цепочка окружностей замыкается после m оборотов, то в формуле 2 нужно заменить n на n/m.

Отметим, что экспонента от двойного отношения, используемого нами, есть не что иное, как расстояние между точками P и Q в модели Пуанкаре в круге геометрии Лобачевского, а его инвариантность относительно инверсии эквивалентна тому, что в этой модели инверсия является движением.

Другое доказательство приводится в [5].

Теорема 4 (Малая теорема Понселе). *Возьмем на плоскости кольцо и, начиная с произвольной точки A, впишем в него ломаную L со звеньями L_1, L_2, ...(т. е. L_k является хордой внешней окружности и касательной внутренней при всех $k \geqslant 1$). Тогда если получившаяся ломаная замкнется (т. е. найдется такое натуральное n, что $L_k = L_{n+k}$ для всех $k \geqslant 1$), то при любом другом выборе начальной точки A' соответствующая ломаная L' тоже замкнется, причем количество звеньев в ломаных будет одинаковым.*

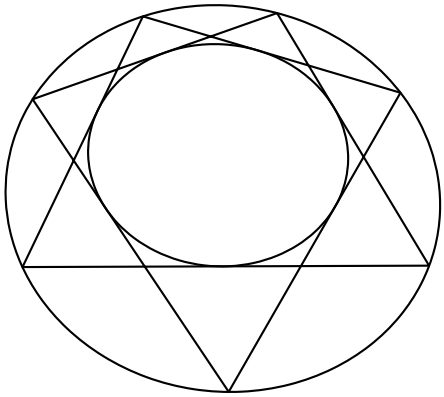


Рис. 6.

Элементарное (но непростое!) доказательство приводится в [6].

Если в теореме 4 заменить окружности на коники (рис. 6), то получится *большая теореме Понселе*. Ее доказательство приводится, например, в [2].

Теперь рассмотрим теоремы Штейнера и Понселе в геометрии Лобачевского.

Теорема 5. *В геометрии Лобачевского верны теорема Штейнера и малая теорема Понселе.*

Доказательство. Для доказательства теоремы Штейнера воспользуемся моделью Пуанкаре в верхней полуплоскости (рис. 7). Поскольку в этой модели окружность Лобачевского совпадает с окружностью Евклида, то справедливость теоремы Штейнера в геометрии Лобачевского равносильна ее справедливости в геометрии Евклида.

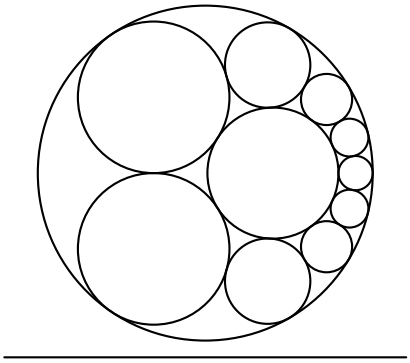


Рис. 7.

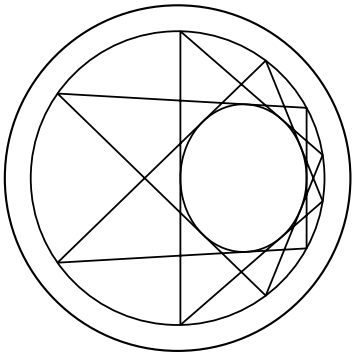


Рис. 8.

Для доказательства большой теоремы Понселе разумно воспользоваться все той же моделью Клейна (рис. 8). В ней окружности Лобачевского являются евклидовымиониками, а прямая Лобачевского — отрезком. Поэтому справедливость малой теоремы Понселе в геометрии Лобачевского следует из справедливости большой теоремы Понселе в геометрии Евклида.

Визуально теоремы Штейнера и Понселе кажутся очень похожими. Действительно, ведь исходная конфигурация в них практически одинакова, только в одном случае в кольцо вписываются окружности, а другом — ломаная. Однако, несмотря на кажущееся сходство в формулировке, эти теоремы имеют принципиально разные доказательства, которые никак не демонстрируют взаимосвязь этих теорем.

Однако сейчас мы увидим, что между этими теоремами есть связь, и поможет нам в этом геометрия Лобачевского.[1)]

Рассмотрим большую теорему Понселе в следующем частном случае: внешняя коника является окружностью, а внутренняя — эллипсом, причем этот эллипс должен быть окружностью Лобачевского в модели Клейна

[1)] Адамар говорил, что часто путь между двумя вещественными результатами проходит через комплексное. А в данном случае путь между двумя евклидовыми теоремами проходит через неевклидову геометрию!

относительно внешней окружности (рис. 3). Тогда любая замкнутая ломаная, вписанная в полученное кольцо, является *вырожденным описанным многоугольником* (*возможно*, *самопересекающимся*) *в геометрии Лобачевского.*

Перейдем теперь в модель Пуанкаре в круге геометрии Лобачевского. В этой модели окружности Лобачевского совпадают с евклидовыми, а прямыми являются дуги окружностей, лежащие внутри абсолюта и перпендикулярные ему. Тогда предыдущая конфигурация примет следующий вид: эллипс станет окружностью, а звенья ломаной — дугами окружностей, каждая из которых касается предыдущей. Если теперь дополнить эти дуги до окружностей, то несложно показать (например, с помощью инверсии), что все они будут касаться (внутренним образом) еще одной окружности. А это как раз и есть теорема Штейнера.

Таким образом, мы фактически показали, что теорема Штейнера является частным случаем большой теоремы Понселе. Также интересен и обратный переход к теореме Понселе. К сожалению, таким способом получить ее доказательство в общем случае нельзя, поскольку окружность в модели Клейна геометрии Лобачевского — это не произвольный эллипс (у него, например, малая ось лежит на диаметре абсолюта).

Теперь с помощью теоремы Понселе в геометрии Лобачевского мы докажем следующую теорему евклидовой геометрии, которая является обобщением теоремы Штейнера и малой теоремы Понселе.

Теорема 6 (Эмх). *Возьмем на плоскости кольцо* (*т. е. две окружности*, *одна из которых расположена строго внутри другой*) *и окружность* ω, *лежащую в нем. Начнем вписывать в это кольцо окружности* $C_1, C_2, \ldots$, *каждая из которых проходит через точку пересечения предыдущей окружности с окружностью* ω (*рис.* 9). *Тогда если получившаяся*

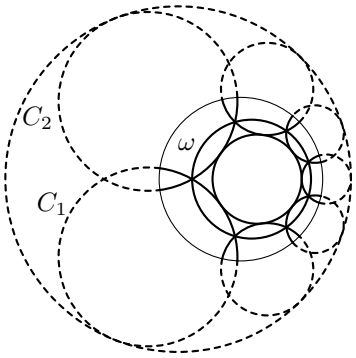


Рис. 9.

цепочка окружностей замкнется (т. е. найдется такое натуральное n, что $C_k = C_{n+k}$ для всех $k \geqslant 1$), то при любом другом выборе начальной окружности C_1' соответствующая цепочка окружностей C_1', C_2', ... тоже замкнется, причем количество окружностей в цепочках будет одинаковым.

Доказательство. Как и при доказательстве теоремы Штейнера, с помошью инверсии переведем граничные окружности кольца в концентрические. Тогда найдется окружность, перпендикулярная всем окружностям C_k кольца (докажите!). Мысленно сотрем все, что лежит вне этой окружности и внимательно посмотрим на то, что осталось. После секундного размышления становится понятно, что перед нами не что иное, как малая теорема Понселе в модели Пуанкаре в круге геометрии Лобачевского!

Упражнение. С помощью теоремы Эмха докажите теорему Штейнера и малую теорему Понселе.

Аналогично теореме 5, верна следующая

Теорема 7. *Теорема Эмха верна в геометрии Лобачевского.*

Упражнение. Докажите эту теорему.

Приведенный выше пример использования геометрии Лобачевского при доказательстве теорем геометрии Евклида является довольно редким и на практике встречается нечасто (см., например, [1, 3]).

Список литературы

[1] Андреев Е. *Невписываемые многогранники* // Квант, №8, 1970. С. 3–9.

[2] Берже М. *Геометрия. Том второй.* М.: Мир, 1984. С. 140–148.

[3] Гальперин Г. А. *Бильярдная формула для измерения расстояний в геометрии Лобачевского* // Математическое просвещение. Третья серия. Вып. 8. 2004. С. 102–109.

[4] Гашков С. Б. *Неравенства для выпуклых многоугольников и многоугольники Рейнхардта* // Математическое просвещение. Третья серия. Вып. 11. 2007. С. 91–103.

[5] Исмагилов Р. *Ожерелье Штейнера, или Любовь к вычислениям* // Квант, №2, 2003. С. 9–12.

[6] Шарыгин И. Ф. *Геометрия. Планиметрия. Задачник. 9–11 кл.* М.: Дрофа, 2001. С. 77, 235–236.

П. В. Бибиков, механико-математический факультет МГУ
e-mail: tsdtp4u@proc.ru

Изогональное сопряжение и задача Ферма

Г. Ганчев Н. Николов

1. Введение

Целью данной работы является доказательство следующего утверждения.

Пусть дан треугольник ABC и две точки X, Y. Если X, Y изогонально сопряжены, то

$$\pm\frac{AX\cdot AY}{AB\cdot AC}\pm\frac{BX\cdot BY}{BC\cdot BA}\pm\frac{CX\cdot CY}{CA\cdot CB}=1, \tag{1}$$

причем, если число отрицательных слагаемых в левой части четно, то условие изогональной сопряженности является и необходимым.

В разделе 2 дано детальное описание геометрических конфигураций, в которых выполнено равенство (1).

Мы будем использовать (1) для геометрической интерпретации решения классической задачи Ферма с произвольными весами.

В разделе 3 будет решена задача Ферма для положительных весов:

Дан треугольник ABC и положительные числа λ, μ, ν. Найти точку Y, минимизирующую функцию

$$\lambda AY+\mu BY+\nu CY.$$

В разделе 4 будет решена задача Ферма для одного отрицательного и двух положительных весов:

Дан треугольник ABC и положительные числа λ, μ, ν. Найти точку Y, минимизирующую функцию

$$-\lambda AY+\mu BY+\nu CY.$$

Мы покажем, как в общем случае по данным числам построить точку X, изогонально сопряженную искомой точке Y.

2. Соотношения, характеризующие изогональное сопряжение

Пусть k — описанная окружность треугольника ABC. Обозначим через i изогональное сопряжение относительно ABC. Мы не будем

Перевод А. А. Заславского.

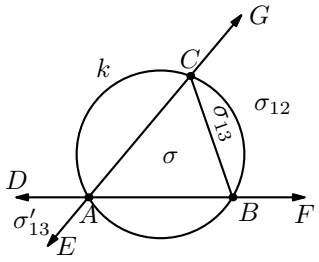


Рис. 1.

рассматривать точки k, отличные от вершин треугольника, и сопряженные им бесконечно удаленные точки.

На рис. 1 изображены области, на которые стороны треугольника и окружность k разбивают углы DAE и FAG.

Напомним, что

1) $i(\sigma) = \sigma$. При этом $i(M) = A$ для любой точки M отрезка BC, $i(M) = B$ для любой точки отрезка AC, $i(M) = C$ для любой точки отрезка AB.

2) $i(\sigma_{12}) = \sigma_{12}$. При этом $i(M) = C$ для любой точки луча BF, $i(M) = B$ для любой точки луча CG.

3) $i(\sigma_{13}) = \sigma'_{13}$, $i(\sigma'_{13}) = \sigma_{13}$. При этом $i(M) = C$ для любой точки луча AD, $i(M) = B$ для любой точки луча AE.

Пусть даны две точки X, Y. Докажем

Утверждение 1.

$$\frac{AX \cdot AY}{AB \cdot AC} + \frac{BX \cdot BY}{BC \cdot BA} + \frac{CX \cdot CY}{CA \cdot CB} \geqslant 1,$$

причем равенство достигается только когда X, Y изогонально сопряжены и лежат в области σ.

Доказательство. Будем рассматривать точки плоскости A, B, C, X, Y как комплексные числа a, b, c, x, y. Тогда требуемое неравенство примет вид

$$\Big|\frac{(x-a)(y-a)}{(b-a)(c-a)}\Big| + \Big|\frac{(x-b)(y-b)}{(c-b)(a-b)}\Big| + \Big|\frac{(x-c)(y-c)}{(a-c)(b-c)}\Big| \geqslant 1. \tag{2}$$

Чтобы доказать неравенство (2), достаточно заметить, что

$$\Big|\frac{(x-a)(y-a)}{(b-a)(c-a)}\Big| + \Big|\frac{(x-b)(y-b)}{(c-b)(a-b)}\Big| + \Big|\frac{(x-c)(y-c)}{(a-c)(b-c)}\Big| \geqslant$$
$$\geqslant \Big|\frac{(x-a)(y-a)}{(b-a)(c-a)} + \frac{(x-b)(y-b)}{(c-b)(a-b)} + \frac{(x-c)(y-c)}{(a-c)(b-c)}\Big|,$$

и

$$\frac{(x-a)(y-a)}{(b-a)(c-a)}+\frac{(x-b)(y-b)}{(c-b)(a-b)}+\frac{(x-c)(y-c)}{(a-c)(b-c)}=1. \tag{3}$$

При этом равенство в (2) достигается тогда и только тогда, когда все три числа

$$\frac{(x-a)(y-a)}{(b-a)(c-a)},\quad \frac{(x-b)(y-b)}{(c-b)(a-b)},\quad \frac{(x-c)(y-c)}{(a-c)(b-c)} \tag{4}$$

действительны и неотрицательны. Числа (4) действительны тогда и только тогда, когда X и Y изогонально сопряжены. Если все они положительны, то точки X, Y лежат внутри треугольника ABC, если же одно из чисел равно нулю, то одна из этих точек совпадает с вершиной треугольника, а другая лежит на противоположной стороне. □

Обозначив $BC=a$, $CA=b$, $AB=c$, получим условие изогональной сопряженности внутренних точек в виде

$$a\cdot AX\cdot AY+b\cdot BX\cdot BY+c\cdot CX\cdot CY=abc.$$

Утверждение 2.

$$-\frac{AX\cdot AY}{AB\cdot AC}+\frac{BX\cdot BY}{BC\cdot BA}+\frac{CX\cdot CY}{CA\cdot CB}\geqslant -1,$$

причем равенство достигается только когда X, Y изогонально сопряжены и лежат в области σ_{12}.

Доказательство. Аналогично доказательству предыдущего утверждения запишем требуемое неравенство в виде

$$\Big|\frac{(x-a)(y-a)}{(b-a)(c-a)}\Big|-\Big|\frac{(x-b)(y-b)}{(c-b)(a-b)}\Big|-\Big|\frac{(x-c)(y-c)}{(a-c)(b-c)}\Big|\leqslant -1. \tag{5}$$

Для доказательства (5) используем (3) и неравенство

$$\Big|\frac{(x-a)(y-a)}{(b-a)(c-a)}\Big|-\Big|\frac{(x-b)(y-b)}{(c-b)(a-b)}\Big|-\Big|\frac{(x-c)(y-c)}{(a-c)(b-c)}\Big|\leqslant$$
$$\leqslant\Big|\frac{(x-a)(y-a)}{(b-a)(c-a)}+\frac{(x-b)(y-b)}{(c-b)(a-b)}+\frac{(x-c)(y-c)}{(a-c)(b-c)}\Big|.$$

Равенство в (5) достигается тогда и только тогда, когда все три числа действительны и выполнены неравенства

$$\frac{(x-a)(y-a)}{(b-a)(c-a)}\geqslant 0,\quad \frac{(x-b)(y-b)}{(c-b)(a-b)}\leqslant 0,\quad \frac{(x-c)(y-c)}{(a-c)(b-c)}\leqslant 0. \tag{6}$$

Эти условия выполняются тогда и только тогда, когда X и Y изогонально сопряжены и лежат в области σ_{12}. □

Полученное условие изогональной сопряженности можно записать в виде

$$-a\cdot AX\cdot AY+b\cdot BX\cdot BY+c\cdot CX\cdot CY=-abc.$$

Отметим также, что для изогонально сопряженных точек X, Y, лежащих в $\sigma_{13} \cup \sigma'_{13}$ выполнено равенство

$$-\frac{AX \cdot AY}{AB \cdot AC} + \frac{BX \cdot BY}{BC \cdot BA} + \frac{CX \cdot CY}{CA \cdot CB} = 1, \tag{7}$$

или

$$-a \cdot AX \cdot AY + b \cdot BX \cdot BY + c \cdot CX \cdot CY = abc.$$

Однако, приведенное выше доказательство необходимости в этом случае не проходит. Удовлетворяет ли левая часть (7) какому-либо неравенству, неизвестно.

3. Задача Ферма для положительных весов

Для треугольника ABC обозначим: $AB = c$, $BC = a$, $CA = b$, $\angle A = \alpha$, $\angle B = \beta$, $\angle C = \gamma$, O, R — центр и радиус описанной окружности k, S — площадь.

Пусть $M \notin k$ — произвольная точка, $A_1B_1C_1$ — педальный треугольник M. Тогда, так как B_1, C_1 лежат на окружности с диаметром AM, $B_1C_1 = AM \sin\alpha = \frac{a\,AM}{2R}$. Аналогично, $C_1A_1 = \frac{b\,BM}{2R}$, $A_1B_1 = \frac{c\,CM}{2R}$.

Выясним теперь, как найти точку M, зная углы треугольника $A_1B_1C_1$. Воспользуемся следующим результатом.

