МАТЕМАТИЧЕСКОЕ ПРОСВЕЩЕНИЕ

Третья серия

выпуск 30

Москва
Издательство МЦНМО

УДК 51.009
ББК 22.1
М34

Издано при поддержке Фонда развития теоретической физики и математики «БАЗИС»

Редакционная коллегия

Бугаенко В. О.
Вялый М. Н.
Гайфуллин А. А.
Гальперин Г. А.
Гусейн-Заде С. М.
Дориченко С. А.
Заславский А. А.
Ильяшенко Ю. С.
Канель-Белов А. Я.
Митрофанов И. В.
Полянский А. А.
Прасолов В. В.
Райгородский А. М.
Семёнов А. Л.
Сосинский А. Б.
Тихомиров В. М.
Устинов А. В.
Френкин Б. Р.
Ященко И. В.

Главный редактор А. М. Райгородский
Отв. секретарь Б. Р. Френкин

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

Математическое просвещение. Третья серия, вып. 30. —
М34 М.: МЦНМО, 2023. — 248 с.
ISBN 978-5-4439-1768-9

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

УДК 51.009
ББК 22.1

ISBN 978-5-4439-1768-9

© МЦНМО, 2023

Содержание

Математический мир

Д. Е. Апушкинская, А. И. Назаров
Ольга Александровна Ладыженская (1922–2004) 7

Л. Х. Кауффман
Памяти Джона Хортона Конвея 31

В. М. Тихомиров
Никита Введенская 44

А. Г. Кушниренко
Создание С. И. Шварцбурдом московской математической школы 425 52

Алгебра и теория чисел

А. Я. Канель-Белов
О работе А. Р. Исмаилова «Углы в плоскости над конечным простым полем» 65

А. Р. Исмаилов
Углы в плоскости над конечным простым полем 67

В. М. Журавлёв, П. И. Самовол
Обманчивая простота 97

Геометрия

А. А. Заславский
О построении линейкой центров окружностей 137

В. М. Журавлёв, П. И. Самовол
Антибиссектрисы: знакомые — незнакомые 141

Комбинаторика

А. Я. Бучаев, А. Б. Скопенков
Простые доказательства оценок чисел Рамсея и уклонения 151

П. П. Рябов
Подсчёт нетранзитивных троек в методе парных сравнений 157

Нам пишут

А. И. Бикеев
Письмо в редакцию 165

По мотивам задачника

Л. Радзивиловский
Постоянная Эйлера 167

Ф. В. Петров
Пентагональная теорема Эйлера 177

А. Я. Канель-Белов
Задачи о линейных рекуррентах 192

Н. Н. Осипов
Задача о треугольнике с заданными длинами биссектрис 209

А. А. Заславский
Несколько задач о треугольниках Понселе 225

Задачник (составители А. Я. Канель-Белов, И. В. Митрофанов)

Условия задач 229

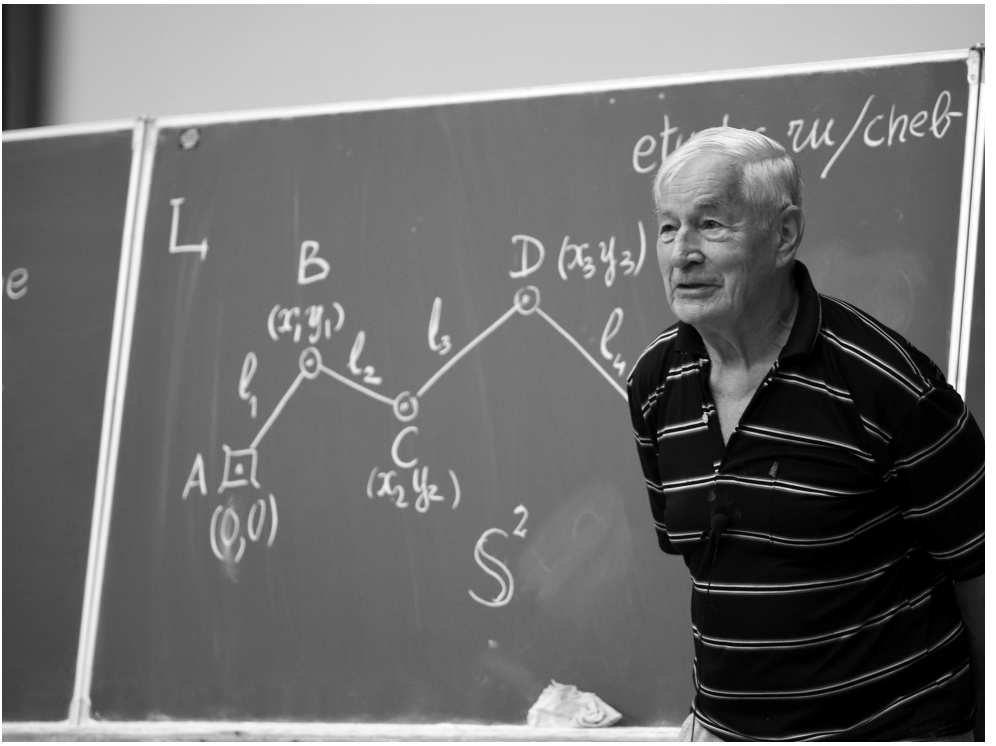
Дополнение и комментарии к задачнику 233

Решения задач из прошлых выпусков 238

Указатель условий, решений и статей по мотивам задач из «Математического просвещения» 241

Указатель к Дополнению и комментариям к задачнику «Математического просвещения» 245

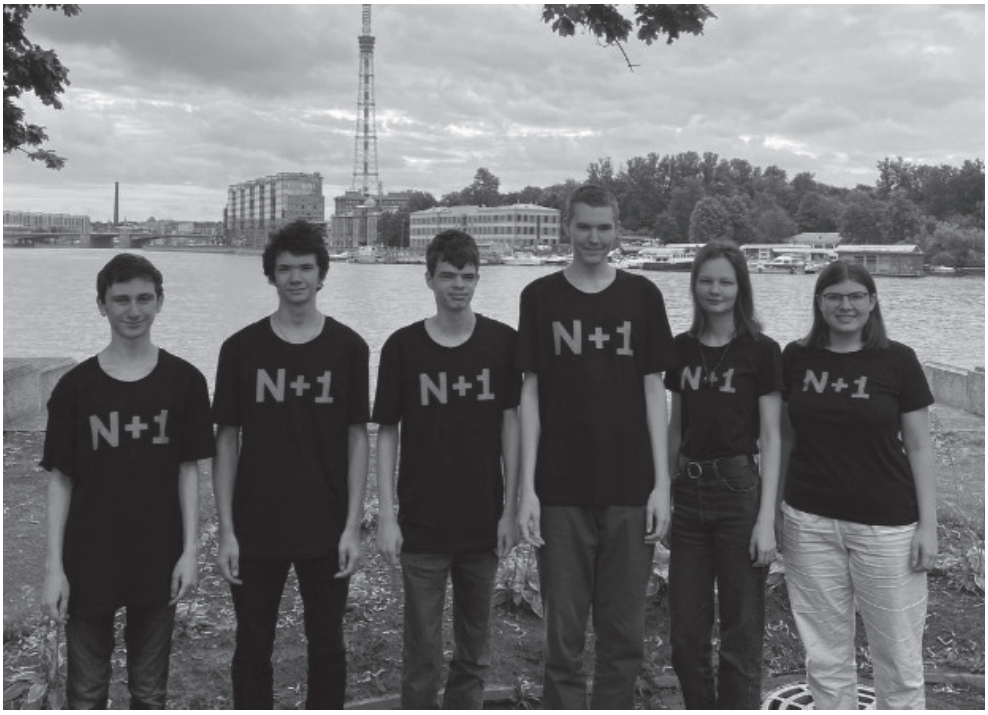
Поздравляем



Алексея Брониславовича Сосинского

с 85-летием!

Поздравляем!



Российские школьники завоевали три золотых и три серебряных медали на 63-й Международной математической олимпиаде, уступив лишь команде из Китая. Абсолютное первое место завоевала Галия Шарафетдинова, набравшая максимальные 42 балла.

На снимке (слева направо): Максим Туревский (Санкт-Петербург), Роман Кузнецов (Санкт-Петербург), Иван Бахарев (Санкт-Петербург), Денис Мустафин (Москва), Галия Шарафетдинова (Казань), Таисия Коротченко (Санкт-Петербург).

Ольга Александровна Ладыженская (1922–2004)

Д. Е. Апушкинская, А. И. Назаров

Ольга Ладыженская родилась 7 марта 1922 году в Кологриве (ныне Костромская область) — маленьком городке на берегу реки Унжи, левом притоке Волги, в 640 километрах от Москвы.

Старинный дворянский род Ладыженских впервые упоминается в летописях в 1375 году. Дед Ольги, Иван Александрович (1867–1943), — земский деятель. После революции был «лишенцем», в 1929 году, спасаясь от ареста, уехал из Кологрива. Его брат, Геннадий Александрович (1853–1916), был известным художником, академиком Императорской Академии Художеств. Его коллекция произведений искусства стала основой музея в Кологриве[1)].

Отец Ольги, Александр Иванович Ладыженский (1894–1937), учился в Институте гражданских инженеров в Петрограде. С началом Первой Мировой войны ушёл добровольцем на фронт. Служил в артиллерии, дослужился до офицера. Когда его полк стоял в Эстляндской губернии, он познакомился с Анной Михайловной Странсон (1893–1978). К неудовольствию родных, она вышла замуж за Александра, отказав своему жениху.

В 1917 году Александр Иванович привёз семью в Кологрив. С 1918 по 1922 он служил в Красной Армии, а в октябре 1922 года стал учи-

---

При подготовке этой статьи использованы материалы интернет-проекта «Воспоминания об О. А. Ладыженской» `https://pdmi.ras.ru/pdmi/memoirs/ladyzhenskaya`.

[1)] В 2003 году музею было присвоено имя Г. А. Ладыженского.

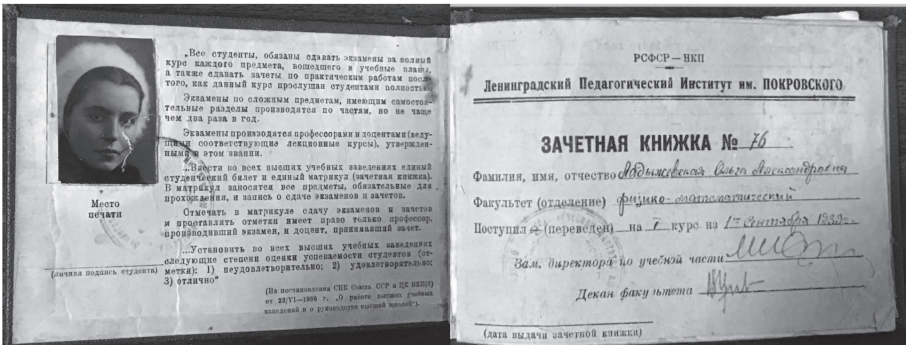
телем математики в Кологривской школе. Одна за другой в семье родились три дочери — Мария, Татьяна и Ольга.

Способности к математике Ольга Александровна проявила очень рано. Как вспоминала она сама,

> *«…мне повезло. Какие-то способности отец у меня обнаружил, и в возрасте* 10 *лет он уже устраивал мне своеобразный экзамен — рассказывал мне элементы высшей математики, а я должна была понять, правильно он рассуждает или нет».*

Беда пришла в семью Ладыженских в ночь на 23 октября 1937 года. Этой ночью в Кологриве было арестовано более 30 человек — работники педагогических учреждений района и несколько школьников старших классов. Большинство из них, включая отца Ольги, были обвинены в «антисоветской агитации, участии в контрреволюционной организации и террористических намерениях» и получили «10 лет без права переписки» — официальный эвфемизм, заменявший в то время слово «расстрел»[2]. В 1956 году все они были реабилитированы «за отсутствием состава преступления».

В 1939 году Ольга заканчивает школу с золотой медалью и едет в Ленинград поступать на математико-механический факультет ЛГУ[3]. Однако, несмотря на блестяще сданные экзамены, ей, как «дочери врага народа», отказали в приёме в университет. Более того, её документы задержали в ЛГУ до сентября, чтобы она не могла сдать их в дру-



Место печати

„Все студенты, обязаны сдавать экзамены за полный курс каждого предмета, вошедшего в учебные планы, а также сдавать зачеты по практическим работам после того, как данный курс прослушан студентами полностью.

Экзамены по сложным предметам, имеющим самостоятельные разделы производятся по частям, но не чаще чем два раза в год.

Экзамены производятся профессорами и доцентами (ведущими соответствующие лекционные курсы), утвержденными в этом звании.

...Ввести во всех высших учебных заведениях единый студенческий билет и единый матрикул (зачетная книжка). В матрикул заносятся все предметы, обязательные для прохождения, и запись о сдаче экзаменов и зачетов.

Отмечать в матрикуле сдачу экзаменов и зачетов и проставлять отметки имеет право только профессор, производивший экзамен, и доцент, принимавший зачет.

...Установить во всех высших учебных заведениях следующие степени оценки успеваемости студентов (отметки): 1) неудовлетворительно; 2) удовлетворительно; 3) отлично"

(личная подпись студента)

(Из постановления СНК Союза ССР и ЦК ВКП(б) от 23/VI—1936 г. „О работе высших учебных заведений и о руководстве учебной школой").

РСФСР — НКП

Ленинградский Педагогический Институт им. ПОКРОВСКОГО

ЗАЧЕТНАЯ КНИЖКА № 76

Фамилия, имя, отчество Ладыженская Ольга Александровна

Факультет (отделение) физико-математический

Поступил (переведен) на 1 курс из 1-го сентября 1939 г.

Зам. директора по учебной части

Декан факультета

(дата выдачи зачетной книжки)

Зачётная книжка Ольги Ладыженской

---

[2] Точная дата расстрела А. И. Ладыженского неизвестна. Согласно базе данных «Жертвы политического террора в СССР», это произошло 26 ноября 1937 года. С другой стороны, ещё в конце октября от родственников прекратили принимать передачи арестованным, что обычно означало приведение приговора в исполнение.

[3] Во время этой поездки она впервые увидела железную дорогу.

гой вуз. К счастью, Ольгу без документов (под обещание принести их позже) приняли в Педагогический институт им. М. Н. Покровского[4] на математический факультет.

Будучи студенткой второго курса, Ольга слушала курсы лекций Б. А. Венкова[5] по алгебре и Г. М. Фихтенгольца[6] по ТФКП, читавшиеся для студентов 4 курса пединститута. Для этого ей потребовалось получить специальное разрешение от деканата. Экзамены по этим курсам Ольга Александровна сдала досрочно — в апреле–мае 1941 года, а экзамены за второй курс — в июне, причём два последних экзамена уже после начала войны.

Есть сведения, что Г. М. Фихтенгольц и И. П. Натансон[7] ходатайствовали о переводе Ладыженской в ЛГУ, но этому переводу помешала война.

Ученики и учителя Кологривской школы, 1942 год. Третья справа во втором ряду сверху — О. А. Ладыженская, второй справа в верхнем ряду — старшеклассник Николай Воробьев[8]. Фото из архива семьи Воробьевых

---

[4] В 1957 году был объединён с ЛГПИ им. А. И. Герцена.

[5] Борис Алексеевич Венков (1900–1962) — профессор ЛГУ, специалист по теории чисел.

[6] Григорий Михайлович Фихтенгольц (1888–1959) — зав. кафедрой математического анализа ЛГУ, специалист в области функционального анализа, автор известного «Курса дифференциального и интегрального исчисления».

[7] Исидор Павлович Натансон (1906–1964) — профессор, зав. кафедрой математического анализа ЛГУ (с 1960), основатель ленинградской школы конструктивной теории функций.

[8] Николай Николаевич Воробьев (1925–1995) — впоследствии профессор, основатель советской школы теории игр.

После начала войны Ольга в числе других студентов участвовала в рытье окопов в окрестностях Ленинграда. Она отказалась эвакуироваться из города вместе с институтом, но позже старшая сестра Мария уговорила её уехать и сумела достать документы для выезда. В конце августа сёстры выехали из Ленинграда и через несколько недель добрались до Городца, где в это время была их мать. Там Ольга работала воспитателем в детском доме. В начале марта 1942 года семья переехала в Кологрив, и осенью Ольга Александровна стала преподавать математику в той школе, где работал её отец и училась она сама.

Ольга также бесплатно у себя дома занималась математикой с желающими. В благодарность мать одного из её учеников, вернувшись в Москву, пошла к ректору Московского университета и убедила его выслать Ладыженской вызов. В результате в конце октября 1943 года Ольга была зачислена на второй курс механико-математического факультета МГУ со стипендией и рабочей карточкой (тут сыграло свою роль и неофициальное ослабление ограничений для лиц с «поражёнными анкетами»). В одной группе с ней учились Ольга Олейник[9)], Виктор Виденский[10)] и Арон Майзелис[11)].

Сразу после поступления Ольга стала активно посещать несколько научных семинаров: семинар А. Г. Куроша[12)] и Б. Н. Делоне[13)] по алгебре, семинар В. В. Степанова[14)] по дифференциальным уравнениям и известный семинар И. М. Гельфанда[15)] по функциональному анализу. На третьем курсе по рекомендации сразу нескольких кафедр мехмата она стала Сталинским стипендиатом.

---

9) Ольга Арсеньевна Олейник (1925–2001) — зав. кафедрой дифференциальных уравнений МГУ (с 1973), академик РАН (1991).

10) Виктор Соломонович Виденский (1922–2015) — впоследствии зав. кафедрой математического анализа ЛГПИ им. Герцена, профессор.

11) Арон Рувимович Майзелис (1921–2005) — один из самых известных ленинградских учителей математики.

12) Александр Геннадьевич Курош (1908–1971) — профессор, зав. кафедрой высшей алгебры МГУ (с 1949).

13) Борис Николаевич Делоне (1890–1980) — профессор МГУ, член-корр. АН СССР (1929), специалист в области геометрии, мастер спорта по альпинизму.

14) Вячеслав Васильевич Степанов (1889–1950) — зав. кафедрой дифференциальных уравнений МГУ, член-корр. АН СССР (1946).

15) Израиль Моисеевич Гельфанд (1913–2009) — профессор МГУ, академик АН СССР (1984), один из крупнейших математиков XX века.

Также, начиная со второго курса, Ольга вела математические кружки для школьников: один — вместе с Акивой и Исааком Ягломами[16)], второй — с Александром Кронродом[17)]. Одна из её учениц, Елена Морозова[18)], вспоминала:

> *«…Братья Ягломы были уже аспирантами, то есть старшими по положению, поэтому Ольга Александровна была для них „девочкой на побегушках“. Но ученики воспринимали её с обожанием. Она была очень внимательна к членам кружка, всегда старалась их выслушать, поддерживала идеи, предлагаемые с места».*

В конце 8-го семестра у Ладыженской возникла идея организовать студенческий семинар для более глубокого изучения теории уравнений в частных производных. Она и А. Д. Мышкис[19)] уговорили И. Г. Петровского[20)] возглавить семинар. Петровский пунктуально посещал этот «самодеятельный» семинар весь следующий год. Участниками этого семинара, кроме Ладыженской и Мышкиса были Олейник, аспиранты М. И. Вишик[21)] и Р. А. Александрян[22)], преподаватели мехмата С. А. Гальперн[23)] и М. А. Крейнес[24)]. В юбилейной статье [1] отмечается:

---

16) Братья-близнецы Акива Моисеевич Яглом (1921–2007) и Исаак Моисеевич Яглом (1921–1988) — в то время аспиранты, впоследствии известные математики, профессора.

17) Александр Семенович Кронрод (1921–1986) — известный математик и специалист по информатике, один из создателей шахматной программы «Каисса».

18) Елена Александровна Морозова (1928–2020) — впоследствии доцент МГУ, лауреат премии М. В. Ломоносова за педагогическую деятельность. Член жюри Всесоюзных и Международных математических олимпиад для школьников, руководитель команды СССР на IV–X ММО.

19) Анатолий Дмитриевич Мышкис (1920–2009) — в то время ассистент мехмата, впоследствии профессор, специалист по дифференциальным урав нениям.

20) Иван Георгиевич Петровский (1901–1973) — профессор МГУ, академик АН СССР (1946), специалист в области дифференциальных уравнений, ректор МГУ (с 1951).

21) Марк Иосифович Вишик (1921–2012) — впоследствии профессор МГУ, специалист в области дифференциальных уравнений.

22) Рафаэль Арамович Александрян (1923–1988) — впоследствии профессор, академик АН Армянской ССР (1986), специалист по уравнениям в частных производных и механике.

23) Самарий Александрович Гальперн (1904–1977) — впоследствии профессор МГУ, специалист в области дифференциальных уравнений.

24) Михаил Александрович Крейнес (1903–1977) — профессор МГУ, специалист по дифференциальным уравнениям и механике.

«В какой-то степени этот семинар способствовал и написанию И. Г. Петровским его статьи, опубликованной в 1946 *году в „Успехах математических наук“ и оказавшей большое влияние на многих математиков, желавших работать над развитием теории УрЧП».*

Из статьи Петровского Ольга Александровна выбрала тему для своей дипломной работы[25)], причём задача была решена ею не только для уравнения $u_t + u_{xxxx} = 0$, предложенного Петровским, но и для всего класса 2b-параболических уравнений с коэффициентами, зависящими от времени. Эта работа получила похвалы от научного руководителя И. Г. Петровского и позднее, в 1950 году, была опубликована в «Математическом сборнике».

В 1947 году Ольга вышла замуж за ленинградского математика Андрея Алексеевича Киселёва[26)] (1916–1994) и переехала в Ленинград, где по рекомендации из МГУ поступила в аспирантуру ЛГУ под руководством С. Л. Соболева[27)].

А. А. Киселёв и О. А. Ладыженская, 1947 год

[25)] Тема работы «О единственности решения задачи Коши для линейного параболического уравнения», защищена с отличием в 1947 году.

[26)] Киселёв был преподавателем у Ольги в институте им. Покровского. Их брак продлился до 1956 года.

[27)] Сергей Львович Соболев (1908–1989) — академик АН СССР (1939), специалист по функциональному анализу и уравнениям в частных производных, один из основателей Сибирского отделения Академии Наук (1957). Его именем назван Институт математики СО РАН.

Безусловно, идеи Соболева, связанные с функциональными пространствами и теоремами вложения, оказали на Ладыженскую большое влияние. Однако она всегда подчёркивала, что по существу Соболев её работой не руководил и задачу для диссертации она выбрала сама. Эта задача была сформулирована Петровским в вышеупомянутой статье 1946 года, но, как и в дипломной работе, Ольга Александровна поставила и решила её в гораздо более общем виде — разработала метод конечных разностей так, что с его помощью можно было доказывать разрешимость краевых и начально-краевых задач для широкого класса уравнений и систем.

Из рассказа В. М. Бабича[28)]:

> *«Я и несколько других студентов присутствовали на заседании кафедры дифференциальных уравнений. Выступала молоденькая, красивейшая Ольга Александровна. Высокомерная, между прочим. Принимали к защите её кандидатскую диссертацию. „Принимальщиками“ от кафедры были Данила Макарович Волков (тогдашний лектор по математической физике) и Николай Михайлович Матвеев (по обыкновенным дифференциальным уравнениям). Она на их вопросы отвечала несколько резковато, но чувствовалось, что её уровень выше, чем уровень этих пожилых представителей кафедры. И один из моих сокурсников сказал мне: „Попомни, Вася, мои слова: вот эта — далеко пойдёт!“».*

Судьбоносным для Ладыженской оказалось знакомство с Владимиром Ивановичем Смирновым[29)], которое состоялось практически сразу после её переезда в Ленинград. Позднее Ольга Александровна писала [2]:

> *«…судьба подарила мне общение с Владимиром Ивановичем в течение примерно 27 лет. Для меня жизнь была бы совершенно другой, если бы я не встретила В. И. Смирнова.*
>
> *Дело в том, что я рано лишилась отца — он был арестован в 1937 году. Тогда мне было 15 лет. Для меня отец был другом. Владимир Иванович заменил мне отца. И это могло произойти*

[28)] Василий Михайлович Бабич (род. 1930) — профессор, зав. лабораторией математических проблем геофизики ПОМИ РАН (1967–2020), в описываемое время студент третьего курса мат-меха ЛГУ.

[29)] Владимир Иванович Смирнов (1887–1974) — академик АН СССР (1943), основатель нескольких кафедр в ЛГУ, автор знаменитого пятитомного «Курса высшей математики». Его именем назван НИИ математики и механики СПбГУ.

только потому, что существовало какое-то удивительное внутреннее сходство между моим отцом и В. И. Смирновым».

С осени 1947 года Владимир Иванович по просьбе Ольги Александровны организовал и возглавил городской семинар по математической физике[30)]. С самого начала (ещё до защиты кандидатской диссертации[31)]) Ольга стала одним из ведущих участников этого семинара.

После защиты Ладыженская стала работать ассистентом на кафедре дифференциальных и интегральных уравнений мат-меха ЛГУ. Однако её прямота в отстаивании своих взглядов и нежелание считаться с «табелью о рангах» привело к конфликту с заведующим кафедрой Н. П. Еругиным[32)]. В. И. Смирнову удалось добиться её перевода на кафедру высшей математики физического факультета ЛГУ, где она проработала всю оставшуюся жизнь. Все студенты отмечали её харизму, но преподавателем Ольга Александровна была суровым. А. И. Русанов[33)] вспоминал [4]:

«Только в нашей группе переведённых на химфак физиков занятия по математике вела О. А. Ладыженская (ныне академик), известная своей строгостью. Как-то на занятии её решили прощупать репликой: „Да Вы на экзамене всем нам тройки поставите!“, на что Ольга Александровна сухо ответила: „Почему всем? Тройку ещё надо заслужить“».

Ольга Александровна занялась проблемой обоснования методов Фурье и Лапласа для гиперболических уравнений второго порядка. Ранее они были обоснованы В. А. Стекловым[34)] лишь в случае одной пространственной переменной. Ладыженская решила эту задачу для

---

30) Этот семинар, носящий ныне имя В. И. Смирнова, отмечает в этом году своё 75-летие.

31) Тема диссертации: «Решение задачи Коши для гиперболических систем методом конечных разностей», защищена в 1949 году.

32) Николай Павлович Еругин (1907–1990) — профессор, специалист в области обыкновенных дифференциальных уравнений, академик АН Белорусской ССР (1956).

33) Анатолий Иванович Русанов (род. 1932) — зав. кафедрой коллоидной химии СПбГУ, академик РАН (1991).

34) Владимир Андреевич Стеклов (1863–1926) — специалист по математической физике и механике, академик Петербургской АН (1912), вице-президент АН СССР (с 1919), организатор Физико-математического института РАН (1921). Его имя носят математические институты в Москве и Петербурге.

нестационарных уравнений, порождаемых произвольными симметрическими эллиптическими операторами второго порядка в ограниченной области с любым из классических краевых условий. Важно отметить, что именно в этом цикле работ была подчёркнута важность понятия обобщённого решения начально-краевой задачи для гиперболических уравнений из определённого функционального пространства, а также полезность работы в целой шкале функциональных пространств. До того подобная концепция встречалась лишь в эллиптических вариационных задачах.

В процессе работы Ладыженская также получила решение проблемы Гельфанда об описании области определения замыкания в L_2 эллиптического оператора с условием Дирихле.

Эти и другие результаты по разрешимости начально-краевых задач для гиперболических уравнений стали основой докторской диссертации, которую Ольга Александровна подготовила уже в 1951 году. Однако «защититься» с её анкетными данными в Ленинграде не представлялось возможным. Обратились к Петровскому для организации защиты в Москве. Но даже влияния ректора МГУ не хватило. Тогда В. И. Смирнов предложил издать диссертацию в виде монографии [3] и способствовал её изданию. Хотя эта книга не была переведена на иностранные языки, её содержание получило известность во многих странах. В 1954 году за эту монографию Ладыженская получила Премию Ленинградского университета.

В марте 1953 года, вскоре после смерти Сталина, Петровский позвонил Ладыженской и сообщил, что теперь её защита состоится. Той же осенью Ольга Александровна получила диплом доктора физико-математических наук.

Вскоре после докторской защиты Ладыженская получила должность доцента, а в 1956 году — профессора ЛГУ. С 1954 года она по совместительству становится сотрудником Ленинградского отделения Математического института им. В. А. Стеклова (ЛОМИ; ныне ПОМИ РАН). В 1961 году Ольга Александровна создала на базе своей группы лабораторию математической физики и затем перешла на основное место работы в ЛОМИ[35)], продолжая работать в университете по совместительству. Заметим, что в течение ряда лет она читала спецкурсы одновременно для студентов двух факультетов (мат-меха и физфака).

[35)] Зав. лабораторией математической физики (1961–1998), главный научный сотрудник (с 1998).

История этой фотографии примечательна: по указанию ректора ЛГУ А. Д. Александрова[36)] были сделаны фотопортреты ведущих профессоров университета. Фотография Ладыженской так понравилась А. Д., что много лет стояла у него на рабочем столе. Гораздо позже, в 1982 году, в поздравительном адресе к 60-летию Ольги Александровны он написал: *«Такое сочетание красоты и таланта в одном человеке кажется нереальным, если бы не Ольга Александровна»*.

В середине 50-х годов под влиянием В. А. Фока[37)] Ладыженская обращается к задачам математической гидродинамики. В первых же работах по этой тематике ей удалось значительно продвинуть теорию разрешимости краевых и начально-краевых задач для системы уравнений Навье — Стокса по сравнению с имевшимися к тому моменту результатами Ж. Лерэ[38)] и Э. Хопфа[39)]. В частности, в статье [5] была доказана однозначная локальная (а при достаточно малых данных задачи — и глобальная) разрешимость первой начально-краевой задачи для уравнений Навье — Стокса в произвольной трёхмерной области[40)]. Спустя год была опубликована работа [6], в которой установлена глобальная однозначная разрешимость начально-краевой задачи в двумерной области. Для этого был использован новый тип функциональных неравенств, позднее названных мультипликативными.