Теорема 1 ([1]). *Пусть даны углы треугольника α_1, β_1, γ_1. Тогда*

i) *Существует единственная точка M внутри k, для которой углы педального треугольника $A_1B_1C_1$ равны α_1, β_1, γ_1. При этом треугольники ABC и $A_1B_1C_1$ одинаково ориентированы.*

ii) *Если $(\alpha_1, \beta_1, \gamma_1) \neq (\alpha, \beta, \gamma)$, то существует единственная точка N вне k, для которой углы педального треугольника $A_2B_2C_2$ равны α_1, β_1, γ_1. При этом треугольники ABC и $A_2B_2C_2$ противоположно ориентированы.*

iii) *Точки M и N инверсны относительно k.*

Выясним теперь, при каких соотношениях между (α, β, γ) и $(\alpha_1, \beta_1, \gamma_1)$ точка M лежит в σ, σ_{12}, σ_{13}, σ'_{13}.

Если M лежит внутри k, то (рис. 2)

$$\angle BMC = \alpha + \alpha_1, \quad \angle CMA = \beta + \beta_1, \quad \angle AMB = \gamma + \gamma_1. \tag{8}$$

Мы считаем, что $\angle BMC > \pi$, если A и M лежат по разные стороны от BC. Соответственно имеем:

$$M \in \sigma \Leftrightarrow \alpha + \alpha_1 < \pi, \quad \beta + \beta_1 < \pi, \quad \gamma + \gamma_1 < \pi.$$

$$M \in BC \Leftrightarrow \alpha + \alpha_1 = \pi, \quad \beta + \beta_1 < \pi, \quad \gamma + \gamma_1 < \pi.$$

$$M \in \sigma_{13} \Leftrightarrow \alpha + \alpha_1 > \pi, \quad \beta + \beta_1 < \pi, \quad \gamma + \gamma_1 < \pi.$$

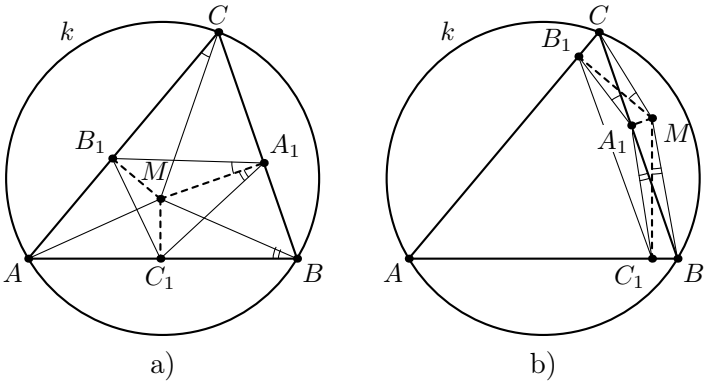


Рис. 2.

Используя (8), строим искомую точку M.

Если M — внутренняя точка треугольника, и N — изогонально сопряжена M, то из (8) и равенства $\angle BMC + \angle BNC = \pi + \alpha$ получаем

$$\angle BNC = \pi - \alpha_1, \quad \angle CNA = \pi - \beta_1, \quad \angle ANB = \pi - \gamma_1. \tag{9}$$

Пусть теперь M лежит вне k. Если M и A по разные стороны от BC, то (рис. 3) $\angle BMC = \alpha_1 - \alpha > 0$.

Следовательно

$$M \in \sigma_{12} \Leftrightarrow \beta > \beta_1, \quad \gamma > \gamma_1, \quad \alpha_1 > \alpha.$$

$$M \in \sigma'_{13} \Leftrightarrow \beta < \beta_1, \quad \gamma < \gamma_1, \quad \alpha_1 < \alpha.$$

Теперь рассмотрим задачу Ферма с положительными весами. Используя неравенство из утверждения 1, дадим геометрическую интерпретацию ее решения.

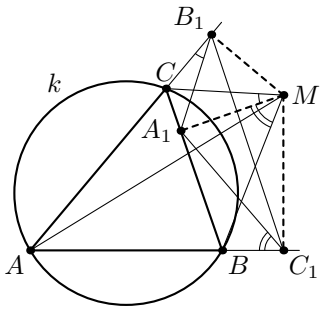


Рис. 3.

Задача 1. *Дан треугольник ABC и положительные числа λ, μ, ν. Найти точку Y, минимизирующую функцию*

$$F(Y) = \lambda AY + \mu BY + \nu CY. \tag{10}$$

Решение. Прежде всего отметим, что если, например, $\nu \geqslant \lambda + \mu$, то для любой точки Y

$$F(Y) \geqslant \lambda AY + \mu BY + (\lambda + \mu)CY = \lambda(AY + CY) + \mu(BY + CY) \geqslant F(C).$$

Поэтому будем считать, что существует треугольник со сторонами λ, μ, ν. Если α_1, β_1, γ_1 — углы этого треугольника, то минимизация (10) эквивалентна минимизации функции

$$f(Y) = AY \sin\alpha_1 + BY \sin\beta_1 + CY \sin\gamma_1.$$

По теореме 1 существует единственная точка X внутри k, для которой углы педального треугольника $A_1B_1C_1$ равны $\angle A_1 = \alpha_1$, $\angle B_1 = \beta_1$, $\angle C_1 = \gamma_1$. Обозначая через R_1 радиус описанной окружности $A_1B_1C_1$, получаем

$$f(Y) = \frac{1}{4RR_1}(a \cdot AX \cdot AY + b \cdot BX \cdot BY + c \cdot CX \cdot CY). \tag{11}$$

Рассмотрим два случая:

– X внутри или на границе треугольника ABC;

– X вне ABC.

В первом случае, применяя к (11) утверждение 1, получаем, что минимум $f(Y)$, равный $\dfrac{S}{4R_1}$, достигается, когда Y — точка, изогонально сопряженная X.

Точнее, если $\alpha + \alpha_1 < \pi$, $\beta + \beta_1 < \pi$, $\gamma + \gamma_1 < \pi$, то X лежит внутри ABC и минимум достигается на точке Y, изогонально сопряженной X. Если же, например, $\gamma + \gamma_1 = \pi$, то X лежит на стороне BC и $Y = C$.

Пусть теперь X вне треугольника ABC (рис. 4). Тогда $\gamma + \gamma_1 = \pi$.

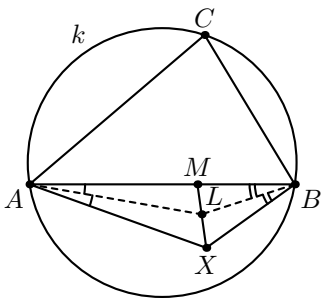


Рис. 4.

Пусть XM — биссектриса угла X треугольника AXB. Тогда для некоторого $q > 1$

$$AX = qAM, \quad BX = qBM.$$

Построим окружность Аполлония k_0 для точек M, X и отношения q. Она проходит через A, B и центр L вписанной в треугольник AXB окружности. Следовательно, C лежит внутри k_0 и $\dfrac{CX}{CM} > q$.

Подставив в (11) $AX = qAM$, $BX = qBM$, получаем

$$f(Y) = \frac{1}{4RR_1}(q(a\cdot AM\cdot AY + b\cdot BM\cdot BY + c\cdot CM\cdot CY) + c(CX - q\cdot CM)CY).$$

Так как $CX - qCM > 0$, минимум $f(Y)$, равный $\dfrac{qS}{R_1}$, достигается, когда Y изогонально сопряжена M, т. е. $Y = C$. □

4. Задача Ферма с весами разных знаков

В этом разделе будет рассмотрена задача Ферма с одним отрицательным и двумя положительными весами. Мы покажем, что ее можно свести к задаче с положительными весами.

Задача 2. *Дан треугольник ABC и положительные числа λ, μ, ν. Найти точку Y, минимизирующую функцию*

$$G(Y) = -\lambda AY + \mu BY + \nu CY. \tag{12}$$

Решение. Воспользуемся следующим соотношением между решениями задач 1 и 2.

Лемма [2]. *Если Q решение задачи* 2, *то*

i) *Q и A лежат по разные стороны от прямой BC*;

ii) *Для любой точки D, лежащей на луче, противоположном QA, точка Q является решением задачи* 1 *для треугольника BCD и весов λ, μ, ν.*

Доказательство. i) Достаточно заметить, что для точки Q, лежащей по ту же сторону от BC, что A, $G(Q) > G(Q')$, где Q' — точка, симметричная Q относительно BC.

ii) Пусть $F_D(Y) = \lambda DY + \mu BY + \nu CY$. Тогда

$$F_D(Y) - F_D(Q) - (G(Y) - G(Q)) = \lambda(DY + YA - (DQ + QA)) = \\ = \lambda(DY + YA - DA) \geqslant 0.$$

Поэтому, если Q — решение задачи 2, то

$$F_D(Y) - F_D(Q) \geqslant G(Y) - G(Q) \geqslant 0.$$ □

Из леммы следует, что точка Q (если задача 2 имеет решение) лежит в области $\sigma_{13} \cup BC \cup \sigma_{12}$.

Если $\lambda > \mu + \nu$, то

$$G(Y) \leqslant (\mu + \nu - \lambda)AY + \mu AB + \nu AC,$$

и задача не имеет решения.

Пусть $\lambda \leqslant \mu + \nu$. Тогда $G(Y) \geqslant -G(A)$, и значит, решение задачи 2 существует. Из леммы и решения задачи 1 следует, что искомой точкой будет:

B при $\mu > \lambda + \nu$; C при $\nu > \lambda + \mu$; B и/или C при $\lambda = \mu + \nu$.

Поэтому будем рассматривать случай, когда λ, μ, ν удовлетворяют неравенству треугольника. Обозначив соответствующие углы через α_1, β_1, γ_1, сведем задачу к минимизации функции

$$g(Y) = -\sin\alpha_1 AY + \sin\beta_1 BY + \sin\gamma_1 CY. \tag{13}$$

Предположим, что точка Q лежит в области σ_{13} (рис. 5)

Рассмотрим треугольник BCA', удовлетворяющий условиям леммы. Из решения задачи 1 следует, что $\angle BQA' = \pi - \gamma_1$, $\angle CQA' = \pi - \beta_1$, т. е. $\angle AQB = \gamma_1$, $\angle AQC = \beta_1$.

Кроме того

$$\beta_1 > \beta, \quad \gamma_1 > \gamma. \tag{14}$$

Возьмем вне k точку P, для которой углы педального треугольника равны α_1, β_1, γ_1. В силу (14) P лежит в области σ'_{13}, и так как $\angle BQC = \pi - \alpha_1$, $\angle AQC = \beta_1$, $\angle AQB = \gamma_1$, точки P и Q изогонально сопряжены. Поэтому

$$g(Q) = \frac{abc}{4RR_1},$$

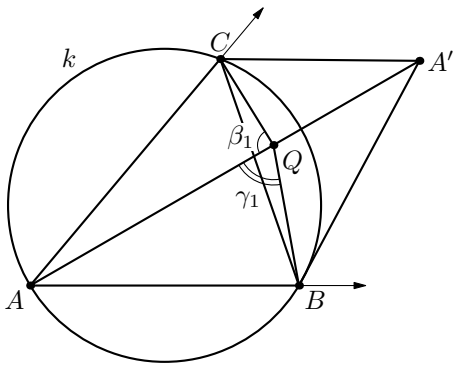


Рис. 5.

где R_1 — радиус педальной окружности P.

С другой стороны

$$g(B) = \frac{ac}{4RR_1}(PC - PA) < \frac{abc}{4RR_1} = g(Q),$$

что противоречит минимальности Q. Следовательно, Q не может лежать в σ_{13}.

Если Q лежит на дуге BC, то $\beta_1 = \beta$, $\gamma_1 = \gamma$, $\alpha_1 = \alpha$. Значит

$$g(Y) = \frac{1}{2R}(-aAY + bBY + cCY) \geqslant 0,$$

причем равенство достигается в точках дуги BC (теорема Птолемея).

Таким образом, решение задачи 2 достигается во всех точках дуги BC, не содержащей A.

Пусть Q лежит в области σ_{12}. Тогда $\beta_1 < \beta$, $\gamma_1 < \gamma$. Возьмем вне k точку P, педальный треугольник которой имеет углы α_1, β_1, γ_1. Рассуждая, как выше, получаем, что оптимальная точка Q изогонально сопряжена P и

$$g_{\min} = -\frac{abc}{4RR_1} = -\frac{S}{R_1}.$$

Во всех остальных случаях минимум достигается в точке B, C или обеих, в зависимости от того, выполнено ли $g(B) < g(C)$, $g(B) > g(C)$ или $g(B) = g(C)$.

Подводя итог, получаем:

1. При $\beta_1 = \beta$, $\gamma_1 = \gamma$ решением задачи 2 будет любая точка дуги BC, не содержащей A, $g_{\min} = 0$.

2. При $\beta_1 < \beta$, $\gamma_1 < \gamma$ решением будет точка Q, изогонально сопряженная P, и

$$g_{\min} = -\frac{S}{R_1}\,.$$

3. Если $\beta_1 > \beta$ или $\gamma_1 > \gamma$, то:

3.1. При $\dfrac{\sin\beta_1 - \sin\gamma_1}{\sin\alpha_1} > \dfrac{\sin\beta - \sin\gamma}{\sin\alpha}$ решением будет точка B;

3.2. При $\dfrac{\sin\beta_1 - \sin\gamma_1}{\sin\alpha_1} = \dfrac{\sin\beta - \sin\gamma}{\sin\alpha}$ решением будут точки B и C;

3.3. При $\dfrac{\sin\beta_1 - \sin\gamma_1}{\sin\alpha_1} < \dfrac{\sin\beta - \sin\gamma}{\sin\alpha}$ решением будет точка C.

Замечание. Стандартные вычисления показывают, что

$$\frac{\sin\beta_1 - \sin\gamma_1}{\sin\alpha_1} > \frac{\sin\beta - \sin\gamma}{\sin\alpha} \quad\Longleftrightarrow\quad \operatorname{tg}\frac{\beta_1}{2}\operatorname{ctg}\frac{\gamma_1}{2} > \operatorname{tg}\frac{\beta}{2}\operatorname{ctg}\frac{\gamma}{2}\,.$$

Следовательно, решением при $\alpha_1 \neq \alpha$, $\beta_1 \geqslant \beta$, $\gamma_1 \leqslant \gamma$ ($\beta_1 \leqslant \beta$, $\gamma_1 \geqslant \gamma$) будет точка B (C).

Разбор вырожденных случаев задач 1, 2, когда точки A, B, C лежат на одной прямой и/или некоторые из весов равны нулю, мы оставляем читателю.

Список литературы

[1] Ganchev G. *Etudes on theme "Inversion"* // Mathematica plus, 1994. No 4. P. 24–32. (In Bulgarian)

[2] Jalal G., Krarup J. *Geometrical solution to the Fermat problem with arbitrary weights* // Annals of Operation Research, 2003. Vol. 123. P. 67–104.

Г. Ганчев, Н. Николов, Bulgarian Academy of Sciences, Institute of Mathematics and Informatics, Acad. G. Bonchev str., bl. 8, 1113 Sofia, Bulgaria

e-mail: ganchev@math.bas.bg
nik@math.bas.bg

Параболические многоугольники

Ф. К. Нилов

В этой статье доказывается несколько теорем о криволинейном параболическом четырехугольнике.

Теорема 1. *Две параболы пересекаются в четырех точках. В полученный «параболический четырехугольник» можно вписать окружность тогда и только тогда, когда его диагонали перпендикулярны.* (См. рис. 1.)

По-видимому, этот красивый факт неизвестен, что подтверждается мнением авторов книги [1].

Формулировки остальных результатов

Сформулируем следующий известный факт.

Теорема 2. *Параболический четырехугольник является вписанным тогда и только тогда, когда оси образующих его парабол перпендикулярны.* (См. рис. 2.)

Из теорем 1 и 2 будет выведено такое утверждение.

Следствие 1. *Любой параболический четырехугольник можно перевести аффинным преобразованием во вписанно-описанный параболический четырехугольник.*

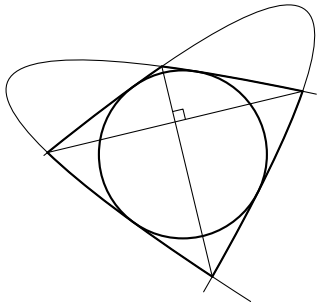


Рис. 1.

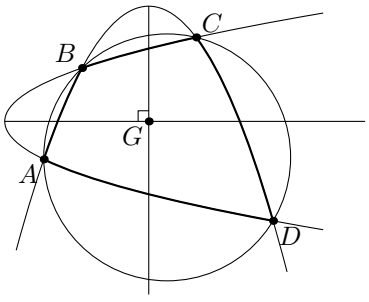


Рис. 2.

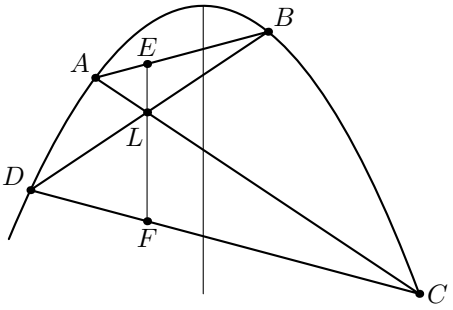


Рис. 3. $AE/EB = DF/FC$

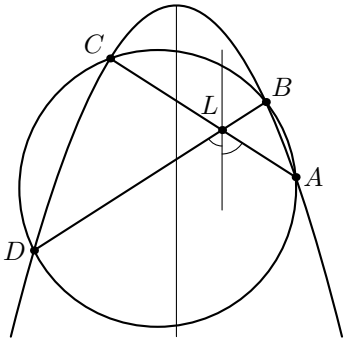


Рис. 4.

Из следствия 1 будет выведен еще один интересный результат.

Прямая EF называется *осевой прямой* выпуклого четырехугольника $ABCD$, если она проходит через точку пересечения диагоналей четырехугольника и пересекает прямые, содержащие стороны AB и CD в точках E и F, для которых $AE/EB = FD/CF$. Осевая прямая четырехугольника зависит от порядка расположения точек A, B, C и D.

Следствие 2. *На параболе лежат четыре точки A, B, C и D. Тогда ось параболы параллельна осевой прямой четырехугольника $ABCD$.* (См. рис. 3.)

Следующий факт будет выведен из следствия 2 как частный случай.

Следствие 3. *Парабола и окружность пересекаются в четырех точках A, B, C и D. Обозначим точку пересечения диагоналей четырехугольника $ABCD$ через L. Тогда биссектриса угла ALD параллельна оси параболы.* (См. рис. 4.)

Следующее утверждение будет выведено из следствия 3.

Утверждение 1. *Точка пересечения осей парабол, образующих вписанный параболический четырехугольник, совпадает с центром тяжести соответствующего прямолинейного четырехугольника.* (На рис. 2 точка G — центр тяжести $ABCD$.)

Следующее утверждение сформулировано А. В. Акопяном и А. А. Заславским. Оно будет выведено из следствия 3 и леммы 1.

Теорема 3. *Внутри окружности взята точка X. Через нее проводятся N хорд, делящие плоскость на $2N$ равных углов. Через концы каждой хорды проводится парабола, касающаяся окружности в этих концах. Тогда вершины параболического $2N$-угольника, получающегося при пересечении этих парабол, лежат на одной окружности.*

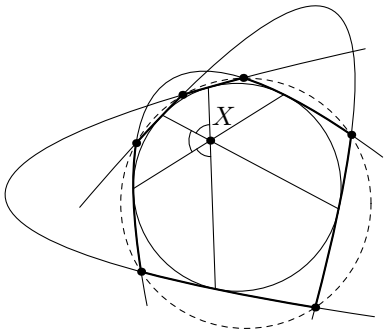


Рис. 5.

Утверждение 2. *Дан описанный параболический шестиугольник, причем любые две параболы, образующие его, пересекаются в четырех точках. Тогда его главные диагонали пересекаются в одной точке.*

Это утверждение будет выведено из леммы 1, сформулированной ниже.

Доказательство теоремы 1.

Сформулируем лемму 1, на которой основано доказательство теоремы 1.

Лемма 1. *Дана парабола, касающаяся окружности в точках A и B. Произвольная точка P плоскости лежит на этой параболе тогда и только тогда, когда расстояние от точки P до прямой AB равно длине касательной, проведенной из точки P к окружности.* (См. рис. 6.)

Доказательство этой леммы приведем позже.

Доказательство части «только тогда» теоремы 1. Обозначим точки касания окружности, вписанной в параболический четырехугольник, с одной параболой через K и L, а с другой — через M и N (см. рис. 7). Рассмотрим одну из вершин A параболического четырехугольника. Из части «только тогда» леммы 1 следует, что расстояния от точки A до прямых KL и MN равны длине касательной, проведенной из A к окружности. Значит, вершина A равноудалена от прямых KL и MN. Аналогичное верно и для других вершин. Поскольку прямые, содержащие биссектрисы углов, образованных прямыми KL и MN, являются диагоналями четырехугольника $ABCD$, то диагонали этого четырехугольника перпендикулярны. □

Основная идея доказательства части «тогда» теоремы 1 принадлежит А. А. Заславскому.

Доказательство части «тогда» теоремы 1. Пусть $ABCD$ — параболический четырехугольник с перпендикулярными диагоналями (см.

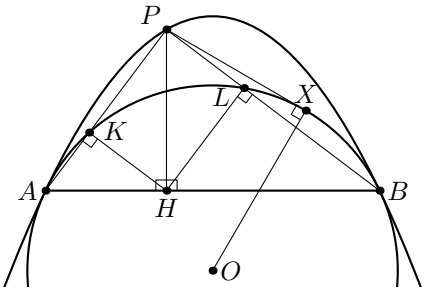


Рис. 6.

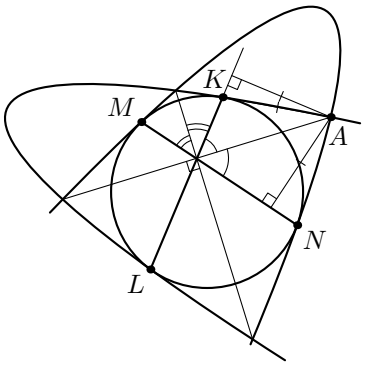


Рис. 7.

рис. 8). Обозначим через L точку пересечения его диагоналей. Известно, что проекции точки L на прямые AB, BC, CD и DA лежат на одной окружности. Докажем, что эта окружность вписана в параболический четырехугольник. Можно считать, что существует такая прямая l_1, проходящая через точку L, что расстояние a от этой прямой до точки A равно длине касательной t_a из точки A к окружности.

(Покажем, почему такая прямая существует. Будем считать, что центр I этой окружности лежит в той же полуплоскости относительно прямой BD, что и точка A. Тогда $\angle ILA$ острый. Существование такой прямой по соображениям непрерывности следует из $AL^2 > t_a^2$. Для доказательства этого неравенства обозначим через r радиус рассматриваемой окружности. Точка L лежит внутри этой окружности. Поскольку $\angle ILA$ острый, $AL^2 > AI^2 - IL^2 > AI^2 - r^2 = t_a^2$.)

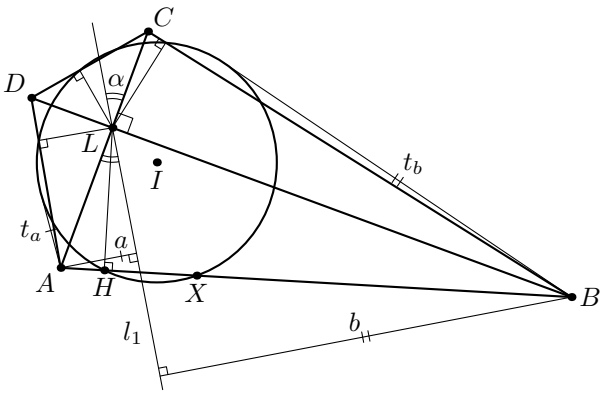


Рис. 8.

Обозначим расстояния от этой прямой до каждой из точек B, C и D через b, c, d, а длины касательных из точек B, C и D к окружности через t_b, t_c и t_d.

Докажем, что $t_b = b$.

Обозначим проекцию точки L на прямую AB через H. Обозначим вторую точку пересечения окружности и прямой AB через X. Тогда

$$\frac{t_a^2}{AL^2} + \frac{t_b^2}{BL^2} = \frac{AH \cdot AX}{AH \cdot AB} + \frac{BX \cdot BH}{BH \cdot AB} = \frac{AX + XB}{AB} = 1 = \\ = \sin^2 \angle(l_1, AC) + \cos^2 \angle(l_1, AC) = \frac{a^2}{AL^2} + \frac{b^2}{BL^2}\,.$$

Это равенство выполнено, поскольку

(a) LH — высота прямоугольного треугольника ALB, опущенная на гипотенузу AB, а значит $AL^2 = AH \cdot AB$ и $BL^2 = BH \cdot AB$.

(b) $AH \cdot AX = t_a^2$ и $BX \cdot BH = t_b^2$.

Поэтому $a = t_a$ влечет $b = t_b$. Аналогично, $c = t_c$ и $d = t_d$.

Поскольку для прямой l_1 выполнено $t_a = a$, $t_b = b$, $t_c = c$ и $t_d = d$, то прямая l_2, симметричная ей относительно AC тоже обладает этим же свойством. Поэтому из части «тогда» леммы 1 следует, что точки A, B, C и D лежат на двух параболах, касающихся окружности в точках пересечения прямых l_1 и l_2 с окружностью. Поэтому в параболический четырехугольник $ABCD$ можно вписать окружность. □

Докажем лемму, на которой основано доказательство части «только тогда» леммы 1.

Лемма 2. *По параболе движется точка P. Пусть AB — хорда параболы, параллельная ее директрисе. Тогда*

(a) *точка C пересечения перпендикуляров, восстановленных в точках A и B к прямым PA и PB, движется по прямой, параллельной AB.* (См. рис. 9.)

Обозначим проекцию точки P на прямую AB через H, а проекции точки H на прямые AP и BP через K и L. Точки A, B, K и L лежат на одной окружности ω, поскольку $\angle KLP = \angle KHP = \angle HAP$. Обозначим через O центр окружности ω. Тогда

(b) *окружность ω не зависит от положения точки P.* (См. рис. 10.)

(c) *окружность ω касается параболы в точках A и B.*

Для доказательства леммы 2 (a) приведем определения и сформулируем известную лемму.

Пучком $[A]$ прямых называется множество прямых, проходящих через точку A.

Соответствие между двумя пучками прямых называется *проективным*, если двойное отношение любых четырех прямых из одного пучка

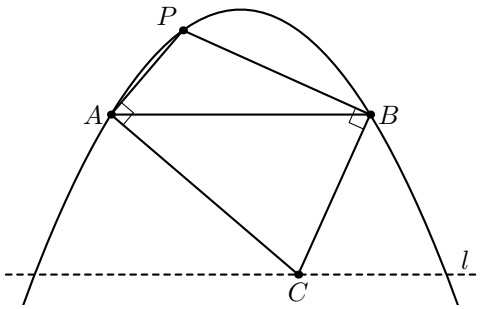


Рис. 9.

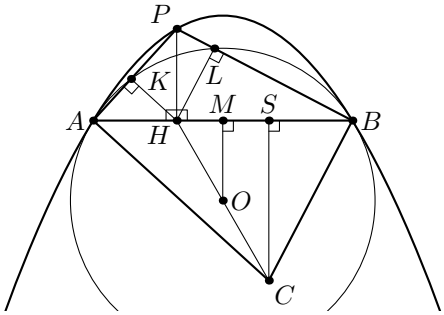


Рис. 10.

равно двойному отношению четырех соответствующих прямых из другого пучка.

Лемма Соллертинского. *Дано проективное соответствие между пучками прямых* $[A]$ *и* $[B]$. *Тогда все точки* P, *являющиеся пересечением соответствующих прямых из пучков* $[A]$ *и* $[B]$, *принадлежат коническому сечению, возможно, вырожденному.*

Доказательство леммы 2 (а). Рассмотрим прямую, проходящую через точку C и параллельную прямой AB. Пусть точка C' движется по этой прямой. Обозначим точку пересечения перпендикуляров, восстановленных в точках A и B к прямым $C'A$ и $C'B$, через P'. Очевидно, что соответствие $AC' \to BC'$ между прямыми из пучков $[A]$ и $[B]$ является проективным. Соответствие $AC' \to AP'$ между прямыми из пучков $[A]$ является проективным, поскольку угол между любыми двумя соответствующими прямыми прямой. Аналогично, соответствие $BC' \to BP'$ между прямыми из пучков $[B]$ является проективным. Значит, соответствие $AP' \to BP'$ между прямыми из пучков $[A]$ и $[B]$ является проективным.

Поэтому из леммы Соллертинского следует, что точки P' лежат на конике или прямой. Кривая γ, по которой движется точка P', симметрична относительно серединного перпендикуляра к отрезку AB. Если γ является прямой, то она является или серединным перпендикуляром к отрезку AB, или прямой, параллельной AB. Оба эти варианта невозможны. Значит, γ является коникой.

Заметим, что кривой γ принадлежит ровно одна бесконечно удаленная точка (эта точка является пересечением перпендикуляров, восстановленных в точках A и B к отрезку AB). Коника, которой принадлежит ровно одна бесконечно удаленная точка, является параболой. Значит, γ является параболой, ось которой перпендикулярна прямой AB. Поскольку эта парабола проходит через точки A, B и P и ее ось параллельна оси данной

параболы, эта парабола совпадает с данной. Поэтому точка C движется по прямой, параллельной AB. □

Доказательство леммы 2 (b). Рассмотрим случай, когда точка P находится в той же полуплоскости относительно прямой AB, что и вершина параболы (случай, когда точка P находится в другой полуплоскости относительно прямой AB, доказывается аналогично). Серединные перпендикуляры к отрезкам AK и LB являются средними линиями трапеций $AKHC$ и $BLHC$. Следовательно, они пересекаются в середине отрезка HC. Значит, середина отрезка HC совпадает с точкой O. Обозначим проекцию точки C на прямую AB через S. Из леммы 2 (a) следует, что длина отрезка CS не зависит от положения точки P на параболе. Обозначим середину отрезка AB через M. Точка O находится на серединном перпендикуляре к отрезку AB, причем $OM = 1/2CS$. Следовательно, положение точки O не зависит от выбора точки P на параболе. □

Доказательство леммы 2 (c). Рассмотрим точку $P = A$. Тогда прямая AP будет касательной к параболе в точке A. Из того, что прямые AO и AP перпендикулярны и точка O лежит на серединном перпендикуляре к отрезку AB, следует, что точка O совпадает с центром окружности, касающейся параболы в точках A и B. Из леммы 2 (b) и вышесказанного следует, что для произвольного положения точки P на параболе, точка O является центром окружности, касающейся параболы в точках A и B. Значит, окружность ω совпадает с окружностью, касающейся параболы в точках A и B. □

Доказательство части «только тогда» леммы 1. Обозначим проекцию точки P на прямую AB через H, а проекции точки H на прямые AP и BP через K и L. Поскольку треугольники HPB и HPL подобны и окружность, касающаяся параболы в точках A и B, проходит через точки K и L (это следует из пункта (c) леммы 2), то $PH = \sqrt{PL \cdot PB}$. Значит, отрезок PH равен длине касательной, проведенной из точки P к окружности, касающейся параболы в точках A и B. □

Доказательство части «тогда» леммы 1. Предположим противное. Пусть точка P не лежит на параболе, касающейся окружности в точках A и B, но расстояние от точки P до прямой AB равно длине касательной, проведенной из точки P к окружности. Рассмотрим случай, когда точка P находится в той же полуплоскости относительно прямой AB, что и вершина параболы. Обозначим проекцию точки P на прямую AB через H. Обозначим точку пересечения прямой PH с параболой через P'. Точки P и P' различны, поскольку точка P не лежит на параболе. Пусть PX и $P'X'$ — отрезки касательных, проведенных из точек P и P' к окружности. Тогда $PH = PX$ по условию. Из части «только тогда» леммы 1 следует, что $P'H = P'X'$. Обозначим центр и радиус окружности через I

и r. Обозначим проекцию точки I на прямую PH через H'. Тогда

$$PH^2 - P'H^2 = PX^2 - P'X'^2 = (PI^2 - r^2) - (P'I^2 - r^2) =$$
$$= PI^2 - P'I^2 = PH'^2 - P'H'^2 = (PH + HH')^2 - (P'H + HH')^2 =$$
$$= PH^2 - P'H^2 + 2HH' \cdot (PH - P'H).$$

Следовательно, $2HH' \cdot (PH - P'H) = 0$. Но $PH \neq P'H$ и $HH' \neq \neq 0$, поскольку хорда AB не является диаметром. Противоречие. Случай, когда точка P находится в другой полуплоскости относительно прямой AB, доказывается аналогично. □

Доказательства остальных результатов.

Доказательство следствия 1. Аффинным преобразованием переведем оси парабол и диагонали параболического четырехугольника в две пары перпендикулярных прямых. Как известно, при произвольном аффинном преобразовании образ оси параболы параллелен оси образа параболы. Значит, оси образа параболического четырехугольника перпендикулярны. Поэтому из теорем 1 и 2 следует, что параболический четырехугольник при таком преобразовании переходит во вписанно-описанный. □

Доказательство следствия 2. Рассмотрим параболический четырехугольник с вершинами в точках A, B, C и D. Используя следствие 1, переведем соответствующий параболический четырехугольник во вписанно-описанный. Его осевая прямая параллельна оси параболы, являющейся образом исходной параболы. Следовательно, и осевая прямая четырехугольника $ABCD$ параллельна оси параболы. □

Доказательство следствия 3. Обозначим точки пересечения биссектрисы угла ALD с прямыми BC и AD через M и N. Тогда $BM/MC = LB/LC = AL/LD = AN/ND$. Значит, биссектрисы углов, образованных диагоналями вписанного четырехугольника являются осевыми прямыми этого четырехугольника. Поэтому из следствия 2 вытекает следствие 3.□

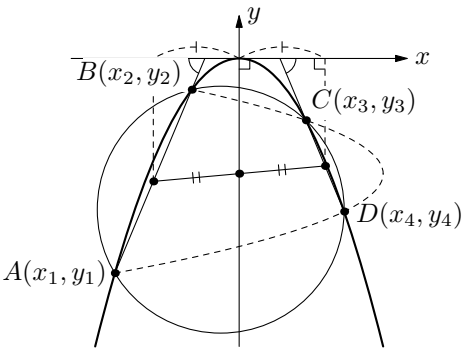


Рис. 11.

Доказательство утверждения 1. Рассмотрим систему координат, в которой одна из парабол имеет уравнение $y = kx^2$ (рис. 11). Обозначим координаты точек A, B, C и D в этой системе через (x_1, y_1), (x_2, y_2), (x_3, y_3)

и (x_4, y_4). Тогда $y_1 = kx_1^2$, $y_2 = kx_2^2$, $y_3 = kx_3^2$, $y_4 = kx_4^2$. Обозначим коэффициенты k прямых AB и CD через k_1 и k_2. По следствию 3 $k_1 = -k_2$. Поэтому $\dfrac{y_2 - y_1}{x_2 - x_1} = k(x_1 + x_2) = \dfrac{-(y_3 - y_4)}{x_3 - x_4} = -k(x_3 + x_4)$. Заметим, что $\dfrac{k(x_1 + x_2)}{2}$ и $\dfrac{-k(x_3 + x_4)}{2}$ являются абциссами середин отрезков AB и CD в заданной системе координат. Отсюда следует, что ось выбранной параболы проходит через середину отрезка, соединяющего середины отрезков AB и CD. Поэтому она проходит через центр тяжести четырехугольника $ABCD$. То же самое можно сказать и про ось другой параболы. Значит, оси парабол пересекаются в центре тяжести четырехугольника $ABCD$. □

Доказательство теоремы 3. Докажем эту теорему для $N = 3$. Из доказательства будет видно, что общий случай доказывается аналогично.