---

36) Александр Данилович Александров (1912–1999) — основатель ленинградской школы «геометрии в целом», ректор ЛГУ (1951–1964), академик АН СССР (1964), мастер спорта по альпинизму.

37) Владимир Александрович Фок (1898–1974) — физик-теоретик, академик АН СССР (1939) и ряда зарубежных академий.

38) Жан Лерэ (Jean Leray, 1906–1998) — французский математик, специалист в области функционального анализа и уравнений в частных производных, член Французской АН (1953) и ряда зарубежных академий.

39) Эберхард Фредерик Фердинанд Хопф (Eberhard Frederich Ferdinand Hopf, 1902–1983) — немецкий и американский математик, специалист в области уравнений в частных производных и динамических систем.

40) Хотя в дальнейшем были некоторые продвижения в этой задаче, вопрос о глобальной разрешимости трёхмерной задачи Навье — Стокса остаётся открытым по сей день и является одной из проблем тысячелетия.

Исследования 50-х годов по гидродинамике были подытожены в монографии «Математические вопросы динамики вязкой несжимаемой жидкости», вышедшей в 1961 году. Книга содержит посвящение:

> *«Трём очень разным, но глубоко уважаемым мной людям: моему отцу, Александру Ивановичу ЛАДЫЖЕНСКОМУ, Владимиру Ивановичу СМИРНОВУ и Жану ЛЕРЭ посвящается эта книга».*

В 1963 году вышел перевод этой книги на английский язык, а в 1970 году — второе русское издание, существенно дополненное и переработанное. Позднее монография была переведена ещё на несколько языков и стала «библией» для всех специалистов по математической гидродинамике.

ICM1958, Эдинбург. Х. О. Кордес[41], О. А. Ладыженская, П. Лакс[42]

В 1958 году Ольга Александровна впервые приняла участие в Международном конгрессе математиков, который проходил в Эдинбурге.

В дальнейшем Ладыженская неоднократно участвовала в конгрессах. Дважды (Москва 1966 и Варшава 1983) она была приглашённым

---

[41] Хейнц Отто Кордес (Heinz Otto Cordes, 1925–2018) — немецкий и американский математик, специалист в области уравнений в частных производных.

[42] Питер Дэвид Лакс (Peter David Lax, род. 1926) — американский математик, специалист в области уравнений в частных производных, член Национальной Академии Наук США (1970), лауреат Абелевской премии (2005) и многих других наград, в том числе Большой золотой медали им. М. В. Ломоносова (2013).

докладчиком, а в 1994 году в Цюрихе была удостоена специальной лекции имени Эмми Нётер[43)].

Ещё одна проблема, которая была в центре внимания Ольги Александровны начиная с 50-х годов — регулярность решений квазилинейных уравнений эллиптического и параболического типов. Большинство результатов в этом направлении было получено Ладыженской в сотрудничестве с её ученицей Н. Н. Уральцевой[44)].

Отправными точками этих исследований были работа Ладыженской 1956 года об оценке градиентов решений эллиптических и параболических квазилинейных уравнений и работы Э. Де Джорджи[45)] и Дж. Нэша[46)] (1957/58), которые установили, что решения линейных равномерно эллиптических и параболических уравнений дивергентного вида с измеримыми коэффициентами удовлетворяют условию Гёльдера.

Развивая технику де Джорджи и Нэша, Ладыженская и Уральцева распространили её на более общие линейные и квазилинейные уравнения эллиптического и параболического типов. Кроме того, они разработали технику вывода априорных оценок для решений эллиптических уравнений с сильными нелинейностями. Это позволило им получить точные результаты о разрешимости и гладкости решений классических краевых задач для квазилинейных уравнений, удовлетворяющих так называемым естественным условиям роста. В частности, это дало полное решение 19-й и 20-й проблем Гильберта для уравнений второго порядка.

Полученные результаты по эллиптическим уравнениям были подытожены в монографии [7], за которую авторы получили премию им. Чебышёва АН СССР[47)]. Тремя годами позже была опубликована монография [8], посвящённая параболическим уравнениям.

---

43) Амалия Эмми Нётер (Amalie Emmi Noether, 1882–1935) — немецкий математик, специалист по абстрактной алгебре и теоретической физике.

44) Нина Николаевна Уральцева (род. 1934) — профессор, зав. кафедрой математической физики ЛГУ/СПбГУ (с 1977).

45) Эннио де Джорджи (Ennio De Giorgi, 1928–1996) — итальянский математик, специалист по уравнениям в частных производных и вариационному исчислению, член Папской академии наук (1981), иностранный член ряда зарубежный академий.

46) Джон Форбс Нэш-мл. (John Forbes Nash, Jr., 1928–2015) — американский математик, специалист по теории игр и уравнениям в частных производных, лауреат Нобелевской премии по экономике (1994) и Абелевской премии (2015).

47) В 1973 году вышло второе, существенно дополненное, издание этой книги.

Из рассказа Н. Н. Уральцевой:

«Надо сказать, что Ольга Александровна очень легко писала. Я имею в виду математические тексты — книги, статьи. У меня с ней совместные три книги. И должна признаться, что бóльшую часть текстов написала она, потому что она это делала очень быстро и очень хорошо.

Нашу первую книгу мы улетели писать в Ереван на месяц в сентябре или октябре 62 года. Нас пригласили туда лекции почитать по своим результатам. <…> Два-три раза в неделю мы читали лекции, а в остальное время писали книгу. Мы сидели, закрывшись в комнате, — каждая на своей кровати — и писали каждая свою часть.

Жили мы сперва в гостинице, а потом нас поселили на турбазе. Однажды вечером приходим домой, в комнате горит свет, и нигде нет наших записок — кто-то их унёс. Мы расстроенные легли спать, утром пошли завтракать, а когда вернулись — записки оказались на месте (видимо, злоумышленникам они не пригодились).

И за месяц пребывания в Армении основная часть книги практически была готова, вернувшись мы уже только правили текст. <…>

Параболическую книжку мы уже писали вместе с Севой Солонниковым[48)]*. Он отвечал за часть с гладкими коэффициентами, про которую мы не знали. Схема работы была такая же, как и в эллиптическом случае — каждый писал свою часть, а окончательное редактирование делала Ольга Александровна».*

Обе монографии получили широкую известность и были переведены на несколько языков. В 1969 году за цикл работ по краевым задачам Ладыженская и Уральцева получили Государственную премию СССР. Заметим, что в 80-х годах они вернулись к этой тематике и получили аналогичные результаты о разрешимости для недивергентных уравнений.

Опишем ещё одно направление исследований, созданное Ольгой Александровной в теории уравнений в частных производных. В своей основополагающей работе [9] она показала, что двумерная система Навье — Стокса с условием Дирихле обладает компактным ω-предельным множеством, равномерно притягивающим любое ограниченное

[48)] Всеволод Алексеевич Солонников (род. 1933) — профессор, специалист по уравнениям в частных производных и математической гидродинамике, иностранный член Лиссабонской академии наук (2019).

множество фазового пространства. В дальнейшем это множество было названо глобальным минимальным *B*-аттрактором.

Статья [9] послужила началом теории аттракторов для уравнений в частных производных. В 1988 году по приглашению Академии деи Линчеи Ладыженская прочла в Риме курс лекций по аттракторам. Эти лекции были изданы в виде монографии [10].

Во второй половине XX века Ольга Александровна была «законодателем моды» в теории уравнений в частных производных, настоящим математическим стратегом. Важно отметить, что она интересовалась в первую очередь не столько решением, сколько постановкой новых задач.

Некоторые работы Ладыженской, её идеи и методы были настолько оригинальны, что были признаны математическим сообществом только после долгих обсуждений. С другой стороны, некоторые коллеги даже утверждали, что такие элегантные решения может найти только женщина.

Научные заслуги О. А. Ладыженской были высоко оценены международным математическим сообществом. В 1990 году она стала академиком[49)] АН СССР. Кроме того, она была избрана иностранным членом Германской академии «Леопольдина» (1985), Национальной академии деи Линчеи (1989), Американской Академии Наук и Искусств (2001), Почётным доктором Боннского университета (2002). Её работы были отмечены многочисленными премиями, в том числе высшей наградой РАН — Большой золотой медалью им. М. В. Ломоносова (2002).

Ольга Александровна создала замечательную научную школу. Обаяние её личности, умение выделять способных студентов, готовность помочь начинающим позволили ей воспитать блестящих учёных. Имена Л. Д. Фаддеева[50)], Н. Н. Уральцевой, В. А. Солонникова, В. С. Буслаева[51)] и других её учеников составляют славу петербургской школы уравнений в частных производных и математической физики. Согласно Mathematics Genealogy Project Ладыженская имеет 275 научных «потомков».

[49)] Член-корреспондент с 1981 года.

[50)] Людвиг Дмитриевич Фаддеев (1934–2017) — физик-теоретик и математик, академик АН СССР (1976) и многих зарубежных академий, директор ЛОМИ/ПОМИ (1976–2000), основатель Международного математического института им. Л. Эйлера, президент Международного математического союза (1987–1990), лауреат премии Шао (2008), Большой золотой медали им. М. В. Ломоносова (2013) и многих других наград.

[51)] Владимир Савельевич Буслаев (1937–2012) — профессор, зав. кафедрой высшей математики и математической физики СПбГУ (с 2000).

Президент РАН Ю. С. Осипов вручает медаль
Ломоносова О. А. Ладыженской

Важнейшую роль в развитии этой научной школы играли городской семинар по математической физике, о котором уже упоминалось, а также личный «маленький» семинар Ольги Александровны.

Из рассказа Н. Н. Уральцевой:

«[Большой] семинар был очень разнообразный по тематике, его создание сразу оживило математическую жизнь в Ленинграде. Там выступали люди самых широких научных интересов, помимо непосредственно матфизиков приглашались очень многие специалисты не только из Ленинграда, но из Москвы, из других мест. <…>

О. А. руководила большим семинаром до последних дней своей жизни. Самые последние, может быть, пару месяцев она перестала посещать семинар, потому что почти ничего не видела. И она не ходила уже на заседания семинара, но потом расспрашивала докладчика один на один и обсуждала».

Из рассказа Г. А. Серегина[52)]:

«Каждый большой семинар был целым представлением! Благодаря Ольге Александровне в первую очередь, а также остальным участникам <…> И докладчики были хорошие — это была большая честь сделать доклад на таком семинаре. Критика в те годы была жёсткая, но, в целом, атмосфера была очень доброжелатель-

[52)] Григорий Александрович Серегин (род. 1950) — профессор, зав. лабораторией математической физики ПОМИ (с 1998).

ная. А на маленьком семинаре всё было жёстче, через него проходили все кандидатские и докторские».

Из воспоминаний В. В. Пухначёва[53]:

«Я чувствовал, что дело идёт к докторской диссертации, и мне очень хотелось пригласить Ольгу Александровну в оппоненты. В 1973 году основные результаты были получены, и состоялось решающее выступление на семинаре в ЛОМИ. Мой доклад длился пять часов с двумя перерывами. „Добро“ было получено. Вскоре я встретился с Виктором Юдовичем[54] *и с гордостью рассказал ему об этом <…> Реакция Виктора: „Подумаешь! Мой доклад продолжался восемь часов с тремя перерывами“».*

С момента возрождения Санкт-Петербургского математического общества в 1959 году О. А. Ладыженская стала одним из самых активных его членов. Более 40 лет она была членом Правления, вице-президентом, а с 1990 по 1998 год — Президентом СПбМО. В 1998 году она была избрана Почётным членом СПбМО.

Мы говорили о математике и семинарах, но интересы Ольги Александровны вовсе не ограничивались математикой и семинарами. Она была личностью многогранной и разнообразно одарённой. Общение с ней высоко ценили многие представители мира литературы и искусства, в том числе Иосиф Бродский, Александр Солженицын[55], композитор Борис Тищенко, пианистка Надежда Голубовская.

Многолетняя дружба связывала Ладыженскую с Анной Ахматовой. Несмотря на значительную разницу в возрасте, их отношения были очень близкими. Имя Ольги Александровны много раз упоминается в записных книжках Ахматовой.

Из воспоминаний Вяч. Вс. Иванова[56] [11]:

«Я оказался в Ленинграде и узнал, что Ахматова с подозрением на инфаркт попала в больницу. Я поспешил к ней. <…> Она рассказала мне о беседе с математиком О. А. Ладыженской, приходившей

---

[53] Владислав Васильевич Пухначёв (род. 1939) — специалист в области механики сплошной среды, член-корр. РАН (1997).

[54] Виктор Иосифович Юдович (1934–2006) — профессор, зав. кафедрой вычислительной математики и математической физики Ростовского гос. университета (с 1972).

[55] История семьи Ладыженских была рассказана Ольгой Александровной Солженицыну и вошла в книгу «Архипелаг Гулаг». Ладыженская включена Солженицыным в список 257 «свидетелей Архипелага».

[56] Вячеслав Всеволодович Ива́нов (1929–2017) — лингвист, академик РАН (2000).

Эта фотография сделана в квартире Ольги Александровны

навещать её в больнице. Она советовалась с Ахматовой, каким из искусств ей заняться — её увлекали и стихи, и живопись. Ахматова с обычным для неё вниманием к каждому человеку, увлекающемуся искусством, подробно со мной обсуждала план, который она наметила по просьбе Ладыженской: занятия именно одним из видов искусств, не всем сразу. К этому она отнеслась с большой серьёзностью».

Из интервью Б. И. Тищенко [12]:

«Я представил свою Вторую симфонию на стихи Марины Цветаевой в квартире Ольги Александровны Ладыженской[57)]*, одного из крупнейших советских математиков (она была подругой Ахматовой). Она пригласила на это представление Анну Андреевну. Ахматова пришла в большом ожерелье из чёрных бус. И когда я закончил играть симфонию, она потрогала бусы и сказала: „Эти бусы мне подарила Марина“».*

Однажды Ольга Александровна рассказала Ахматовой о своей поездке в Выборг. Её эмоциональный рассказ произвёл на Анну Андреевну сильное впечатление. Поэт Анатолий Найман, литературный сек-

[57)] Ольга Александровна не играла на музыкальных инструментах, но по совету Н. И. Голубовской купила хороший рояль и время от времени организовывала домашние концерты для друзей.

ретарь Ахматовой, который за несколько дней до того также ездил с Ахматовой в Выборг, пишет [13, с. 189]:

> *«Ахматова посмотрела на меня с притворной сокрушённостью и обидой и сообщила гостье, что мы ничего такого там не заметили. Через день, если не на следующий, ею были написаны стихи „Огромная подводная ступень“ и так далее*[58)]*, с посвящением Ладыженской».*

Ладыженская была в числе 11 человек, которым Ахматова давала читать рукописи «Поэмы без героя» и «Реквиема», которые не могли быть напечатаны в СССР. Более того, она убедила Анну Андреевну сделать магнитофонную запись «Реквиема» и более 20 лет скрытно хранила плёнку. Подчеркнём, что обнаружение такой записи КГБ могло серьёзно поставить под угрозу профессиональную карьеру её хранителя. Сегодня благодаря Ладыженской мы можем слышать бессмертные строки «Реквиема» в исполнении автора.

Ольга Александровна была человеком увлекающимся. Она старалась заниматься спортом, ходила в походы, любила путешествия.

Из рассказа Н. Н. Уральцевой:

> *«Помню, поехали зимой кататься на Серенаду — любимое место прогулок между Комарово и Зеленогорском. Поехали вчетвером — мы с мужем, Ольга Александровна и ещё один знакомый. Добрались до крутой горки под названием „Лоб“, О. А. посмотрела вниз и поехала — кубарем, конечно. Пришлось обоим мужикам съезжать, и мне тоже. Всё кубарем, но лыжи у всех остались целы.*
>
> *Ещё помню, что, когда я была аспиранткой, мы катались на лыжах в Кавголово, и Ольга Александровна повредила там свой мениск довольно серьёзно. Речь даже шла о возможной операции, но её удалось избежать. Во всяком случае, О. А. не могла ходить на лекции, и мне пришлось её заменять (помню, как я боялась на первой лекции). Она тогда читала объединённый спецкурс „Краевые задачи“ для физфака и мат-меха, группе матфизиков и физиков-теоретиков. Потом эта история повторилась: лет через десять другой её аспирант (довольно известный слаломист) тоже с ней катался на лыжах в Кавголово. И О. А. опять повредила мениск, и ему пришлось читать ту же самую лекцию, что и мне, касающуюся коэрцитивных оценок для эллиптических операторов второго порядка».*

[58)] Найман приводит первую строку из стихотворения „В Выборге“.

Из воспоминаний В. В. Пухначёва:

«Не только научные интересы приводили Ольгу Александровну в Сибирь. Её любовь к путешествиям привела её на озеро Байкал с островом Ольхон и на Красноярские столбы.

Кто бывал на Столбах, тот знает, что там в моде скалолазание без страховки. Мне посчастливилось сопровождать Ольгу Александровну в этом путешествии. Ей было тогда 53 *года, но роль наблюдательницы наших* (*порой рискованных*) *восхождений была явно ей не по душе. Ольга Александровна вместе с нами покорила шесть Столбов*!»

Во время путешествий Ольга Александровна проявляла такую же страсть и неутомимость при осмотре достопримечательностей, как и при обсуждении математических результатов.

Из воспоминаний В. Я. Иврия[59)]:

«В июле 1998 *года О. А. была в Торонто на ежегодной конференции SIAM, куда она была приглашена прочесть специальную John von Neumann Lecture. <…> О. А. упомянула, что видела объявление на Королевском Музее Онтарио о выставке импрессионистов, и выразила желание её посетить <…> Моя жена* (*тоже Ольга*) *вызвалась её сопровождать на выставку.*

На следующий день моя жена отправилась на встречу с Ольгой Александровной, чтобы пойти в Галерею Искусств. Вернулась она вечером совершенно измождённая. Выяснилось, что осмотрев выставку импрессионистов, они собирались уходить, но вдруг О. А. узнала о постоянной выставке Группы Семи (*канадских художников*) *и решила ознакомиться с ней тоже. Моя жена* (*кстати, тоже изрядная любительница изобразительных искусств*) *считала, что этого уже будет многовато, но возможно. После этой выставки вдруг оказалось, что есть ещё залы индейского искусства, и О. А. решила не упустить и их, а когда они уже собрались уходить, то обнаружились залы иннуитской* (*эскимосской*) *резьбы по моржовому клыку и, разумеется, их необходимо было посетить тоже. „Оленька, ты не понимаешь, это такое искусство*!*“. И после этого она ещё решила пойти на сессию SIAM, чтобы попить кофе*!

Санкт-петербуржцы, которым я об этом рассказал, комментировали однозначно: *„Типичная О. А.*!*“*»

[59)] Виктор Яковлевич Иврий (род. 1949) — советский и канадский математик, специалист в области уравнений в частных производных, член Канадской АН (1998).

Из воспоминаний Т. Н. Шилкина[60]:

«Ольга Александровна до последних дней испытывала острый интерес к жизни. Ей было интересно всё, что её окружало, она постоянно стремилась увидеть и узнать как можно больше нового, испытать новые ощущения, по максимуму „погрузиться в жизнь“.

В Нью-Йорке она изъявила желание подняться на Empire State Building. Хотя основной подъём происходил на лифте, последний участок в несколько лестничных пролётов нужно было преодолеть пешком. Хотя было очевидно, что подниматься по лестнице ей тяжело, О. А. ни на секунду не допускала мысли, что можно отказаться от этой затеи. <…>

Мне казалось, что любую лестницу, любой подъём О. А. воспринимает как своего рода вызов и наперекор своему возрасту идёт навстречу этому новому вызову».

Многие отмечали, что Ольга Александровна очень любила всякую живность. Везде, где она во время поездок останавливалась на сколь-нибудь продолжительное время, она старалась посетить зоопарк. Её любимым телеканалом был «Animal planet».

[60] Тимофей Николаевич Шилкин (род. 1971) — специалист в области математической гидродинамики, с. н. с. лаборатории математической физики ПОМИ. В 2001 году он сопровождал Ольгу Александровну в её поездке в США.

Из воспоминаний М. Ганзбургера[61]:

«Во время каждого своего визита к нам Ольга хотела сделать что-то, связанное с животными, не ограничиваясь знакомством и игрой с нашими домашними собаками и кошками. Например, во время своего первого визита в Айову она спросила, может ли она увидеть скунса! Очевидно, что в России скунсы не водятся. Конечно, мы немного боялись подойти к нему близко, но в конце концов мы нашли одного, которого она смогла увидеть. Она была очень рада этому, и, к счастью, никаких катастрофических последствий не произошло.

Возможно, более авантюрным с её стороны был эпизод с аллигатором. Я рассказал Ольге, что моя дочь Маргарет и её муж Мэтью управляют частным заповедником и что у Мэтью там живёт „домашний“ аллигатор. Она выразила желание увидеть аллигатора (которые повсеместно встречаются во Флориде), и мы повезли её в заповедник. Она почти не проявила страха, когда встретила аллигатора вблизи, а не в зоопарке; ей определённо понравилась эта встреча».

Ольга Александровна была человеком глубоко верующим, но никогда не выставляла это напоказ. При этом её отношение к людям определялось не словами «ради Бога», но всегда «ради человека». Она была верна девизу «Кто, если не я?», всегда готовая прийти на помощь окружающим, не ожидая их просьб. Эта помощь могла быть разнообразной: деньгами, одеждой, жильём, организацией дежурств у больного, административными хлопотами… В жуткие девяностые годы она ходила с карманами, набитыми мелочью, и раздавала нищим.

Говоря о личных качествах Ольги Александровны, нельзя не упомянуть её редкое гражданское мужество.

Из рассказа Н. Н. Уральцевой:

«Все, кто помнит Ольгу Александровну, отмечают, что она была очень отважным и смелым человеком. Даже во времена, когда люди старались помалкивать, она не могла сдерживаться, и если нужно было защищать свою позицию, она это делала очень открыто. Позднее Ольга Александровна нередко выступала в защиту хороших студентов с „плохой“ анкетой.

---

[61] Макс Ганзбургер (Max Gunzburger, род. 1947) — американский математик, специалист в области вычислительных методов и математической гидродинамики.

Я помню, что она собирала деньги для помощи политзаключённым, в том числе Револьту Пименову[62]*. Делала она это аккуратно, тайно, среди друзей, не информируя посторонних. В трудные времена, когда были гонения на Солженицына, она дружила с Солженицыным, — это было также небезопасно».*

В последние годы жизни у Ольги Александровны были проблемы со зрением, которые обострились к 2003 году, несмотря на усилия врачей.

Из воспоминаний Р. С. Сакса[63]:

«Осенью 2003 *года Ольга Александровна пригласила меня приехать к ней <…> Когда я приехал, выяснилось, что она почти потеряла зрение: видела краем глаза только крупные буквы. И ей нужен был помощник — читать и переводить работы, которые она отобрала перед поездкой в США на зиму. <…>*

Работ оказалось очень много, и мы несколько дней сидели допоздна, разбирая их. Видимо, какие-то оттиски она собиралась взять с собой. Статьи были на английском, я с ходу переводил и читал ей по-русски. О. А. тут же решала, интересна ей работа или нет, или просила прочитать ей заново какое-то место. Казалось, она не уставала — приносила мне всё новые кипы бумаг. В последний вечер перед моим отъездом мы сидели с ней до трёх часов ночи, пока я не взмолился. Она сказала: „Слабак!“ и ушла к себе».

Ольга Александровна любила солнечный свет, поэтому каждую зиму, в самый тёмный период в Санкт-Петербурге, она старалась, по её собственному выражению, «перебраться в тёплые страны». 12 января 2004 года она должна была отправиться во Флориду. Вечером 11 января она легла спать, чтобы отдохнуть перед дальней поездкой.

Она не проснулась.

Говорят, что такая смерть даётся лишь избранным.

Из воспоминаний П. З. Мкртычяна[64]:

«<…> я бы хотел вспомнить тот скорбный январский день 2004 *года, когда мы провожали в последний путь Ольгу Александровну.*

---

[62] Револьт Иванович Пименов (1931–1990) — д. ф.-м. н., специалист в области геометрии. Участник диссидентского и правозащитного движения в СССР, неоднократно подвергался репрессиям.

[63] Ромэн Семенович Сакс (род. 1938) — профессор, специалист в области уравнений в частных производных, в. н. с. Института математики Уфимского НЦ РАН.

[64] Павел Зорикович Мкртычян (род. 1952) — специалист в области уравнений в частных производных, доцент СПбГУТ.

Ольга Александровна Ладыженская была и остаётся великим математиком. Но великого математика можно похоронить траурно-торжественно, со всеми подобающими почестями, воздав должную дань уважения достижениям и заслугам, но обойтись без слёз. А в тот день было настоящее всеобщее людское горе с морем искренних человеческих слёз».

О. А. Ладыженская похоронена на Комаровском кладбище[65)]. Её могила находится недалеко от могил А. А. Ахматовой и В. И. Смирнова.

Список литературы

[1] *Серегин Г. А.*, *Уральцева Н. Н.* Ольга Александровна Ладыженская (к 80-летию со дня рождения) // УМН. 2003. Т. 58, вып. 2(350). С. 181–206.

[2] Владимир Иванович Смирнов, 1887–1974 / Изд. 2, доп. Отв. ред. О. А. Ладыженская, В. М. Бабич. М.: Наука, 2006.

[3] *Ладыженская О. А.* Смешанная задача для гиперболического уравнения. М.: ГИТТЛ, 1953.

[4] *Русанов А. И.* К 70-летию… меня. СПб., 2002.

[5] *Киселёв А. А.*, *Ладыженская О. А.* О существовании и единственности решения нестационарной задачи для вязкой несжимаемой жидкости // Изв. АН СССР. Сер. матем. 1957. Т. 21, № 5. С. 655–680.

[6] *Ладыженская О. А.* Решение «в целом» краевой задачи для уравнений Навье — Стокса в случае двух пространственных переменных // ДАН СССР. 1958. Т. 123, № 3. С. 427–429.

[7] *Ладыженская О. А.*, *Уральцева Н. Н.* Линейные и квазилинейные уравнения эллиптического типа. М.: Наука, 1964.

[8] *Ладыженская О. А.*, *Солонников В. А.*, *Уральцева Н. Н.* Линейные и квазилинейные уравнения параболического типа. М.: Наука, 1967.

[9] *Ладыженская О. А.* О динамической системе, порождаемой уравнениями Навье — Стокса // Записки научн. семин. ЛОМИ. 1972. Т. 27. С. 91–115.

[10] *Ladyzhenskaya O.* Attractors for Semigroups and Evolution Equations. Cambridge: Cambridge University Press, 1991.

[11] *Иванов Вяч. Вс.* Беседы с Анной Ахматовой // Воспоминания об Анне Ахматовой. М.: Сов. писатель, 1991. С. 473–502.

[65)] Комаровский некрополь — кладбище в посёлке Комарово, пригороде Санкт-Петербурга. На нём находятся более двухсот могил известных учёных, деятелей литературы и искусства. Объект всемирного наследия ЮНЕСКО.

[12] Газета «Частный корреспондент», 15.08.2010.

[13] *Найман А. Г.* Рассказы об Анне Ахматовой. М.: Худ. лит., 1989.

Дарья Евгеньевна Апушкинская, РУДН
apushkinskaya@gmail.com

Александр Ильич Назаров, ПОМИ РАН и СПбГУ
al.il.nazarov@gmail.com

Памяти Джона Хортона Конвея

Л. Х. Кауффман

§ 1. Введение

Джон мог усадить вас и показать волшебный фокус, а затем научить, как его делать (если вы могли такое усвоить). Джон мог усадить вас и прочитать короткую чёткую лекцию о скейн-соотношениях (что он и делал для многих из нас в 1970-е годы), и вы думали — это остроумно. И это меняло вашу жизнь.

Вот вкратце моё впечатление от Джона Конвея.

Впервые я встретил его в 1970-х, когда он приезжал к Вере Плесс в Иллинойсский университет в Чикаго (где я учился с 1971 г., а теперь заслуженный профессор). Он сделал доклад о многочлене Александера и как его можно вычислить индуктивно с помощью теории скейн-соотношений — рекурсии включали только диаграммы узлов и зацеплений. Никаких других инструментов не требовалось. Топологи изучали многочлен Александера с помощью таких структур, как свободное дифференциальное исчисление Фокса, группы гомологий, модули, бесконечное циклическое накрытие дополнения узла, фундаментальная группа, представления групп, специальный арсенал алгебраической топологии. А этот волшебник объяснил нам, как получить многочлен Александера из чистой комбинаторики, которую мог понять старшеклассник. (На самом деле было сказано, что он открыл этот способ, будучи старшеклассником.) Затем он сообщил, что рассказал нам это ещё в 1969 году, но тогда лишь немногие его слушали. Так или иначе, в этот раз мы стали слушать.

Я снова встретил его, когда был приглашённым профессором в Энн-Арборе (Мичиган), и он ещё кое-что рассказал о скейн-соотношениях. Я задавал ему вопросы об этом подходе, очень трудные и выглядевшие

Kauffman L. H. John Horton Conway — a recollection. Статья написана для «Математического просвещения». Перевод Б. Р. Френкина.

неясными, а он сказал: «Всё это содержится в скейн-соотношениях». И я поверил ему. В итоге я нашёл модель для рассказанного им с помощью работы Зайферта 1930-х годов, а потом нашёл другую модель с помощью работы Александера 1920-х. Работа Александера в моём сознании преобразовалась, став особой комбинаторикой, причём аналогичной некоторым структурам статистической физики (статистическим суммам), и я написал книгу об этих новых способах работы с многочленами Александера (Kauffman, Formal Knot Theory, Princeton University Press 1981 [9]). Но я не подозревал, какие глубины скрыты в этом месте. Не подозревал этого и Конвей.