Следующая лемма очевидна.

Лемма. *Через точку внутри окружности проведены две хорды. Тогда парабола, касающиеся окружности в концах первой хорды, и парабола, касающаяся окружности в концах второй хорды, пересекаются в четырех точках.*

Из леммы 1 и этой леммы следует, что главные диагонали шестиугольника являются биссектрисами углов, на которые хорды делят плоскость. Поэтому хорды и главные диагонали делят плоскость на 12 равных углов (рис. 12). Рассмотрим две главные диагонали шестиугольника, концы которых принадлежат одной параболе. Тогда хорда, принадлежащая этой параболе, является биссектрисой угла, образованного этими диагоналями. Из этого и следствия 3 следует, что концы этих главных диагоналей, являющиеся вершинами шестиугольника, лежат на окружности. Мы доказали, что концы любых двух главных диагоналей шестиугольника лежат на одной окружности. Поэтому все вершины шестиугольника лежат на одной окружности. □

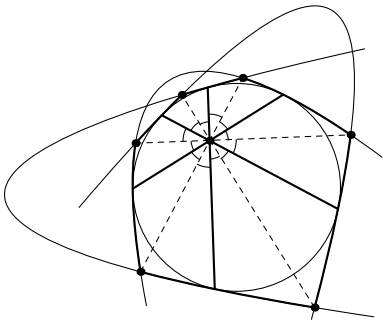


Рис. 12.

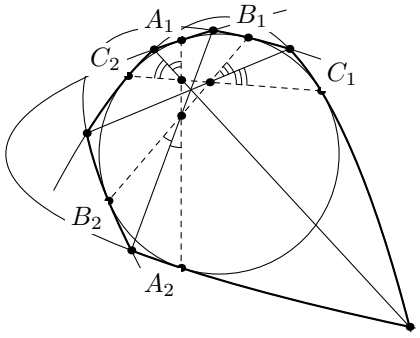


Рис. 13.

Доказательство утверждения 2. (См. рис. 13.)

Обозначим точки касания окружности с одной параболой через A_1 и A_2, со второй — через B_1 и B_2, с третьей — через C_1 и C_2. Из леммы 1 следует, что главные диагонали описанного параболического шестиугольника являются биссектрисами треугольника, образованного прямыми A_1A_2, B_1B_2 и C_1C_2. Значит, они пересекаются в одной точке. □

Покажем, как можно построить с помощью циркуля и линейки бесконечно много точек параболического четырехугольника с вершинами в четырех данных точках. Известно, что через четыре точки можно провести только две параболы. Приведем план этого построения. Обозначим через A, B, C и D четыре данные точки. Построим две осевые прямые четырехугольника $ABCD$. Они будут параллельны осям парабол, образующих параболический четырехугольник. Обозначим эти параболы через p_1 и p_2. Проведем окружность через точки A, B и C. Из следствия 3 следует, что если эта окружность и парабола p_1 (или p_2) пересекаются в четырех точках, то прямые, соединяющие эти точки, образуют равные углы с осевыми прямыми четырехугольника $ABCD$, следовательно, можно построить четвертую точку пересечения окружности с параболой p_1 (или p_2). Таким образом, построены пять точек параболы p_1 (или p_2). Значит, можно построить бесконечно много точек, принадлежащих параболическому четырехугольнику.

Благодарности

Автор благодарит А. А. Заславского за конструктивное обсуждение работы и за предложенную им идею доказательства части «тогда» теоремы 1 и А. Б. Скопенкова за ценные замечания при подготовке текста.

Список литературы

[1] А.В. Акопян, А.А. Заславский. *Геометрические свойства кривых второго порядка*. М.: МЦНМО, 2007.

[2] С. В. Маркелов. *Парабола как окружность* // Десятая летняя конференция Турнира городов. М.: МЦНМО, 1999. С. 36–42, 112–123.

[3] А. А. Заславский. *Геометрические преобразования*. М.: МЦНМО, 2003.

Ф. К. Нилов, лицей «Вторая школа», г. Москва

Конкурсы и олимпиады

Студенческие олимпиады и межкафедральный семинар на мехмате Московского государственного университета*

В. И. Богачев А. М. Райгородский А. Б. Скопенков†
Н. А. Толмачев

Великий ученый А. Н. Колмогоров говорил, что до тридцати лет математику разумнее всего заниматься решением конкретно поставленных задач. А значит, умение решать сложные задачи является одним из важнейших для молодого математика. В этой заметке рассказывается об опыте поддержания престижа умения решать трудные задачи, а также универсальности математического образования, при помощи *студенческих математических олимпиад* и *межкафедрального семинара имени А. Н. Колмогорова* на механико-математическом факультете Московского государственного университета им. М. В. Ломоносова. Приводятся задачи олимпиад и семинара.

Студенческие олимпиады

Примерно с 2001 года на мехмате МГУ возобновлена замечательная традиция проведения студенческих олимпиад. Отдельные кафедры проводят олимпиады и заочные конкурсы по теории вероятностей[1)], геометрии

*Полный обновляемый вариант этой информационной заметки находится по адресу: `http://dfgm.math.msu.su/files/skopenkov/stolymp.pdf`

†частично поддержан Российским Фондом Фундаментальных Исследований, Гранты номер 05-01-00993, 07-01-00648a и 06-01-72551-NCNILa, Грантами Президента РФ НШ-4578.2006.1 и МД-4729.2007.1, а также стипендией П. Делиня, основанной на его Премии Бальзана 2004 года.

[1)] См. `http://mech.math.msu.su/probab/olimpia/olimpia.htm`

и топологии[2)], алгебре[3)], анализу, механике, дифференциальным уравнениям и уравнениям с частными производными.

Большинство этих соревнований проводятся для студентов 1–2 курса и помогают студенту выбрать кафедру. Проводятся также общематематические олимпиады — олимпиада, посвященная Пифагору (2004 и 2005, [1]), и Заключительный тур всемехматовской олимпиады (с 2006; председатель жюри зав. отделением математики акад. РАН А. Т. Фоменко, зам. председателя жюри проф. В. И. Богачев). Важно, что при правильной организации студенческих олимпиад участие в них лишь помогает студенту начать научную работу [18, 21]. Задачи Заключительных туров выкладываются в интернете[4)] и приводятся ниже (после условия задачи в скобках указывается фамилия предложившего, который не обязательно является автором задачи; некоторые фамилии утрачены).

Команда мехмата МГУ участвует в международной студенческой математической олимпиаде IMC[5)] в тех случаях, когда это участие оплачивается спонсорами. Победители международных студенческих олимпиад регулярно получают приглашения учиться в престижнейших университетах мира, но, как правило, отказываются от них в пользу продолжения обучения в Московском Государственном Университете.

Задачи заключительных туров — плод коллективного труда сотрудников мехмата МГУ (окончательные варианты задач готовятся В. И. Богачевым); работы проверяют авторы этой заметки и М. Б. Скопенков. Мы надеемся, что со временем состав жюри будет расширяться. Мы приглашаем всех математиков передавать В. И. Богачеву задачи для заключительного тура (не по электронной почте!).

Правила приглашения на Заключительный тур и последующего формирования команды мехмата МГУ на международную олимпиаду основаны на объективных критериях и известны всем заинтересованным лицам (см., например, полный вариант этой заметки в интернете). Здесь мы приведем лишь составы команд:

(2001) Лившиц Е., Никокошев И., Поярков А., Скопенков М. и Черепанов Е.

(2006) Ефимов А. (гран-при), Калинин М. (1 премия), Козлов П. (1 премия) и Смирнов С. (3 премия) (Астахов В. прошел в команду, но не смог участвовать в олимпиаде).

(2007) Астахов В. (1 премия), Баранов Д. (1 премия), Ефимов А. (гран-при), Перепечко А. (1 премия) и Смирнов С. (1 премия) (Прасолов М.

[2)] См. `http://dfgm.math.msu.su/files/skopenkov/geomolym.pdf` и [9]

[3)] См. `http://www.math.msu.su/department/algebra/olymp-06.html`

[4)] См. `http://dfgm.math.msu.su/files/skopenkov/stolymp.pdf`

[5)] См. `http://www.imc-math.org`

и Абрамов Я. прошли в команду, но не участвовали в олимпиаде ввиду отсутствия загранпаспортов).

В 2006 и 2007 команды занимали II место в неофициальном командном зачете.

Мы благодарим М. Скопенкова за полезные замечания, а также Д. Вельтищева и М. Вельтищева за предоставление компьютерных версий рисунков.

Межкафедральный семинар

Традиция необязательных (про)семинаров для младшекурсников, направленных на изучение математики посредством решения задач и не являющихся узкоспециализированными, восходит к А. С. Кронроду (1950-е) и Е. М. Ландису (1970-е). Межкафедральный семинар имени А. Н. Колмогорова проводится с 2006 года. На нем решаются и разбираются интересные задачи из *разных* областей математики (этим наш семинар отличается от других). По формулировкам большинство их доступно даже первокурсникам (знающим текущий лекционный материал), но решения многих из них сложны. Эти задачи подобраны так, что в процессе их решения и обсуждения участники познакомятся с важными математическими понятиями и теориями. По каждой теме решаются и разбираются как простые ключевые задачи, так и более трудные задачи (в том числе олимпиадные и нерешенные).

Занятия семинара объединяются в циклы из 1–2 занятий, связанных общей темой или идеей. Разные циклы относятся к разным областям математики; эти циклы почти независимы друг от друга (поэтому можно изучать только те циклы, которые студенту наиболее интересны). Тем более занятия каждого семестра не зависят от занятий прошлого семестра! Например, майские занятия посвящены подготовке команды мехмата МГУ к международной олимпиаде. Большинство материалов доступно в интернете[6)], некоторые приводятся в этой заметке.

Некоторые занятия проводятся замечательными математиками, не являющимися соруководителями семинара (весна 2006 — А. А. Черный, осень 2006 — А. А. Клячко-мл. и В. Ю. Протасов, весна 2007 — А. Я. Белов-Канель и Э. Б. Винберг). Мы приглашаем всех математиков присылать руководителям предложения о проведении занятий семинара.

Активная работа в семинаре поможет студентам успешно участвовать в студенческих олимпиадах, развить математический кругозор (за счет знакомства с *идеями* из разных областей математики без долговременного

[6)] См. `http://dfgm.math.msu.su/materials.php`

изучения их *языка*), сделать первые математические открытия и, возможно, грамотно выбрать научное направление и руководителя.

Семинар назван именем великого математика А. Н. Колмогорова, который начал свой путь в науку в 19 лет с решения трудной проблемы о рядах Фурье, а в дальнейшем внес выдающийся вклад в разные области математики, тесно связанные с приложениями: теорию вероятностей, теорию динамических систем, гидродинамику и теорию сложности.

Задачи заключительных туров всемехматовских олимпиад

2001-1. Докажите, что для любых чисел a и b если $a > b > 0$, то $a^{b^a} > b^{a^b}$. (*П. Бородин*)

2001-2. Формулировка этой задачи утрачена.

2001-3, 2006-4. Пусть $k_1, \ldots, k_n$ — натуральные числа (не обязательно различные). Доказать, что сумма абсолютных величин коэффициентов многочлена $\prod_{j=1}^{n}(1 - z^{k_j})$ не меньше $2n$. (*С. Конягин*)

2001-4. Доказать, что для любой непрерывной на $[0, 1]$ действительной функции f найдется такое число a, что $\int\limits_0^1 \frac{dx}{|f(x) - a|} = \infty$. (*С. Конягин*)

2001-5. Существует ли такая постоянная C, что для любой непрерывно дифференцируемой на прямой действительной функции f, имеющей вторую производную, определенную всюду, кроме, может быть, конечного числа точек, условия $|f(x)| \leqslant 1$ для всех $x \in (-\infty, \infty)$ и $|f(x)f''(x)| \leqslant 1$ во всех точках существования $f''(x)$ влекут неравенство $|f'(x)| \leqslant C$ для всех $x \in (-\infty, \infty)$?

2001-6. Пусть G — группа нечетного порядка, не превосходящего 2001. Доказать, что существует такое множество $S \subset G$, содержащее не более 20 элементов, что каждый элемент G есть произведение нескольких различных элементов множества S.

2006-1. Пусть f — неотрицательная непрерывная функция на $[0, +\infty)$, причем $\int_0^T f(x)\,dx \leqslant T$ для всех $T \geqslant 0$. Докажите, что функция $\frac{f(x)}{1 + x^2}$ имеет конечный интеграл по $[0, +\infty)$. (*Фольклор*)

2006-2. Существуют ли два таких коммутирующих линейных оператора в $\mathbb{R}^3$, что нет базиса, в котором матрицы обоих операторов имеют жорданову форму? (*А. Ошемков и А. Скопенков*)

2006-3. См. теорему Петерсена-Морли [13, §3].

2006-5. Дан набор 11-мерных векторов, у каждого из которых 5 нулевых и 6 единичных координат. Диаметр набора (т. е. максимум попарных расстояний между его точками) равен $\sqrt{8}$.

(а) Какова максимальная возможная мощность такого набора?

(б) Докажите, что данный набор можно разбить на не более чем 18 частей меньшего диаметра. (*А. Райгородский*)

2006-6. Дана бесконечно дифференцируемая функция f на $\mathbb{R}^2$. Пусть U — такой открытый круг, что

$$\int\int_U \frac{|f(x)-f(y)|}{|x-y|^3}\,dx\,dy < \infty, \quad \text{где } \frac{|f(x)-f(y)|}{|x-y|^3} := 0 \text{ при } x = y.$$

Докажите, что функция f постоянна на U. (*В. Богачев*)

2007-1. Пусть P — многочлен степени d на прямой со старшим коэффициентом 1. Докажите, что длина множества $\{t\colon\ |P(t)| \leqslant c\}$ не превосходит $2dc^{1/d}$. (*В. Богачев*)

2007-2. (i) В конечном множестве выбрано конечное число подмножеств, пересечение любых двух из которых содержит не менее двух элементов. Докажите, что элементы данного множества можно так раскрасить в два цвета, чтобы никакое выбранное подмножество не было бы одноцветным.

(ii) То же с заменой условия «пересечение любых двух из которых содержит не менее двух элементов» на «пересечение никаких двух из которых не может содержать ровно один элемент». (*А. Райгородский*)

2007-3. Докажите, что для всякой вещественной матрицы $A = (a_{ij})$ порядка n выполнено неравенство

$$|\det(I+A)| \leqslant \exp\bigl(\operatorname{trace} A + \frac{1}{2}\sum_{i,j=1}^{n} a_{ij}^2\bigr).$$

(*неравенство Карлемана*)

2007-4. Дана последовательность вещественных чисел a_n. Известно, что для всякого $\lambda \in (1,2)$ последовательность чисел $a_{[\lambda^n]}$, имеет конечный предел. (Здесь $[r]$ — целая часть числа r.) Обязана ли сходиться сама последовательность $\{a_n\}$? (*А. Черный*)

2007-5. Существует ли в трехмерном пространстве многогранник (не обязательно выпуклый), все грани которого — шестиугольники? Определение многогранника и его грани см. в [5, с. 4. строка 2 снизу].

(*М. Скопенков*)

Указания и решения к некоторым задачам всемехматовских олимпиад

Авторы благодарны А. Москвину, Р. Авдееву и С. Конягину за предоставление своих решений задач 1, 2 и 4 2006 года, соответственно.

2006-1. Введем функцию $g(T) := \int_0^T f(t)dt$. Тогда из условия следует, что $0 \leqslant g(t) \leqslant t$ для любого $t > 0$. Для $M > 0$

$$\int_0^M \frac{f(t)dt}{1+t^2} = \int_0^M \frac{g'(t)dt}{1+t^2} = \int_0^M \frac{dg(t)}{1+t^2} = \frac{g(t)}{1+t^2}|_0^M + \int_0^M \frac{2tg(t)dt}{(1+t^2)^2}.$$

Оценим этот интеграл. Первое слагаемое в последнем выражении стремится к нулю при $M \to \infty$. Подынтегральная функция второго слагаемого положительна и ограничена интегрируемой на $[0, +\infty)$ функцией: $0 \leqslant \frac{2tg(t)dt}{(1+t^2)^2} \leqslant \frac{2t^2}{(1+t^2)^2}$. Значит, второе слагаемое имеет предел при $M \to \infty$. Отсюда следует утверждение задачи.

2006-2. Ответ: да.

Рассмотрим два линейных оператора, заданных в стандартном базисе следующими матрицами:

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}.$$

Непосредственно проверяется, что эти два оператора коммутируют.

Предположим, что существует общий базис (e_1, e_2, e_3), в котором обе матрицы приводятся к жордановой форме. У матрицы B два собственных значения 1 и 2, которым соответствуют собственные вектора $e_1 = (\mu, 0, 0)^T$ и $e_3 = (2\nu, 0, \nu)^T$. Поскольку в жордановой форме матрицы B присутствует жорданова клетка размера 2×2 с собственным значением 1 и e_1 — единственный (с точностью до пропорциональности) собственный вектор матрицы B с собственным значением 1, то можно выбрать вектор $e_2 = (\alpha, \beta, \gamma)$, для которого $(B - E)e_2 = e_1$. Из этого равенства получаем $e_2 = (\alpha, -\mu, \mu)^T$.

Заметим, что e_1 и e_3 — собственные векторы оператора A, отвечающие собственному значению 1. В жордановой форме матрицы A тоже присутствует клетка размера 2×2 с собственным значением 1. Поэтому вектор $(A - E)e_2 = (-\mu, 0, 0)^T$ равен либо e_1, либо e_3. Это не так (поскольку $\mu \neq 0$). Получили противоречие.

2001-3, 2006-4. Обозначим рассматриваемый многочлен через $f(z)$. Так как $f(1) = 0$, то $f(z) = \sum\limits_{j=1}^{r} z^{m_j} - \sum\limits_{j=1}^{r} z^{l_j}$, где никакое слагаемое из первой суммы не совпадает ни с каким слагаемым из второй. Поэтому искомая

сумма модулей коэффициентов равна $2r$. Далее, $f'(1) = \ldots = f^{(n-1)}(1) = 0$. Поэтому $\sum\limits_{j=1}^{r} m_j^p = \sum\limits_{j=1}^{r} l_j^p$, $p = 1, \ldots, n-1$. Значит, имеем соответствующие равенства для элементарных симметрических многочленов: $\sigma_i(m_1, \ldots, m_r) = \sigma_i(l_1, \ldots, l_r)$, $i = 1, \ldots, n-1$. Если бы $r \leqslant n-1$, то наборы $(m_1, \ldots, m_r)$ и $(l_1, \ldots, l_r)$ совпадали бы с точностью до перестановки, и тогда $f(z) \equiv 0$. Полученное противоречие показывает, что $r \geqslant n$.

2006-5-а. Ответ: C_{10}^4.

11-мерный вектор, состоящие из 5 нулевых и 6 единичных координат, можно интерпретировать как 5-элементное подмножество 11-элементного множества. Каждому такому вектору можно сопоставить набор из номеров тех мест, на которых стоят нули. При этом набору из 11-мерных векторов, диаметр которого равен $\sqrt{8}$, соответствует набор 5-элементных подмножеств 11-элементного множества, каждые два из которых пересекаются. Теперь вопрос можно переформулировать следующим образом:

> *каково максимально возможное число* 5*-элементных подмножеств* 11*-элементного множества, любые два из которых пересекаются?*

Примером из C_{10}^4 таких подмножеств является набор 5-элементных множеств, содержащих элемент 11 множества $\mathbb{Z}_{11} := \{1, 2, \ldots, 10, 11\}$.

Определим 5-элементные подмножества

$$A_s(\sigma) := \{\sigma(s), \sigma(s+1), \sigma(s+2), \sigma(s+3), \sigma(s+4)\}, \quad \text{где } \sigma \in S_{11} \text{ и } s \in \mathbb{Z}_{11}.$$

Подмножество $A_s(\sigma)$ не пересекается ни с $A_{s+5}(\sigma)$, ни с $A_{s+6}(\sigma)$. Поэтому произвольный набор 5-элементных подмножеств 11-элементного множества $\mathbb{Z}_{11}$, любые два из которых пересекаются, содержит не более пяти подмножеств из $A_1(\sigma), A_2(\sigma), \ldots, A_{11}(\sigma)$. Всего 5-элементных подмножеств C_{11}^5. Значит, число 5-элементных подмножеств в нашем наборе не превосходит $\dfrac{5}{11} C_{11}^5 = C_{10}^4$.

2006-5-б. Разобьем множество всех 11-мерных векторов из нулей и единиц на 16 подмножеств следующим образом. Каждое подмножество определяется первыми четырьмя числами в первых четырех разрядах. Очевидно, что таких подмножеств ровно 16. Нетрудно проверить, что расстояние между любыми двумя векторами из пересечения одного подмножества с данным набором не превосходит $\sqrt{7} < \sqrt{8}$.

2006-6. Для всякой дважды непрерывно дифференцируемой функции f разность $f(y) - f(x) - f'(x)(y-x)$ есть $O(|x-y|^2)$. Так как функция $|x-y|^{-1}$ интегрируема на $U \times U$ ввиду интегрируемости функции $|x|^{-1}$

на U (последнее легко проверить в полярных координатах), получаем интегрируемость $|x-y|^{-3}f'(x)(y-x)$ на $U\times U$. По теореме Фубини при почти каждом $x\in U$ функция $y\mapsto |x-y|^{-3}f'(x)(y-x)$ интегрируема на U. Заметим, что это возможно лишь при $f'(x)=0$. Для этого достаточно проверить, что для ненулевого вектора v функция $z\mapsto |z|^{-3}(v,z)$ не интегрируема в окрестности нуля. Действительно, поворотом системы координат приходим к случаю, когда $v=ce_1$, $e_1=(1,0)$. В полярных координатах интеграл модуля указанной функции есть интеграл от $cr^{-1}|\cos\theta|$ по $(0,r_0)\times[0,2\pi]$, т. е. бесконечен. Итак, $f'(x)=0$ при почти всех $x\in U$, откуда $f'(x)=0$ в U, т. е. f — постоянная.

Комментарий к задаче 2006-6. Доказанное легко обобщить на случай, когда от f требуется лишь измеримость (этот случай значительно более сложным способом был рассмотрен в [3]). Такой более общий случай сводится к случаю гладкой функции f с помощью сверток $f_\delta(x)=$ $=\int_U f(x+\delta u)\varrho(u)\,du$, $\quad x\in(1-\delta)U$, $\delta\in(0,1)$, где ϱ — неотрицательная гладкая функция с носителем в U и интегралом 1. Остается заметить, что при фиксированном $\varepsilon>0$ и $\delta<\varepsilon$ интегралы от $|x-y|^{-3}|f_\delta(x)-f_\delta(y)|$ по $(1-\varepsilon)U\times(1-\varepsilon)U$ конечны (тогда функции f_δ постоянны в $(1-\varepsilon)U$, значит, их предел f равен почти всюду некоторой постоянной). Это ясно из оценки

$$\int\int_{(1-\varepsilon)U}\frac{|f_\delta(x)-f_\delta(y)|}{|x-y|^3}\,dx\,dy\leqslant\int\int_U\frac{|f(x)-f(y)|}{|x-y|^3}\,dx\,dy,$$

получаемой непосредственно из определения f_δ с учетом того, что $x+$ $+\delta u, y+\delta u\in U$ при $x,y\in(1-\varepsilon)U$, $u\in U$, $\delta<\varepsilon$.

2007-5. Ответ: существует.

Основная идея состоит в том, чтобы искать требуемый многогранник среди невыпуклых (и даже не гомеоморфных шару) многогранников. Вот набросок только одной из возможных конструкций «торообразного» многогранника, удовлетворяющего условию. Возьмем многогранник в форме «рамки», то есть объединения четырех усеченных четырехугольных пирамид, с подходящим образом склеенными боковыми гранями. Он имеет 16 четырехугольных граней. Чтобы получить искомый многогранник, нужно теперь выбрать подходящим образом 8 попарно несмежных ребер и «срезать» их малые окрестности (а для тех ребер, двугранные углы при которых больше π, нужно, наоборот, «нарастить» многогранник). Получим 8 новых шестиугольных граней и из каждой четырехугольной грани получим шестиугольную, то есть у построенного многогранника все грани будут шестиугольниками.

Замечание. Очевидный подсчет эйлеровой характеристики показывает, что не существует *выпуклого* многогранника с требуемым свойством.

Проблема Борсука. Универсальные покрышки (А.М. Райгородский)

Проблема Борсука. *Требуется найти минимальное число $f(n)$ частей меньшего диаметра, на которые может быть разбито произвольное множество диаметра* 1 *в* $\mathbb{R}^n$. *Иными словами,*

$$f(n) = \max_{\Omega} \min\{f \ : \ \Omega = \Omega_1 \cup \cdots \cup \Omega_f, \ \operatorname{diam}\Omega_i < \operatorname{diam}\Omega \text{ для любого } i\},$$

где $\operatorname{diam}\Omega = \sup\limits_{x,y\in\Omega} |x-y|$.

Гипотеза Борсука. $f(n) = n+1$ [2, 7, 10–12, 19, 20].

1. (a) Докажите, что каждое множество $\Omega \subset \mathbb{R}^2$ диаметра 1 покрывается правильным шестиугольником с расстоянием 1 между параллельными сторонами.

(b) Разбейте шестиугольник из (a) на три части диаметра $\frac{\sqrt{3}}{2}$. Выведите отсюда справедливость гипотезы Борсука на плоскости.

(c) (неулучшаемость результата (b)). Приведите на плоскости пример такой фигуры диаметра 1, которую нельзя разбить на три части диаметра $< \frac{\sqrt{3}}{2}$.

2. Разбейте трехмерный шар на четыре части диаметра

(a) < 1, (b) $= \sqrt{\frac{3+\sqrt{3}}{6}}$.

3. Разбейте n-мерный шар на $n+1$ часть диаметра

(a) < 1, (b) как можно меньшего диаметра.

4. (a) Докажите теорему Юнга: *всякое множество* $\Omega \subset \mathbb{R}^n$ *диаметра* 1 *покрывается шаром радиуса* $\sqrt{\frac{n}{2n+2}}$ [4].

(b) Выведите из теоремы Юнга, что $f(n) \leqslant 2^n$.

5*. Теорема Борсука – Люстерника – Шнирельмана. Докажите, что

(a) трехмерный шар нельзя разбить на три части меньшего диаметра [2].

(b) n-мерный шар нельзя разбить на n частей меньшего диаметра [8].

Для изучения функции $f(n)$ уже оказалось полезным следующее понятие.

Множество $U \subset \mathbb{R}^n$ называется *универсальной покрышкой*, если для любого множества $\Omega \subset \mathbb{R}^n$ диаметра 1 существует такое движение φ, что $\Omega \subset \varphi(U)$.

Задача 1a означает, что в качестве универсальной покрышки в $\mathbb{R}^2$ можно взять правильный шестиугольник с расстоянием 1 между параллельными сторонами.

6. (a) Докажите, что универсальной покрышкой (в $\mathbb{R}^n$) является множество $B_1 \cap B_2 \subset \mathbb{R}^n$, где B_1 — шар радиуса $\sqrt{\frac{n}{2n+2}}$ и B_2 — шар радиуса 1 с центром на границе шара B_1.

(b) Выведите из (a), что $f(n) \leqslant 2^{n-1} + 1$.

(c)* Можно ли в какой-нибудь размерности уточнить результат (b)?

(d)* Докажите, что множество $B_1 \cap B_2$ нельзя разбить на 4 части меньшего диаметра.

7. (a) Докажите, что правильный октаэдр является универсальной покрышкой в размерности 3, если расстояние между его параллельными гранями равно 1 (т. е. если октаэдр задается уравнением $|x|+|y|+|z| \leqslant \sqrt{3}/2$).

(b) Отсечем от октаэдра из (a) в трех взаимно перпендикулярных направлениях три пирамиды; отсечения производятся посредством плоскостей, параллельных координатным и отстоящих от начала координат на расстояние 0.5. Докажите, что полученный 11-гранник U_1 является универсальной покрышкой.

(c) Разбейте 11-гранник U_1 на 4 части диаметра < 1. Выведите отсюда справедливость гипотезы Борсука в пространстве.

(d) Разбейте 11-гранник U_1 на 4 части диаметра $\leqslant 0.9888$.

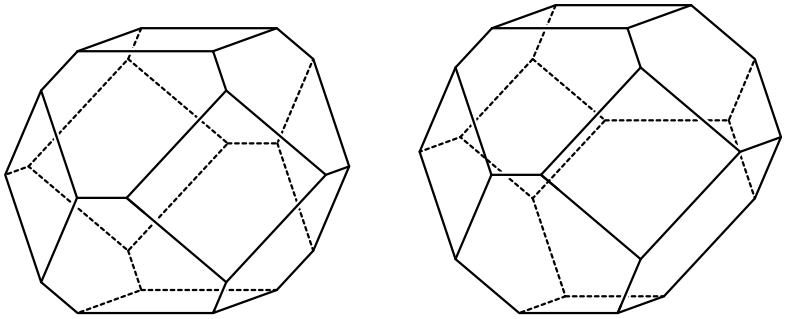


Рис. 1. *Многогранники U_1 и U_2*

8*. *Ромбододекаэдром* называется многогранник, являющийся выпуклой оболочкой множества точек в $\mathbb{R}^3$ вида $(\pm 1, \pm 1, \pm 1)$ (восемь вершин) и $(0, 0, \pm 2)$ (шесть вершин). Это двенадцатигранник, грани которого суть ромбы.

(a) Докажите, что в качестве универсальной покрышки в $\mathbb{R}^3$ можно взять ромбододекаэдр, у которого расстояние между любыми двумя параллельными гранями равно 1.

(b) Докажите, что данный ромбододекаэдр останется универсальной покрышкой, если отсечь от него «шапочки» по тому же принципу, что и в задаче 7b.

(c) Разбейте множество без шапочек из (a) на 4 части диаметра < 1.

(d) Разбейте множество без шапочек из (a) на 4 части диаметра $\leqslant 0.98$.

9. 11-гранник U_1 определен в задаче 7b. Определим многогранник U_2 аналогично, отсекая от правильного октаэдра шесть пирамид шестью плоскостями, параллельными диагональным сечениям октаэдра. Три из этих плоскостей (взаимно перпендикулярные) проходят на расстоянии 0.5 от центра октаэдра, три остальные плоскости (тоже взаимно перпендикулярные) — на расстоянии 0.525.

(a) Докажите, что для любого множества $\Omega \subset \mathbb{R}^3$ диаметра 1 существует такое движение φ, что либо $\Omega \subset \varphi(U_1)$, либо $\Omega \subset \varphi(U_2)$.

(b) Разбейте каждое из множеств U_1, U_2 на 4 части диаметра < 1.

(c) Разбейте каждое из множеств U_1, U_2 на 4 части диаметра $\leqslant 0.9843$.

10*. Проблема Гэйла. Существует ли множество в $\mathbb{R}^3$, которое нельзя разбить на 4 части диаметра < 0.9?

11*. Верна ли гипотеза Борсука

(a) в $\mathbb{R}^4$, (b) для конечных наборов точек в $\mathbb{R}^4$?

12*. Назовем множество точек *двухдистанционным*, если расстояние между любыми двумя его элементами принадлежит некоторому множеству $\{a, b\}$. Верна ли гипотеза Борсука для двухдистанционных множеств

(a) в $\mathbb{R}^4$, (b) в $\mathbb{R}^n$?

Задачи 10, 11 и 12b являются нерешенными.

13. [15] Выпуклое множество $\Omega \subset \mathbb{R}^n$ называется *множеством постоянной ширины,* если расстояние между любыми двумя его параллельными опорными гиперплоскостями (т. е. прямыми для $n = 2$) одно и то же. Примеры: круг, треугольник Рело.

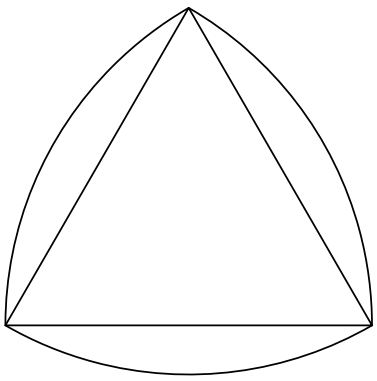


Рис. 2. *Треугольник Рело*

(a) Докажите, что любое выпуклое множество $\Omega \subset \mathbb{R}^2$ диаметра 1 покрывается множеством постоянной ширины 1 (и, как следствие, диаметра 1).

(b) То же с заменой $\mathbb{R}^2$ на $\mathbb{R}^n$.

(c) Докажите теорему Ленца: *n-мерное множество постоянной ширины нельзя разбить на n частей меньшего диаметра.*

14. Проблема Грюнбаума. [6] *Требуется найти минимальное число $g(n)$ (открытых) шаров диаметра* 1, *которыми может быть покрыто произвольное множество диаметра* 1 *в* $\mathbb{R}^n$. *Иными словами,*

$$g(n) = \max_{\Omega} \min\{g : \Omega \subset B_1 \cup \cdots \cup B_g, \quad \operatorname{diam} B_i = \operatorname{diam} \Omega \text{ для любого } i\}.$$

(a) Найдите $g(2)$.

(b) Найдите или оцените $g(3)$.

(c) Докажите, что при достаточно большом n выполнено неравенство $g(n) > n + 1$. Найдите как можно меньшее значение размерности n, в которой это так.

(d) Докажите, что $g(n) > n + 1$ при $n \geqslant 4$.

(e)* Докажите, что $g(n) > c^n$ для некоторого $c > 1$.

Графы и игры
(А.М. Райгородский)

Игра Эренфёйхта. Даны графы $G = (V, E)$ и $H = (W, F)$. Также фиксировано некоторое число $t > 0$. Двое — Добытчик и Повторитель — играют в игру, которую мы обозначим $EHR(G, H, t)$. Всего в игре t раундов. В каждом раунде сперва делает ход Добытчик, затем настает черед Повторителя. Всякий раз Добытчик выбирает по своему усмотрению один из двух графов и из множества его вершин извлекает какую-нибудь одну. Таким образом, в i-м раунде игры Добытчик, делая свой ход, берет либо произвольную вершину $x_i \in V$, либо произвольную вершину $y_i \in W$. Повторитель вслед за Добытчиком также должен достать из какого-то графа некоторую его вершину; только у него уже нет такой свободы выбора, как у Добытчика, и свою вершину он обязан брать из графа G, коль скоро его противник воспользовался графом H, и наоборот. В конечном итоге выбранными окажутся $x_1, \ldots, x_t \in V$ и $y_1, \ldots, y_t \in W$. Мы скажем, что Повторитель выиграл, если ему удалось так «скопировать» действия Добытчика, чтобы графы $G|_{\{x_1,\ldots,x_t\}}$ и $H|_{\{y_1,\ldots,y_t\}}$ были «упорядоченно изоморфны». Здесь $G|_{\{x_1,\ldots,x_t\}} = (\{x_1, \ldots, x_t\}, E')$, так что $(x_i, x_j) \in E'$ тогда и только тогда, когда $(x_i, x_j) \in E$. Графы *упорядоченно изоморфны*, коль скоро условие $(x_i, x_j) \in E'$ равносильно условию $(y_i, y_j) \in F'$.

1. Пусть в графе G есть изолированная вершина, а в графе H таких вершин нет. Докажите, что у Добытчика всегда имеется выигрышная стратегия в игре $EHR(G, H, 2)$.

2. Пусть граф G содержит K_4 (полный подграф на четырех вершинах). Предположим, что в H таких подграфов нет. При каком минимальном t у Добытчика заведомо есть выигрышная стратегия в игре $EHR(G, H, t)$?