В 1983 Воган Джонс (руководясь идеями из теории алгебр фон Неймана и статистической физики) открыл новый инвариант со скейн-тождеством, которое было небольшой модификацией тождества Конвея для многочлена Александера. Конвей мог бы его открыть, если бы задался вопросом, что происходит при изменении какого-либо коэффициента или знака в его формуле для многочлена Александера! В тот момент многие, включая меня, ухватились за эту идею — и началась новая эпоха в теории узлов. Открылась связь с физикой, а Конвей открыл связь с диаграммами и рекурсией. Всё это вовлекло нас в дьявольскую пляску, которая с тех пор продолжается все эти годы. Мир изменился.

Джон был глубоким математиком и действующим магом. Он хотел вызвать изумление своей магией, и он хотел вовлечь вас в создание и отделку этой магии. Он был изобретателем и наставником. Он мог очень напряжённо работать, чтобы привести кусочек математики в такое состояние, когда он глубоко нетривиален и однако может быть несколькими штрихами объяснён почти любому. Так обстоит дело с игрой «Жизнь», теорией скейн-соотношений, фокусами с верёвкой, аудиоактивностью[1)], сюрреальными числами и многим другим, что он любил. Этот труд любви, превращающий математику в созидательную магию, был самой характерной чертой Джона Хортона Конвея. Она всегда будет жить в сердце каждого, с кем он соприкасался.

§ 2. Теория скейнов и так далее

Одно из важнейших достижений Конвея в теории узлов — его теория рациональных танглов. Здесь я дам лишь некий её набросок. На рис. 1 вы увидите два тангла T и S (кусочки танглов связаны с четырьмя

[1)] См. § 3. — *Прим. перев.*

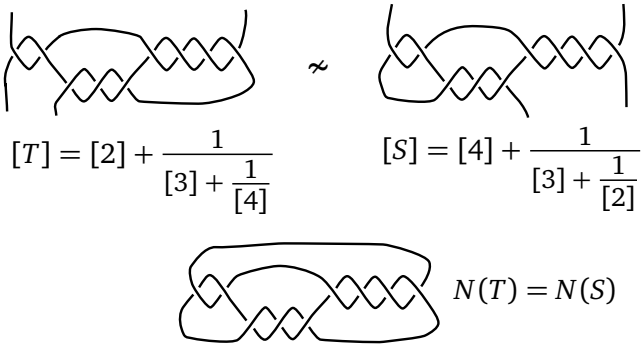


Рис. 1. Цепные дроби и рациональные узлы

свободными концами), один помечен цепной дробью

$$[2, 3, 4] = 2 + \frac{1}{3 + \frac{1}{4}} = 2 + \frac{4}{13} = \frac{30}{13},$$

а другой — цепной дробью

$$[4, 3, 2] = 4 + \frac{1}{3 + \frac{1}{2}} = 4 + \frac{2}{7} = \frac{30}{7}.$$

По теореме Конвея о танглах [4] оказывается, что такими дробями классифицируется топологический тип танглов. Чтобы получить танглы данного типа, мы фиксируем концы и позволяем танглам двигаться. Два тангла на рис. 1 оказываются топологически не эквивалентными. Но, как показывается рисунок, они связаны. Оба они замыкаются в один и тот же рациональный узел, помеченный на рисунке как $N(T) = N(S)$. Теперь заметим, что обе дроби имеют один и тот же числитель (30), а что касается знаменателей, то $7 \times 13 = 91$ — число с остатком 1 при делении на 30. Это не случайно. Есть красивый способ классифицировать рациональные узлы (замыкания рациональных танглов) по их цепным дробям. Можно выбрать обозначение $(4, 3, 2)$ с точностью до обращения $(2, 3, 4)$ в качестве индикатора рационального узла на рисунке. На этой основе Конвей разработал простые обозначения для рациональных узлов и затем применил их вместе с вложениями в определённые графы, чтобы создать очень удобные обозначения узлов, позволяющие очень изящно маркировать тысячи узлов в соответствующих таблицах.

Ниже следует краткое введение в теорию скейнов Джона Конвея [4]. Начнём с рис. 2, где я схематически изобразил диаграмму узла или зацепления K_+ и другую диаграмму K_-, которая отличается лишь пере-

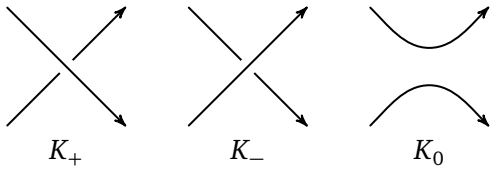


Рис. 2. Скейн-тройка

ключением перекрёстка (переменой местами верхнего и нижнего ребра, что показано для случая единственного перекрёстка). На том же рисунке представлена ещё одна диаграмма K_0, где перекрёсток заменён двумя параллельными дугами. Это так называемое *разрешение* перекрёстка. Три диаграммы K_+, K_-, K_0, вместе взятые, называются *скейном* (*скейн-тройкой*), и Конвей сообщил нам ключевое соотношение для своего многочлена $\nabla_K(z)$, который сопоставляется каждой ориентированной диаграмме зацепления:

$$\nabla_{K_+} - \nabla_{K_-} = z\nabla_{K_0}.$$

Наряду с этим *скейн-соотношением* он сообщает нам, что

$$\nabla_O = 1,$$

где O обозначает незаузленную окружность. Он также сообщает, что если K и K' — топологически эквивалентные узлы или зацепления, то

$$\nabla_K = \nabla_{K'}.$$

Это полный набор правил для отыскания инварианта $\nabla_K(z)$ любого ориентированного зацепления K.

На рис. 3 мы иллюстрируем простейшее следствие из этих аксиом. Базовая скейн-тройка состоит из U, U', V, где U и U' — тривиальные узлы, а V — пара незаузленных окружностей. Значения многочлена Александера — Конвея для U и U' равны 1, так что их разность равна 0. Отсюда получаем, что $z\nabla_V = 0$, так что $\nabla_V = 0$. Можно показать, что таким образом многочлен Александера — Конвея получает значение 0 для тривиального зацепления любого количества компонент.

На рис. 4 мы иллюстрируем эту ситуацию для некоторых конкретных диаграмм. Здесь T — диаграмма трилистника, а U — результат «переключения» одного перекрёстка на диаграмме T. Можно положить $K_+ = T$, $K_- = U$ и $K_0 = L$, где L — двухкомпонентное зацепление в верхнем ряду рисунка. Таким образом,

$$\nabla_T - \nabla_U = z\nabla_L \quad \text{и} \quad \nabla_L - \nabla_V = z\nabla_W.$$

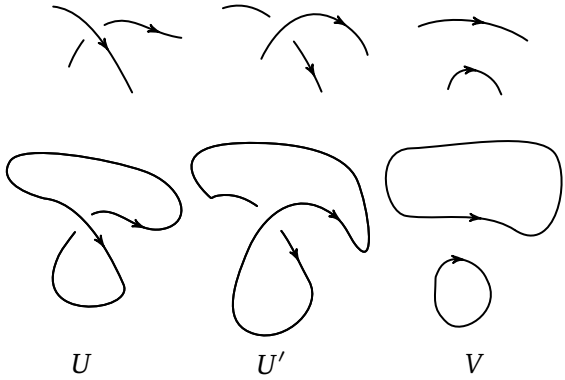


Рис. 3. Скейн-тройка для тривиального зацепления

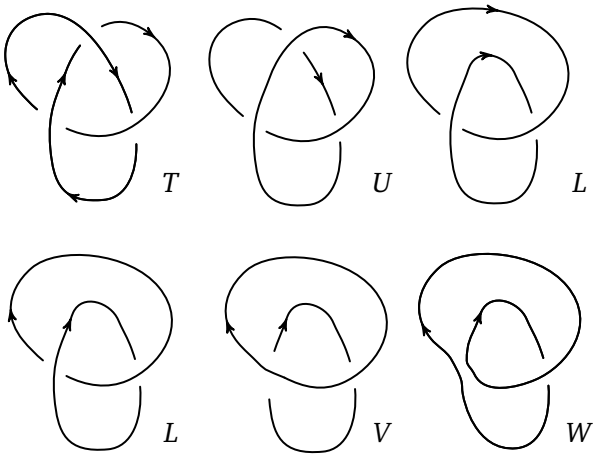


Рис. 4. Скейн-тройка для трилистника

Но U и W — тривиальные узлы, а V — тривиальное зацепление. Кроме того, мы проверили, что у тривиального зацепления нулевой многочлен. Отсюда получаем, что $\nabla_T - 1 = z\nabla_L$ и $\nabla_L = z$, так что $\nabla_T = 1 + z^2$.

Любой узел или зацепление можно сделать на диаграмме тривиальным, «переключив» («перевернув») некоторые его перекрёстки, как мы сделали в случае трилистника T и зацепления Хопфа L. Благодаря этому можно применить скейн-соотношение Конвея, чтобы вычислить многочлен Александера — Конвея $\nabla_K(z)$ для любого узла или зацепления K. Замечательно, что, хотя во многих пунктах этого вычисления возможен различный выбор, ответ всегда однозначен и является топологическим инвариантом зацепления K.

Не столь общеизвестно, что Конвей понимал скейн-теорию гораздо шире, а не как следствие из единственного базового скейн-соотно-

шения, приведённого выше. Конвей мог поведать вам, что узел или зацепление K живёт в «скейн-комнате» $\{K\}$ и можно ввести неассоциативные операции $\oplus, \ominus$ между скейн-комнатами таким образом, что

$$\{K_+\} = \{K_-\} \oplus \{K_0\} \quad \text{и} \quad \{K_-\} = \{K_+\} \ominus \{K_0\}.$$

В пределах данной комнаты $\{K\}$ можно найти любой вариант узла или зацепления K, который может появиться после деформации или объемлющей изотопии. Это означает, что все обитатели комнаты топологически эквивалентны между собой, и они могут быть диаграммами вроде показанных выше или полными трёхмерными вложениями узла или зацепления. Исследуя скейн-тройку, мы берём три представителя K_+, K_-, K_0, по одному из каждой комнаты, причём представители должны быть одинаковы за исключением мест, где происходит «переключение» или разрешение перекрёстка. И мы говорим, что комната $\{K_+\}$ *скейн-эквивалентна* конкатенации $\{K_-\} \oplus \{K_0\}$. Таким способом можно получить *скейн-разложение* узла или зацепления. На рис. 4 можно видеть, что

$$\{T\} = \{U\} \oplus \{L\}, \quad \{L\} = \{V\} \oplus \{W\},$$

так что

$$\{T\} = \{U\} \oplus (\{V\} \oplus \{W\}).$$

Это окончательное скейн-разложение узла T выражает трилистник в скейн-тройке как композицию двух тривиальных узлов и тривиального зацепления. Для любого узла существует такое скейн-разложение на тривиальные узлы и тривиальные зацепления. Решающую роль играет неассоциативность скейн-операций.

Два узла или зацепления называются *скейн-эквивалентными*, если у них одинаковое разложение на тривиальные узлы и зацепления. Полное описание классов скейн-эквивалентности узлов и зацеплений — открытая проблема до сего дня. Определив понятие скейна, Конвей открыл совершенно новую область топологии.

В контексте теории скейнов многочлен Александера — Конвея превращается в один из способов записать скейн-инварианты, причём

$$\nabla(A \oplus B) = \nabla(A) + z\nabla(B) \quad \text{и} \quad \nabla(A \ominus B) = \nabla(A) - z\nabla(B).$$

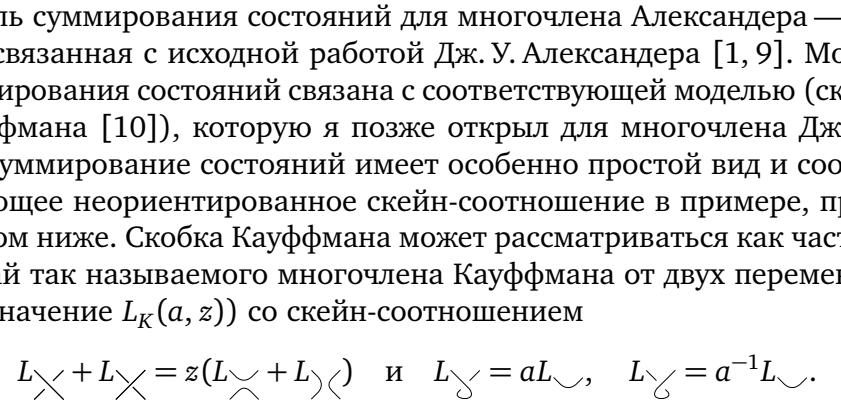
Что было не очевидно для Конвея в 1970-е годы, так это факт, что кроме многочлена Александера — Конвея и его аналогов от нескольких переменных существуют и другие линейные скейн-инварианты. Самый впечатляющий из них появился вслед за многочленом Джонса [7].

Его часто называют Homflypt-многочленом по его авторам (из независимых групп) Hoste, Ocneanu, Millett, Freyd, Lickorish, Yetter, Przytycki, Traczyk (см. [6, 15]). Линейное соотношение для него имеет вид

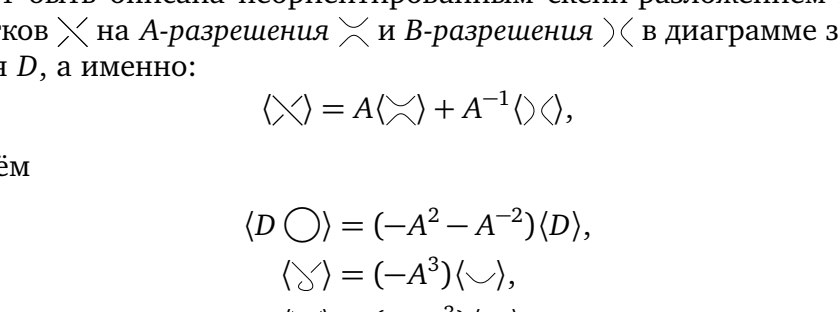
$$aP_{K_+} - a^{-1}P_{K_-} = zP_{K_0}$$

и сопоставляет ориентированному узлу или зацеплению K многочлен Лорана $P_K(a, z)$, который является инвариантом его топологического типа. Многочлен Джонса — частный случай Homflypt-многочлена. Ключевое свойство этих многочленов — их способность отличать многие узлы от их зеркальных образов. Математический контекст, из которого происходят эти новые скейн-многочлены, включает многие вопросы математической физики, алгебр Ли и алгебр Хопфа [2, 3, 7, 16]. Эти многочлены служат основой новейших достижений в изучении инвариантов Васильева и гомологии зацеплений.

Некоторые вопросы теории скейнов стали ясны в связи с моими работами. Один из них — модель многочлена Александера — Конвея, которая использовала работу Зайферта 1930-х годов [8]. Другой — модель суммирования состояний для многочлена Александера — Конвея, связанная с исходной работой Дж. У. Александера [1, 9]. Модель суммирования состояний связана с соответствующей моделью (скобка Кауффмана [10]), которую я позже открыл для многочлена Джонса. Это суммирование состояний имеет особенно простой вид и соответствующее неориентированное скейн-соотношение в примере, приведённом ниже. Скобка Кауффмана может рассматриваться как частный случай так называемого многочлена Кауффмана от двух переменных (обозначение $L_K(a, z)$) со скейн-соотношением

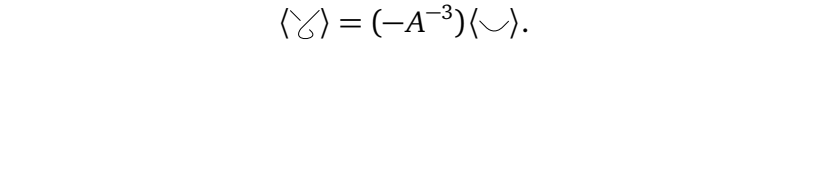


Модель скобочного многочлена [10, 11] для многочлена Джонса может быть описана неориентированным скейн-разложением перекрёстков на *A-разрешения* и *B-разрешения* в диаграмме зацепления D, а именно:



(1)

причём



(2)

(3)

(4)

В терминах скейн-теории Конвея мы имеем неориентированную скейн-тройку с уравнением

$$\{\times\} = \{\asymp\} \oplus \{)(\}.$$

Исследуя это уравнение в каждом перекрёстке диаграммы узла, получаем неориентированное скейн-разложение, где теперь допускается, что операция $\oplus$ ни коммутативна, ни ассоциативна. Тогда скобочный многочлен оценивает этот неориентированный скейн, удовлетворяющий уравнению

$$\langle \{X\} \oplus \{Y\} \rangle = A\langle \{X\} \rangle + A^{-1}\langle \{Y\} \rangle.$$

Как и в случае ориентированного скейна, этот неориентированный скейн содержит неразгаданные тайны, которые медленно раскрываются. Есть лишь предположение, что скобочный многочлен может

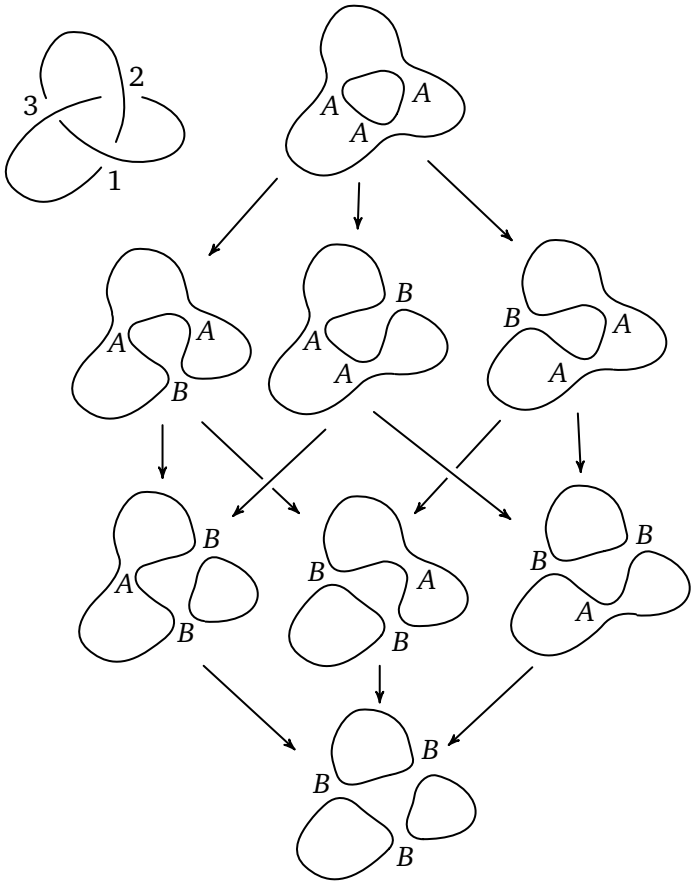


Рис. 5. Скобочные состояния и комплекс Хованова

выявить тривиальный узел, но доказано [13], что тривиальный узел выявляется обобщением скобки Кауффмана в теории гомологий, которое сделано Михаилом Ховановым [12]. Что ещё скрыто в ориентированных и неориентированных скейнах узлов и зацеплений?

На рис. 5 приведена подсказка насчёт гомологии Хованова. На этом рисунке мы иллюстрируем все случаи скобочного суммирования состояний. Его можно также истолковать как полное скейн-разложение трилистника. Каждая диаграмма добавляет слагаемое в скобочный многочлен, и их сумма составляет весь скобочный многочлен. Хованов исследует эту диаграмму состояний и видит, что она образует категорию. Объекты категории — сами состояния. Морфизмы, порождающие категорию, — стрелки на рисунке. Каждая стрелка соединяет два состояния, отличающиеся разрешением ровно одного перекрёстка, причём стрелка направлена от состояния с меньшим количеством разрешений к состоянию, где на одно разрешение больше. Хованов строит свою теорию гомологий для узлов, исходя из соответствующей теории гомологий для этой категории. Здесь мы соприкасаемся с основами алгебраической топологии, где нерв категории допускает симплициальную структуру, а соответствующий функтор в некоторую категорию модулей подключает богатые возможности гомологической алгебры. Ничто из этого не произошло бы, если бы Конвей не открыл скейн.

§ 3. Аудиоактивность

Я хочу рассказать о загадке, которую Конвей превратил в небольшую остроумную теорию [5]. История этой загадки хорошо известна. Её рассказывал сам Конвей — устно и даже не раз письменно.

Джон был в некоем обществе, где ему предъявили следующую последовательность чисел: 1, 11, 21, 1211, 111221, 312211, … и спросили, какое число будет следующим и по какому правилу строится последовательность. Согласно рассказу Конвей был озадачен, и когда ему рассказали решение, он был восхищён процессом, который приводит к этой последовательности. На следующий день в самолёте он начал исследование его потрясающих свойств.

Видите ли вы следующий член последовательности? Прервите чтение и задумайтесь! Следующий абзац раскроет секрет.

Прочтите последовательность вслух и громко:

1
одна единица:11
две единицы: 21

одна двойка, одна единица: 1211
одна единица, одна двойка, две единицы: 111221
три единицы, две двойки, одна единица: 312211

Каждая строка описывает предыдущую.

11 говорит «одна единица» и описывает 1.
21 говорит «две единицы» и описывает 11.
1211 говорит «одна двойка, одна единица» и описывает 21.
111221 говорит «одна единица, одна двойка, две единицы» и описывает 1211.
312211 говорит «три единицы, две двойки, одна единица» и описывает 111221.

Так что следующий член последовательности имеет вид 13112221 и описывает 312211. Можно продолжить последовательность следующим образом:

1
11
21
1211
111221
312211
13112221
1113213211
31131211131221
…

Не хотел бы и дальше лишать вас удовольствия исследовать территорию, которую открыл Джон Конвей с помощью аудиоактивной[2)] последовательности. Поэтому закончу своим собственным небольшим изысканием. Начнём с произвольного символа и будем рекурсивно описывать описания:

*
1*
111*
311*
13211*
111312211*

[2)] Этот термин Конвея образован по аналогии с «радиоактивностью» и означает, что строение последовательности обнаруживается при её громком произнесении. — *Прим. перев.*

31131122211*
1321132132211*
…

Вы заметите интересную закономерность, что каждый раз третья строка после данной является (почти) её продолжением. В действительности если начать с символа 3, то продолжения будут точными:

3
13
1113
3113
132113
1113122113
311311222113
13211321322113
…

Это значит, что можно построить такие три бесконечные последовательности A, B и C (см. рис. 6), что

B описывает A,
C описывает B,
A описывает C!
A = 1113122113121113222113…
B = 3113112221131112311332 2113…
C = 13211321322113311213212322 2113…

Получились три последовательности, каждая из которых описывает следующую по кругу, и все возникают из описания символа 3.

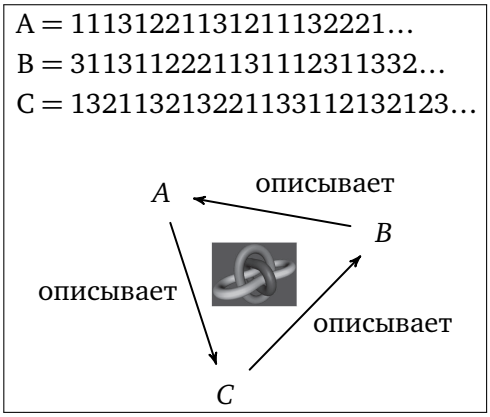


Рис. 6. Описание тройки

В этой загадке и этом примере мы видим замечательную мощь рекурсивного описания — целые миры возникают, казалось бы, совсем из ничего.

Отметим, что 22 описывает себя. Это единственная последовательность с таким свойством в этом языке.

То, как 22 производит себя, я могу сравнить с машиной Джона фон Неймана B [14], которая может себя построить[3]. Универсальная машина B была «универсальным строителем». Дайте ей описание x, и B построит объект X с таким описанием. Так что можно написать

$$B, x \longrightarrow X, x.$$

Машина B использует описание x, чтобы построить X. Результатом является X вместе с его описанием x. Фантастика: машина B может построить себя. Просто дайте ей её собственное описание, и тогда

$$B, b \longrightarrow B, b,$$

т. е. B создаёт свою копию.

Пусть стрелка

$$nx \longrightarrow xxx \cdots x \ (n \text{ раз } x)$$

«ничего больше не описывает» и создаёт строку с описанием nx. Это аналог того, что делает машина фон Неймана, и nx — описание результата. Тогда $2x \longrightarrow xx$, и мы видим, что строка $22 \longrightarrow 22$ создаёт свою копию. Разумеется, это частный случай схемы фон Неймана. Его самосозидающая машина — это почти философская идея: «Строит себя по своему собственному описанию». Но мы видим, что такая идея может появиться в простых описаниях «обычных строк» — таких, как мы с вами, а также аудиоактивное 22 Джона Хортона Конвея.

Список литературы

[1] *Alexander J. W.* Topological invariants of knots and links // Trans. Amer. Math. Soc. 1928. Vol. 30, iss. 2. P. 275–306.

[2] *Atiyah M. F.* The Geometry and Physics of Knots. Cambridge: Cambridge University Press, 1990. (Lezioni Lincee. [Lincei Lectures]).

[3] *Bar-Natan D.* On Khovanov's categorification of the Jones polynomial // Algebraic and Geometric Topology. 2002. Vol. 2. P. 337–370.

[3] В подлиннике присутствует фраза: «Descriptions were called „blueprints“ in those days». В переводе употребляется термин «описание». — *Прим. перев.*

[4] *Conway J. H.* An enumeration of knots and links, and some of their algebraic properties // Computational Problems in Abstract Algebra. Oxford: Pergamon, 1970. P. 329–358.

[5] *Conway J. H.* The weird and wonderful chemistry of audoactive decay // Open Problems in Communication and Computation / Ed. by T. M. Cover and B. Gopinath. Springer-Verlag, 1987. P. 173–188.

[6] *Freyd P.*, *Yetter D.*, *Hoste J.*, *Lickorish W. B. R.*, *Millett K.*, *Ocneanu A.* A New Polynomial Invariant of Knots and Links // Bull. Amer. Math. Soc. 1985. Vol. 12, № 2. P. 239–246.

[7] *Jones V. F. R.* A polynomial invariant of links via von Neumann algebras // Bull. Amer. Math. Soc. 1985. № 12. P. 103–111.

[8] *Kauffman L. H.* The Conway polynomial // Topology. 1980. Vol. 20, № 1. P. 101–108.

[9] *Kauffman L. H.* Formal Knot Theory. Princeton University Press, 1983. (Mathematical Notes; Vol. 30).

[10] *Kauffman L. H.* State Models and the Jones Polynomial // Topology. 1987. Vol. 26. P. 395–407.

[11] *Kauffman L. H.* New invariants in the theory of knots // Amer. Math. Monthly. 1988. Vol. 95, № 3. P. 195–242.

[12] *Khovanov M.* A categorification of the Jones polynomial // Duke Math. J. 2000. Vol. 101, № 3. P. 359–426.

[13] *Kronheimer P. B.*, *Mrowka T. S.* Khovanov homology is an unknot-detector // Publ. Math. de l'IHES. 2011. № 113. P. 97–208.

[14] *Neumann J. von*, *Burks A. W.* Theory of Self-Reproducing Automata, University of Illinois Press, 1966.

[15] *Przytycki J.*, *Traczyk P.* Conway Algebras and Skein Equivalence of Links // Proc. Amer. Math. Soc. 1987. Vol. 100. P. 744–748.

[16] *Witten E.* Quantum field Theory and the Jones PolynomialË // Commun. Math. Phys. 1989. Vol. 121. P. 351–399.

Луис Хирш Кауффман, Иллинойсский университет (Чикаго)

kauffman@uic.edu, loukau@gmail.com

Никита Введенская

В. М. Тихомиров

6 мая 2022 года закончился жизненный путь прекрасного человека, замечательного математика и вычислителя Никиты Дмитриевны Введенской. Она родилась в Ташкенте 9 октября 1930 года.

Она была одарена счастливой возможностью гордиться своим отцом. Её отец — Дмитрий Алексеевич Введенский (1887–1956) был выдающимся хирургом и патриотом своей Родины в самом высоком смысле этого слова. Он прожил необычайно яркую жизнь, защищая свою Родину в Первую мировую войну сначала в царской армии, а затем в русском экспедиционном корпусе во Франции. Когда началась Отечественная война, Дмитрию Алексеевичу было 53 года, ему полагалась бронь, но он добился того, что его, во исполнение его доброй воли, отправили на фронт, и он закончил войну в Берлине. Дмитрий

Алексеевич был награждён высокими орденами царской России, Франции и Советского Союза. С 1934 года до ухода на пенсию в 1954 году он заведовал урологической клиникой Ташкентского медицинского института (с перерывом на фронт). В 1921 году, когда Дмитрию Алексеевичу было 33 года, он женился на девушке, которая была на 13 лет его моложе и работала в его госпитале медсестрой. В октябре 1930 года у Дмитрия Алексеевича и Веры Андреевны родилась дочь, которой они дали двойное имя: Никита-Наталья, но в дружеском общении её всегда звали Никитой.

Ташкенский дом Введенских часто посещали высокоинтеллигентные и широко мыслящие друзья — врачи, учёные, литературоведы. Всё это оказало большое влияние на формирование личности Никиты Введенской.

В это время в Ташкентском университете работали математические кружки. Никите нравилось решать задачи, и она поехала в Москву поступать на механико-математический факультет Московского государственного университета.

Никита поступила на мехмат в 1948 году. В ту пору мехмат был небольшим факультетом, размещавшимся на одном этаже старого здания университета на Моховой. Но уровень факультета был исключительно высок. Лекции и семинары вели замечательные профессора и преподаватели, а необычайной особенностью факультета было наличие очень большого числа научных семинаров, среди которых были такие семинары мирового значения, как семинар Д. Е. Меньшова и Н. К. Бари, продолжающий тематику Н. Н. Лузина, развитие которой привело к рождению московской математической школы; топологический кружок П. С. Александрова, основанный им вместе с П. С. Урысоном, ставший центром общей топологии в мире; семинар по теории вероятностей А. Н. Колмогорова и А. Я. Хинчина, на котором были получены в тридцатые – пятидесятые годы крупнейшие результаты в этой области; семинар И. Г. Петровского, на котором создавалась общая теория уравнений с частными производными; работал один из самых разносторонних семинаров всех времён — семинар И. М. Гельфанда. В студенческие годы Никиты стали пробиваться ростки той науки, которая неслыханным образом расширилась в XX веке и получила название информатики. На мехмате было создано отделение вычислительной математики, стали преподавать программирование и вычислительную математику.