3. Пусть граф G содержит K_5. Допустим, граф H планарен. Существует ли t, при котором у Добытчика всегда есть выигрышная стратегия в игре $EHR(G, H, t)$?

Определение радиуса графа. Назовем *расстоянием* между двумя вершинами x, y графа $G = (V, E)$ длину $d(x, y)$ кратчайшего реберного пути, которым эти вершины соединены. Обозначим через $e(x)$, $x \in V$, величину $e(x) = \max\limits_{y \in V} d(x, y)$. Будем говорить, что $r(G) = \min\limits_{x \in V} e(x)$ — это *радиус* графа G.

4. Пусть $r(G) \leqslant 2$, а $r(H) > 2$. Существует ли t, при котором у Добытчика всегда есть выигрышная стратегия в игре $EHR(G, H, t)$?

5. Для каждого $t > 0$ постройте примеры таких графов G, H, что у Повторителя есть выигрышная стратегия в игре $EHR(G, H, t)$.

Язык первого порядка для графов. Алфавит языка первого порядка для описания тех или иных свойств графов состоит из символов $x, y, \ldots$, обозначающих вершины графа. Далее, имеются значки «=» и «$\sim$»; здесь под $x \sim y$ подразумевается смежность вершин x, y. Есть также стандартные логические символы типа кванторов $\forall$ и $\exists$, импликации, конъюнкции, дизъюнкции, отрицания и проч. Фразы должны быть конечными.

6. Запишите свойство «граф имеет изолированную вершину» на языке первого порядка.

7. Запишите свойство «граф содержит K_4» на языке первого порядка.

8. Запишите свойство «граф имеет радиус $\leqslant 2$» на языке первого порядка.

9. Можно ли записать на языке первого порядка свойство «граф связен»?

10. Можно ли записать на языке первого порядка свойство «граф не планарен»?

11*. Докажите, что если граф G обладает свойством A, которое можно записать на языке первого порядка, а граф H этим свойством не обладает, то существует $t = t(A)$, при котором Добытчик заведомо располагает выигрышной стратегией в игре $EHR(G, H, t)$.

Случайные графы. Для каждого целого положительного n положим $V_n = \{1, \dots, n\}$ и зафиксируем $p = p(n) \in (0, 1)$. Рассмотрим вероятностное пространство $(\Omega_n, \mathcal{B}_n, P_n)$, в котором $\Omega_n = \{G = (V_n, E)\}$, так что $|\Omega_n| = 2^{C_n^2}$, $\mathcal{B}_n = 2^{\Omega_n}$ и $P_n(G) = p^{|E|}(1-p)^{C_n^2 - |E|}$. Назовем произвольный элемент из Ω_n *случайным графом в модели* $G(n, p)$. Можно понимать это так: в случайном графе на данных n вершинах ребра проводятся независимо друг от друга с вероятностью p. Иными словами, речь идет о схеме Бернулли с C_n^2 независимыми испытаниями. Найти вероятность того, что случайный граф $G \in \Omega_n$ обладает некоторым свойством A, — это то же самое, что найти вероятность множества $B \in \mathcal{B}_n$ всех графов $G \in \Omega_n$, которые этим свойством обладают. Мы скажем, что G обладает свойством A (*асимптотически*) *почти наверное* (*п.н.*), если

$$P_n(G \text{ обладает свойством } A) \to 1, \quad n \to \infty.$$

12. Докажите, что при $p = o\left(\frac{1}{n}\right)$ граф п.н. двудолен.

13. Докажите, что при $p = o\left(\frac{1}{n}\right)$ граф п.н. не содержит треугольников.

14. Докажите, что при $p \geqslant \frac{3 \log n}{n}$ граф п.н. связен.

15. Пусть дана функция $p = p(k) \in (0, 1)$, G — случайный граф в модели $G(n, p(n))$, а H — случайный граф в модели $G(m, p(m))$. Пусть, далее, A — некоторое свойство графа, которое можно записать на языке первого порядка. Предположим, наконец, что для данного p и для произвольного фиксированного t выполнено

$$\lim_{n\to\infty} \lim_{m\to\infty} P(\text{Повторитель имеет выигрышную стратегию в игре } EHR(G, H, t)) = 1.$$

С помощью результата задачи 11* докажите, что тогда свойство A либо п.н. выполнено, либо п.н. не выполнено.

16. Скажем, что граф $G = (V, E)$ обладает свойством F_s (где s — целое положительное), если для любых натуральных a, b, $a + b \leqslant s$, и для произвольных $u_1, \dots, u_a, v_1, \dots, v_b \in V$ найдется такая вершина $x \in V$, что x смежна с каждой вершиной u_i, $i = 1, \dots, a$, и x не смежна ни с одной из вершин v_j, $j = 1, \dots, b$. Предположим, что графы G и H обладают свойством F_s. Докажите, что тогда Повторитель заведомо располагает выигрышной стратегией в игре $EHR(G, H, t)$ с любым $t \leqslant s$.

17. Докажите, что при $p = const$ и $s = const$ п.н. граф обладает свойством F_s.

18. С помощью результатов задач 15, 16 и 17 докажите, что при любом постоянном p имеет место *закон нуля и единицы* для свойств графов, ко-

торые записываются на языке первого порядка: такое свойство либо п.н. выполнено, липо п.н. не выполнено.

19*. Докажите, что при $p = n^{-\alpha}$, $\alpha \in \mathbb{Q}$, не всегда имеет место закон нуля и единицы для свойств графов, которые записываются на языке первого порядка. (Нужно привести пример числа α, а также некоторого свойства, асимптотическая вероятность которого в модели $G(n,p)$ не есть ни 0, ни 1.)

20**. Докажите, что результат задачи 18 верен при всех $p = n^{-\alpha}$, $\alpha \notin \mathbb{Q}$.

Принцип вложенных отрезков, или примени теорему Бэра о категории

(А. Б. Скопенков)

Этот цикл задач посвящен мощному средству доказательства теорем существования. В анализе с помощью нее доказывается, например, теорема Банаха об обратном операторе, которая применяется для доказательства существования решений нелинейных уравнений. В топологии теорема Бэра применяется, например, к вложениям компактов и к аппроксимации отображений гомеоморфизмами (ср. [9, 22]).

0. Объединение открытых интервалов $U \subset \mathbb{R}$ не является ограниченным. Докажите, что существует такое x, что $nx \in U$ для бесконечно большого количества целых n.

Указание. Сначала докажите, что

– существует такое $x_1 \in (0,1)$, что $n_1 x_1 \in U$ для некоторого $n_1 > 1$.

Тогда

– существует такое $\epsilon_1 > 0$, что $n_1(x_1 - \epsilon_1, x_1 + \epsilon_1) \in U$.

Потом докажите, что

– существует такое $x_2 \in (x_1 - \epsilon_1, x_1 + \epsilon_1)$, что $n_2 x_2 \in U$ для некоторого $n_2 > 2$.

И т.д.

Такие решения, основанные на принципе вложенных отрезков, удобно придумывать и записывать на языке *теоремы Бэра о категории.*

Напомним, что подмножество $U \subset \mathbb{R}$ называется

открытым, если для любого $x \in U$ существует такое $\varepsilon > 0$, что $(x - \varepsilon, x + \varepsilon) \subset U$.

вседу плотным, если для любых $a, b \in \mathbb{R}$ пересечение $(a,b) \cap U$ непусто.

1. Теорема Бэра о категории. Пересечение счетного числа открытых всюду плотных подмножеств прямой является всюду плотным (и, в частности, непустым).

Приведенное решение задачи 1 коротко записывается так: по теореме Бэра о категории $\bigcap\limits_{n=1}^{\infty}\bigcup\limits_{k=n}^{\infty}\frac{1}{k}U\neq\varnothing$.

2. Докажите, что существует такая последовательность $x_n\in\mathbb{R}$, что для любой возрастающей ограниченной последовательности $y_n\in\mathbb{R}$ найдется номер n, для которого $|x_n-y_n|\leqslant 1/n$.

3. Докажите следующее для функций $\mathbb{R}\to\mathbb{R}$.

(a) Поточечный предел непрерывных функций обязательно имеет точку непрерывности.

Указание. Множество точек непрерывности функции f — это

$$\bigcap_{n=1}^{\infty}\bigcup_{k=1}^{\infty}\{x\ :\ |f(y_1)-f(y_2)|<\frac{1}{n}\text{ при }x-\frac{1}{k}<y_1<y_2<x+\frac{1}{k}\}.$$

(b) Производная любой дифференцируемой функции имеет точку непрерывности.

(c)* Любая монотонная функция имеет точку дифференцируемости.

Указание. Здесь точки дифференцируемости «почти все» по мере, а не по Бэру.

(d) Любая липшицева функция имеет точку дифференцируемости.

Указание. Используйте предыдущий пункт и разложение липшицевой функции в разность монотонных.

4. Докажите, что если функция двух переменных непрерывна по каждой переменной, то она имеет точку непрерывности.

5. Дана бесконечно дифференцируемая функция $f\colon\mathbb{R}\to\mathbb{R}$, причем для любого x и для

(a) всех чисел $n>N_x$;

(b)* бесконечного количества чисел n;

(c)* некоторого $n=n(x)$

выполнено $f^{(n)}(x)=0$. Докажите, что f — многочлен.

Указание к (a). Пусть f не многочлен. Положим $U_n:=\mathbb{R}-\bigcap\limits_{k=n}^{\infty}(f^{(k)})^{-1}(0)$. Тогда U_n открыто и непусто, $U_1\supset U_2\supset\ldots$ и $\bigcap\limits_{n=1}^{\infty}U_k=\varnothing$. Из этих свойств множеств U_n вытекает, что *существуют такие* n *и максимальный интервал* $(a,b)\subset U_n$, *что для некоторого* $\epsilon>0$ *один из интервалов* $(a,a+\epsilon)$ *и* $(b-\epsilon,b)$ *не пересекает множество* U_{n+1} (докажите!). Не уменьшая общности, $(a,a+\epsilon)\cap U_{n+1}=\varnothing$, т. е. $f^{(n+1)}([a,a+\epsilon])=0$. Так как $f^{(n)}(a)=0$, то $f^{(n)}([a,a+\epsilon])=0$, что противоречит условию $(a,b)\subset U_n$.

6. Докажите, что

(a)* прямая не представима в виде объединения попарно непересекающихся неточечных замкнутых отрезков.

(b) плоскость не представима в виде объединения замкнутых кругов с попарно непересекающимися непустыми внутренностями.

7. (a) Дано замкнутое ограниченное подмножество $A \subset \mathbb{R}^2$. Для любых двух точек $x, y \in A$ существует разбиение $A = X \sqcup Y$ на замкнутые множества, для которого $x \in X$ и $y \in Y$ (такие множества называются *нульмерными*). Докажите, что существует непрерывное инъективное отображение (т. е. *вложение* или реализация) $a : A \to \mathbb{R}$.

(b)* Дано замкнутое ограниченное подмножество $A \subset \mathbb{R}^{100}$. Для любых двух точек $x, y \in A$ существует разложение $A = X \cup Y$ в объединение замкнутых множеств, пересечение которых нульмерно, причем $x \in X$ и $y \in Y$ (такие множества называются *одномерными*). Докажите, что существует непрерывное инъективное отображение $a\colon A \to \mathbb{R}^3$.

(c)* *Теорема Менгера – Небелинга – Понтрягина*. Дайте определение n-мерного (замкнутого ограниченного) множества в $\mathbb{R}^N$ и докажите, что любое n-мерное множество вложимо в $\mathbb{R}^{2n+1}$.

Список литературы

[1] Авдеев Р., Москвин А., *Студенческая олимпиада по математике* // Математическое просвещение, сер. 3, вып. 12, 2008. С. 223–227.

[2] Болтянский В. Г., Гохберг И. Ц. *Теоремы и задачи комбинаторной геометрии*. М.: Наука, 1965.

[3] Брезис Х. *Как распознать постоянные функции. Связь с пространствами Соболева* // Успехи мат. наук. Т. 54, вып. 4, 2002. С. 59–74.

[4] Данцер Л., Грюнбаум Б., Кли В. *Теорема Хелли*. М.: Мир, 1968.

[5] Долбилин Н. П. Жемчужины теории многогранников. М.: МЦНМО, 2000.

[6] Грюнбаум Б. *Этюды по комбинаторной геометрии и теории выпуклых тел*. М.: Наука, 1971.

[7] Гервер М. Л. *Проблема Борсука* // Математическое просвещение, сер. 3, вып. 3, 1999. С. 168–183.

[8] Люстерник Л. А., Шнирельман Л. Г. *Топологические методы в вариационных задачах*. М.: Госиздат, 1930.

[9] Ошемков А., Скопенков А. *Олимпиады по геометрии и топологии* // Математическое просвещение, сер. 3, вып. 11, 2007. С. 131–140.

[10] Райгородский А. М. *Проблема Борсука и хроматические числа некоторых метрических пространств* // Успехи Матем. Наук. Т. 56, вып. 1, 2001. С. 107–146.

[11] Райгородский А. М. *Проблема Борсука.* М: МЦНМО, 2006.

[12] Скопенков А. *N-мерный куб, многочлены и решение проблемы Борсука* // Математическое просвещение, сер. 3, вып. 3, 1999. С. 184–188.

[13] Скопенков М. *Теорема о высотах треугольника и тождество Якоби* // Математическое Просвещение, сер. 3, вып. 11, 2007. С. 79–89.

[14] Эрдёш П., Спенсер Дж. *Вероятностные методы в комбинаторике*. М.: Мир, 1976.

[15] Яглом И. М., Болтянский В. Г. *Выпуклые фигуры*. М.: Гостехиздат, 1951.

[16] Alon N., Spencer J. *The probabilistic method.* Wiley - Interscience Series in Discrete Math. and Optimization, Second Edition, 2000.

[17] Bollobás B. *Random Graphs*. Cambridge Univ. Press, Second Edition, 2001.

[18] Efimov A. *The asymptotics for the number of real roots of the Bernoulli polynomials*. Eprint, 2006. arXiv:math/0606361.

[19] Raigorodskii A. M. *The Borsuk partition problem*: *the seventieth anniversary* // Mathematical Intelligencer, V. 26, N4, 2004. P. 4–12.

[20] Skopenkov A. *Borsuk's problem* // Quantum. Vol. 7, no 1, 1996. P. 16–21, 63.

[21] Skopenkov M. *On approximability by embeddings of cycles in the plane* // Topol. Appl. Vol. 134, 2003. P. 1–22.

[22] Skopenkov A. *A characterization of submanifolds by a homogeneity condition* // Topol. Appl. Vol. 154, 2007. P. 1894-1897.
`http://dx.doi.org/10.1016/j.topol.2007.03.002`,
`http://arxiv.org/abs/math.GT/0606470`

В. И. Богачев, А. М. Райгородский, Н. А. Толмачев: механико-математический факультет Московского государственного университета им. М. В. Ломоносова

А. Б. Скопенков: механико-математический факультет МГУ, Независимый московский Университет, Московский институт открытого образования
e-mail: `skopenko@mccme.ru`

Студенческая олимпиада по математике

Р. Авдеев А. Москвин

В декабре 2005 года на механико-математическом факультете МГУ была проведена олимпиада по математике для студентов 1–2 курсов. На решение шести предложенных задач участникам давалось пять часов. Для успешного выполнения всех заданий олимпиады было достаточно владения материалом первого семестра.

До 1989 г. общефакультетские олимпиады проводились регулярно, а в 2004 г. эта традиция возобновилась по инициативе студентов. Умение решать нестандартные задачи очень важно для начинающих математиков. Для развития этого умения одних только лекций и семинаров может быть недостаточно. Олимпиады помогают восполнить этот недостаток.

Организация и проведение олимпиады являлись результатом коллективного труда преподавателей и студентов старших курсов факультета. Тематика олимпиады охватила различные разделы математики: в составлении задач, а затем и в проверке работ принимали участие представители различных кафедр.

Отметим лучшие результаты среди участников. По 5 задач решили первокурсник Александр Ефимов, второкурсники Алексей Лазарев и Кирилл Попков. По 4 задачи — первокурсники Василий Астахов, Алексей Головко, Александр Перепечко, Андрей Трепалин и второкурсник Дмитрий Пермяков.

Задачи олимпиады

1. Доказать, что угол между концентрическими равносторонними гиперболами равен удвоенному углу между их асимптотами. (*А. Акопян*)

2. Доказать, что не существует многочлена $f(x_1, x_2, x_3, x_4) \in \mathbb{C}[x_1, x_2, x_3, x_4]$, для которого решением системы

$$\begin{cases} x_1x_2 = x_3x_4, \\ f(x_1, x_2, x_3, x_4) = 0 \end{cases}$$

является в точности множество $\{(x_1, x_2, x_3, x_4) \in \mathbb{C}^4 \mid x_1 = 0, x_3 = 0\}$. (*Р. Авдеев*)

3. Рассмотрим множество Γ графов без петель и кратных ребер, включая пустой граф. Пусть $G \in \Gamma$ — граф, а x — его произвольная вершина. Обозначим через G_x подграф, получающийся из G выбрасыванием вершины x, а через $\overline{G}_x$ — подграф, получающийся из G выбрасыванием вершины x и всех вершин, с которыми вершина x не соединена ребром (вершины выбрасываются вместе со всеми выходящими из них ребрами).