Научное творчество Н. Д. Введенской состоит из трёх периодов, соответствующих трём основным местам её работы. В первый период

(в аспирантуре МГУ) она развивала направление общей теории уравнений с частными производными, где лидером был Иван Георгиевич Петровский. Затем она перешла в Отделение прикладной математики (впоследствии — Институт прикладной математики имени М. В. Келдыша), где стала заниматься приложением вычислительной математики к проблемам естествознания под руководством Константина Ивановича Бабенко. А в третий период Никита Дмитриевна работала в Институте проблем передачи информации им. А. А. Харкевича над проблемами теории информации, где ведущим инструментом является теория вероятности. Здесь роль лидера играл Роланд Львович Добрушин.

Свои студенческие годы Никита провела с большим увлечением и энтузиазмом. Она хорошо училась и с первого курса стала посещать математические кружки А. С. Кронрода и Е. Б. Дынкина, что оказало на неё большое влияние. На этих кружках она обрела друзей на всю жизнь — Р. Л. Добрушина, Ф. А. Березина, В. А. Успенского, Р. А. Минлоса и других.

Р. Л. Добрушин и В. А. Успенский рассказывали мне о знакомстве с Никитиным отцом, запомнившимся им на всю жизнь.

Кажется, в 1949 году Дмитрий Алексеевич приехал в Москву и ему захотелось повстречаться с Никитиными друзьями. Он пригласил Никиту, Р. Л. Добрушина и В. А. Успенского в ресторан. Их обслуживал почтенный официант. Было очевидно, что он работал официантом ещё до революции. На его вопрос «Что вам будет угодно заказать?» Дмитрий Алексеевич завязал следующий разговор — он стал называть блюда из знаменитого трактира Тестова (располагавшегося до революции на углу Воскресенской — ныне Революции — и Театральной площадей):

— Пожалуйста, специально для меня — гурьевской каши.

— Увы, перестали варить полвека назад — был ему ответ.

— Ну, тогда всем нам по раковому супу с растегайчиками.

— Увы, сейчас это не готовят.

— Ну тогда тестовского поросёнка, пожалуйста.

Официант согнулся в поклоне с широко разведёнными руками и сказал:

— Тестов умер…

Такой весёлой и свободной личностью остался в памяти моих друзей отец Никиты.

Вернёмся к ранним университетским годам Никиты. Она была одним из руководителей школьных кружков, активно участвовала в проведении математических олимпиад. Я впервые увидел Никиту на от-

крытии Двенадцатой московской математической олимпиады 1949 года. Она всё время фотографировала президиум, выступавших и школьников для стенгазеты, информации об олимпиаде и для истории. На XIV олимпиаде Никита была секретарём председателя олимпиады Бориса Николаевича Делоне, в 1952 году в «Успехах математических наук» появилась её первая заметка (совместно с Б. Н. Делоне) о проведении этой олимпиады.

С тех же самых времён начались её пешие, лыжные и лодочные прогулки, однодневные и длительные походы с друзьями, которые закончились лишь около её девяностолетия, когда она фактически лишилась зрения. К этим темам мы ещё вернёмся.

Никита выбрала в качестве своего основного научного направления уравнения с частными производными. Её научным руководителем стала ученица И. Г. Петровского Ольга Арсеньевна Олейник, тогда ещё кандидат наук, будущий академик. Начиная с курсовых работ (первая из которых писалась на втором курсе) и до самых последних дней жизни основную долю своего времени Никита уделяла плодотворной творческой деятельности в области математики. Ещё в студенческие годы она стала посещать научный семинар О. А. Олейник.

В этом семинаре в те годы вместе с Никитой Введенской принимали участие Арлен Ильин, Сусанна Каменомостская, Татьяна Вентцель, Анатолий Калашников, Леонид Волевич. Это был очень активный и деятельный коллектив одарённых математиков. На этом семинаре Никита неоднократно выступала с научными сообщениями. Никита была человеком с очень быстрой реакцией. Мне запомнился один эпизод. Как-то раз Никита высказала некое математическое утверждение. Последовала реплика из аудитории:

— Но это же тривиально!

Никита тут же парировала:

— Это не только тривиально, но это можно и доказать!

Как-то после того, как Ольга Арсеньевна Олейник защитила докторскую диссертацию, в Университет пришла киногруппа для съёмки её семинара. В это время Никита делала доклад. Руководитель съёмки сказал, что докладчик может говорить что угодно. Никита тут же продолжила в вольном кронродовском стиле: «Пусть T — температура крокодила!», что вызвало возмущение у киношников, которые потребовали начать всё сначала. Дело в том, что кино смотрят и глухие люди, которые восстанавливают текст по губам!

Никита очень хорошо училась и естественно, что О. А. Олейник её рекомендовала в аспирантуру, куда Никита поступила в 1953 году.

Никита подготовила диссертацию в срок и защищала её в Стекловском институте. Я присутствовал при этой защите. После разных формальностей председатель сказал, что слово имеет диссертант Наталья Дмитриевна Введенская. Никита вышла к кафедре и начала со слов:

— Меня, на самом деле, зовут Никита.

После этого она рассказала о своей диссертации, и защита прошла очень успешно.

Партийное бюро не рекомендовало оставить её в Московском университете, и она приняла предложение поступить в Отделение прикладной математики АН СССР. Сперва Никита Дмитриевна продолжала заниматься завершением своей тематики из олейниковского семинара и написала несколько работ на эту тему.

Отделение прикладной математики в 40–50-е годы было призвано решать важнейшие государственные проблемы, связанные с космосом, атомной энергией, авиацией и прочим. Это требовало применения новейших вычислительных средств. В сороковые годы ещё не было специализации по вычислительной математике. Участие в формировании отделения прикладной математики принимал Иван Георгиевич Петровский. По его рекомендации было принято несколько людей, занимавшихся абстрактными областями математики, совершенно не связанными с вычислениями. Но уровень мехмата был настолько высок, что эти люди в очень короткий срок овладели новой специальностью и стали крупнейшими специалистами в этой области. Среди таких была Никита Дмитриевна Введенская.

Она стала вычислителем очень высокого класса. Достаточно назвать заглавия двух её работ «Расчёт пограничного слоя, возникающего при обтекании конуса под углом атаки» и «О решении уравнений пограничного слоя в окрестности критической точки». Обе работы посвящены актуальнейшим проблемам, связанным со сверхзвуковой авиацией. Н. Д. Введенская продолжала работать в области гидро- и аэродинамики, решая проблемы обтекания, свыше пятнадцати лет, даже перейдя на другое место работы.

В 1964 году Никита Дмитриевна перешла на работу в Институт проблем передачи информации имени А. А. Харкевича. Здесь она проработала почти 60 лет, до последних дней своей жизни. Научная деятельность Н. Д. Введенской в этот период была посвящена задачам передачи сообщений по каналам связи, вопросам маршрутизации сообщений в сетях и проблемам случайного множественного доступа. Таким образом, истоком для трёх направлений её творчества были такие выдающиеся учёные, как И. Г. Петровский, М. В. Келдыш и А. Н. Кол-

могоров. А непосредственными научными руководителями Никиты Дмитриевны были ученица Петровского О. А. Олейник, последователь Келдыша — К. И. Бабенко и ученик Колмогорова в области теории вероятностей и теории информации — Р. Л. Добрушин.

Хотел бы отметить работу Н. Д. Введенской совместно с С. Г. Гиндикиным «Формула Пуассона для преобразования Радона и численный алгоритм реконструкции изображения» 1984 года. Это одна из первых работ, которые математическим образом описывают процесс получения изображения в компьютерной рентгеновской томографии, что было исключительно актуальным именно в те годы.

В результате многолетней научной деятельности ею были получены замечательные результаты, которые легли в основу её докторской диссертации.

Степень доктора физико-математических наук была присуждена Н. Д. Введенской в 2001 году.

Последняя публикация Никиты Дмитриевны Введенской датируется 2020 годом, когда ей исполнилось 90 лет.

Огромное место в жизни Никиты Дмитриевны Введенской занимали её товарищеские и дружеские связи. Можно сказать даже больше: она сыграла исключительную роль в объединении целого поколения выдающихся представителей науки и культуры. Диапазон лет рождения её близких друзей простирается от начала 20-х до 40-х годов XX века. Среди особо близких друзей из москвичей, которых она постоянно собирала, были А. М. Яглом, М. Л. Лидов, В. В. Иванов, Р. Л. Добрушин, В. А. Успенский, Ф. А. Березин, Р. А. Минлос, С. П. Маркиш, В. М. Алексеев, Л. Р. Волевич, А. А. Зализняк, Е. В. Падучева, Б. Т. Поляк, В. И. Арнольд, А. Д. Иоффе, Л. А. Бассалыго. Иногородние и иностранные друзья — А. М. Вершик, Луи Ниренберг, Джейкоб Шварц, И. А. Ибрагимов, Л. Д. Фадеев и другие, — когда прибывали в Москву, тоже любили посещать Никитин дом. В особо торжественных случаях Никита созывала несколько десятков друзей и подруг.

Собрания у Никиты не были салоном в духе описанного Толстым салона Анны Павловны Шерер. Никита тщательно готовилась к собраниям: ходила на рынок, закупала овощные и мясные продукты, из которых затем готовила закуски и прекрасные горячие блюда (вторые). Она закупала вина, но и гости приносили с собой горячительные напитки, которых всегда было достаточно. Никита была великолепной хозяйкой и не только прекрасно готовила, но и замечательно настаивала водку. Приходившие подруги всегда предлагали ей помощь по хозяйству, но она очень резко это обрывала. Она сама накрывала на стол,

сама подавала еду — и начиналось пиршество. Среди гостей Никиты были люди самых разнообразных профессий: математики, лингвисты, физики, историки, филологи, искусствоведы и все они были необычайно содержательные и глубокие люди. Начинались обсуждения самых разнообразных вопросов — науки, поэзии, литературных новинок, политики, положения в мире, воспоминаний. Особо притягательным во всём этом было ощущение свободы, которое было столь ценным.

Подобные встречи у Никиты были несравненны: ничего сходного никто больше устроить не мог.

Никита была верным и преданным другом. Она постоянно обзванивала всех, старалась придти на помощь в любую трудную минуту, одарить каждого советом и рассказом о каком-то ярком событии. Последний день рождения Никиты, на котором собрались её друзья, произошёл 9 октября 2021 года. Собралось около десяти человек. Это был единственный раз, когда Никита уже не имела сил приготовить ужин. Но всё остальное было как прежде — обсуждения, споры, новости. В последние месяцы её жизни особую роль в организации помощи ей играл Борис Теодорович Поляк.

Никита была очень спортивным и активным человеком. С ранних студенческих лет она стала ходить в походы, сначала по Подмосковью, а потом на лыжах и на байдарках всё дальше и дальше от Москвы. Каждое лето, начиная с середины 60-х годов, она ходила в большие походы в горы, а с 70-х годов каждую субботу зимой она стала совершать очень длительные лыжные прогулки с какими-нибудь новыми друзьями. Эти прогулки продолжались с раннего утра до позднего вечера, и за это время она преодолевала что-то около 60–70 километров. Такие длительные прогулки продолжались до тех пор, пока она почти не лишилась зрения.

Никита Дмитриевна была человеком с большим общественным темпераментом. Её неизменно интересовала судьба университета, в котором она училась, отделения прикладной математики, где она обрела новую профессию вычислителя высокого уровня, Института проблем передачи информации, где она провела большую часть своей творческой жизни.

Её очень глубоко волновала судьба нашей страны. Многие близкие люди Никиты Дмитриевны в 80–90-е годы покинули СССР и Россию. Для Никиты вопрос об эмиграции никогда не вставал. Вот её слова: «Что касается эмиграции, то, во-первых, у меня всегда была такая странная идея, что надо оставаться в стране, потому что, может быть, придётся ей помочь. Вот такое чувство патриотизма, что нужно

стоять за свою страну». Будучи независимым и прямым человеком, она выступала в защиту тех, над кем, с её точки зрения, совершалось нарушение прав человека. Она участвовала в демонстрациях, писала и подписывала протестные письма, всячески старалась поддержать отказников и помочь им.

Всей своей жизнью Никита показала, что она любила свою страну и всё время жила с надеждой, что произойдут изменения к лучшему.

Светлая память о Никите Дмитриевне Введенской навсегда сохранится в сердцах тех людей, которые были с ней связаны.

Владимир Михайлович Тихомиров, мехмат МГУ
vmtikh@gmail.com

Создание С. И. Шварцбурдом московской математической школы 425

А. Г. Кушниренко

Настоящие воспоминания написаны мной в ответ на приведённое ниже письмо моего ученика Миши Шифрина, которого я в середине 60-х годов прошлого века учил математике в организованной А. С. Кронродом московской школе № 7 под руководством Н. Н. Константинова вместе с М. Л. Гервером и А. Д. Вентцелем, а также, в разные полугодия, с Ильёй Вахутинским и Ирой Кристи. С согласия Миши, привожу его письмо и свой ответ. Ниже все цитаты выделяются курсивом. Автор благодарен свой однокласснице Жене Гохват, которая ознакомилась с данным текстом и сделала ряд существенных замечаний.

Четверг, 27 мая 2021, 12:48 + 03:00 от Михаил Шифрин

Толя, привет!

У меня к тебе появился исторический вопрос: мои однокурсники, учившиеся в 444 школе, запутались в её ранней истории. Может быть ты, как один из первых выпускников математических классов, помнишь, когда появились матклассы 444 школы? Было ли это вначале в 425-й? Когда перебрались в 444-ю? Когда и в какой класс ты поступал, когда закончил? Действительно ли ты учился на год раньше, чем Ося Бернштейн и Саша Геронимус? В общем, всё, что касается ранней истории.

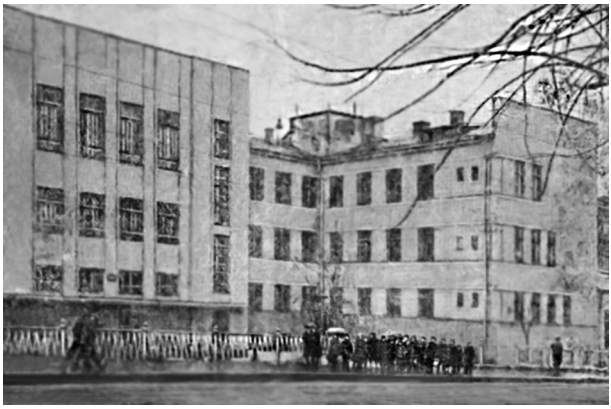
Всего хорошего, Миша

Дорогой Миша!

Спасибо за повод погрузиться в приятные воспоминания. Школы 425 и 444 занимают важное место в жизни трёх поколений нашей семьи. Я поступил в «математический» класс 425 школы в 1959 году и окончил её в 1962. В том же 1962 году школа 425 (её математические классы) переехала в школу 444. И в этой 444 школе учился, а затем и работал десять лет учителем информатики мой сын Юрий Кушниренко. Наконец, 11 лет проучилась в 444 школе моя внучка Анна Кушниренко, окончив её в сложный 2020 год.

С течением времени предыстория школы 444 забывается. По сути, это неизбежно и даже правильно, но для выпускников первого математического класса Шварцбурда 1962 года число 425 такое же родное, как для всех остальных выпускников число 444, так что я в меру сил пытаюсь продлить жизнь воспоминаниям о числе 425.

Первый математический класс в СССР[1)] замечательный советский педагог Семён Исаакович Шварцбурд открыл 8 сентября 1959 года в школе 425 города Москвы. Семён Исаакович удачно оседлал и использовал веяния своего времени. Та форма обучения, которую он с единомышленниками организовал в 1959 году, вначале формально называлось не математическим классом, а классом 11-летнего производственного политехнического обучения (см. Приложение). Еди-



Школа 425: выпускной математический класс 1962 года

[1)] В статье: *Константинов Н. Н.*, *Семёнов А. Л.* Результативное образование в математической школе // Чебышевский сборник, 2021, т. 22, вып. 1, с. 413–446, утверждается, что в 1959 году параллельно с нашим классом в Москве были открыты ещё два: во второй школе и в седьмой школе. Однако помню, что Семён Исаакович в 9 классе неоднократно подбадривал нас тем, что мы первопроходцы.

Вычислительный центр АН СССР

номышленниками были учитель математики, методист и директор школы В. Д. Головина и ряд известных московских педагогов и математиков: В. Г. Ашкинузе, Н. Я. Виленкин и др. Набор в два 9-х класса производственного обучения в школе 425 на Большой Семёновской улице прошёл в первую неделю сентября 1959.

Для прохождения производственного обучения один класс был прикреплён к заводу «Салют». Названием специальности было что-то вроде «станочник металлорежущих станков», а второй класс был прикреплён к Вычислительному центру Академии наук СССР, название специальности было что-то вроде «Оператор электронных вычислительных машин».

В «станочном» классе в основном были местные ребята, живущие поблизости от школы, а в «ЭВМ-ном» были ученики, живущие хоть и не близко к школе, но всё-таки набранные из одного Сталинского района г. Москвы (с 1961 года — Первомайского района). Весь набор в наш класс прошёл в спешке и суете. Лично я, как обычно, пошёл 1 сентября в свой 9 класс в 695 школе, и вдруг, 5 сентября, на урок математики пришёл завуч и объявил, что начался такой вот интересный набор в «ЭВМ-ный» класс. Объявили всем, но меня попросили позже зайти к завучу и посоветовали подумать. Видимо, это было связано с тем, что у меня на московской олимпиаде по физике была премия за 8 класс. Решение нужно было принять практически за день,

что я и сделал, и 8 сентября 1959 мы с моим одноклассником по 695 школе Вадиком Флегонтовым уже пришли на первый урок математики у Семёна Исааковича в 425 школе. В наш класс набрали 18 девушек и 10 юношей. В отличие от класса следующего года, набранного более тщательно, он не был математическим по настрою. Почти ни для кого в классе математика не была мечтой и целью жизни. Большинство учеников класса осознавало, что нам выпал «счастливый билет», нас безо всяких испытаний «записали» в элитное мероприятие, открылась возможность заниматься по расширенной в сторону ЭВМ программе. И мы добросовестно и с удовольствием этим занимались, особо не жертвуя никакими другими интересными сторонами жизни. Например, я продолжил заниматься радиосвязью на УКВ на коллективной радиостанции RA3KPT и в 9 классе заработал первый разряд. До весны выпускного 1962 года я смутно думал, что стану радиоинженером, этого не случилось в результате моего знакомства с Н. Н. Константиновым, описанного в короткой заметке в 29 выпуске третьей серии «Математического Просвещения» (М.: МЦНМО, 2022, с. 107–110).

По каким официальным и неофициальным правилам проходил набор в следующий за нами класс, я не знаю. Но по уровню владения школьной математикой и уровню интереса к математике новый набор был гораздо более «математическим», чем наш. В новом классе было много детей известных родителей, много ребят из олимпиадно-кружкового круга. Были Ося Бернштейн, Лида Гончарова, Волик Фишман и Вика Осипова, которые занимались топологией с Митей Фуксом, был Саша Геронимус, внук известного педагога-геометра. Был Андрей Бюшгенс, сын известного учёного-механика. В новом классе было много ярких личностей, с которыми судьба сталкивала меня десятки лет после окончания школы: Лёня Литвачук, долгие годы проработавший учителем в 444 школе, Миша Кулагин, с которым наши контакты начались на радиолюбительской почве и продолжились в конце XX – начале XXI века в ходе совместных работ МГУ и РАН по информатике.

Однако, как наш несколько насторожившийся класс понял в первый месяц занятий в 10 классе, с появлением нового «математического» 9 класса нас «не разлюбили», Семён Исаакович с одинаковым удовольствием работал и с нашим классом, и с более математически сильным следующим. Его целью была отработка общей системы математических классов. Эта цель была достигнута:

В 1961 году Министерством просвещения РСФСР были утверждены квалификационная характеристика, учебный план, программы по общему курсу математики, специальным учебным предметам. Основой

для разработки послужил опыт 425 школы (см. https://schv444.mskobr.ru/obwie_svedeniya/history*).*

Трудно сказать, насколько Семён Исаакович был доволен результатами класса-первенца, набранного впопыхах. С точки зрения «производственного обучения» наш выпуск смотрелся отлично: по окончании школы большинство учеников нашего класса поступило в технические вузы, у многих полученная профессия и первое место работы в академических институтах, различных ВЦ и НИИ были связаны с программированием и ЭВМ. На мехмат МГУ нас поступило пятеро: Женя Гохват, Вадик Флегонтов, Володя Ткаченко, Лариса Кувшинова и я. Насколько мне известно, успешную классическую научную карьеру сделал один выпускник нашего класса, Юра Тюпкин. Себя я считаю сделавшим половину классической карьеры. Юра Тюпкин всю жизнь занимался математической физикой и геофизикой и стал доктором физ.-мат. наук. Лично я защитил кандидатскую диссертацию под руководством В. И. Арнольда и стал профессиональным математиком: доказал одну известную теорему про многогранники Ньютона и придумал вошедший в математический обиход термин «малочлен» (англ. fewnomial). Однако в 1979 учёный совет мехмата предложил мне прочесть курс программирования на механико-математическом факультете МГУ, я увлёкся, и далее много занимался вопросами практического программирования и методики его преподавания в университетах, школах и, в последние годы, в детских садах.

Выпускная фотография математического класса школы 425 — май 1962 года. Семён Исаакович Шварцбурд (в центре) и Клим Владимирович Ким (в первом ряду)

Учили нас по всем предметам очень хорошо. Была замечательная, хотя и с непростым характером, учительница литературы Рина Зельмановна Окунь. На многих уроках она устраивала дискуссии по философским и морально-этическим вопросам, заводила весь класс и доводила градус дискуссии до уровня современных постановочных ток-шоу. Была замечательная учительница химии, был интересный учитель физики, который занимался с нами по трёхтомнику Ландсберга. Была отличная учительница немецкого языка Инесса Ивановна Бойко, я с ней поддерживаю контакты до сегодняшнего дня (май 2021). Насколько я помню, Иннеса Ивановна сыграла важную роль в поиске и выборе нового «гнезда» для математических классов в Сталинском районе при «отбирании здания» у 425 школы в 1962 году.

Теперь о спецпредметах.

У нас отдельно была школьная математика, с элементами анализа, типа пределов, графиков и производных, которую замечательно вёл Семён Исаакович, и отдельно производственное обучение, которое включало а) производственную практику в ВЦ АН СССР и б) теорию, как бы мы сегодня сказали, вычислительной математики и электронно-вычислительной техники, которую вёл блестящий молодой сотрудник ВЦ АН СССР Клим Владимирович Ким. Мы все к нему за годы учёбы очень привязались (см. `https://vk.com/@three444-istorii-o-shkole`).

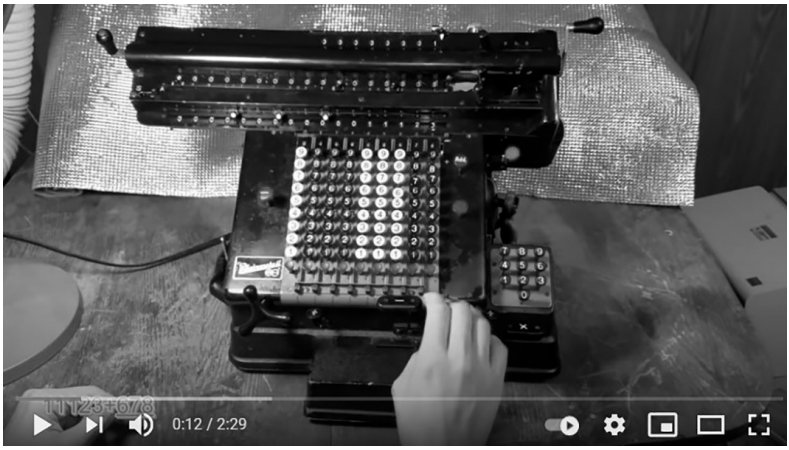
Школьная математика. Семён Исаакович вёл её замечательно, одинаково интересно и понятно и для самых слабых и для самых сильных учеников. Уроки были интересны и по содержанию и по неповторимой манере эмоционально богатой подачи материала. Подобно И. М. Гельфанду, он любил подробно объяснять самые простые вещи, интересовался жизнью учеников и помогал ученикам советами в самых разных ситуациях, а на уроках иногда рассказывал случаи из жизни.

Производственная практика в ВЦ АН СССР проходила в 2 этапа.

Этап 1. 1959–60 уч. год. Арифмометры и «расчётные схемы»

В первый год обучения практика шла на электромеханических арифмометрах «Рейнметалл».

Это оказалось для нашего класса некоторым разочарованием. Мы ожидали практики на ЭВМ в огромных машинных залах, которые мы видели по телевизору.



Но нам сказали «потерпите год», и действительно, в 10 классе практика начала проходить на ЭВМ, об устройстве которой нам рассказали в конце 9 класса.

Обучение на арифмометрах было, несмотря на наше некоторое первоначальное разочарование, весьма поучительным. Именно на этом этапе мы практически считали значения многочленов по схеме Горнера, исключали по Гауссу и практически сравнивали скорость схо-

Ученик 11 математического класса 425 школы на практике в ВЦ АН СССР. Машинный зал ЭВМ БЭСМ-2. 1962

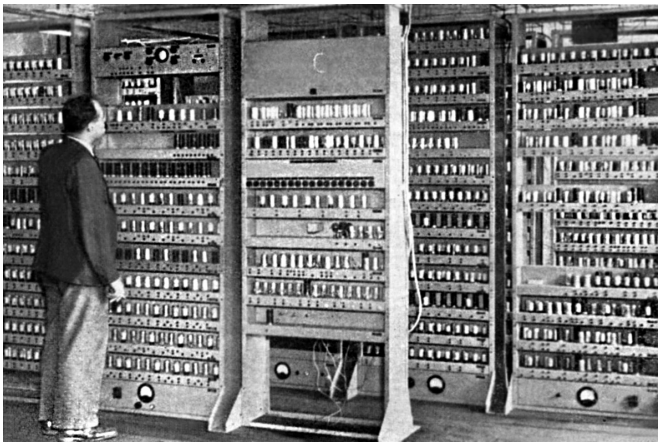
димости простой итерации и итерации Зейделя при решении системы до десятка линейных уравнений. Важно ещё, что практика проходила в огромном зале с 30 арифмометрами и мы видели, как десятки взрослых с утра до ночи считают на арифмометрах, не укладываются в сроки, работают сверхурочно, и мы видели, что эти вычисления есть часть какого-то большого важного дела, кому-то срочно нужны.

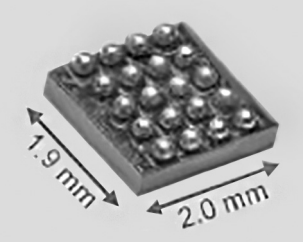
Счёт вёлся с записью промежуточных результатов в большие разграфлённые альбомы. Кажется, они называлось «расчётные схемы». Во многих случаях в схеме предусматривались подсчёты контрольных сумм, что позволяло увидеть некоторые свои ошибки на ходу, а не в ходе сравнения с дублирующим вариантом. Все ручные подсчёты дублировались. А результат, проверенный дублированием, использовался не для производственных целей, а для контроля компьютерной программы, которая затем и проводила производственные вычисления. В 1959 году программисты ещё не решались, а начальство ещё не разрешало доверять результатам работы программы, правильность работы которой не была подтверждена ручным счётом контрольного примера. Итак, хотя весь 1959–1960 учебный год практика у нас была на арифмометрах, но это не было упражнением в нажимании клавиш, математическое содержание вычислений излагалось на теоретических занятиях.

Этап 2. 1960–1962 гг. БЭСМ-2

Придя в ВЦ АН СССР на Вавилова, дом 40, в 1959 году, мы узнали, что в ВЦ установлены две ЭВМ. Из вестибюля главного входа отходили два коридора первого этажа. Левый вёл к секретной ЭВМ «Стрела», на входе в этот коридор 24 часа в сутки стоял часовой с расчехлённым оружием. Правый коридор вёл к нашей несекретной БЭСМ-2. Не могу удержаться и привожу рядом, как иллюстрацию быстротекучести времени, два снимка: машинный зал нашей любимой БЭСМ-2 и снимок современного однокристального компьютера ARM Cortex-M0+, который при размерах 1,9 × 2,0 × 0,5 мм имеет на порядок большую оперативную память, на два порядка лучшее быстродействие и на 6 порядков меньшее энергопотребление, чем БЭСМ-2.

Разумеется, мы спрашивали у сотрудников ВЦ, что именно считается на этих ЭВМ, разумеется, нам никогда толком не отвечали, но ходила легенда, что «атомную бомбу можно считать на арифмометре, а ракету уже нельзя, нужна ЭВМ». Это было недалеко от истины, большинство применений ЭВМ тех времён были военные. Как я прочёл в Википедии при редактировании данных воспоминаний, «на ЭВМ





типа БЭСМ-2 рассчитывалась траектория полёта ракеты, которая доставила на Луну герб СССР» (см. https://ru.wikipedia.org/wiki/БЭСМ).

На производственной практике, начиная с 10 класса, каждому ученику выделялось время для работы на ЭВМ. Доставалось 1–2 раза в неделю по 5 минут. В выпускном классе я иногда выпрашивал 15 минут. Такое время давали только ночью. Скажем, 15 минут, начиная с половины третьего ночи. Туда едешь последним автобусом, обратно домой едешь первым автобусом и первым поездом метро. Иногда я ездил на велосипеде со своей Первомайской улицы, около 60 км туда и обратно.

Первые учебные задачи, которые мы считали, были традиционные. В 10 классе в верхнем ящике письменного стола у меня дома целый год пролежал — для показа гостям — узкий рулончик бумаги, на котором моя первая программа напечатала простые числа, меньшие 1000. Насколько я помню, в нашем классе на ЭВМ решались только учебные задачи. До подбора нашему классу посильных практических задач дело у наших учителей не дошло. Но несколько выпускных учебных задач в нашем классе были достаточно сложны. Например, в своей выпускной работе 11 класса я считал на компьютере потери в волноводе радиолокационной станции. Эту задачу мне нашла моя мама Евгения Ивановна Брагинцева, работавшая в Яузском радиотехническом институте на Большой Почтовой, бывший НИИ-20. Предварительный расчёт был сделан маминими сослуживцами на логарифмической линейке. Результаты этого расчёта мне не дали. Мне был дан для контроля результат для упрощённого волновода, для которого имелась

явная формула. С ним результаты моей программы совпали. Результат более сложного расчёта я передал маминым сослуживцам, получил для школы официальный отзыв, а для себя неофициальное сообщение: «Ваша программа подтвердила с точностью до первого знака результаты нашего расчёта на логарифмической линейке». Деталей я так и не узнал. Мне, выросшему в обстановке секретности тех времён, было ясно, что расспрашивать о деталях не следует. А вот в следующем за нами классе Клим Владимирович довёл несколько работ школьников до практических применений. Вот, что он об этом пишет:

В процессе практики некоторые ученики школы сделали великолепные программы для реальных заказчиков, как правило без особой моей помощи. Это означает, что это были очень способные дети! Одна программа была сделана по моей теме и для моих плановых заказчиков — это программа решения транспортной задачи. Её авторы Иосиф Бернштейн, ныне известный математик, Волик Фишман, Лида Гончарова и молодой человек по фамилии Геронимус.

Теоретическая часть производственного обучения

Это был достаточно глубокий трёхлетний курс вычислительной математики и вычислительного программирования.

Вычислительная математика. Всё, что касалось нелинейных задач, было одномерным — алгоритмы интерполяции, интегрирования, приближённого вычисления корня. Линейная алгебра была много-

мерная. Вычисление определителя, исключение по Гауссу, нахождение обратной матрицы, характеристический многочлен, приведение к диагональному виду (без разбора случаев кратных собственных чисел и без упоминания жордановой формы). Вершиной всего этого было доказательство двух достаточных условий сходимости метода простой итерации: через норму и через спектр (правда, только для вещественного спектра). В основном мы учились по конспектам уроков, подспорьем был замечательный учебник Б. П. Демидович, И. А. Марон, Основы вычислительной математики, Москва, 1960 год. Физматгиз.

Программирование. Отчётливо помню, как в один тёплый солнечный день мая 1960 года наш преподаватель Клим Владимирович, приехав на мотороллере на Большую Семёновскую со своей улицы Вавилова, предложил проголосовать: кто за то, чтобы следующий сдвоенный урок провести на свежем воздухе. Все согласились, мы пошли в ближайший к школе сквер и там, рисуя гвоздём на земляной дорожке, за полтора часа Клим Владимирович объяснил нам, девятиклассникам, архитектуру и систему команд трёхадресной ЭВМ БЭСМ-2. И даже успел написал программу суммирования массива.

За эти полтора часа, спасибо трёхадресной архитектуре, педагогическому мастерству Клима Владимировича и поднимающей настроение солнечной весенней погоде, все мы за час полностью ухватили основную идею ЭВМ и программирования. А дальше, начиная с 10 класса, была практика и мы программировали разные вычислительные алгоритмы. Регистров переадресации в архитектуре БЭСМ-2 ещё не было, команды приходилось модифицировать в процессе выполнения. Технология программирования была простая и надёжная, всё писалось в машинных числовых 8-ричных кодах на специально разграфлённых бланках мягким карандашом и при необходимости стиралось резинкой и корректировалось. На пульте ЭВМ БЭСМ-2 были 4 ряда тумблеров для задания адреса стартовой команды и трёх адресов для отладочных остановов: по адресу команды, по адресу чтения и по адресу записи. Тумблеры переключались туго. После 15-минутной ночной отладки болели подушечки больших пальцев.

Выпускной вечер в июне 1962 у нас прошёл ещё в здании 425 школы, а летом здание отобрали в пользу Московского автомеханического института и школе пришлось искать новое место. С 1 сентября 1962 занятия в математических классах продолжились в школе 444 по адресу: Нижняя Первомайская улица, дом 14. Именно по этому непривычному адресу и номеру школы наш выпуск 1962 года пришёл в 1963 году на вечер встречи.

Приложение

Закон «Об укреплении связи школы с жизнью и о дальнейшем развитии системы народного образования в СССР», принят 24 декабря 1958 г. (https://www.prlib.ru/history/619837)

Началом реформы образования 1958–1964 годов стала речь Хрущёва на XIII съезде ВЛКСМ в апреле 1958 года, в которой, в частности, говорилось об отрыве школы от жизни общества. Затем последовала записка Хрущёва в Президиум ЦК КПСС, в которой он описывает реформу более подробно и даёт уже более определённые рекомендации по перестройке школы. Затем предлагаемые меры приняли форму тезисов ЦК КПСС и СМ СССР «Об укреплении связи школы с жизнью» и далее — закона «Об укреплении связи школы с жизнью и о дальнейшем развитии системы народного образования в СССР» от 24 декабря 1958 года, где главной задачей среднего образования объявлялось преодоление отрыва школы от жизни, в связи с чем единая трудовая школа становилась политехнической.

Главной целью реформы была объявлена подготовка технически грамотных кадров для промышленности и сельского хозяйства. Вместо 7-летнего вводилось всеобщее обязательное 8-летнее образование. Переход на него был осуществлён к 1963 г. Полное среднее образование, срок которого был увеличен с 10 до 11 лет, предусматривалось осуществлять на основе соединения обучения с трудом в дневной или вечерней школе, либо в техникуме. Два дня в неделю школьники старших классов дневных школ должны были работать на предприятиях или в сельском хозяйстве. Выпускники средней школы наряду с аттестатом зрелости получали свидетельство о специальности. В 1966 году реформа была отменена.

Анатолий Георгиевич Кушниренко, МГУ, НИИСИ РАН
agk_@mail.ru

Алгебра и теория чисел

О работе А. Р. Исмаилова «Углы в плоскости над конечным простым полем»

А. Я. Канель-Белов

В работе с математически одарёнными школьниками превалирует решение задач. Олимпиады представляют собой соревнования по решению задач, летние конференции Турнира Городов, а также проектные смены в «Сириусе» являются переходной формой от олимпиад к научному творчеству. Вместе с тем математика не сводится к решению задач — важное значение имеет воспитание *теоретического мышления*. Теоретическое мышление необходимо и для решения задач, особенно трудных, в том числе и олимпиадных. И недостаток теоретического мышления сказывается не только на общей культуре, но и на самой олимпиадной подготовке.

В воспитании теоретического мышления одним из аспектов служит работа с *параллельными мирами*. Есть комплексные числа $a+bi$, $i^2=-1$ и тригонометрические функции, с ними связанные, есть *гиперболические числа* $a+bj$, $j^2=+1$ и гиперболические функции, с ними связанные. Есть скалярное произведение $x_1x_2+y_1y_2$, а есть и *псевдоскалярное* $x_1x_2-y_1y_2$. На сфере есть соответствие полюс-экватор, связанное со скалярным произведением: вектор, направленный из начала координат на полюс, перпендикулярен плоскости экватора. С псевдоскалярным произведением связан *поляритет* или *полярное соответствие*. Имеются аналогии между сферической и неевклидовой геометриями (неевклидова плоскость как сфера «мнимого радиуса»). Помимо мира веще-

ственных чисел, с которым связана обычная геометрия, есть p-адический мир, а также мир остатков по модулю p. Эта тема затронута в статье *Ковальджи А. К.*, *Канель-Белов А. Я.* «Занятия по математике — листки и диалог» («Математическое просвещение», сер. 3, вып. 19, М.: МЦНМО, 2015, с. 206–233). См. также *Яглом И. М.* «Принцип относительности Галилея и неевклидова геометрия», М.: Наука, 1969.

Примечательно, что идея «параллельных миров» и построения параллельной геометрии появилась у школьника. И она имеет методическое значение. Некоторые конструкции, например конструкция прямой, переносятся непосредственно. С понятием *угла*, однако, возникает проблема, поскольку, например, мультипликативная группа остатков по модулю p (или p^2) имеет порядок, взаимно простой с p, так что углы лежат в другом мире. Школьник пытается с этим разобраться, и определённые результаты в этом направлении у него есть, хотя отметим, что взаимосвязь между разными мирами до сих пор не вполне понята.

Алексей Яковлевич Канель-Белов, университет Бар-Илана (Израиль)
kanel@mccme.ru

Углы в плоскости над конечным простым полем

А. Р. Исмаилов*

С вещественными числами связана евклидова геометрия. Возникает вопрос: какая геометрия будет связана с остатками по простому модулю? В этой ситуации аналогом плоскости служит $\mathbb{Z}_p \times \mathbb{Z}_p$. Прямые можно определить как решения уравнения вида

$$ax + by + c \equiv 0 \pmod{p}.$$

Аналогично евклидову случаю, прямые могут быть параллельны и перпендикулярны. В классическом случае (плоскость $\mathbb{R}^2$) естественно определяется понятие угла между прямыми. В $\mathbb{Z}_p \times \mathbb{Z}_p$ возникает аналогичный вопрос: как ввести углы? Единичная окружность задаётся уравнением

$$x^2 + y^2 \equiv 1 \pmod{p}.$$

Оказывается, за множеством его решений скрывается структура, которая чем-то напоминает обычные углы. Можно даже определить синусы и косинусы. Однако что с этим дальше делать? Казалось бы, просто получается аналогичная тригонометрия.

Возьмём угол в 45°:

$$\sin\frac{\pi}{4} = \cos\frac{\pi}{4} = \frac{1}{\sqrt{2}}.$$

Если в нашей структуре углов по модулю p имеется аналог угла в 45 градусов, то $\sqrt{2}$ будет среди остатков по модулю p, и наоборот. Получается критерий того, будет ли число 2 квадратичным вычетом по модулю p.

Отсюда начинает раскрываться основная тема нашей статьи: как можно использовать структуру, возникающую в поле остатков $\mathbb{Z}_p$, чтобы получать факты, выходящие за рамки обычной тригонометрии?

* На момент написания статьи автор был учеником школы «Воробьёвы горы», г. Москва.

§ 1. Введение

Мы начнём с построения аналога обычных углов над полем $\mathbb{Z}_p$ и затем тригонометрических функций над $\mathbb{Z}_p$ (сами углы не будут принадлежать $\mathbb{Z}_p$). Проводя аналогию между тем, что происходит с обычными углами, и тем, что происходит с углами нового вида, мы докажем в § 4 ряд фактов: наличие $\sqrt{2}$, $\sqrt{3}$ по модулю p, несоизмеримость некоторых углов с 2π. В дальнейшем мы сможем показать, что существует бесконечно много простых чисел вида $kn-1$, используя аналог многочлена деления круга (теорема 3, следствие 1).

§ 2. Углы

Пусть $p>2$ — простое число. В этом разделе мы будем работать в поле $\mathbb{Z}_p$. Чтобы ввести углы, рассмотрим решения уравнения $x^2+y^2=1$, которые образуют единичную окружность.

Случай $p=4n+1$. В этом случае имеются два квадратных корня из -1, которые мы обозначим j и $-j$. Тогда

$$x^2+y^2=1 \quad \Leftrightarrow \quad (x+jy)(x-jy)=1.$$

Заметим, что существует биекция между упорядоченными парами $(x,y)\in\mathbb{Z}_p\times\mathbb{Z}_p$ и упорядоченными парами $(a,b)\in\mathbb{Z}_p\times\mathbb{Z}_p$, где (x,y) сопоставляется точке $(a,b)=(x+jy,x-jy)$. Действительно, (x,y) восстанавливается по (a,b) как $\left(\frac{a+b}{2},\frac{a-b}{2j}\right)$. Назовём последнее выражение прообразом (a,b). Заключаем, что пары (x,y), являющиеся решениями уравнения $x^2+y^2=1$, биективно соответствуют парам (a,b), у которых $ab=1$, или, другими словами, парам вида $(a,1/a)$ при $a\neq 0$. Поэтому уравнение $x^2+y^2=1$ имеет ровно $p-1$ решение.

Две пары (a_1,b_1) и (a_2,b_2) можно поэлементно перемножить:

$$(a_1,b_1)\cdot(a_2,b_2)=(a_1a_2,b_1b_2).$$

Такое произведение соответствует «комплексному» умножению их прообразов (x_1,y_1) и (x_2,y_2) соответственно:

$$(x_1,y_1)\cdot(x_2,y_2)=(x_1x_2-y_1y_2,x_1y_2+x_2y_1),$$

результатом которого будет прообраз пары (a_1a_2,b_1b_2). Последнее утверждение следует из тождеств

$$a_1a_2=(x_1+jy_1)(x_2+jy_2),b_1b_2=(x_1-jy_1)(x_2-jy_2).$$

Эти равенства можно переписать как

$$a_1a_2 = (x_1x_2 - y_1y_2) + j(x_1y_2 + x_2y_1),$$
$$b_1b_2 = (x_1x_2 - y_1y_2) - j(x_1y_2 + x_2y_1).$$

При рассмотрении образов, т. е. пар (a, b), под умножением будем понимать поэлементное умножение. При рассмотрении прообразов, т. е. пар (x, y), под умножением будем подразумевать «комплексное» умножение. Назовём $(x, -y)$ парой, сопряжённой паре (x, y); если образ первой — это (a, b), то образом второй будет (b, a).

Все ненулевые пары (a, b), где $a \neq 0$ и $b \neq 0$, образуют группу по умножению. Пары (a, b) с $ab = 1$ образуют её подгруппу; поскольку они имеют вид $(a, 1/a)$, подгруппа изоморфна мультипликативной группе $(\mathbb{Z}_p)^*$, которая, в свою очередь, изоморфна циклической группе C_{p-1}, т. е. группе $(\mathbb{Z}_{p-1}, +)$ по сложению. Тогда решения (x, y) уравнения $x^2 + y^2 = 1$ образуют группу по «комплексному» умножению, изоморфную $\mathbb{Z}_{p-1}$.

Случай $p = 4n + 3$. Многочлен $x^2 + 1$ неприводим над полем $\mathbb{Z}_p$. Его полем разложения является $\mathbb{Z}_p(i)$, где через i мы обозначаем корень из поля разложения (другим корнем будет $-i$). Зададим сопряжение как операцию, сопоставляющую элементу $z = x + iy \in \mathbb{Z}_p(i)$ элемент $\bar{z} = x - iy$, где $x, y \in \mathbb{Z}_p$. Сопряжение является автоморфизмом поля $\mathbb{Z}_p(i)$. Пусть норма элемента z имеет вид

$$N(z) = z\bar{z} = x^2 + y^2 \in \mathbb{Z}_p.$$

У нас $p \equiv 3 \pmod 4$, и по теореме Жирара $N(z) = 0 \Leftrightarrow z = 0$. Также $N(z_1z_2) = N(z_1)N(z_2)$. Следовательно, N — это гомоморфизм из группы $\mathbb{Z}_p(i)^*$ в группу $\mathbb{Z}_p^*$. Мощность множества $A = \{x^2 \mid x \in \mathbb{Z}_p\}$ равна $(p+1)/2$. По принципу Дирихле множество $A + A$ содержит все остатки по модулю p: для любого $r \in \mathbb{Z}_p$ множество $r - A$ должно иметь хотя бы один общий элемент с A. Образ отображения N — это множество $\mathrm{Im}(N) = \mathbb{Z}_p^*$. Ядром отображения N является множество $\ker(N) = \{z \mid N(z) = 1\}$. Из изоморфизма $\mathrm{Im}(N) \cong \mathbb{Z}_p(i)^*/\ker(N)$ (первая теорема об изоморфизме) следует равенство

$$|\ker(N)| = |\mathbb{Z}_p(i)^*| : |\mathrm{Im}(N)| = |\mathbb{Z}_p(i) \setminus \{0\}| : |\mathbb{Z}_p^*| = \frac{p^2 - 1}{p - 1} = p + 1.$$

Так как ядро отображения N — это подгруппа из $p + 1$ элемента в группе $\mathbb{Z}_p(i)^*$, согласно теореме Лагранжа получаем $z^{p+1} = 1$ для всякого $z \in N$. Однако многочлен $z^{p+1} - 1$ имеет не более $p + 1$ корней, поэтому

$$N(z) = 1 \quad \Leftrightarrow \quad z^{p+1} = 1.$$

Следовательно, имеет место изоморфизм $\ker(N) \cong \mathbb{Z}_{p+1}$, где $\mathbb{Z}_{p+1}$ понимается как группа по сложению.

Количество решений уравнения $N(z) = l$ равно $p+1$ при $l \in \mathbb{Z}_p \setminus \{0\}$, так как N является гомоморфизмом из $\mathbb{Z}_p(i)^*$ в $\mathbb{Z}_p^*$ с образом $\mathbb{Z}_p \setminus \{0\}$ и мощностью ядра $|\ker(N)| = p+1$. Поэтому существует всего $2(p+1)$ чисел z с нормой $N(z) = \pm 1$. Они тоже образуют подгруппу в $\mathbb{Z}_p(i)^*$. Это группа по умножению, изоморфная группе $\mathbb{Z}_{2(p+1)}$ по сложению.

Вводим углы. С этого момента выражение $p \pm 1$ будет совмещать оба случая: в случае $p = 4n+1$ будет подразумеваться число $p-1$, а в случае $p = 4n+3$ — число $p+1$. В обоих случаях изоморфизм, установленный между $\mathbb{Z}_{p\pm 1}$ и группой решений уравнения $x^2 + y^2 = 1$, сопоставляет остаткам по модулю $p \pm 1$ решения уравнения $x^2 + y^2 = 1$. Решение $(1, 0)$ соответствует остатку 0. Решению $(-1, 0)$ соответствует $(p \pm 1)/2$, так как это элементы порядка 2 в своих группах. Паре решений $(0, 1)$ и $(0, -1)$ соответствует либо $(p \pm 1)/4$, $-(p \pm 1)/4$, либо $-(p \pm 1)/4$, $(p \pm 1)/4$, так как это элементы порядка 4. Заметим, что мы можем заменить наш изоморфизм на другой так, что если остатку r соответствует какое-то решение $x^2 + y^2 = 1$ при исходном изоморфизме, то остатку $-r$ соответствует это же решение при новом изоморфизме. Поэтому можно выбрать изоморфизм, который отображает $(p \pm 1)/4$ в $(0, 1)$ и $-(p \pm 1)/4$ в $(0, -1)$. Итак, определим *негеометрические углы* как остатки по модулю $\mathbb{Z}_{p\pm 1}$, причём этим остаткам в результате некоторого изоморфизма, удовлетворяющего нашим условиям (отображающего $(p \pm 1)/4$ в $(0, 1)$ и $-(p \pm 1)/4$ в $(0, -1)$), будут сопоставляться решения уравнения $x^2 + y^2 = 1$.

В случае $p = 4n+3$ мы можем дополнительно ввести то, что здесь будет называться *геометрическими углами*. Подгруппа по умножению, состоящая из чисел z с нормой $N(z) = \pm 1$, изоморфна группе $\mathbb{Z}_{2(p+1)}$ по сложению, из чего следует, что её элементы являются решениями уравнения $z^{2(p+1)} = 1$. Заметим, что верно равенство $N(z^2) = N(z)^2 = (\pm 1)^2 = 1$, поэтому чётные остатки являются прообразами чисел с нормой 1. Но тогда нечётные остатки являются прообразами элементов с нормой -1. Рассуждая аналогично, придём к тому, что решение $(1, 0)$ уравнения $x^2 + y^2 = \pm 1$ соответствует нулевому остатку, а решение $(-1, 0)$ — остатку $p+1$. Как и в предыдущем случае, можно считать, что остатки $(p+1)/2$ и $-(p+1)/2$ сопоставлены решениям $(0, 1)$ и $(0, -1)$ соответственно. Итак, определим геометрические углы как остатки по модулю $2(p+1)$, причём этим остаткам при некотором изоморфизме, удовлетворяющем нашим условиям (отображающем

$(p+1)/2$ в $(0,1)$ и $-(p+1)/2$ в $(0,-1)$), будут сопоставляться решения уравнения $x^2+y^2=\pm 1$.

§ 3. Модулярные синусы и косинусы

Теперь введём синус и косинус. Как для геометрических, так и для негеометрических углов определим косинус угла как x, а синус угла как y из сопоставляемой этому углу пары (x,y). Обозначим их через $\cos_p$ и $\sin_p$ соответственно. Для негеометрических углов получим набор значений:

α	0	$\frac{p\pm 1}{4}$	$\frac{p\pm 1}{2}$	$3\frac{p\pm 1}{4}$
$\sin_p \alpha$	0	1	0	-1
$\cos_p \alpha$	1	0	-1	0

Остатки α и $-\alpha$ соответствуют паре взаимно обратных элементов из группы решений уравнения $x^2+y^2=1$, но тогда они сопряжены друг с другом, так как в обоих случаях произведение элемента группы решений $x^2+y^2=1$ на его сопряжённый даёт единичный элемент. Поэтому $\cos_p \alpha = \cos_p(-\alpha)$ и $\sin_p(-\alpha) = -\sin_p \alpha$. Сумма углов α и β как остатков соответствует умножению соответствующих элементов группы решений, но тогда, рассмотрев формулу для этого умножения, мы получим формулы

$$\cos_p(\alpha+\beta) = \cos_p \alpha \cos_p \beta - \sin_p \alpha \sin_p \beta,$$
$$\sin_p(\alpha+\beta) = \sin_p \alpha \cos_p \beta + \sin_p \beta \cos_p \alpha.$$

Если мы заменим β на $-\beta$, то получим формулы синуса и косинуса разности. Прибавление $(p\pm 1)/2$ к углу соответствует умножению всех решений на элемент $(-1,0)$:

$$\cos_p\Big(\alpha+\frac{p\pm 1}{2}\Big) = -\cos_p \alpha, \quad \sin_p\Big(\alpha+\frac{p\pm 1}{2}\Big) = -\sin_p \alpha.$$

Если угол α соответствует паре (x,y), то угол $-\alpha$ соответствует паре $(x,-y)$. Прибавление числа $(p\pm 1)/4$ к углу $-\alpha$ сопоставляется умножению решения, которое соответствует этому углу, на $(0,1)$. Поэтому

$$\cos_p\Big(\frac{p\pm 1}{4}-\alpha\Big) = \sin_p \alpha \quad \text{и} \quad \sin_p\Big(\frac{p\pm 1}{4}-\alpha\Big) = \cos_p \alpha.$$

Синус равен 0 тогда и только тогда, когда косинус равен ± 1, т. е.

$$\sin_p \alpha = 0 \quad \Leftrightarrow \quad \alpha \in \Big\{0, \frac{p\pm 1}{2}\Big\}.$$

Аналогично

$$\cos_p \alpha = 0 \quad \Leftrightarrow \quad \alpha \in \left\{\frac{p\pm 1}{4}, -\frac{p\pm 1}{4}\right\}.$$

Используя формулы суммы углов и равенство $\sin_p^2 \alpha + \cos_p^2 \alpha = 1$, можно получить стандартные тригонометрические тождества:

$$\sin_p 2\alpha = 2\sin_p \alpha \cos_p \alpha, \qquad \cos_p 2\alpha = \cos_p^2 \alpha - \sin_p^2 \alpha,$$
$$\sin_p 3\alpha = -4\sin_p^3 \alpha + 3\sin_p \alpha, \quad \cos_p 3\alpha = 4\cos_p^3 \alpha - 3\cos_p \alpha.$$

Геометрические углы. Пусть $p \equiv 3 \pmod 4$. В отличие от негеометрических углов, мы позволяем выражению $x^2 + y^2$ быть равным не только 1, но и -1 (подробнее на с. 70). Поэтому $z\bar{z} = \pm 1$. Тогда

$$\cos_p(-\alpha) = \pm\cos_p \alpha \quad \text{и} \quad \sin_p(-\alpha) = \mp\sin_p \alpha,$$

где знак зависит от того, на что надо умножить z, чтобы получить 1: на $\bar{z}$ или на $-\bar{z}$. Формулы синуса и косинуса суммы углов не меняются. Рассмотрим синус разности двух углов:

$$\sin_p(\alpha - \beta) = \sin_p \alpha \cos_p(-\beta) + \cos_p \alpha \sin_p(-\beta).$$

Мы уже знаем, что $1/z = \pm\bar{z}$. Поэтому при умножении угла на -1 противоположное значение примет либо только косинус, либо только синус (значения синуса в первом и косинуса во втором случае останутся неизменными). Следовательно, верна формула

$$\sin_p(\alpha - \beta) = \pm(\sin_p \alpha \cos_p \beta - \sin_p \beta \cos_p \alpha).$$

Аналогично в случае косинуса разности углов имеем

$$\cos_p(\alpha - \beta) = \sin_p \alpha \sin_p(-\beta) - \cos_p \alpha \cos_p(-\beta) =$$
$$= \pm(\cos_p \alpha \cos_p \beta + \sin_p \alpha \sin_p \beta).$$

Мы также знаем следующие значения косинуса и синуса:

α	0	$\frac{p+1}{2}$	$p+1$	$3\frac{p+1}{2}$
$\sin_p \alpha$	0	1	0	-1
$\cos_p \alpha$	1	0	-1	0

Следовательно,

$$\sin_p(\alpha + (p+1)) = -\sin_p \alpha \quad \text{и} \quad \cos_p(\alpha + (p+1)) = -\cos_p \alpha.$$

Также

$$\sin_p\left(\alpha + \frac{p+1}{2}\right) = \cos_p \alpha \quad \text{и} \quad \cos_p\left(\alpha + \frac{p+1}{2}\right) = -\sin_p \alpha.$$

Синус равен нулю при $\cos_p^2 \alpha = \pm 1$. Так как число -1 не является квадратичным вычетом по модулю p, мы заключаем, что $\cos_p \alpha = \pm 1$, и тогда $\sin_p \alpha = 0 \Leftrightarrow \alpha \in \{0, p+1\}$. Аналогичным образом для косинуса мы выводим следующее:

$$\cos_p \alpha = 0 \quad \Leftrightarrow \quad \alpha \in \left\{\frac{p+1}{2}, -\frac{p+1}{2}\right\}.$$

Геометрические и негеометрические углы представляют из себя объекты, которые мы будем называть углами по модулю p, хотя связанные с ними структуры, вообще говоря, отличаются от поля $\mathbb{Z}_p$.

§ 4. Некоторые приложения

Можно провести аналогию между обычными углами и углами по модулю p. Например, далее мы увидим, как с помощью аналогии между углами по модулю p и такими углами, как например $\pi/4$ и $\pi/3$, можно понять что-то про квадратичные вычеты. В этом разделе рассматриваются негеометрические углы. Покажем, как с их помощью можно получить некоторые известные факты.

Существование $\sqrt{2}$ по модулю p. Мы докажем, что число 2 — квадратичный вычет по простому модулю $p > 2$, если и только если $p \equiv \pm 1 \pmod 8$. Пусть $p \equiv \pm 1 \pmod 8$. Тогда существует остаток $(p \pm 1)/8$ по модулю $p \pm 1$. Рассмотрим его синус:

$$\sin_p\left(\frac{p \pm 1}{8}\right) = \sin_p\left(\frac{p \pm 1}{4} - \frac{p \pm 1}{8}\right) = \cos_p\left(\frac{p \pm 1}{8}\right).$$

Однако сумма квадратов синуса и косинуса равна

$$1 = \sin_p^2\left(\frac{p \pm 1}{8}\right) + \cos_p^2\left(\frac{p \pm 1}{8}\right) = 2\sin_p^2\left(\frac{p \pm 1}{8}\right) \quad \Rightarrow \quad 2 = \left(\sin_p \frac{p \pm 1}{8}\right)^{-2}.$$

Поэтому 2 будет квадратичным вычетом по модулю p.

Теперь предположим, что число 2 является квадратичным вычетом по модулю p. Через $\sqrt{2}$ обозначим один из корней многочлена $x^2 - 2$, который мы рассматриваем над полем $\mathbb{Z}_p$. Так как пара $(1/\sqrt{2}, 1/\sqrt{2})$ удовлетворяет уравнению $x^2 + y^2 = 1$, найдётся такой угол $\alpha \in \mathbb{Z}_{p\pm 1}$, что $\cos_p \alpha = \sin_p \alpha = 1/\sqrt{2}$. Тогда

$$\cos_p 2\alpha = \cos_p^2 \alpha - \sin_p^2 \alpha = 0 \quad \Rightarrow \quad 2\alpha \equiv \pm\frac{p \pm 1}{4} \pmod{p \pm 1}.$$

Отсюда следует, что

$$2 \mid \frac{p \pm 1}{4} \quad \Rightarrow \quad p \equiv \pm 1 \pmod 8.$$

Существование $\sqrt{3}$ по модулю p. Докажем, что число 3 — квадратичный вычет по простому модулю $p > 3$, если и только если $p \equiv \pm 1 \pmod{12}$. Пусть $12 \mid p \pm 1$. Тогда мы можем рассмотреть угол $(p \pm 1)/6$. Отметим, что

$$0 = \sin_p\Big(3\frac{p \pm 1}{6}\Big) = -4\sin_p^3\Big(\frac{p \pm 1}{6}\Big) + 3\sin_p\Big(\frac{p \pm 1}{6}\Big) = \\ = \sin_p\Big(\frac{p \pm 1}{6}\Big)\Big(3 - 4\sin_p^2\Big(\frac{p \pm 1}{6}\Big)\Big).$$

Ясно, что $\sin_p((p \pm 1)/6) \neq 0$, но тогда число $3 = (2\sin_p((p \pm 1)/6))^2$ будет квадратичным вычетом по модулю p.