Доказать, что существует (хотя бы одна) функция $f\colon \Gamma \to \mathbb{Z}$, удовлетворяющая следующим трем условиям:

1) $f(\varnothing) = 1$ ($\varnothing$ — пустой граф);

2) $f(\cdot) = 0$ ($\cdot$ — граф с одной вершиной);

3) $f(G) = f(G_x) - f(\overline{G}_x)$, где G — произвольный граф с $n \geqslant 2$ вершинами, а x — произвольная вершина графа G (граф $\overline{G}_x$ может быть пустым). (*Р. Авдеев*)

4. Выяснить, существует ли функция $f(x) \in C^1(-\varepsilon, \varepsilon)$ со следующими свойствами:

a) $f(0) = 0$;

b) $f'(x) \neq 0$ при $x \neq 0$;

c) $\lim\limits_{x \to 0} \dfrac{f(x)}{f'(x)} = \infty$. (*И. Х. Сабитов*)

5. Две плоскости в пространстве пересекаются под углом $\dfrac{3\pi}{4}$. Пусть O — одна из точек пересечения. Отрезок OA равномерно вращается в первой плоскости относительно точки O. Найти все углы $\alpha \in (0, \dfrac{\pi}{2})$, для которых существует такое непрерывное (но не обязательно равномерное) вращение отрезка OC во второй плоскости относительно точки O, что в любой момент времени $\angle AOC = \alpha$. (*А. Т. Фоменко*)

6. а) Доказать, что для любого множества A, состоящего из n различных действительных чисел, найдется такое число u, что количество чисел, представимых в виде $a_1 + ua_2$, $a_1, a_2 \in A$, больше $n^2 - n$, но строго меньше n^2.

б) Доказать, что количество чисел вида $a_1(a_3 - a_4) + a_2(a_5 - a_6)$, $a_1, \ldots, a_6 \in A$, больше $n^2 - n$. (*С. В. Конягин*)

Решения задач

1. Введем на плоскости систему координат, в которой уравнение первой из гипербол запишется в виде

$$xy = 1.$$

Тогда вторая гипербола получается из первой линейным преобразованием, переводящим асимптоты в асимптоты, т. е.

$$\begin{cases} \tilde{x} = \lambda(x\cos\varphi + y\sin\varphi), \\ \tilde{y} = \lambda(-x\sin\varphi + y\cos\varphi), \end{cases}$$

где $\varphi \in (-\frac{\pi}{2}, \frac{\pi}{2}]$ — угол между осями гипербол (он же — один из углов между асимптотами). В новой системе координат уравнение второй гиперболы имеет вид $\tilde{x}\tilde{y} = 1$, а в старой —

$$(x\cos\varphi + y\sin\varphi)(-x\sin\varphi + y\cos\varphi) = \lambda^{-2}.$$

Направляющий вектор касательной к кривой второго порядка $\{F(x,y) = 0\}$ в точке (x_0, y_0) имеет вид $(-F'_y(x_0,y_0), F'_x(x_0,y_0))$. Пусть (x_0, y_0) — точка пересечения наших гипербол. Тогда направляющий вектор касательной к первой гиперболе в этой точке — это $\vec{\xi} = (-x_0, y_0)$, ко второй — $\vec{\eta} = (-x_0\cos 2\varphi - y_0\sin 2\varphi, -x_0\sin 2\varphi + y_0\cos 2\varphi)$. Имеем

$$\cos(\vec{\xi}, \vec{\eta}) = \frac{(\vec{\xi}, \vec{\eta})}{|\vec{\xi}| \cdot |\vec{\eta}|} = \cos 2\varphi,$$

откуда и следует утверждение задачи.

2. Пусть такой многочлен $f(x_1, x_2, x_3, x_4)$ существует. Покажем, что тогда во множестве $A = \{(x_1, x_2, x_3, x_4) \in \mathbb{C}^4 \mid x_2 = 0, x_4 = 0\}$ лежит кроме начала координат еще по крайней мере одна точка, удовлетворяющая системе.

Действительно, каждая точка множества A удовлетворяет первому уравнению системы. Пусть $g(x_1, x_3) = f(x_1, 0, x_3, 0)$. Осталось показать, что у этого многочлена в $\mathbb{C}(x_1, x_3)$ имеется не меньше двух нулей. По условию, один нуль — это начало координат $(0, 0)$. Поэтому свободный член этого многочлена равен нулю. Если $g(x_1, x_3) \equiv 0$, то в качестве нуля можно взять любую точку, отличную от начала координат. Пусть $g(x_1, x_3) \not\equiv 0$. Запишем многочлен $g(x_1, x_3)$ в виде

$$g(x_1, x_3) = h_n(x_3)x_1^n + \ldots + h_1(x_3)x_1 + h_0(x_3),$$

где $h_k(x_3)$ — многочлены, зависящие только от x_3, причем $h_n(x_3)$ — ненулевой многочлен, стоящий при наибольшей степени по x_1 многочлена $g(x_1, x_3)$.

Если эта наибольшая степень отлична от нуля, то существует такое значение $x_3 = c \neq 0$, что $h_n(c) \neq 0$. Значит, многочлен $g(x_1, c)$ не является константой и имеет хотя бы один корень $x_1 = d$. Получаем $g(d, c) = 0$.

Теперь пусть $g(x_1, x_3) = h_0(x_3)$. Многочлен $h_0(x_3)$ имеет нулевой свободный член, и поэтому $x_3 = 0$ — его корень. Значит, можно положить $x_1 = 1$ и получить $g(1, 0) = 0$.

3. Единственная функция, удовлетворяющая условиям задачи, имеет вид

$$f(G) = \sum_{k=0}^{n} (-1)^k H_k,$$

где n — количество вершин графа G, H_k — количество полных подграфов графа G, содержащих k вершин. В частности, $H_0 = 1$, $H_1 = n$. Полный граф — граф, у которого любая пара вершин соединена ребром. Полный подграф определяется множеством своих вершин (порядок вершин неважен). Осталось показать, что предъявленная функция действительно удовлетворяет рекуррентному соотношению. Это можно сделать, подсчитав числа H_k графа G через эти же числа графов G_x и $\overline{G}_x$:

$$H_k(G) = H_k(G_x) + H_{k-1}(\overline{G}_x),$$

откуда

$$f(G) = \sum_{k=0}^{n} (-1)^k H_k(G) = \sum_{k=0}^{n} (-1)^k (H_k(G_x) + H_{k-1}(\overline{G}_x)) =$$
$$= \sum_{k=0}^{n} (-1)^k H_k(G_x) - \sum_{k=0}^{n-1} (-1)^k H_k(\overline{G}_x) = f(G_x) - f(\overline{G}_x).$$

4. Из условия следует, что $f'(0) = 0$. Без ограничения общности считаем, что $f'(x) > 0$ при $x > 0$. Тогда функция $f(x)$ монотонно возрастает на $(0, \varepsilon)$. Из определения предела получаем, что существует $\delta > 0$, такое что для любого $x \in (0, \delta)$ выполнено неравенство $f(x) > f'(x)$. Можно считать $\delta < 1$. Возьмем произвольную точку $y \in (0, \delta)$. По теореме Лагранжа существует точка $\xi \in (0, y)$, для которой $f(y) = f'(\xi)y$. Но $f'(\xi) < f(\xi) < f(y)$, откуда $f(y) < f(\xi)y < f(y)y$. Так как $f(y) > 0$, то получаем $y > 1$. Противоречие. Значит, требуемой функции не существует.

Ответ: не существует.

5. Реализуем наши плоскости в пространстве следующим образом: $\Pi_1 = \{y = z\}$, $\Pi_2 = \{z = 0\}$. Единичный вектор $\overline{OA}$, гладко вращающийся в первой плоскости, зададим как $(\sin\varphi, \frac{1}{\sqrt{2}}\cos\varphi, \frac{1}{\sqrt{2}}\cos\varphi)$, а единичный вектор $\overline{OC}$ во второй плоскости — $(\sin\psi, \cos\psi, 0)$. Тогда условие на угол α между векторами $\overline{OA}$ и $\overline{OC}$ запишется в виде $\cos(\overline{OA}, \overline{OC}) = \sin\varphi\sin\psi + \frac{1}{\sqrt{2}}\cos\varphi\cos\psi = \cos\alpha$, или

$$\frac{\sin\varphi}{\sqrt{\frac{1}{2} + \frac{\sin^2\varphi}{2}}}\sin\psi + \frac{\cos\varphi}{\sqrt{1 + \sin^2\varphi}}\cos\psi = \frac{\cos\alpha}{\sqrt{\frac{1}{2} + \frac{\sin^2\varphi}{2}}}.$$

Введем обозначение: $f(\varphi) = \dfrac{\cos\alpha}{\sqrt{\frac{1}{2} + \frac{\sin^2\varphi}{2}}}$. Несложно показать, что существует такая гладкая строго возрастающая функция $\theta(\varphi)$, для которой выполнены условия

$$\sin\theta(\varphi) = \frac{\sin\varphi}{\sqrt{\frac{1}{2} + \frac{\sin^2\varphi}{2}}},\ \cos\theta(\varphi) = \frac{\cos\varphi}{\sqrt{1+\sin^2\varphi}},$$

причем $\theta(\varphi + 2\pi) = \theta(\varphi) + 2\pi$. Поэтому имеет смысл равенство:

$$\cos(\psi - \theta(\varphi)) = f(\varphi). \tag{1}$$

Мы хотим построить непрерывную функцию $\psi = \psi(\varphi)$ такую, что выполнено равенство (1), а также условие $\psi(\varphi+2\pi) = \psi(\varphi)+2\pi$. Ограничение на α следующее: $|f(\varphi)| \leqslant 1$ для любого $\varphi \in \mathbb{R}$. Отсюда $\cos\alpha \leqslant \dfrac{1}{\sqrt{2}}$, а этого уже достаточно для построения функции $\psi = \psi(\varphi)$:

$$\psi(\varphi) = \theta(\varphi) + \arccos(f(\varphi)).$$

Ответ: $\alpha \in (0, \frac{\pi}{4}]$.

6. а) Пусть $A = \{b_1 < b_2 < \cdots < b_n\}$. Выберем m, для которого $b_m - b_{m-1}$ минимально. Тогда условию задачи удовлетворяет $u = (b_n - b_1)/(b_m - b_{m-1})$. Действительно, для двух различных наборов индексов i, j и k, l, где можно считать $i > k$, равенство $b_i + ub_j = b_k + ub_l$ равносильно соотношению $(b_i - b_k)(b_m - b_{m-1}) = (b_n - b_1)(b_l - b_j)$. Из него с необходимостью вытекает $i = n, k = 1$. Значит, должно выполняться равенство $b_m - b_{m-1} = b_l - b_j$. В силу условия минимальности разности $b_m - b_{m-1}$ этому равенству удовлетворяют не более $n-1$ пар l, j. В то же время одна такая пара имеется: $l = m, j = m-1$. Отсюда получаем, что для выбранного u различных чисел вида $a_1 + ua_2$, где $a_1, a_2 \in A$, имеется не меньше $n^2 - n + 1$ и не больше $n^2 - 1$.

б) Пусть снова $A = \{b_1 < b_2 < \ldots < b_n\}$. Выберем m, для которого $b_m - b_{m-1}$ минимально. Положим $u = (b_n - b_1)/(b_m - b_{m-1})$. Тогда из пункта а) следует, что различных чисел вида $b_k + ub_l$ больше, чем $n^2 - n$. Значит, чисел вида $(b_m - b_{m-1})(b_k + ub_l) = b_k(b_m - b_{m-1}) + b_l(b_n - b_1)$ больше $n^2 - n$. А это и требовалось доказать.

Р. Авдеев: механико-математический факультет Московского государственного университета им. М. В. Ломоносова
e-mail: suselr@yandex.ru

А. Москвин: механико-математический факультет Московского государственного университета им. М. В. Ломоносова
e-mail: moskvin-ay@mail.ru

Издательство МЦНМО

Б. П. Гейдман, И. Э. Мишарина, Е. А. Зверева. **Математика. 1 класс.** Учебник для первого класса начальной школы. 1-е полугодие 2007. 136 с. 2-е полугодие 2007. 112 с.

Б. П. Гейдман, И. Э. Мишарина, Е. А. Зверева. **Математика. 2 класс.** Учебник для второго класса начальной школы. 1-е полугодие 2007. 112 с. 2-е полугодие 2007. 112 с.

Б. П. Гейдман, И. Э. Мишарина, Е. А. Зверева. **Математика. 3 класс.** Учебник для третьего класса начальной школы. 1-е полугодие 2007. 112 с. 2-е полугодие 2007. 128 с.

Б. П. Гейдман, И. Э. Мишарина, Е. А. Зверева. **Математика. Рабочие тетради для 1 класса начальной школы.** Рабочая тетрадь №1 2007. 48 с. Рабочая тетрадь №2 2007. 48 с. Рабочая тетрадь №3 2007. 48 с. Рабочая тетрадь №4 2007. 64 с.

Б. П. Гейдман, И. Э. Мишарина. **Методические рекомендации по работе с комплектом учебников «Математика. 1 класс».** 2007. 108 с.

Б. П. Гейдман, И. Э. Мишарина. **Методические рекомендации по работе с комплектом учебников «Математика. 2 класс».** 2007. 142 с.

Ю. М. Григорьев, В. М. Муравьёв, В. Ф. Потапов. **Олимпиадные задачи по физике. Международная олимпиада «Туймаада».** Под ред. Б. В. Селюка. 2007. 160 с.

Задачи лингвистических олимпиад. 1965–1975. Ред.-сост. В. И. Беликов, Е. В. Муравенко, М. Е. Алексеев. 2007. 570 с.

В. В. Еремин. **Теоретическая и математическая химия для школьников. Подготовка к химическим олимпиадам.** 2007. 392 с.

С. А. Хованский, кн. **Князья Хованские.** 2007. 424+72 с.

Князья Хованские — один из наиболее известных дворянских родов России, принадлежавший к высшему слою аристократии. В настоящую книгу вошли (в существенно дополненном виде) итоги изысканий князя Сергея Александровича Хованского по истории его рода. В приложениях к книге содержатся работы Н. П. Чулкова, О. Н. Наумова и архивные материалы.

Материалы Второй международной научной конференции по проблемам безопасности и противодействия терроризму. Московский государственный университет им. М. В. Ломоносова. 25–26 октября 2006 г. 2007. 664 с.

Нам пишут

Дополнение к статье Д. А .Михалина, И. М. Никонова «Одна задача о нахождении фальшивой монеты»

А. Я. Канель-Белов Б. Р. Френкин

При редактировании статьи[1)] мы заметили один факт общего характера, позволяющий дать другое доказательство основного результата.

Напомним, что рассматривались задачи следующего вида. *Имеется некоторое количество монет, из них одна фальшивая, немного отличающаяся по весу от других, а все остальные настоящие и одинаковые. Можно ли за данное число взвешиваний на рычажных весах без гирь найти фальшивую монету*: а) *определив ее относительный вес* (*т. е. легче она или тяжелее остальных*), б) *не определяя относительный вес*? *При этом мы можем иметь запас настоящих монет либо не иметь.*

Последующие рассуждения базируются на факте, который доказывается по аналогии с решением задачи 4.

Основная лемма. *Пусть за n взвешиваний можно найти фальшивую среди m монет* (*возможно, не определив ее относительный вес*). *Тогда при наличии дополнительной заведомо настоящей монеты можно среди $m-1$ монет за n взвешиваний найти фальшивую и определить ее относительный вес.*

Действительно, добавим дополнительную монету к $m-1$ исходным и будем действовать по алгоритму для m монет и n взвешиваний, причем взвесим дополнительную монету лишь в тот момент (если он наступит), когда невзвешенных монет не должно остаться. Это можно сделать,

[1)] «Математическое просвещение», вып. 11, с. 149–158, 2007 г.

поскольку невзвешенные монеты неразличимы в рамках алгоритма взвешивания. В итоге мы найдем фальшивую монету, и нужно показать, что мы определили ее относительный вес, т. е. что она попала на весы. Если это неверно, то фальшивая монета — невзвешенная, причем единственная невзвешенная (в противном случае мы не знаем, какая из невзвешенных монет фальшивая). Но тогда дополнительная монета взвешена, а значит, взвешены и все монеты. Получено противоречие, которое и доказывает наше утверждение.

Многократно применяя основную лемму, получаем

Следствие 1. *Пусть за n взвешиваний можно найти фальшивую среди m монет (возможно, не определив ее относительный вес). Тогда при наличии достаточного запаса настоящих монет можно среди любого меньшего количества монет за n взвешиваний найти фальшивую и определить ее относительный вес*[2)].

Отметим, что *проведенные рассуждения не зависят от того, используются ли заведомо настоящие монеты в алгоритме для m монет.*

Следствие 2. *Независимо от наличия запаса настоящих монет, нельзя за n взвешиваний найти фальшивую из более чем $(3^n+1)/2$ монет, даже если не требуется определить ее относительный вес.*

Действительно, в противном случае мы могли бы, согласно следствию 1, за n взвешиваний найти фальшивую среди $(3^n + 1)/2$ монет и определить ее относительный вес. Но это противоречит результату задачи 2а из статьи.

Рассматривая первое взвешивание, получаем теперь

Основной результат статьи (задача 5). *За n взвешиваний при отсутствии запаса настоящих монет нельзя из более чем $(3^n - 1)/2$ монет найти фальшивую (даже если не требуется определить ее относительный вес).*

Действительно, пусть из некоторого количества монет (при отсутствии запаса настоящих) можно найти фальшивую за n взвешиваний.

Рассмотрим первое взвешивание. Если чашки не уравновесились, то фальшивая монета — среди взвешенных, и для каждой из взвешенных монет мы знаем ее относительный вес в случае, если она фальшивая. За оставшиеся $n-1$ взвешиваний можно найти фальшивую среди этих монет.

[2)] Заведомо настоящих монет в любой ситуации требуется не больше, чем «подозрительных» (подлежащих проверке). Действительно, если на обеих чашках весов есть заведомо настоящие, то по одной можно снять. Повторяя это действие, получим, что все монеты на одной из чашек — «подозрительные», и заведомо настоящих требуется не большее количество.

Следовательно (см. решение задачи $1'$ из статьи), их количество не больше 3^{n-1} — а в действительности меньше, поскольку четно.