Пусть теперь число 3 является квадратичным вычетом по модулю p, причём $p > 3$. Обозначим через $\sqrt{3}$ один из корней многочлена $x^2 - 3$, лежащего в поле $\mathbb{Z}_p$. Уравнение $x^2 + y^2 = 1$ имеет решение $(-1/2, \sqrt{3}/2)$, связанное с углом α. Угол 2α можно сопоставить решению $(-1/2, -\sqrt{3}/2)$, а угол 3α — решению $(1, 0)$. Следовательно, $\alpha \not\equiv 0 \pmod{p \pm 1}$, но $3\alpha \equiv 0 \pmod{p \pm 1}$, значит, модуль должен делиться на 3. Так как для $p \equiv 1 \pmod 4$ под $p \pm 1$ мы договорились подразумевать $p - 1$, а для $p \equiv -1 \pmod 4$ под $p \pm 1$ подразумевается $p + 1$, получим $4 \mid p \pm 1$. Комбинируя делимость на 3 и на 4, получаем, что $p \equiv \pm 1 \pmod{12}$.

Иррациональность и обычные углы. Докажем, что для таких натуральных c и d, что $d^2 - 2c^2 = 1$, число $1/(2\pi) \cdot \arcsin(1/d)$ иррационально, причём arcsin здесь понимается в стандартном смысле. Например, в качестве c и d можно взять числа 2 и 3 соответственно.

Во-первых, имеет место равенство

$$\Big(\frac{\sqrt{2}c}{d}\Big)^2 + \Big(\frac{1}{d}\Big)^2 = 1.$$

Обозначим $\arcsin(1/d)$ через θ. Мы покажем, что число $\theta/(2\pi)$ иррационально, предположив обратное. Пусть $\theta = 2\pi\frac{n}{m}$, где $n, m \in \mathbb{N}$. Выберем любое простое p, взаимно простое с d и такое, что $8 \mid p + 1$. Позже (в этом разделе) мы поймём, почему таких простых бесконечно много. Работая в $\mathbb{Z}_p(i)$ или $\mathbb{Z}_p$, под $\sqrt{2}$ мы подразумеваем один из корней многочлена $x^2 - 2$ в поле $\mathbb{Z}_p$, под делением подразумеваем умножение на обратный элемент, и так как $(p, d) = 1$, возможно деление на d. Элемент

$$z = \frac{\sqrt{2}c}{d} + i\frac{1}{d}$$

принадлежит $\mathbb{Z}_p(i)$. В поле $\mathbb{C}$ из равенства

$$e^{i\theta} = \frac{\sqrt{2}c}{d} + i\frac{1}{d}$$

следует тождество

$$\left(\frac{\sqrt{2}c}{d}+i\frac{1}{d}\right)^m = e^{i\theta m} = e^{i\cdot 2\pi n} = 1.$$

Докажем аналогичное утверждение для $\mathbb{Z}_p(i)$.

Лемма 4.1. *В поле $\mathbb{Z}_p(i)$ имеет место равенство*

$$\left(\frac{\sqrt{2}c}{d}+i\frac{1}{d}\right)^m = 1.$$

Доказательство. Если рассматривать $\mathbb{Q}(i,\sqrt{2})$ как векторное пространство над $\mathbb{Q}$, то числа $1, i, \sqrt{2}, \sqrt{2}\,i$ образуют базис расширения $\mathbb{Q}(i,\sqrt{2})$. Тогда из равенства

$$\left(\frac{\sqrt{2}c}{d}+i\frac{1}{d}\right)^m = 1$$

в $\mathbb{Q}(i,\sqrt{2})$ следует, что

$$\left(\frac{\sqrt{2}c}{d}+i\frac{1}{d}\right)^m = 1$$

в $\mathbb{Z}_p(i)$. Действительно, пусть

$$e^{i\theta k} = t_{k1} + t_{k2}i + t_{k3}\sqrt{2} + t_{k4}\sqrt{2}\,i$$

в $\mathbb{C}$, где все $t_{ki} \in \mathbb{Q}$. Нетрудно видеть, что $t_{01} = 1$, $t_{02} = t_{03} = t_{04} = 0$. Следовательно, мы можем получить $e^{i\theta(k+1)}$ из $e^{i\theta k}$, рассмотрев в $\mathbb{Q}(i,\sqrt{2})$ произведение

$$\left(t_{k1} + t_{k2}i + t_{k3}\sqrt{2} + t_{k4}\sqrt{2}\,i\right)\left(\frac{\sqrt{2}c}{d}+i\frac{1}{d}\right).$$

Раскрывая скобки и приводя подобные в этом выражении, для всех четырёх новых «координат» можно получить выражения в виде линейных комбинаций предыдущих четырёх координат с рациональными коэффициентами, чьи знаменатели взаимно просты с p, так как $(p,d)=1$. В случае рациональных чисел, у которых знаменатели взаимно просты с p, все их преобразования можно рассмотреть по модулю p (дробь a/b соответствует остатку $a\cdot b^{-1}$). Поэтому, например, если мы посредством сложения и умножения получили 1 в $\mathbb{Q}$, то, применив этот способ к соответствующим остаткам, мы получим 1 по модулю p. В $\mathbb{Q}(i,\sqrt{2})$ имеют место равенства $t_{m1} = 1$, $t_{m2} = t_{m3} = t_{m4} = 0$. Если мы теперь рассмотрим преобразования, которые произошли с нашими «координатами» по модулю p, получим

$$\left(\frac{\sqrt{2}c}{d}+i\frac{1}{d}\right)^m = 1\cdot 1 + 0\cdot i + 0\cdot\sqrt{2} + 0\cdot i\sqrt{2} = 1$$

по модулю p. □

Вернёмся к $\mathbb{Z}_p(i)$: количество элементов группы решений уравнения $x^2+y^2=1$ равно $p+1$, поэтому верно равенство

$$\left(\frac{\sqrt{2}\,c}{d}+i\frac{1}{d}\right)^{\gcd(m,\,p+1)}=1.$$

Чтобы воспользоваться последним утверждением, докажем следующую лемму.

Лемма 4.2. *Существует бесконечно много простых p таких, что $8 \mid p+1$ и $(m, p+1) \mid 8$, и $(p, d)=1$.*

Доказательство. Для всех r_i рассмотрим систему сравнений

$$\begin{cases} p \equiv 7 \pmod{16}, \\ p \equiv 1 \pmod{r_i}, \end{cases}$$

где r_i — все нечётные простые делители чисел m и d. По китайской теореме об остатках существует арифметическая прогрессия натуральных чисел, удовлетворяющая этим сравнениям, причём разность этой прогрессии взаимно проста с её элементами. Тогда по теореме Дирихле о простых числах в арифметической прогрессии имеется бесконечно много простых чисел, удовлетворяющих условиям леммы. □

Если $(m, p+1) \mid 8$, то в $\mathbb{Z}_p(i)$ верно равенство

$$\left(\frac{\sqrt{2}c}{d}+i\frac{1}{d}\right)^{8}=1.$$

В нашем случае это означает, что $(\sqrt{2}\,c/d, 1/d)$ имеет вид либо $(\pm 1, 0)$, либо $(0, \pm 1)$, либо $(\pm 1/\sqrt{2}, \pm 1/\sqrt{2})$. Первый случай невозможен, второй означает, что $c \equiv 0 \pmod{p}$, а третий даст нам условие $d^2-2 \equiv 0 \pmod{p}$. Тогда по лемме 4.2 найдётся нужное нам простое число, для которого последние два случая невозможны. Это приводит к противоречию. Отсюда получаем, например, что число $1/(2\pi)\cdot\arcsin(1/3)$ иррационально. То же самое верно для любого такого натурального числа d, что при некотором натуральном c выполнено уравнение Пелля $d^2-2c^2=1$.

Аналогично мы можем доказать, что для таких $c, d \in \mathbb{N}$, что $d^2-3c^2=1$ и $d \neq 2$, число $1/(2\pi)\cdot\arcsin(1/d)$ иррационально. В частности, по системе сравнений

$$\begin{cases} p \equiv 11 \pmod{6\cdot 12}, \\ p \equiv 1 \pmod{r_i} \quad \forall\, r_i, \end{cases}$$

где r_i — все простые делители чисел m и d, превосходящие 3, мы можем построить нужную арифметическую прогрессию. Исходя из по-

хожих соображений, можно доказать, что пересечение $\mathbb{Q}(i)$ и множества всех комплексных чисел вида $e^{i2\pi\theta}$, где θ рационально, — это $\{1, i, -1, -i\}$. Действительно, пусть $\theta = n/m$ и $e^{i\theta} = a/d + ib/d$, где $n, a, b \in \mathbb{Z}$ и $m, d \in \mathbb{N}$. Мы можем рассмотреть систему сравнений

$$\begin{cases} p \equiv 3 \pmod 8, \\ p \equiv 1 \pmod{r_i} \end{cases}$$

для всех r_i, где r_i — все нечётные простые делители чисел m и d. Найдётся бесконечно много простых, удовлетворяющих этой системе сравнений. Обозначим одно из них через p. Тогда из равенства

$$1 = e^{i\theta m} = \left(\frac{a}{d} + i\frac{b}{d}\right)^m$$

в $\mathbb{C}$ мы также, как и в лемме 4.1, получаем, что

$$\left(\frac{a}{d} + i\frac{b}{d}\right)^m = 1$$

в $\mathbb{Z}_p(i)$. Но, так как $(m, p+1) = 4$, имеет место равенство

$$\left(\frac{a}{d} + i\frac{b}{d}\right)^4 = 1$$

в $\mathbb{Z}_p(i)$, поэтому один из двух остатков $a/d, b/d$ должен быть равен 0 в $\mathbb{Z}_p$. Тогда если $e^{i\theta} \notin \{1, i, -1, -i\}$, то, так как в нашей арифметической прогрессии бесконечно много простых чисел, среди них найдётся такое, при котором мы получим противоречие.

§ 5. Модулярный тангенс

В случае геометрических углов значения $\sin_p(-\alpha)$ могут быть равны $-\sin_p \alpha$ или $\sin_p \alpha$. Более того, нельзя сказать, что любой остаток $a \in \mathbb{Z}_p$ — например, остаток 2 по модулю 11 — представим как синус некоторого угла ($a = \sin_p \alpha$). Оказывается, что в случае тангенса картина более приятная. Однако начнём с более простого типа углов.

Негеометрические углы. Тангенсом угла $\alpha \neq \pm(p \pm 1)/4$ будем называть функцию $\operatorname{tg}_p \alpha = \sin_p \alpha / \cos_p \alpha$ (деление в поле $\mathbb{Z}_p$). Когда $\cos_p \alpha = 0$, тангенс не определён. Кроме того, можно заметить, что равенство $\operatorname{tg}_p \alpha = 0$ имеет место лишь при $\sin_p \alpha = 0$. Тогда $\alpha \in \{0, (p \pm 1)/2\}$.

Верны тождества $\operatorname{tg}_p(-\alpha) = -\operatorname{tg}_p \alpha$ и $\operatorname{tg}_p(\alpha + (p \pm 1)/2) = \operatorname{tg}_p \alpha$. Также

$$\operatorname{tg}_p\left(\frac{p \pm 1}{4} - \alpha\right) = \frac{1}{\operatorname{tg}_p \alpha},$$

когда $\operatorname{tg}_p \alpha \neq 0$. Формула тангенса суммы углов, которая выполнена в стандартном случае, тоже верна; если тангенсы углов α, β, $\alpha+\beta$ определены, то имеем

$$\frac{\operatorname{tg}_p \alpha + \operatorname{tg}_p \beta}{1-\operatorname{tg}_p \alpha \operatorname{tg}_p \beta} = \frac{\sin_p \alpha \cos_p \beta + \sin_p \beta \cos_p \alpha}{\cos_p \alpha \cos_p \beta - \sin_p \alpha \sin_p \beta} = \operatorname{tg}_p(\alpha+\beta).$$

Заметим, что

$$\operatorname{tg}_p \alpha = \operatorname{tg}_p \beta \quad \Leftrightarrow \quad \sin_p \alpha \cos_p \beta - \sin_p \beta \cos_p \alpha = 0 \quad \Leftrightarrow \quad \sin_p(\alpha-\beta)=0.$$

Поэтому $\alpha-\beta \in \{0, (p\pm 1)/2\}$. Так как $(p\pm 1)/2$ — период нашего тангенса, множество значений последнего равно

$$\left\{ \operatorname{tg}_p \alpha \colon \alpha \in \left[0, \frac{p\pm 1}{2}\right) \setminus \left\{\frac{p\pm 1}{4}\right\}\right\}.$$

Значения, которые принимает тангенс на

$$\left\{0, \ldots, \frac{(p\pm 1)}{2} - 1\right\} \setminus \left\{\frac{(p\pm 1)}{4}\right\},$$

отличаются попарно, поэтому он имеет ровно $(p\pm 1)/2-1$ различных значений.

Геометрические углы. Напомним, что под геометрическими углами подразумевается тип углов, возникающий при рассмотрении решений уравнения $x^2+y^2=\pm 1$. Тангенс геометрических углов при $\alpha \neq \pm(p+1)/2$ определяется как $\operatorname{tg}_p \alpha = \sin_p \alpha / \cos_p \alpha$. Снова

$$\operatorname{tg}_p \alpha = 0 \quad \Leftrightarrow \quad \alpha \in \{0, p+1\}.$$

По-прежнему верно равенство $\operatorname{tg}_p(\alpha+(p+1)) = \operatorname{tg}_p \alpha$. Так как обратное к z — это $\bar{z}$ или $-\bar{z}$, имеем $\operatorname{tg}_p(-\alpha) = -\operatorname{tg}_p \alpha$. Также верно, что

$$\operatorname{tg}_p\left(\alpha + \frac{p+1}{2}\right) = -\frac{1}{\operatorname{tg}_p \alpha}, \quad \text{если} \quad \operatorname{tg}_p \alpha \neq 0.$$

Формула тангенса суммы углов верна, так как верны формулы синуса и косинуса суммы углов. Однако тогда верна и формула для разности: если тангенсы углов α, β, $\alpha-\beta$ определены, то

$$\operatorname{tg}_p(\alpha+(-\beta)) = \frac{\operatorname{tg}_p \alpha + \operatorname{tg}_p(-\beta)}{1-\operatorname{tg}_p \alpha \operatorname{tg}_p(-\beta)} = \frac{\operatorname{tg}_p \alpha - \operatorname{tg}_p \beta}{1+\operatorname{tg}_p \alpha \operatorname{tg}_p \beta}.$$

Отметим, что

$$\operatorname{tg}_p \alpha = \operatorname{tg}_p \beta \quad \Leftrightarrow \quad \sin_p \alpha \cos_p \beta - \sin_p \beta \cos_p \alpha = 0 \quad \Leftrightarrow \quad \pm \sin_p(\alpha-\beta)=0.$$

Поэтому $\alpha-\beta \in \{0, p+1\}$. Следовательно, значения тангенса возникают ровно по одному разу для углов от 0 до p включительно, и тангенс

не определён в точке $\alpha = (p+1)/2$. Но тогда получаем, что множество значений тангенса — все остатки по модулю p. Другими словами, каждый остаток по модулю p появляется ровно два раза среди всех значений тангенса, и соответствующих ему два угла отличаются на $p+1$; также тангенс не определён для двух углов, отличающихся на $p+1$.

Корни уравнения. Снова рассмотрим геометрические углы. Нетрудно заметить, что верны формулы

$$\frac{2\operatorname{tg}_p \alpha}{1+\operatorname{tg}_p^2 \alpha} = \frac{2\sin_p \alpha \cos_p \alpha}{\sin_p^2 \alpha + \cos_p^2 \alpha} = \pm \sin_p 2\alpha,$$
$$\frac{1-\operatorname{tg}_p^2 \alpha}{1+\operatorname{tg}_p^2 \alpha} = \frac{\cos_p^2 \alpha - \sin_p^2 \alpha}{\sin_p^2 \alpha + \cos_p^2 \alpha} = \pm \cos_p 2\alpha.$$

Тогда получим пару $(-\sin_p 2\alpha, -\cos_p 2\alpha)$, когда угол нечётный, так как в этом случае $\sin_p^2 \alpha + \cos_p^2 \alpha = -1$, и пару $(\sin_p 2\alpha, \cos_p 2\alpha)$, когда угол чётный, так как в этом случае $\sin_p^2 \alpha + \cos_p^2 \alpha = 1$ (вспомним, что для геометрических углов верны формулы синуса и косинуса суммы углов). Так как тангенс может быть равен любому остатку, у нас есть возможность получать решения уравнения $z^{p+1} = 1$, сопоставляя остаток t по модулю p элементу из $\mathbb{Z}_p(i)$ вида

$$\pm\frac{1-t^2}{1+t^2} \pm i\frac{2t}{1+t^2}.$$

Рассмотрим негеометрические углы в случае $p = 4n+1$. Их тангенс не может быть равен $\pm j$, где под j подразумевается один из корней многочлена x^2+1 в поле $\mathbb{Z}_p$: иначе выполнялось бы равенство $\sin_p^2 \alpha + \cos_p^2 \alpha = 0$. Заметим, что мы можем снова получать решения уравнения $x^2+y^2=1$ из остатков по модулю p: если взять $t \neq \pm j$, то

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

Если также $t \neq \pm 1$, то существует тангенс данного угла, равный $\dfrac{2t}{1-t^2}$.

§ 6. Многочлены для тангенса

Мы знаем, что $\operatorname{tg} 2\theta = 2\operatorname{tg}\theta/(1-\operatorname{tg}^2\theta)$. Представим $\operatorname{tg} n\theta$ как рациональную функцию от $\operatorname{tg}\theta$.

Рассмотрим следующую рекуррентную последовательность пар многочленов $p_n, q_n \in \mathbb{Z}[x]$

$$p_0 = 0, \quad p_{n+1} = p_n + q_n x,$$
$$q_0 = 1, \quad q_{n+1} = q_n - p_n x.$$

Приведём несколько первых элементов последовательности:

n	0	1	2	3	4	5
p_n	0	x	$2x$	$3x-x^3$	$4x-4x^3$	$5x-10x^3+x^5$
q_n	1	1	$1-x^2$	$1-3x^2$	$1-6x^2+x^4$	$1-10x^2+5x^4$

Лемма 6.1. *При $n>0$ верно следующее*:

Случай		*Степень*	*Старший коэффициент*
$2 \mid n$	p_n	$n-1$	$(-1)^{n/2-1}n$
	q_n	n	$(-1)^{n/2}$
$2 \nmid n$	p_n	n	$(-1)^{(n-1)/2}$
	q_n	$n-1$	$(-1)^{(n-1)/2}n$

Младший моном многочлена q_n равен x^0. Младший моном многочлена p_n равен nx.

Доказательство. Проведём индукцию по n. Для случая $n=1$ наше утверждение верно. Опишем переход от n к $n+1$. Если $2 \mid n$, то

$$p_{n+1}=p_n+q_nx \quad \text{и} \quad \deg p_n<\deg q_n \quad \Rightarrow \quad \deg p_{n+1}=n+1.$$

При этом $(-1)^{n/2}=(-1)^{((n+1)-1)/2}$. Перейдём к многочлену q_{n+1} следующим образом:

$$q_{n+1}=q_n-p_nx \quad \Rightarrow \quad \deg q_{n+1}\leqslant \max(\deg q_n, \deg(-p_nx))=n=(n+1)-1.$$

Коэффициент при старшей степени многочлена q_{n+1} равен

$$(-1)^{n/2}-(-1)^{n/2-1}n=(-1)^{((n+1)-1)/2}(n+1).$$

Если $2 \nmid n$, то $p_{n+1}=p_n+q_nx$, и поэтому

$$\deg p_{n+1}\leqslant \max(\deg p_n, \deg(q_nx))=n=(n+1)-1.$$

Коэффициент при старшей степени многочлена p_{n+1} равен

$$(-1)^{(n-1)/2}+(-1)^{(n-1)/2}n=(-1)^{(n+1)/2-1}(n+1).$$

Далее,

$$q_{n+1}=q_n-p_nx, \deg p_n>\deg q_n \quad \Rightarrow \quad \deg q_{n+1}=n+1.$$

Старший коэффициент равен $(-1)^{(n-1)/2}(-1)=(-1)^{(n+1)/2}$. Так как $q_{n+1}=q_n-p_nx$, коэффициент при x^0 остается неизменным, следовательно, тождественно равен 1. Так как $p_{n+1}=p_n+q_nx$, коэффициент при x^0 тождественно равен 0, а коэффициент при x^1 увеличивается на 1 на каждом шаге. □

Так как мы собираемся рассматривать соотношение p_n и q_n, желательно избежать случая $0/0$. Докажем, что такой ситуации не возникает.

Лемма 6.2. *Многочлены p_n и q_n взаимно просты. Для любого простого $p > 2$ их редукции по модулю p взаимно просты как многочлены в $\mathbb{Z}_p[x]$.*

Доказательство. Взаимная простота двух многочленов равносильна тому, что у них нет общих корней ни в одном расширении поля. Докажем последнее по индукции. База индукции при $n \leqslant 1$ верна. Опишем переход от n к $n+1$. Пусть многочлены $p_n + q_n x$ и $q_n - p_n x$ имеют общий корень z. Если $z = 0$, то $p_n(z) = q_n(z) = 0$, что приводит к противоречию. Когда $z \neq 0$, из равенства $p_n(z) = 0$ или равенства $q_n(z) = 0$ следует $p_n(z) = q_n(z) = 0$. Значит, $p_n(z)q_n(z) \neq 0$. Тогда

$$p_n(z) = -q_n(z)z = -p_n(z)z^2 \quad \Rightarrow \quad z^2 = -1.$$

Теперь покажем, что p_n и q_n не могут одновременно быть равны 0, когда $z^2 = -1$. Чтобы это сделать, посмотрим на значения, которые они принимают:

n		0	1	2	3
i	$p_n(i)$	0	i	$2i$	$4i$
	$q_n(i)$	1	1	2	4
$-i$	$p_n(-i)$	0	$-i$	$-2i$	$-4i$
	$q_n(-i)$	1	1	2	4

Ясно, что, начиная с $n = 1$, ненулевые значения p_n и q_n удваиваются на каждом шаге, и потому два многочлена никогда не будут одновременно равны 0 в $\pm i$. Заметим, что это рассуждение работает во всех трёх случаях: $\mathbb{C}$, $\mathbb{Z}_p(i)$ при $p \equiv 3 \pmod 4$ и $\mathbb{Z}_p$ при $p \equiv 1 \pmod 4$, причём в каждом случае под i подразумевается корень из -1 в соответствующем поле. □

В следующей лемме под tg будем подразумевать как обычный тангенс, так и tg_p; аналогично для синуса и косинуса.

Лемма 6.3. *В случае углов из $\mathbb{R}$ и в случае углов по модулю простых чисел (как геометрических, так и негеометрических) формула*

$$\frac{p_n(\mathrm{tg}\,\alpha)}{q_n(\mathrm{tg}\,\alpha)} = \mathrm{tg}\, n\alpha$$

верна, когда тангенс углов α и $n\alpha$ определён. Случай, когда $\mathrm{tg}\,\alpha$ определён, а $\mathrm{tg}\, n\alpha$ — нет, встречается тогда и только тогда, когда

$$q_n(\mathrm{tg}\,\alpha) = 0.$$

Доказательство. Проведём индукцию по n. База в случае $n \leqslant 1$ ясна. Опишем переход от $n-1$ к n. Предположим, что $\operatorname{tg}\alpha$ определён. Если $\operatorname{tg}(n-1)\alpha$ тоже определён, то $q_{n-1}(\operatorname{tg}\alpha) \neq 0$, и мы имеем

$$\operatorname{tg} n\alpha = \operatorname{tg}(\alpha + (n-1)\alpha) = \frac{\operatorname{tg}\alpha + \dfrac{p_{n-1}(\operatorname{tg}\alpha)}{q_{n-1}(\operatorname{tg}\alpha)}}{1 - \operatorname{tg}\alpha\,\dfrac{p_{n-1}(\operatorname{tg}\alpha)}{q_{n-1}(\operatorname{tg}\alpha)}} =$$

$$= \frac{p_{n-1}(\operatorname{tg}\alpha) + \operatorname{tg}\alpha \cdot q_{n-1}(\operatorname{tg}\alpha)}{q_{n-1}(\operatorname{tg}\alpha) - \operatorname{tg}\alpha \cdot p_{n-1}(\operatorname{tg}\alpha)} = \frac{p_n(\operatorname{tg}\alpha)}{q_n(\operatorname{tg}\alpha)}.$$

Заметим, что

$$q_n(\operatorname{tg}\alpha) = 0 \quad \Leftrightarrow \quad q_{n-1}(\operatorname{tg}\alpha) - p_{n-1}(\operatorname{tg}\alpha)\operatorname{tg}\alpha = 0 \quad \Leftrightarrow$$
$$\Leftrightarrow \quad \operatorname{tg}\alpha \operatorname{tg}(n-1)\alpha = 1 \quad \Leftrightarrow$$
$$\Leftrightarrow \quad \cos\alpha\cos(n-1)\alpha - \sin\alpha\sin(n-1)\alpha = 0 \quad \Leftrightarrow \quad \cos n\alpha = 0.$$

Отсюда следует, что $\operatorname{tg} n\alpha$ не определён. Если $\operatorname{tg}(n-1)\alpha$ не определён, то $\cos(n-1)\alpha = 0$, при этом $q_{n-1}(\operatorname{tg}\alpha) = 0$, но тогда $p_{n-1}(\operatorname{tg}\alpha) \neq 0$. Отсюда получаем формулу

$$\operatorname{tg}(\alpha + (n-1)\alpha) = -\frac{1}{\operatorname{tg}\alpha} = \frac{p_{n-1}(\operatorname{tg}\alpha)}{-p_{n-1}(\operatorname{tg}\alpha)\operatorname{tg}\alpha} = \frac{p_n(\operatorname{tg}\alpha)}{q_n(\operatorname{tg}\alpha)}. \qquad \square$$

Из этой леммы следует равенство

$$\operatorname{tg}(n \operatorname{arctg} x) = \frac{p_n(x)}{q_n(x)}$$

для действительных x. Заметим, что ввиду взаимной простоты многочленов $p_n(x)$ и $q_n(x)$ любое представление $\operatorname{tg}(n \operatorname{arctg} x)$ в виде отношения двух многочленов должно иметь вид

$$\frac{p_n(x)K(x)}{q_n(x)K(x)},$$

где $K(x)$ — некоторый отличный от p_n и q_n многочлен.

Теперь мы можем представить p_n и q_n в виде произведения линейных множителей.

Лемма 6.4. *Пусть A — старший коэффициент в p_n, а B — старший коэффициент в q_n. Тогда в $\mathbb{R}$ верны равенства*

$$p_n(x) = A\prod_{\substack{k=0\\ k\neq n/2}}^{n-1}\Big(x - \operatorname{tg}\frac{\pi}{n}k\Big), \quad q_n(x) = B\prod_{\substack{k=0\\ k\neq n,\, 2\nmid k}}^{2n-1}\Big(x - \operatorname{tg}\frac{\pi}{2n}k\Big).$$

Доказательство. Нетрудно заметить, что $x_k = \operatorname{tg}(\pi k/n)$ — корни многочлена p_n, $0 \leqslant k \leqslant n-1$, $k \neq n/2$. Их количество совпадает со степенью p_n. Отсюда вытекает первая формула из утверждения леммы. Теперь заметим, что $\operatorname{tg} n \operatorname{arctg} x$ не определён лишь при $x = \operatorname{tg}(\pi k/(2n))$, где k нечётно и не кратно n. Для такого x имеем $q_n(x) = 0$. При чётных n имеем $\deg q_n = n$, а при нечётных $\deg q_n = n-1$. Другими словами, мы только что рассмотрели корни многочлена q_n, количество которых равно $\deg q_n$. □

Если мы умножим угол на n, а потом на m, то получим, что

$$\operatorname{tg}\Big(n\Big(\operatorname{arctg}(\operatorname{tg}(m \operatorname{arctg} x))\Big)\Big)$$

равен $\operatorname{tg} nm \operatorname{arctg} x$, если определён. Покажем теперь, что композиция дробей $p_m(x)/q_m(x)$ и $p_n(x)/q_n(x)$ даёт дробь $p_{nm}(x)/q_{nm}(x)$.

Лемма 6.5. *Верны равенства многочленов*

$$p_{nm}(x) = p_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n, \quad q_{nm}(x) = q_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n.$$

Доказательство. Ясно, что

$$p_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n, q_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n \in \mathbb{R}[x].$$

Рассмотрим старшие коэффициенты и степени этих многочленов. Используем лемму 6.1. Если $2 \mid m$, то $\deg p_m = m-1$ и $\deg q_m = m$. Многочлен p_n можно записать как $a_0 + a_1x + a_2x^2 + \ldots$, тогда многочлен

$$p_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n$$

можно записать как

$$a_0q_m(x)^n + a_1\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n + a_2\left(\frac{p_m(x)}{q_m(x)}\right)^2 q_m(x)^n + \ldots$$

Нас интересует старший моном в многочлене

$$p_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n.$$

Чтобы его найти, мы можем посмотреть отдельно на старшие степени x в каждом из слагаемых суммы, приведённой выше. Так как $\deg q_m > \deg p_m$, старшая степень x появляется только внутри монома

$$a_k\left(\frac{p_m(x)}{q_m(x)}\right)^k q_m(x)^n$$

с минимальным k, при котором $a_k \neq 0$. Тогда старший член

$$p_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n$$

совпадает со старшим членом $np_m(x)q_m(x)^{n-1}$, т. е. с мономом

$$(-1)^{\frac{m}{2}-1+\frac{m}{2}(n-1)}nmx^{nm-1} = (-1)^{nm/2-1}nmx^{nm-1}.$$

Аналогичным образом старший член многочлена

$$q_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n$$

будет присутствовать только внутри $q_m(x)^n$, что даёт моном $(-1)^{nm/2}x^{nm}$.