Если же весы в равновесии, то фальшивая монета — среди невзвешенных, причем ее можно найти за оставшиеся $n-1$ взвешиваний. Согласно следствию 2, количество невзвешенных монет не превосходит $(3^{n-1}+1)/2$. Значит, общее количество монет не превосходит $(3^{n-1}-1)+(3^{n-1}+1)/2 = (3^n-1)/2$, что и требовалось.

Резюмируя доказанное здесь и в статье, получаем следующую картину.

Пусть из данного количества монет можно найти фальшивую за n взвешиваний. Тогда максимальное возможное количество монет равно:

если относительный вес фальшивой монеты известен заранее — 3^n (*независимо от наличия запаса настоящих монет*);

если относительный вес не известен и его требуется узнать — *при отсутствии запаса настоящих монет* $(3^n-3)/2$, *при наличии* $(3^n-1)/2$;

если не требуется узнать относительный вес — *при отсутствии запаса настоящих монет* $(3^n-1)/2$, *при наличии* $(3^n+1)/2$.

А. Я. Канель-Белов, МИОО
Б. Р. Френкин, ЦЭМИ, МЦНМО

Сколько ступенек на эскалаторе?

К. Э. Каибханов

Каждый может принимать решение, обладая достаточной информацией. Хороший руководитель принимает решение и при ее нехватке. Идеальный — действует в абсолютном неведении.

Как-то раз, встав на ступеньку эскалатора, я обратил внимание на номер ступеньки: 285. Возник естественный вопрос: сколько всего ступенек? Ясно, что не меньше 285. Можно ли сделать какое-нибудь разумное предположение о числе ступенек исходя только из того, что имеется ступенька с номером 285? Решением этой задачи мы и займемся.

Сначала формализуем задачу. Пусть имеется ящик («урна», как любят писать в учебниках по теории вероятностей) с карточками, пронумерованными числами от 1 до n. Число n нам неизвестно. Предлагается наудачу извлечь из ящика одну карточку и по выпавшему номеру k сделать предположение о числе карточек. Другими словами, надо придумать такую функцию φ, которая натуральному числу k — номеру выпавшей карточки — ставит в соответствие натуральное число $\varphi(k)$ — предполагаемое число карточек.

Какую бы функцию мы ни взяли, если число n большое, то при случайном значении k значение $\varphi(k)$ вряд ли точно совпадет с n. Поэтому речь идет не об угадывании правильного ответа, а о некотором разумном выборе функции φ — выборе, который в некотором смысле лучше других.

Давайте придадим всему этому количественный характер. Пусть n карточек занумерованы числами от 1 до n. Мы с одинаковой вероятностью, равной $1/n$, можем достать любую из них. Тогда равновероятно, что абсолютная погрешность $|\varphi(k) - n|$ примет значения $|\varphi(1) - n|$, $|\varphi(2) - n|$, …, $|\varphi(n) - n|$. Естественно считать, что чем меньше величина

$$\lambda_n(\varphi) = \frac{1}{n^2} \sum_{k=1}^{n} |\varphi(k) - n| \,, \tag{1}$$

тем удачнее выбрана функция φ. Обозначим

$$\lambda(\varphi) = \lim_{n\to\infty} \lambda_n(\varphi). \tag{2}$$

Величину $\lambda(\varphi)$ — функцию от функции — мы возьмем за оценку погрешности функции φ. Чем меньше $\lambda(\varphi)$, тем удачнее выбрана функция φ. (Следует отметить, что предел (2) существует не для всех функций φ. В рассматриваемом ниже случае линейной функции предел существует.)

Мы ограничимся решением задачи наилучшего выбора функции φ в классе линейных функций, то есть займемся поиском функции $\varphi(k) = ak$, для которой величина $\lambda(\varphi)$ принимает наименьшее значение. Для такой функции

$$\lambda_n(\varphi) = \frac{1}{n^2}\sum_{k=1}^{n} |ak - n| = \sum_{k=1}^{n} \left|a \cdot \frac{k}{n} - 1\right| \cdot \frac{1}{n}\,.$$

Поскольку последнее выражение является интегральной суммой функции $f(x) = |ax - 1|$ на отрезке $[0; 1]$, переходя к пределу при $n \to \infty$, получаем:

$$\lambda(\varphi) = \int_0^1 |ax - 1|\, dx\,.$$

Пользуясь определением модуля и свойствами интеграла, вычисляем:

$$\int_0^1 |ax-1|\,dx = \int_0^{1/a} (1-ax)\,dx + \int_{1/a}^1 (ax-1)\,dx =$$

$$= \left(x - \frac{a}{2}x^2\right)\Big|_{x=0}^{1}/a + \left(\frac{a}{2}x^2 - x\right)\Big|_{x=1/a}^{1} = \left(\frac{1}{a} - \frac{1}{2a}\right) + \left(\frac{a}{2} - 1\right) - \left(\frac{1}{2a} - \frac{1}{a}\right) =$$

$$= \frac{a}{2} + \frac{1}{a} - 1 = \left(\sqrt{\frac{a}{2}} - \sqrt{\frac{1}{a}}\right)^2 + \sqrt{2} - 1 \geqslant \sqrt{2} - 1,$$

причем равенство достигается лишь при условии $\frac{a}{2} = \frac{1}{a}$, то есть при $a = \sqrt{2}$.

Таким образом, наилучшей среди функций вида $\varphi(k) = ak$ оказалась функция $\sqrt{2}\cdot k$. Например, при $k = 285$ разумно предположить, что число всех ступенек $n \approx 285\sqrt{2} \approx 403$.

* * * * * *

Оценка погрешности по формулам (1–2) не единственно возможная. Например, рассмотрим формулы

$$\lambda_{n,p} = \frac{1}{n^{p+1}}\sum_{k=1}^{n} |\varphi(k) - n|^p,$$

$$\lambda_p(\varphi) = \lim_{n\to\infty} \lambda_{n,p}(\varphi),$$

где $p > 0$. По-прежнему будем искать наилучшую функцию среди линейных функций: $\varphi(k) = ak$. Тогда, как легко проверить,

$$\lambda_{n,p}(\varphi) = \sum_{k=1}^{n} \left| a \cdot \frac{k}{n} - 1 \right|^p \cdot \frac{1}{n},$$

$$\lambda_p(\varphi) = \int_0^1 |ax - 1|^p \, dx,$$

$$\lambda_p = \frac{1}{p+1} \cdot \frac{1}{a} \cdot ((a-1)^{p+1} + 1).$$

Продифференцировав по a величину $\lambda_p(\varphi)$ и приравняв производную к нулю, получаем уравнение

$$(a-1)^p(pa+1) = 1.$$

Функция $f(a) = (a-1)^p(pa+1)$ является произведением двух положительных строго возрастающих функций и, следовательно, строго возрастает на $[1; +\infty)$. Поскольку $f(1) = 0 < 1$ и $f(2) = 2p + 1 > 1$, из непрерывности функции f следует, что в некоторой единственной точке $a_p \in (1; 2)$ выполнено равенство $f(a_p) = 1$. Легко проверить, что величина $\lambda_p(\varphi)$ принимает минимальное значение именно при $a = a_p$.

К. Э. Каибханов, Таганрогский технологический институт Южного федерального университета, г. Таганрог

Задачный раздел

В этом разделе вниманию читателей предлагается подборка задач разной степени сложности, в основном трудных. Составителям этой подборки кажется, что предлагаемые ниже задачи окажутся интересными как для сильных школьников, интересующихся математикой, так и для студентов-математиков.

Мы обращаемся с просьбой ко всем читателям, имеющим свои 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). Если автор задачи нам неизвестен, то в скобках указывается «фольклор».

1. $\cos\alpha = 1/3$. Докажите, что градусная мера угла α иррациональна. (*Фольклор*)

2. В пространстве расположено несколько плоскостей общего положения (никакие три не параллельны одной прямой, и все не пересекаются в одной точке). Они делят пространство на несколько частей и в каждой части записан знак — плюс или минус. Разрешается изменить все знаки во всех частях внутри любого тетраэдра, образованного данными плоскостями. Докажите, что за несколько операций можно сделать так, чтобы во всех ограниченных частях стояли плюсы. (*А. Канель*)

3. Вершины A и B графа G назовем *эквивалентными*, если существует такая последовательность вершин $A = A_0, A_1, \ldots, A_n = B$, что любые две соседние вершины A_i и A_{i+1} можно соединить k путями без общих промежуточных вершин. Докажите, что любые две эквивалентные вершины можно соединить k путями без общих ребер. (*А. Скопенков*)

4. Пусть $a_1, \ldots, a_n$ — положительные числа, M — их среднее арифметическое, G — их среднее геометрическое. Докажите, что для любого $1 \leqslant i \leqslant n$ выполняется неравенство:

$$1 + \rho < a_i/M < 1 + \rho',$$

где $\rho < 0$ и $\rho' > 0$ корни трансцендентного уравнения

$$(1 + x)e^{-x} = (G/M)^n. \qquad (А.\ Тартаковский)$$

5. Можно ли из трех стержней и нескольких нитей изготовить жесткую пространственную конструкцию так, чтобы стержни не соприкасались между собой, а были бы связаны нитками, прикрепленными к их концам? (*Фольклор*)

6. Докажите, что монотонная функция дифференцируема в некоторой точке. (*Теорема Лебега*)

7. а) Может ли определитель 10×10 матрицы с коэффициентами $0, \pm 1$ превосходить 2007? б) (Задача на исследование.) Оцените максимально возможный определитель для матрицы $n \times n$ с коэффициентами $0, \pm 1$. (*Фольклор*)

8. Пусть на плоскости даны два подобных и противоположно ориентированных треугольника с общим ортоцентром. Обозначим их через $\triangle A_1B_1C_1$ и $\triangle A_2B_2C_2$. Докажите, что прямые A_1A_2, B_1B_2, C_1C_2 имеют общую точку или параллельны друг другу. (*А. В. Акопян*)

9. В клетках бесконечной целочисленной решетки стоят целые числа. Докажите, что сумма чисел в некотором квадрате делится на 2008. (*С. В. Охитин, А. Я. Белов*)

10. Назовем множество C перестановок n элементов *хорошим*, если для любого ненулевого набора чисел $v_1, \ldots, v_n$ такого, что $\sum_i v_i = 0$, найдется такая перестановка π из множества C, что $\sum_{i=1}^{k} v_{\pi(i)} > 0$ для всех k от 1 до $n-1$. Если заменить строгое равенство на нестрогое, то получится определение *неплохого* множества. Какова мощность наименьшего хорошего (неплохого) множества? а) Мощность наименьшего неплохого множества равна n. б) Существует хорошее множество мощности $n2^n$. в) (открытая проблема) Доказать, что мощность хорошего множества экспоненциально велика по n. (*В. Л. Попов, Э. Б. Винберг*)

11. Многочлены P, Q и R таковы, что $R(P(x), Q(x)) \equiv x$. Докажите, что степень P делит степень Q, либо степень Q делит степень P. (*Терема Абъянкара – Моха*)

12. *Линейной рекуррентой порядка* n называется такая последовательность $\{u_k\}$, что при всех k

$$a_0u_{k+n} + a_1u_{k+n-1} + \cdots + a_nu_k = 0$$

где a_i — некоторые константы, не все равные нулю одновременно. *Нулем* линейной рекурренты называется такое k, что $u_k = 0$. Докажите, что множество нулей линейной рекурренты есть объединение конечного набора точек и конечного набора арифметических прогрессий. (*А. Я. Канель*)

Решения задач из предыдущих выпусков

9.6. Условие. Рассмотрим всевозможные однокруговые турниры n шахматистов. Для каждого турнира найдем количества $s_1 \leqslant \cdots \leqslant s_n$ очков, набранных игроками, и возьмем в n-мерном пространстве точку с координатами $(s_1, \ldots, s_n)$. Доказать, что выпуклая оболочка этих точек является $(n-1)$-мерным многогранником, комбинаторно эквивалентным соответствующему кубу, а его вершины соответствуют турнирам, в которых в любой паре участников набравший больше очков выигрывает в личной встрече.

Решение. Очевидно, что $s_1, \ldots, s_n$ удовлетворяют условиям:

$$\begin{aligned} s_1 + \cdots + s_n &= \frac{n(n-1)}{2}, \\ s_1 + \cdots + s_k &\geqslant \frac{k(k-1)}{2}, \quad k = 1, \ldots, n-1. \end{aligned} \tag{1}$$

Следовательно, все отмеченные точки лежат в $(n-1)$-мерной гиперплоскости. Если не учитывать, что s_i полуцелые, то условия (1) и $s_i \leqslant s_{i+1}$ определяют многогранник, в вершинах которого, по крайней мере, $n-1$ из них обращаются в равенства. При этом, если $s_1 + \cdots + s_k = k(k-1)/2$, то $s_k \leqslant k-1$ и $s_{k+1} \geqslant k$, т. е. в каждой из $n-1$ пар условий $s_k \leqslant s_{k+1}$ и $s_1 + \cdots + s_k \geqslant k(k-1)/2$ в равенство обращается ровно одно. Любому из 2^{n-1} способов выбрать это условие соответствует точка вида

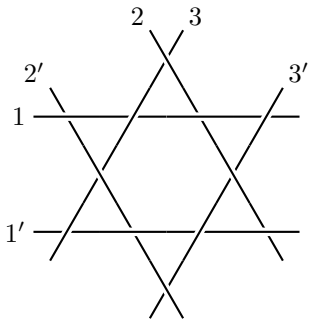
$$\begin{aligned} &s_1 = \cdots = s_{k_1} = \frac{k_1 - 1}{2}, \\ &s_{k_1+1} = \cdots = s_{k_1+k_2} = k_1 + \frac{k_2 - 1}{2}, \\ &\ldots, \\ &s_{k_1+\cdots+k_l+1} = \cdots = s_n = k_1 + \cdots + k_l + \frac{n - 1 - k_1 - \cdots - k_l}{2}, \end{aligned}$$

а каждой такой точке соответствует турнир, в котором участники разбиты на $l+1$ группу численностью $k_1, \ldots, k_l$ и $(n-k_1-\cdots-k_l)$, причем участники из одной группы играют друг с другом вничью, а во встрече участников из разных групп побеждает тот, номер группы которого больше.

Отметим также, что полученный многогранник вписан в сферу с центром в точке $(\frac{n-1}{4}, \frac{n+1}{4}, \ldots, \frac{3(n-1)}{4})$, а его объем равен $n^{n-3/2}$.

Более подробно об этой задаче и ее приложениях см. А. А. Заславский, «Геометрия парных сравнений» // Автоматика и телемеханика, №3, 2007, с. 199–205. (*А. А. Заславский*)

9.8. Условие. Может ли фигура, указанная на рисунке, изображать несколько попарно скрещивающихся прямых, спроецированных на плоскость?



Ответ: нет.

Обозначим через $[ab]$ точку прямой a, проектирующуюся на плоскость рисунка в точку пересечения прямых a и b.

Повернем прямую 3 в плоскости, перпендикулярной плоскости рисунка, относительно точки $32'$, до пересечения с прямой 1. Других точек пересечения не появится. Обозначим повернутую прямую 3 снова через 3 (а про старую прямую 3 забудем). Получился новый набор прямых, дающий проекцию, отличающуюся от данной только тем, что прямые 1 и 3 пересекаются.

(Можно было бы «сделать» точками пересечения все 6 вершин «внутреннего» шестиугольника, но это уже не нужно.)

Обозначим через ab проекцию точки $[ab]$ на прямую ℓ, перпендикулярную плоскости рисунка, вдоль плоскости, проходящей через прямые 1 и 3. Отождествим прямую ℓ с множеством вещественных чисел так, чтобы ноль отождестился с образом прямой 1 при указанной параллельной проекции, и положительное направление было в нашу сторону.

Тогда $23 > 0$ и $21 < 0$. Значит, $3'2 < 23' < 0$. Из этого и $3'1 > 0$ вытекает, что $1'3' < 3'1' < 0$. Из этого и $1'3 < 0$ вытекает, что $2'1' < 1'2' < < 0$. Это противоречит тому, что $2'1 < 0$ и $2'3 > 0$. (*А. Б. Скопенков*)

10.6. Условие. Внутри выпуклого четырехугольника взята точка, равноудаленная от противоположных сторон. Оказалось, что она лежит

на прямой, соединяющей середины диагоналей. Докажите, что четырехугольник является либо вписанным, либо описанным, либо трапецией.

Решение. Пусть четырехугольник не описанный и не трапеция. Тогда прямая, соединяющая середины диагоналей, является геметрическим местом вписанных в него коник. Таким образом, к конике, отличной от окружности, проведены две пары касательных, равноудаленных от ее центра. Так как касательные в каждой паре не параллельны, они симметричны относительно одной из осей коники. Если эта ось в обеих парах одна и та же, то сам четырехугольник симметричен и в него можно вписать окружность. Следовательно, прямые равноудаленные от противоположных сторон четырехугольника, перпендикулярны. Так как углы между этими прямыми равны полусуммам противоположных углов четырехугольника, он является вписанным. (*А. А. Заславский*)

Опечатки, замеченные в №11

Страница, Строка	Напечатано	Следует читать
8, 19 сверху	Фактическая ошибка: Г. Я. Перельман никогда не эмигрировал в США.	
8, 20 сверху	Нью Йорка	Нью-Йорка
87, 6 снизу	замена $v'' \to v'' + (\lambda + \lambda')u$	замена $v'' \to v'' + (\lambda + \lambda')u''$

Редактор В. В. Ященко
Подготовка оригинал-макета: LaTeX2ε,
METAPOST, М. Н. Вялый

Подписано в печать 07.02.2008 г. Формат $70 \times 100/16$.
Бумага офсетная №1. Печать офсетная. Печ. л. 15,0. Тираж 1000.

Издательство Московского Центра
непрерывного математического
образования
119002, Москва, Большой Власьевский пер., 11. Тел. (495) 241 74 83

Отпечатано с готовых диапозитивов в ППП «Типография «Наука»
121099, г. Москва, Шубинский пер., 6
Заказ №302