Если $2 \nmid m$: $\deg p_m = m$ и $\deg q_m = m-1$. Теперь в приведённых рассуждениях старшая степень x появляется лишь в слагаемом с максимальным k, при котором $a_k \neq 0$. Если $2 \mid n$: в случае многочлена

$$p_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n$$

мы рассматриваем слагаемое $(-1)^{n/2-1}np_m(x)^{n-1}q_m(x)$, из которого получаем моном

$$(-1)^{n/2-1+(n-1)(m-1)/2+(m-1)/2}nmx^{nm-1} = (-1)^{nm/2-1}nmx^{nm-1}.$$

Аналогичным образом для многочлена

$$q_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n$$

мы рассматриваем слагаемое $(-1)^{n/2}p_m(x)^n$, из которого получаем моном

$$(-1)^{(n+(m-1)n)/2}x^{nm} = (-1)^{nm/2}x^{nm}.$$

Если $2 \nmid n$: для полинома

$$p_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n$$

мы рассмотрим $(-1)^{(n-1)/2}p_m(x)^n$, получим моном

$$(-1)^{(n-1)/2}(-1)^{(m-1)n/2}x^{nm} = (-1)^{(nm-1)/2}x^{nm}.$$

Далее, в случае многочлена

$$q_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n$$

мы будем работать со слагаемым $(-1)^{(n-1)/2}np_m(x)^{n-1}q_m(x)$. Оно должно дать моном

$$(-1)^{(n-1)/2}n(-1)^{(n-1)(m-1)/2}(-1)^{(m-1)/2}mx^{nm-1} = (-1)^{(nm-1)/2}nmx^{nm-1}.$$

Таким образом, оба многочлена

$$p_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n \quad \text{и} \quad q_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n$$

имеют старшие члены, идентичные старшим членам многочленов p_{nm} и q_{nm} соответственно. Теперь значение рациональной дроби

$$\frac{p_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n}{q_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n}$$

совпадает с $p_{nm}(x)/q_{nm}(x)$ для бесконечно большого количества значений x. Используя доказанное выше, получаем нужное равенство. □

Доказанный факт позволяет выразить p_{2n} через p_n и q_n. Воспользуемся этим, чтобы доказать следующую лемму. Через $\nu_p(n)$ обозначим степень вхождения простого p в ненулевое целое n.

Лемма 6.6. *Пусть $n = 2^k n' > 0$, где $k = \nu_2(n)$. Тогда $c(p_n) = 2^k$, где $c(p_n)$ — содержание многочлена p_n.*

Доказательство. Проведём индукцию по $\nu_2(n)$. База индукции: для нечётного n старший коэффициент многочлена p_n равен ± 1, так что $c(p_n) = 1$. Опишем индукционный переход от $\nu_2(n)$ к $\nu_2(n) + 1$. В лемме 6.5 поменяем местами n и m, после этого положим $m = 2$ и воспользуемся формулами для p_2, q_2. В итоге получим $p_{2n} = 2p_nq_n$. Но тогда $c(p_{2n}) = 2c(p_n)c(q_n) = 2c(p_n)$, так как младший коэффициент многочлена q_n равен 1. □

§ 7. Фундаментальные многочлены

При разложении многочлена $x^n - 1$ на множители получим многочлены деления круга, которые имеют полезные приложения. Многочлены деления круга связаны с мультипликативной группой $\mathbb{Z}_p^*$, вследствие чего удаётся установить связь с её мощностью $p - 1$. Однако группы, связанные с углами, помимо мощности $p - 1$ могут иметь мощность $p + 1$. Поэтому попытаемся разложить $p_n(x)$ в произведение многочленов меньшей степени.

Для нечётного n положим $s(n) = (-1)^{(n-1)/2}$. Так как $s(n) \equiv n \pmod 4$, имеем $s(nm) = s(n)s(m)$, когда n и m нечётны.

Определение. Определим n-й фундаментальный многочлен, где $n \in \mathbb{N}$, следующим образом:

$$\varphi_1(x) = x, \quad \varphi_2(x) = 2;$$

при $n > 2$

$$\varphi_n(x) = A \prod_{\substack{k=0 \\ (k,n)=1 \\ 2k \neq n}}^{n-1} \left(x - \operatorname{tg} \frac{\pi}{n} k\right),$$

где

$$A = \begin{cases} -2, & \text{если } n = 4, \\ +2, & \text{если } n = 2^k, \text{ где } k \neq 2 \text{ и } k > 0, \\ s(p), & \text{если } n = p^k, \text{ где } p > 2, \\ s(p)p, & \text{если } n = 2p^k, \text{ где } p > 2, \\ 1, & \text{иначе.} \end{cases}$$

Лемма 7.1. *Для всех $n \in \mathbb{N}$ справедлива формула*

$$p_n(x) = \prod_{d|n} \varphi_d(x).$$

Доказательство. Мы знаем, что корни многочлена p_n — числа вида $\operatorname{tg} \frac{\pi}{n} k$ при $2k \neq n$, $0 \leqslant k < n$, но каждое из них встречается в произведении в правой части по одному разу: для $\operatorname{tg} \frac{\pi}{n} k$ надо взять $d = (k, n)$. Поэтому надо проверить только равенство старших коэффициентов.

Для нечётного $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, где p_i — простые числа, большие 2, старший коэффициент в правой части имеет вид

$$s(p_1)^{\alpha_1} \cdot \ldots \cdot s(p_k)^{\alpha_k} = s(n) = (-1)^{(n-1)/2}.$$

Для $n = 2p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ старший коэффициент в правой части будет иметь вид

$$2 \underbrace{s(p_1)^{\alpha_1} \cdot \ldots \cdot s(p_k)^{\alpha_k}}_{\text{от } d = p^\alpha} \underbrace{p_1^{\alpha_1} s(p_1)^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} s(p_k)^{\alpha_k}}_{\text{от } d = 2p^\alpha} = (-1)^{n/2-1} n.$$

Для $n = 2^k p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ при $k > 1$ имеем

$$-2^k \underbrace{s(p_1)^{\alpha_1} \cdot \ldots \cdot s(p_k)^{\alpha_k}}_{\text{от } d = p^\alpha} \underbrace{p_1^{\alpha_1} s(p_1)^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} s(p_k)^{\alpha_k}}_{\text{от } d = 2p^\alpha} = (-1)^{n/2-1} n,$$

где отрицательный знак перед 2^k обусловлен тем, что старший коэффициент в $\varphi_{2^2}(x)$ равен -2. □

Через $c(P)$ обозначим содержание многочлена P.

Лемма 7.2. *Пусть $P, Q \in \mathbb{Z}[x]$. Если $Q \mid P$ как многочлен в $\mathbb{Q}[x]$, и $c(Q) \mid c(P)$, то $P/Q \in \mathbb{Z}[x]$, и $c(P/Q) = c(P)/c(Q)$.*

Доказательство. Без ограничения общности можно предположить, что $c(Q) = 1$: иначе мы можем разделить и P, и Q на $c(Q)$. Пусть $P(x) = Q(x)R(x)$, где $R(x) \in \mathbb{Q}[x]$. Через t обозначим такое наименьшее натуральное число, что $tR(x) \in \mathbb{Z}[x]$. Тогда $(t, c(tR(x))) = 1$, так как иначе нашлось бы меньшее t. Поэтому

$$tP(x) = Q(x)(tR(x)) \quad \Rightarrow \quad tc(P) = c(Q)c(tR(x)) = c(tR(x)) \quad \Rightarrow$$
$$\Rightarrow \quad t = 1 \quad \Rightarrow \quad R(x) \in \mathbb{Z}[x]. \quad \square$$

Используя эту лемму, мы можем показать, что фундаментальные многочлены имеют целые коэффициенты.

Лемма 7.3. *Верно, что $\varphi_n(x) \in \mathbb{Z}[x]$, причём*

$$c(\varphi_n) = \begin{cases} 2, & \text{если } n = 2^k \text{ для } k \in \mathbb{N}, \\ 1, & \text{иначе}, \end{cases}$$

$$\varphi_n(0) = \begin{cases} p, & \text{если } n = p^\alpha \text{ при простом } p \text{ и } \alpha \in \mathbb{N}. \\ 0, & \text{если } n = 1, \\ 1, & \text{иначе}. \end{cases}$$

Доказательство. Проведём индукцию по n. База индукции $n = 1$ очевидна. Чтобы осуществить индуктивный переход, выведем наше утверждение для n из всех предыдущих. Мы знаем, что

$$p_n(x) = \varphi_n(x) \prod_{\substack{d \mid n \\ d < n}} \varphi_d(x).$$

Пусть $k = \nu_2(n)$. В лемме 6.6 было показано, что $c(p_n) = 2^k$. По предположению индукции имеем

$$c\Bigg(\prod_{d \mid n,\, d < n} \varphi_d(x)\Bigg) = \prod_{\substack{d \mid n \\ d < n}} c(\varphi_d(x)) = \begin{cases} 2^{k-1}, & \text{если } n = 2^k, \\ 2^k, & \text{иначе}. \end{cases}$$

Число 2^k делит $c(p_n(x))$. Применим предыдущую лемму 7.2. В качестве многочлена P рассмотрим $p_n(x)$, а в качестве многочлена Q — произведение всех $\varphi_d(x)$, где $d < n$ и d делит n. Выбранные многочлены P и Q имеют целые коэффициенты, в частности, для Q это верно по предположению индукции. По лемме 7.2 получаем $\varphi_n(x) \in \mathbb{Z}[x]$. Кроме того, $c(\varphi_n) = 2$, когда $n = 2^k$, так как $c(p_n) = 2^k$.

Пусть $D(x) = p_n(x)/x$. Тогда $D(x) \in \mathbb{Z}[x]$ и $D(0) = n$ согласно лемме 6.1. Поэтому

$$D(0) = \varphi_n(0) \prod_{\substack{d|n \\ 1<d<n}} \varphi_d(0) = \varphi_n(0) \begin{cases} \dfrac{n}{p}, & \text{если } n = p^\alpha, \\ n, & \text{иначе.} \end{cases}$$

Отсюда следует требуемое. □

Ясно, что $p_n(x)$ не имеет кратных корней как многочлен из $\mathbb{C}[x]$ по лемме 6.4. Оказывается, то же верно при рассмотрении $p_n(x)$ как многочлена из $\mathbb{Z}_p[x]$.

Теорема 1. *Для простого $p \nmid n$ многочлен p_n не имеет кратных корней ни в одном расширении $\mathbb{Z}_p$.*

Доказательство. Предположим противное. Обозначим через z кратный корень из некоторого расширения $\mathbb{Z}_p$. Ясно, что $z^2 + 1 \neq 0$, так как иначе $p_n(z) \neq 0$ (см. таблицу из леммы 6.2). Если z — кратный корень, то $p_n'(z) = 0$. Тогда $p_n'(z)q_n(z) - p_n(z)q_n'(z) = 0$. Найдём последний многочлен.

Лемма 7.4. *Верно следующее равенство многочленов*:

$$p_n'(x)q_n(x) - p_n(x)q_n'(x) = n\frac{p_n^2(x) + q_n^2(x)}{x^2+1}.$$

Доказательство. Пусть $n \neq 0$. Для любого такого x, что $q_n(x) \neq 0$, верны равенства

$$\frac{p_n'(x)q_n(x) - p_n(x)q_n'(x)}{q_n^2(x)} = \left(\frac{p_n(x)}{q_n(x)}\right)' = (\operatorname{tg} n \operatorname{arctg} x)' =$$
$$= (n \operatorname{arctg} x)'\left(\frac{d}{dx}\operatorname{tg}\right)(n \operatorname{arctg} x).$$

Мы также знаем, что

$$\frac{d}{dx}\operatorname{tg} x = \frac{1}{\cos^2 x} = 1 + \operatorname{tg}^2 x,$$

поэтому

$$(n \operatorname{arctg} x)'\left(\frac{d}{dx}\operatorname{tg}\right)(n \operatorname{arctg} x) = \frac{n}{x^2+1}\left(1 + \left(\frac{p_n(x)}{q_n(x)}\right)^2\right) =$$
$$= \frac{n}{x^2+1}\frac{p_n^2(x) + q_n^2(x)}{q_n^2(x)} = n\frac{\dfrac{p_n^2(x) + q_n^2(x)}{x^2+1}}{q_n^2(x)}.$$

Можно заметить, что $p_n^2(\pm i) + q_n^2(\pm i) = 0$, а также $c(x^2+1) = 1$. Тогда x^2+1 делит $p_n^2(x) + q_n^2(x)$ как многочлен в $\mathbb{Z}[x]$, так как

$$\frac{p_n^2(x) + q_n^2(x)}{x^2+1} \in \mathbb{Z}[x].$$

Поэтому для бесконечного количества значений x выполнено равенство

$$p_n'(x)q_n(x) - p_n(x)q_n'(x) = n\frac{p_n^2(x) + q_n^2(x)}{x^2+1}. \qquad \square$$

Значит,

$$0 = p_n'(z)q_n(z) - p_n(z)q_n'(z) = n\frac{p_n^2(z) + q_n^2(z)}{z^2+1} = n\frac{q_n^2(z)}{z^2+1} \neq 0,$$

так как $p_n(z)$ и $q_n(z)$ не могут равняться нулю одновременно. Это приводит к противоречию. $\square$

Порядком угла α будем называть такое наименьшее натуральное m, что $\operatorname{tg} m\alpha = 0$. Порядок определён не только для обычных углов, соизмеримых с 2π, но и для углов по модулю. Корни многочлена $\varphi_n(x)$ как элемента из $\mathbb{R}[x]$ связаны с углами порядка n. Докажем аналогичное утверждение для поля $\mathbb{Z}_p$.

Теорема 2. *Пусть p — нечётный простой делитель многочлена $\varphi_n(x)$ для некоторого $x \in \mathbb{Z}$. Если p не делит n, то $p-1 \equiv 0 \pmod{n}$ при $p \equiv 1 \pmod 4$ и $p+1 \equiv 0 \pmod{n}$ при $p \equiv -1 \pmod 4$.*

Доказательство. Пусть $p \nmid n$. Рассмотрим возможные ситуации.

Предположим, что $p \equiv -1 \pmod 4$. Тогда по лемме 7.1 и лемме 6.2 имеем

$$\varphi_n(x) \equiv 0 \pmod p \quad \Rightarrow \quad p_n(x) \equiv 0 \pmod p \ \text{ и } \ q_n(x) \not\equiv 0 \pmod p.$$

Пусть $x \equiv \operatorname{tg}_p \alpha \pmod p$ для некоторого геометрического угла α. Тогда из леммы 6.3 следует сравнение $\operatorname{tg}_p n\alpha \equiv 0 \pmod p$, что даёт нам $n\alpha \in \{0, p+1\}$. Пусть m — такое наименьшее натуральное число, что $\operatorname{tg}_p m\alpha \equiv 0 \pmod p$. Это равносильно сравнению $m\alpha \equiv l(p+1) \pmod{2(p+1)}$, где l — некоторое целое число. Ясно, что $m \mid p+1$. Также $m \mid n$, так как $n\alpha \in \{0, p+1\}$, и m — такое наименьшее число, что $m\alpha \equiv l(p+1) \pmod{2(p+1)}$. Допустим, что $m < n$, но тогда $p_m(x) \equiv \equiv 0 \pmod p$. Так как p_m представимо как произведение фундаментальных многочленов, для некоторого $d \mid m$ получим $\varphi_d(x) \equiv 0 \pmod p$, причём $m \mid n$. Так как p_n тоже представимо как произведение фундаментальных многочленов, в котором $\varphi_d(x)$ и $\varphi_n(x)$ имеют общий

корень в поле $\mathbb{Z}_p$, мы получаем, что p_n имеет кратный корень в $\mathbb{Z}_p$. Это приводит к противоречию (см. теорему 1). Поэтому $m = n$ и $n \mid p+1$.

Предположим, что $p \equiv 1 \pmod 4$. Имеем

$$\varphi_n(x) \equiv 0 \pmod p \quad \Rightarrow \quad p_n(x) \equiv 0 \pmod p.$$

Тогда $x \not\equiv \pm j \pmod p$, где j — корень многочлена x^2+1 в $\mathbb{Z}_p$. Если $x \equiv \pm 1 \pmod p$, то $\varphi_4(x) \equiv 0 \pmod p$. Приведём значения многочленов p_n и q_n при $x \equiv \pm 1 \pmod p$:

n		0	1	2	3	4
1	$p_n(1)$	0	1	2	2	0
	$q_n(1)$	1	1	0	-2	-4
-1	$p_n(-1)$	0	-1	-2	-2	0
	$q_n(-1)$	1	1	0	-2	-4

При $n = 4$ получаем значения, которые отличаются от значений в случае $n = 0$ умножением на -4. Так как $p_n(x) \equiv 0 \pmod p$, получаем, что $4 \mid n$. Но тогда $n = 4$: иначе многочлен $p_n(x)$ будет иметь кратный корень, так как $\varphi_n(x) \equiv \varphi_4(x) \equiv 0 \pmod p$. Требуемое утверждение выполняется. Теперь можем считать, что $x \not\equiv \pm 1 \pmod p$ и $x \not\equiv \pm j \pmod p$. Тогда

$$\frac{p_2(x)}{q_2(x)} = \frac{2x}{1-x^2} = \operatorname{tg}_p \alpha$$

для некоторого угла α (конец § 5).

Пусть $n = 2n'$ — чётное число. Мы доказали следующее равенство многочленов:

$$p_n(x) = p_{n'}\left(\frac{p_2(x)}{q_2(x)}\right) q_2(x)^{n'},$$

где $q_2(x) \not\equiv 0 \pmod p$. Отсюда получаем

$$p_{n'}\left(\frac{p_2(x)}{q_2(x)}\right) \equiv 0 \pmod p \quad \Rightarrow \quad \operatorname{tg}_p n'\alpha \equiv 0 \pmod p.$$

Пусть m — порядок угла α. Ясно, что $m \mid (p-1)/2$ и $m \mid n'$. Предположим, что $m < n'$, тогда имеет место равенство

$$p_{2m}(x) = p_m\left(\frac{p_2(x)}{q_2(x)}\right) q_2(x)^m = 0.$$

Однако $2m$ делит n, и поэтому найдётся такое d, что $d \mid n$, $d < n$ и $\varphi_d(x) \equiv \equiv 0 \pmod p$, из чего следует, что $p_n(x)$ имеет кратный корень. Поэтому $m = n' \Rightarrow n \mid p-1$.

Пусть n — нечётное число. Мы уже доказали равенство многочленов

$$p_n\left(\frac{p_2(x)}{q_2(x)}\right)q_2(x)^n = p_{2n}(x) = p_2\left(\frac{p_n(x)}{q_n(x)}\right)q_n(x)^2 = 2p_n(x)q_n(x).$$

Правая часть даёт 0. Поэтому

$$p_n\left(\frac{p_2(x)}{q_2(x)}\right) \equiv 0 \pmod p \quad \Rightarrow \quad \operatorname{tg}_p n\alpha \equiv 0 \pmod p.$$

Пусть m — порядок α. Ясно, что $m \mid (p-1)/2$ и $m \mid n$. Пусть $m < n$. Тогда

$$p_m\left(\frac{p_2(x)}{q_2(x)}\right) \equiv 0 \pmod p.$$

Отсюда следует равенство

$$p_{2m}(x) = p_m\left(\frac{p_2(x)}{q_2(x)}\right)q_2(x)^m = 0.$$

Кроме того, $2m$ делит $2n$. Найдётся такое d, что $d \mid 2m$ и $\varphi_d(x) \equiv 0 \pmod p$, причём $d \neq n$, так как иначе $n \mid 2m \Rightarrow n \mid m \Rightarrow m \geqslant n$. Тогда $p_{2m}(x)$ будет иметь кратный корень, что приводит к противоречию. Следовательно, $n = m \mid (p-1)/2$, из чего получаем $n \mid p-1$. □

Наконец, мы можем доказать следующее утверждение.

Теорема 3. *Для любого натурального k найдётся такое простое p, что $k \mid p+1$.*

Доказательство. Мы можем заменить k на любое его кратное, не теряя общности. Тогда будем считать, что $4 \mid k$ и k не является степенью простого числа. Заметим, что $\varphi_k(0) = 1$. Следовательно, $4 \mid x$. Отсюда получаем сравнение $\varphi_k(x) \equiv 1 \pmod 4$.

Пусть $k = 4k'$. Так как старший коэффициент многочлена $\varphi_k(x)$ равен 1, на интервале от его наибольшего корня до $+\infty$ выполнено неравенство $\varphi_k(x) \geqslant 0$. Поэтому между двумя наибольшими корнями имеем $\varphi_k(x) < 0$. Отметим, что $(2k'-1, 4k') = 1$, поэтому

$$\operatorname{tg}\frac{\pi}{4k'}(2k'-1) = \frac{1}{\operatorname{tg}(\pi/(4k'))}$$

будет максимальным корнем, а значение второго по величине корня будет не больше

$$\operatorname{tg}\frac{\pi}{4k'}(2k'-2) = \frac{1}{\operatorname{tg}(2\pi/(4k'))}.$$

Пусть $\alpha = \pi/(4k')$. Тогда длина интервала между двумя наибольшими корнями будет не меньше

$$\frac{1}{\operatorname{tg}\alpha} - \frac{1}{\operatorname{tg}2\alpha} = \frac{1}{\operatorname{tg}\alpha} - \frac{1-\operatorname{tg}^2\alpha}{2\operatorname{tg}\alpha} \geqslant \frac{1}{\operatorname{tg}\alpha} - \frac{1}{2\operatorname{tg}\alpha} = \frac{1}{2\operatorname{tg}\alpha}.$$

Отметим, что $\operatorname{tg}\alpha \leqslant 1$ для нашего k. Обозначим текущее значение числа k через k_0. Посмотрим, как изменится наше рассуждение, если бы вместо k_0 была его степень k_0^t: в этом случае мы бы получили интервал длины не меньше $1/(2\operatorname{tg}(\pi/k_0^t))$. Так как $\operatorname{tg}\alpha \to 0$ при $\alpha \to 0$, найдётся такое t, что на нашем интервале мы найдём целое x, делящееся на k_0. Тогда для него $-\varphi_{k_0^t}(x)$ — натуральное число, и верны сравнения

$$-\varphi_{k_0^t}(x) \equiv -\varphi_{k_0^t}(0) \equiv -1 \pmod{k_0}.$$

Отсюда $-\varphi_{k_0^t}(x) \equiv 3 \pmod 4$ и $(-\varphi_{k_0^t}(x), k_0) = 1$. Поэтому среди простых делителей числа $-\varphi_{k_0^t}(x)$ найдётся такое p, что $p \equiv 3 \pmod 4$, p взаимно просто с k_0^t, и тогда $k \mid p+1$ по теореме 2. □

Следствие 1. *Для любого натурального k имеется бесконечно много простых вида $kn-1$.*

Доказательство. Предположим противное. По теореме 1 множество, состоящее из простых чисел требуемого вида, непусто. Тогда обозначим через p' наибольшее простое вида $p' = n'k - 1$. Согласно теореме 1 найдётся такое простое p, что $p+1$ кратно $k(n'+1)$. Поэтому существует натуральное m, для которого $p = k(n'+1)m - 1$. Так как $p > p'$, мы получаем противоречие. □

Мы уже знаем, что $p_n(x)$ можно разложить в произведение фундаментальных многочленов. Однако можно ли провести дальнейшее разложение многочлена $p_n(x)$, оставаясь в $\mathbb{Z}[x]$? Ответ на этот вопрос даёт

Лемма 7.5. *При $\nu_2(n) \leqslant 1$ многочлен $\varphi_n(x)$ неприводим над кольцом $\mathbb{Z}$. При $\nu_2(n) \geqslant 2$ многочлен $\varphi_n(x)$ представляется в виде произведения двух приведённых неприводимых многочленов, принадлежащих $\mathbb{Z}[x]$, и константы A следующим образом*:

$$\varphi_n(x) = A \prod_{\substack{k=0\\(k,n)=1\\s(k)=+1}}^{n-1} \Big(x - \operatorname{tg}\frac{\pi}{n}k\Big) \prod_{\substack{k=0\\(k,n)=1\\s(k)=-1}}^{n-1} \Big(x - \operatorname{tg}\frac{\pi}{n}k\Big),$$

где константа A равна старшему коэффициенту многочлена $\varphi_n(x)$.

Доказательство. Рассмотрим расширение $\mathbb{Q}\Big(\operatorname{tg}\frac{\pi}{n}k\Big)$, где $\operatorname{tg}\frac{\pi}{n}k$ — один из корней многочлена $\varphi_n(x)$. Мы можем подставить $\operatorname{tg}\frac{\pi}{n}k$ в формулу $p_r(x)/q_r(x)$, и тогда если $\operatorname{tg}\frac{\pi}{n}t$ определено, то оно принадлежит $\mathbb{Q}\Big(\operatorname{tg}\frac{\pi}{n}k\Big)$. Через $\operatorname{tg}\frac{\pi}{n}t$ можно выразить $\sin\frac{2\pi}{n}t$ и $\cos\frac{2\pi}{n}t$. Заметим,

что $\sin\frac{2\pi}{n}\frac{ln}{2}$ и $\cos\frac{2\pi}{n}\frac{ln}{2}$ принадлежат $\mathbb{Q}$ для любого $l \in \mathbb{Z}$. Поэтому при всех $t \in \mathbb{Z}$ числа $\sin\frac{2\pi}{n}t$ и $\cos\frac{2\pi}{n}t$ входят в $\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right)$.

Расширим поле $\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right)$ до поля $\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right)(i)$. Заметим, что

$$\dim_{\mathbb{Q}} \mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right)(i) = \dim_{\mathbb{Q}} \mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right) \dim_{\mathbb{Q}(\operatorname{tg}\frac{\pi}{n}k)} \mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right)(i) = \\ = 2\dim_{\mathbb{Q}} \mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right),$$

где $\dim_K L$ — размерность поля L над его подполем K. Также заметим, что $\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k, i\right)$ содержит все корни из единицы

$$e^{i2\pi t/n} = \cos\frac{2\pi}{n}t + i\sin\frac{2\pi}{n}t.$$

Пересечение $\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k, i\right)$ и множества корней из единицы содержит все корни 4-й степени из единицы, т. е. $\pm 1, \pm i$, и все корни n-й степени из единицы. Если в $\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k, i\right)$ перемножить два корня из единицы, мы снова получим корень из единицы. Поэтому в нашем расширении все корни из единицы будут иметь порядок $[n, 4]$, и тогда размерность этого расширения будет делиться на $\varphi([n, 4])$, так как, обозначив $[n, 4]$ через m, имеем

$$\dim_{\mathbb{Q}} \mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right)(i) = \dim_{\mathbb{Q}(e^{2\pi i/m})} \mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right)(i) \dim_{\mathbb{Q}} \mathbb{Q}(e^{2\pi i/m}) = \\ = \dim_{\mathbb{Q}(e^{2\pi i/m})} \mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right)(i)\varphi(m).$$

Отсюда

$$\dim_{\mathbb{Q}} \mathbb{Q}(\operatorname{tg}\frac{\pi}{n}k) \geqslant \frac{\varphi([n, 4])}{2}.$$

Поэтому степень минимального многочлена $\operatorname{tg}\frac{\pi}{n}k$ будет не меньше $\frac{1}{2}\varphi([n, 4])$.

Если $\nu_2(n) \leqslant 1$, то $\deg \varphi_n(x) = \varphi(n) = \frac{1}{2}\varphi([n, 4])$, за исключением случая $n = 2$, когда $\operatorname{tg}(\pi/2)$ не определён и $\varphi_2(x) = 2$. Иначе положим $n = 4n'$. Тогда

$$q_{2n'}(x) = q_{n'}^2(x) - p_{n'}^2(x) = (q_{n'}(x) - p_{n'}(x))(q_{n'}(x) + p_{n'}(x)).$$

Мы также знаем, что

$$p_{4n'}(x) = 2p_{2n'}(x)q_{2n'}(x).$$

Ясно, что $\varphi_n(x)$ не входит в разложение многочлена $p_{2n'}(x)$ на фундаментальные многочлены, но присутствует в разложении многочлена $p_{4n'}(x)$, поэтому

$$\varphi_n(x) \mid 2q_{2n'}(x) = 2(q_{n'}(x) - p_{n'}(x))(q_{n'}(x) + p_{n'}(x)),$$

где под делимостью понимается делимость многочленов в $\mathbb{Z}[x]$. Заметим, что многочлен $q_{n'}(x) - p_{n'}(x)$ не имеет общих корней с $q_{n'}(x)$, поэтому его корни соответствуют $1 = p_{n'}(x)/q_{n'}(x)$; другими словами, $\operatorname{tg}(n' \operatorname{arctg} x) = 1$, но тогда все его корни — это числа вида $\operatorname{tg} \frac{\pi}{4n'}k$, где k нечётно и $s(k) = +1$. Аналогично все корни многочлена $q_{n'}(x) + p_{n'}(x)$ — числа вида $\operatorname{tg} \frac{\pi}{4n'}k$, где k нечётно и $s(k) = -1$. Понятно, что

$$q_{n'}(x) + p_{n'}(x), q_{n'}(x) - p_{n'}(x) \in \mathbb{Z}[x].$$

Рассмотрим разложение $\varphi_n(x)$ на неприводимые многочлены над $\mathbb{Z}[x]$. Так как $\varphi_n(x) \mid 2(q_{n'}(x) - p_{n'}(x))(q_{n'}(x) + p_{n'}(x))$, каждый неприводимый множитель в этом разложении будет иметь корни вида $\operatorname{tg} \frac{\pi}{4n'}k$, где $2 \nmid k$, и либо все они имеют $s(k) = 1$, либо $s(k) = -1$. Тогда $\varphi_n(x)$ представим как произведение хотя бы двух многочленов. Так как степень минимального многочлена $\operatorname{tg} \frac{\pi}{n}k$, где $(k, n) = 1$, должна быть хотя бы $\frac{1}{2}\varphi(n)$, мы заключаем, что $\varphi_n(x)$ представим в виде произведения ровно двух многочленов степени $\frac{1}{2}\varphi(n)$. Также если n — степень двойки, то $c(\varphi_n(x)) = 2$, и мы можем представить $\varphi_n(x)$ как $\pm 2\left(\frac{1}{\pm 2}\varphi_n(x)\right)$, где $\frac{1}{\pm 2}\varphi_n(x) \in \mathbb{Z}[x]$. Старший коэффициент многочлена $\frac{1}{\pm 2}\varphi_n(x)$ равен 1 (знак зависит от того, равно ли число n четырём). Отсюда следует требуемое. □

Приложение

§ 1. Другой подход к вопросу о несоизмеримости углов

Результаты о несоизмеримости углов (с. 74–77) могут быть получены другим способом. Известно, что размерность $\mathbb{Q}(e^{(2\pi i/n)+m})$ над полем $\mathbb{Q}$ равна $\varphi(n)$, где m и n взаимно просты. Заметим, что если n имеет ровно k простых делителей $p_1, \ldots, p_k$, то верно неравенство

$$\varphi(n) = n \cdot \prod_{i=1}^{k} \frac{p_i - 1}{p_i} \geqslant n \cdot \prod_{i=2}^{k+1} \frac{i-1}{i} = \frac{n}{k+1} \geqslant \frac{n}{\log_2 n + 1}.$$

Поэтому для всякого M существует такое N, что $\varphi(n) > M$ при $n > N$. Тогда пересечение любого конечного расширения поля $\mathbb{Q}$ и множества $\{e^{i2\pi\theta} \mid \theta \in \mathbb{Q}\}$ образует группу по умножению. Она конечна: иначе найдётся элемент l, для которого значение $\varphi(l)$ превосходит размерность

расширения. Обозначим эту группу через G. Для любого элемента $z \in G$ верно равенство $z^{|G|} = 1$, из чего получаем, что G состоит из корней уравнения $z^{|G|} = 1$. Тогда $\varphi(|G|)$ делит размерность расширения.

Если мы рассмотрим пересечение $\mathbb{Q}(i)$ и $\{e^{i2\pi\theta} \mid \theta \in \mathbb{Q}\}$, то получим, что 4 делит $|G|$, так как подмножество $\{1, i, -1, -i\} \subseteq G$ образует подгруппу из четырёх элементов. В то же время $\varphi(|G|) \leqslant 2$, из чего следует $|G| = 4$.

Если рассматриваемое расширение есть $\mathbb{Q}(e^{2\pi i/n})$ при $2 \mid n$, то $n \mid |G|$, и в то же время $\varphi(|G|) \leqslant \varphi(n)$. Так как $2 \mid n$, значение $\varphi(nt)$ не превосходит $\varphi(n)$ лишь при $t = 1$. Поэтому G состоит из чисел вида $\{e^{i2\pi k/n} \mid k \in \mathbb{Z}\}$. Это можно применить к расширениям

$$\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(e^{2\pi i/8}) \quad \text{и} \quad \mathbb{Q}(i, \sqrt{3}) = \mathbb{Q}(e^{2\pi i/12}).$$

§ 2. Быстрое преобразование Фурье

Быстрое преобразование Фурье (FFT) рассматривается в статье М. Я. Кельберта [1]. Известно, что существует обобщение дискретного преобразования Фурье для случая конечных полей. Рассмотрим это обобщение. Пусть $p \equiv 3 \pmod 4$.

Ортогональный базис. Наличие корней из единицы позволяет построить базис в пространстве функций, действующих из $\mathbb{Z}/(p+1)\mathbb{Z}$ в $\mathbb{Z}_p(i)$. Определим билинейное отображение, действующее на функциях f и g, следующим образом:

$$\langle f, g \rangle = \sum_{k=0}^{p} f(k) g(-k). \tag{1}$$

В качестве базиса рассмотрим набор функций вида $f_z(k) = z^k$, где через z обозначен один из корней уравнения $z^{p+1} - 1$: для любой пары корней z_1 и z_2 имеем

$$\langle f_{z_1}, f_{z_2} \rangle = \sum_{k=0}^{p} (z_1 z_2^{-1})^k.$$

Если $z_1 \neq z_2$, то $\langle f_{z_1}, f_{z_2} \rangle = 0$, иначе получим $p + 1 \equiv 1 \pmod p$. Если существует линейная комбинация наших функций, дающая 0, в которой при некотором f_z стоит ненулевой коэффициент, то применение к ней и к $f(z)$ билинейного отображения (1) дает 0, так как $\langle 0, f_z \rangle = 0$. С другой стороны, мы получим ненулевой коэффициент перед f_z, что противоречит выбору линейной комбинации.

FFT. Мы можем рассмотреть аналоги FFT по модулю простого числа, включая многомерные преобразования Фурье. Интерес могут представлять случаи простых чисел Мерсенна, например, числа $2^{19}-1$ и $2^{31}-1$. Если $p=2^q-1$, то существует алгоритм для преобразования Фурье, который использует корни уравнения $z^{2^t}=1$, $t \leqslant q$, $t \in \mathbb{N}$, принадлежащие $\mathbb{Z}_p(i)$. Отметим, что в этом случае можно найти корень из единицы порядка 2^q: произвольно выбранный корень из единицы с вероятностью $1/2$ окажется корнем порядка 2^q. При достаточном количестве повторений этой операции вероятность получить корень порядка 2^q стремится к 1. Кроме того, если размерности рассматриваемых объектов (многочленов, матриц и т. д.) достаточно малы, то можно сначала применить преобразование Фурье по модулю $2^{19}-1$ и по модулю $2^{31}-1$, а затем восстановить числа по двум остаткам. Стоит отметить, что возможны более эффективные реализации операции взятия остатка по модулю простых чисел данного вида, так как модуль имеет вид 2^q-1.

Заключение

Нами были рассмотрены аналоги углов и тригонометрических функций в $\mathbb{Z}_p$. В дальнейшем можно попробовать ввести гиперболические углы, для которых, вероятно, мощность группы решений будет равна $p-1$ в обоих случаях. Далее можно попытаться задать аналоги гиперболических функций sinh, cosh, tanh.

Благодарности

Автор признателен А. Я. Канель-Белову за помощь в работе над статьёй.

Список литературы

[1] *Кельберт М. Я.* Что такое преобразование Фурье? // Математическое просвещение. Сер. 3. Вып. 4. М.: МЦНМО, 2000. С. 188–202. `http://mi.mathnet.ru/mp66`

Абдуламин Русланович Исмаилов, студент матфака ВШЭ
`nameundefinednamovich@gmail.com`

Обманчивая простота

В. М. Журавлёв, П. И. Самовол

Говорят, истина лежит между двумя противоположными мнениями. Неверно! Между ними лежит проблема.

Иоганн Вольфганг Гёте

Стоящие с семнадцатого века вопросы построения больших простых чисел, проверки на простоту и разложения чисел на сомножители ставят теперь новые и конкретные проблемы. Насколько могут быть быстрыми алгоритмы нахождения ответов на эти вопросы? Проблема проверки на простоту уже решена. Две другие проблемы ещё не получили своего теоретического решения. Тем не менее, первая из них кажется более простой, чем другая.

Ю. И. Манин, А. А. Панчишкин. Введение в современную теорию чисел

§ 1. Красивые не простые степени

В 1986 году была издана книга [13], авторы которой Б. А. Кордемский и А. А. Ахадов в предисловии отмечают: «Некоторые из предлагаемых авторами задач близки по форме и содержанию задачам школьных учебников. Другие — по трудности на ступеньку выше, оставаясь всё же в границах доступности для учащихся VIII–X классов и всех, окончивших школу. Но те и другие задачи нацелены на проникновение разумом в удивительный мир чисел, на раскопку его богатств, на возбуждение математической любознательности и собственной инициативы». Книга была красочно иллюстрирована и рассчитана на учащихся.

Обратим внимание на одну из задач.

Задача 1 (Красивые не простые степени, [13, с. 82, 86.]).
1) Докажите, что $7777^{2222} + 2222^{7777}$ делится на 9.
2) Докажите, что $2222^{2222} + 4444^{4444} + 8888^{8888}$ делится на 3.
3) Докажите, что сумма $2^{2145} + 3^{2145}$ делится на 241, на 341 и на 11.

Первому пункту задачи даже посвящена иллюстрация книги (рис. 1).

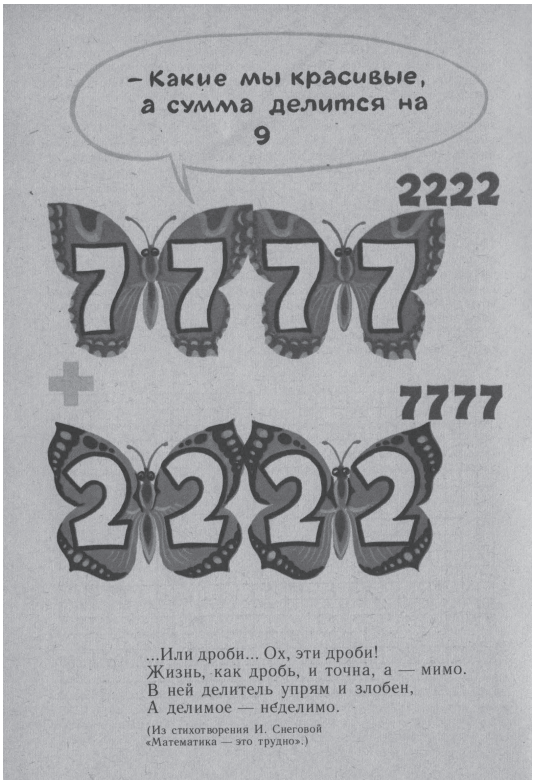


Рис. 1. Иллюстрация из книги [13]

Поскольку числа 2222 и 7777 делятся на 1111, понятно, что сумма $7777^{2222} + 2222^{7777}$ делится на 1111. Идея в том, чтобы показать ученику, что так сконструированные числа могут иметь другие делители. Заинтересовать учащегося поиском закономерностей, не лежащих на поверхности.

Напомним формулы сокращённого умножения, изучаемые в школе:

$$A^n - B^n = (A-B)(A^{n-1} + A^{n-2}B + \ldots + AB^{n-2} + B^{n-1}) \quad \text{для} \quad n \in \mathbb{N},$$
$$A^{2k+1} + B^{2k+1} = (A+B)(A^{2k} - A^{2k-1}B + \ldots - AB^{2k-1} + B^{2k}) \quad \text{для} \quad k \in \mathbb{N}.$$

Если учащийся знает эти формулы, то, применив приём «прибавить—отнять», он решит задачу в пару строчек. Действительно, прибавим и отнимем единицу, получим

$$7777^{2222} + 2222^{7777} = (7777^{2222} - 1^{2222}) + (2222^{7777} + 1^{7777}).$$

Первая скобка делится на 7776 и, следовательно, на 9, а вторая скобка делится на 2223, т. е. тоже делится на 9. Значит, сумма делится на 9.

Похожие задачи мы можем найти в разных источниках (см., например, [9, 16, 23]).

Задача 2.

1) [23, с. 20, задача 63]. Докажите, что $2222^{5555} + 5555^{2222}$ делится на 7.

2) [9, с. 140, задача 11.56]. Докажите, что число $222^{555} + 555^{222}$ составное.

3) [16, с. 85, задача 4г]. Число $30^{239} + 239^{30}$ составное.

Пункт 2 можно усложнить: докажите, что сумма из п. 2 делится на 7.

В книгах, рассчитанных на педагогов, мы видим более строгие формулировки похожих задач.

Задача 3 [21, с. 8, задача 3]. Докажите равенства:

а) $19^{71} + 71^{19} = 360m + 90$;

б) $19^{77} + 77^{19} = 456n + 96$.

Задача 4 [16, с. 85, задача 4в]. Если p и q — различные простые числа, то $p^q + q^p \equiv p + q \pmod{pq}$.

В книге [23], ставшей классикой литературы для математических кружков, отметим ещё одну задачу.

Задача 5 [23, с. 21, задача 70]. При каких натуральных n сумма $5^n + n^5$ делится на 13? Каково наименьшее n, удовлетворяющее этому условию?

В § 3 мы вернёмся к этой задаче.

В приведённых примерах рассматриваются суммы вида $a^n + n^a$, где $a, n \in \mathbb{N}$. В зависимости от пары a, n такая сумма может быть как составным, так и простым числом.

Исключим из рассмотрения простейшие случаи, когда $a = 1$ или $n = 1$. Очевидно, что если числа a и n имеют общий делитель d, то сумма будет делиться на d и, следовательно, будет составным числом. Такие примеры мы видели выше.

Чтобы задача выглядела более содержательной, числа a и n будем считать взаимно простыми, т. е. НОД$(a, n) = 1$. Минимальный пример,

когда сумма является простым числом, мы получим для пары $a = 2$ и $n = 3$, тогда $2^3 + 3^2 = 17$ — простое число. (В силу симметрии, пара $a = 3$, $n = 2$ даёт то же простое число 17.)

Нас будут интересовать два вопроса.

1) Есть ли другие примеры таких пар $2 \leqslant a$ и $2 \leqslant n$, что сумма $a^n + n^a$ является простым числом?

2) Если сумма $a^n + n^a$ является составным числом, где a и n — взаимно простые числа, то какие делители она имеет?

§ 2. Олимпиадные задачи и теорема Софи Жермен

Наши изыскания начнём со случая $a = 4$. Пусть читатели нас не осуждают за перепрыгивание случаев $a = 2$ и $a = 3$, мы вернёмся к ним чуть позже.

Для начала докажем одну теорему, носящую имя Софи Жермен (Marie-Sophie Germain). Софи Жермен переписывалась со многими математиками своего времени, в том числе с Гауссом, Даламбером, Лагранжем, Фурье. Она становится первой женщиной, получившей право участия в заседаниях Парижской Академии наук. Подробности биографии Софи Жермен можно прочесть в [10].

Теорема 1 (Софи Жермен, [9, с. 139, задача 11.51а]). *Число n^4+4 — составное при всех натуральных $n \neq 1$.*

Доказательство. Применим упоминавшийся нами искусственный приём: добавим и вычтем $4n^2$. Имеем

$$n^4 + 4 = n^4 + 4n^2 + 4 - 4n^2 = (n^2 + 2)^2 - (2n)^2 = (n^2 + 2n + 2)(n^2 - 2n + 2).$$

Так как $n > 1$, получаем, что

$$n^2 - 2n + 2 = (n - 1)^2 + 1 > 1.$$

Число $n^4 + 4$ представимо в виде произведения двух множителей, не равных ему самому и единице, следовательно, это число составное. Что и требовалось доказать. □

Изящество и простота доказательства не могут не вызвать восхищения. Эта идея в завуалированном виде возникает в олимпиадных задачах.

Задача 6 (олимпиада Чехословакии, 1973, [12, с. 12, задача 1.9]). Докажите, что существует бесконечно много значений $n \in \mathbb{N}$, для которых любое число вида $m^4 + n$ ($m \in \mathbb{N}$) является составным.

Задача 7 (XV Всероссийская олимпиада, 1989, [25], [9, с. 142, задача 11.92]). Докажите, что число $4^{545} + 545^4$ является составным.

Задача 7 является частным случаем задачи, предлагавшейся на венгерской математической олимпиаде 1977 года.

Задача 8 (олимпиада Венгрии, 1977, [12, с. 15, задача 2.17]). Докажите, что для любого простого числа $p > 5$ уравнение $x^4 + 4^x = p$ в целых числах не имеет решений.

В формулировке задачи область допустимых значений переменной x — целые числа. Однако понятно, что её расширение с натуральных чисел до целых ничего нового нам не даёт.

Действительно, если $x < 0$, то $x^4 + 4^x$ — не целое. При $x = 0$ имеем $x^4 + 4^x = 1$. А, как известно, единица не является ни составным, ни простым числом.

Решение задачи 8. Учитывая вышесказанное, нам осталось рассмотреть случай, когда x — натуральное число. При $x = 1$ имеем $x^4 + 4^x = 5$, но по условию $p > 5$. Итак, остаётся $x \in \mathbb{N}$, $x \geqslant 2$. Докажем, что в этом случае $x^4 + 4^x$ является составным числом.

Если $x = 2k$, где $k \in \mathbb{N}$, то $x^4 + 4^x = 2^4k^4 + 4^{2k}$ делится на 16, следовательно, не является простым.

Если $x = 2k + 1$, где $k \in \mathbb{N}$, то применим формулы сокращённого умножения для разложения на множители. Имеем

$$\begin{aligned} x^4 + 4^x &= x^4 + 4^{2k+1} = x^4 + (2^{2k+1})^2 = \\ &= x^4 + 2 \cdot 2^{2k+1}x^2 + (2^{2k+1})^2 - 2 \cdot 2^{2k+1}x^2 = \\ &= (x^2 + 2^{2k+1})^2 - (2^{k+1}x)^2 = \\ &= (x^2 + 2^{2k+1} + 2^{k+1}x)(x^2 + 2^{2k+1} - 2^{k+1}x) = \\ &= ((x + 2^k)^2 + 2^{2k})((x - 2^k)^2 + 2^{2k}). \end{aligned}$$

Поскольку каждый из сомножителей больше 1, исходное выражение является составным числом. Что и требовалось доказать. □

Хотя решение задач занимает пару абзацев, они предлагались на соревнованиях достаточно высокого уровня.

Упражнение 1 [9, с. 139, задача 11.51б]. Число $n^4 + 4m^4$ — составное при всех натуральных n и m, одновременно не равных 1.

Итак, случай $a = 4$ полностью разобран. Сумма $4^n + n^4$ является составным числом для любого натурального $n \geqslant 2$.

Вернёмся теперь к решению задачи 5.

§ 3. Случай $5^n + n^5$

В книге [23] решение задачи 5 занимает несколько страниц. Идея решения состоит в вычислении остатков каждого из слагаемых при делении на 13. Для удобства эти остатки вносятся в таблицу. После этого становится видна некоторая периодическая закономерность.

Посмотрим на это решение, опуская детали.

Решение задачи 5. Рассмотрим последовательность $\{n^5\}$, $n = 0, 1, 2, \ldots$ Сопоставим этой последовательности другую последовательность $\{r'_n\}$, где r'_n — остаток от деления n^5 на 13. Таким образом, последовательности 0, 1, 32, 243, 1024, 3125, … мы сопоставили последовательность 0, 1, 6, 9, 10, 5, … Последовательность $\{r'_n\}$ периодична с периодом 13.

Аналогично рассмотрим последовательность $\{5^n\}$, $n = 0, 1, 2, \ldots$, и сопоставим ей последовательность $\{r''_n\}$, где r''_n — остаток от деления 5^n на 13. Теперь последовательности 1, 5, 25, 125, 625, 3125, … мы сопоставили последовательность 1, 5, 12, 8, 1, 5, … Как видим, члены последовательности начали повторяться начиная с пятого. Значит, последовательность $\{r''_n\}$ периодична с периодом 4. Действительно, остаток от деления 5^n на 13 совпадает с остатком от деления $5^{(4k+n)} = 5^n \cdot (5^4)^k$ на 13 для любого целого $k \geqslant 0$, поскольку 5^4 даёт остаток 1 при делении на 13.

Таким образом, последовательность $\{r_n\}$, являющаяся последовательностью остатков от деления суммы $5^n + n^5$ на 13, периодична с периодом $52 = 4 \cdot 13$.

Внесём полученные данные в таблицу 1.

Продолжив нашу таблицу, убедимся, что остаток от деления $5^n + n^5$ на 13 равен нулю только в случаях $n = 52k + 12$, $n = 52k + 14$, $n = 52k + 21$, $n = 52k + 31$, где $k \in \mathbb{Z}$, $k \geqslant 0$.

Наименьшее n, при котором сумма $5^n + n^5$ делится на 13, равно 12. Это также видно из таблицы 1. □

Таблица 1

n	0	1	2	3	4	5	6	7	8	9	10	11	12
n^5	0	1	32	243	1024	3125	7776	16 807	32 768	9^5	10^5	11^5	12^5
r'_n	0	1	6	−4	−3	5	2	−2	−5	3	4	−6	−1
5^n	1	5	25	125	625	3125	15 625	78 125	390 625	5^9	5^{10}	5^{11}	5^{12}
r''_n	1	5	−1	−5	1	5	−1	−5	1	5	−1	−5	1
r_n	1	6	5	4	−2	−3	1	6	−4	−5	3	2	0

Мы специально разобрали это решение, чтобы отметить возникающие закономерности. В дальнейшем мы укажем ряд теорем, упрощающих такие рассуждения.

Сделаем выводы из решения задачи. Во-первых, в последовательности $\{5^n + n^5\}$ бесконечно много чисел, делящихся на 13 (четыре семейства).

Во-вторых, нам ничто не мешало взять другое простое число p и провести аналогичные рассуждения. Мы получили бы другую периодическую последовательность остатков и для каких-то значений n сумма $5^n + n^5$ делилась бы на p.

Упражнение 2. При каких натуральных n сумма $5^n + n^5$ делится на а) 3; б) 7; в) 11? Каково наименьшее n, удовлетворяющее этому условию?

Упражнение 3. Докажите, что для любого простого p существует бесконечно много натуральных n таких, что сумма $5^n + n^5$ делится на p.

Итак, в последовательности $\{5^n + n^5\}$ бесконечно много составных чисел. Но встречаются ли в этой последовательности простые числа?

Если n нечётное, то сумма $5^n + n^5$ делится на 2. Если 5 и n не взаимно простые, то $5^n + n^5$ делится на 5. Поэтому если в последовательности $\{5^n + n^5\}$ есть простые числа, то число n должно иметь вид $n = 2(5k + r)$, где $r = 1, 2, 3, 4$, а k — целое неотрицательное число.

Таблица 2

n	$5^n + n^5$
2	$57 = 3 \cdot 19$
4	$1649 = 17 \cdot 97$
6	$23\,401 = 7 \cdot 3343$
8	$423\,393 = 3 \cdot 141\,131$
12	$244\,389\,457 = 13 \cdot 19 \cdot 463 \cdot 2137$
14	$6\,104\,053\,449 = 3^2 \cdot 13 \cdot 19 \cdot 2\,745\,863$
16	$152\,588\,939\,201 = 17^2 \cdot 4513 \cdot 116\,993$
18	$3\,814\,699\,155\,193 = 19 \cdot 3121 \cdot 64\,329\,907$
22	$2\,384\,185\,796\,169\,257 = 23 \cdot 4999 \cdot 20\,736\,197\,641$
24	$59\,604\,644\,783\,353\,249$ (простое)
26	$1\,490\,116\,119\,396\,647\,001 = 3 \cdot 7 \cdot 17 \cdot 31 \cdot 1283 \cdot 104\,945\,433\,641$
28	$37\,252\,902\,984\,636\,350\,993 = 29 \cdot 1303 \cdot 985\,865\,588\,287\,939$

Используя онлайн-калькулятор [27], удаётся провести вычисления вплоть до $n \leqslant 90$. Часть вычислений мы внесли в таблицу 2.

Значения $n = 12$ и $n = 14$ дают составные числа, которые делятся на 13, что согласуется с решением задачи 5.

Пара $a = 5$, $n = 24$ даёт 17-значное простое число

$$5^{24} + 24^5 = 59\,604\,644\,783\,353\,249.$$

Отметим, что определить простоту 17-значного числа в начале XX века было не просто, а во времена Ферма и Эйлера практически невозможно. Напомним, что Ферма думал, что число

$$F_5 = 2^{2^5} + 1 = 4\,294\,967\,297$$

— простое[1]. Эйлер опроверг это утверждение в 1732 году, найдя разложение на простые сомножители

$$2^{2^5} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417.$$

Но развитие вычислительных машин и методов позволяет сейчас это сделать в течение нескольких минут.

Существуют ли в последовательности $\{5^n + n^5\}$ простые числа при $n > 90$?

Приоткроем карты: нам известно ещё одно простое число в этой последовательности — это $5^{1036} + 1036^5$. В этом числе 725 десятичных знаков.

Подождём с комментариями, а сейчас самое время рассмотреть другие значения a.

§ 4. Случай $2^n + n^2$

Следующую задачу можно найти в задачнике «Кванта» [11] и в более поздних изданиях, например в книге [1].

Задача 9 (С. Майзус, [11, М663]). Найдите все простые числа p, для которых число $2^p + p^2$ тоже простое.

Отметим, что в условии задачи 8 число x было целым (как мы выяснили, даже натуральным), а в условии задачи 9 появляется ограничение простотой показателя. Зачем же автор задачи ввёл такое ограничение?

При $p = 2$ получаем составное число 8. При $p = 3$ — простое число 17. Остаётся рассмотреть случай $p > 3$. Докажем более сильное утверждение, из которого будет следовать ответ к задаче 9.

[1] Числа вида $F_n = 2^{2^n} + 1$, где $n \geqslant 0$, называются числами Ферма.

Задача 10. Если натуральное число $n > 3$ не делится на 3, то число $2^n + n^2$ — составное.

Решение. Если n — чётное число, то сумма $2^n + n^2$ делится на 4 и, следовательно, является составным числом.

Пусть теперь n — нечётное число и НОД$(3, n) = 1$. Применим приём, который мы использовали при решении задачи 1:

$$2^n + n^2 = (2^n + 1) + (n^2 - 1) = (2+1)(2^{n-1} - 2^{n-2} + \ldots + 1) + (n-1)(n+1).$$

Слагаемое $2^n + 1 = (2+1)(2^{n-1} - 2^{n-2} + \ldots + 1)$ делится на 3. Поскольку n не делится на 3, получаем, что $n^2 - 1 = (n+1)(n-1)$ делится на 3. Поскольку оба слагаемых делятся на 3, их сумма делится на 3. Значит, число $2^n + n^2$ — составное. □

Упражнение 4. При каких натуральных n сумма $2^n + n^2$ делится на а) 5; б) 11?

Упражнение 5. а) Докажите, что сумма $2^n + n^2$ не делится на 7 ни для какого натурального n.

б) Докажите, что существует бесконечно много простых чисел p таких, что сумма $2^n + n^2$ не делится на p ни для какого натурального n.

(*Указание*. Примените теорему Дирихле о простых числах в арифметических прогрессиях.)

Сравните с условием упражнения 3.

Резюмируем сказанное. Если число p простое, то число $2^p + p^2$ простое только при $p = 3$. Если n — чётное число или НОД$(3, n) = 1$, то сумма $2^n + n^2$ является составным числом.

Для удобства введём обозначение $\delta_n = 2^n + n^2$. Итак, если мы хотим в последовательности $\{\delta_n\} = \{2^n + n^2\}$ найти ещё простые числа, то мы должны рассмотреть случай $n = 3(2k+1) = 6k+3$, где $k \in \mathbb{N}$.

Уже при $k = 1$ мы находим, что $\delta_9 = 2^9 + 9^2 = 593$ — простое число.

Используя онлайн-калькулятор, удаётся провести вычисления для $1 \leqslant k \leqslant 42$. Частичные результаты вычислений для $1 \leqslant k \leqslant 24$ приведены в таблице 3. Мы находим простые числа при $k = 2$, $k = 3$, $k = 5$, т. е. при $n = 15$, $n = 21$, $n = 33$ соответственно.

Полученные результаты удобно занести в таблицу 3.

Существуют ли среди чисел вида $2^n + n^2$ простые при $n > 255$?

Чтобы ответить на этот вопрос, нам пришлось отказаться от онлайн-калькулятора.

Студент 2 курса университета Тель-Авива Джонатан Хашпер (Jonathan Khashper) написал небольшую программу и провёл вычисления на домашнем компьютере. Он нашёл три следующих простых числа.

Таблица 3

k	n	$2^n + n^2 = 2^{3(2k+1)} + (3(2k+1))^2$
1	9	593 (простое)
2	15	32 993 (простое)
3	21	2 097 593 (простое)
4	27	$134\,218\,457 = 73 \cdot 521 \cdot 3529$
5	33	8 589 935 681 (простое)
6	39	$549\,755\,815\,409 = 17 \cdot 43 \cdot 752\,059\,939$
7	45	$35\,184\,372\,090\,857 = 11 \cdot 17 \cdot 5689 \cdot 33\,072\,899$
8	51	$2\,251\,799\,813\,687\,849 = 83 \cdot 1979 \cdot 79\,691 \cdot 172\,027$
9	57	$144\,115\,188\,075\,859\,121 = 11 \cdot 137 \cdot 179 \cdot 221\,587 \cdot 2\,411\,011$
10	63	$9\,223\,372\,036\,854\,779\,777 = 17 \cdot 41 \cdot 13\,232\,958\,445\,989\,641$
11	69	$590\,295\,810\,358\,705\,656\,473 = 857 \cdot 688\,793\,244\,292\,538\,689$
12	75	$37\,778\,931\,862\,957\,161\,715\,193 = 71\,329 \cdot 11\,594\,347 \cdot 45\,681\,172\,811$
13	81	$2\,417\,851\,639\,229\,258\,349\,418\,913 = 59 \cdot 67 \cdot 307 \cdot 604\,681\,729 \cdot 3\,294\,864\,907$
14	87	$154\,742\,504\,910\,672\,534\,362\,398\,097 = 19 \cdot 151\,163 \cdot 53\,877\,882\,575\,230\,758\,001$
15	93	$9\,903\,520\,314\,283\,042\,199\,193\,002\,441 = 11 \cdot 3067 \cdot 293\,550\,710\,326\,438\,100\,577\,793$
16	99	$633\,825\,300\,114\,114\,700\,748\,351\,612\,489 = 17 \cdot 1049 \cdot 35\,542\,269\,955\,370\,083\,594\,928\,033$
17	105	$40\,564\,819\,207\,303\,340\,847\,894\,502\,583\,057 = 4\,561\,633 \cdot 8\,892\,609\,117\,678\,546\,443\,322\,929$
18	111	$2\,596\,148\,429\,267\,413\,814\,265\,248\,164\,622\,369 = 2\,940\,725\,100\,673 \cdot 882\,825\,949\,516\,080\,897\,953$
19	117	$166\,153\,499\,473\,114\,484\,112\,975\,882\,535\,056\,761 = 193 \cdot 860\,898\,961\,000\,593\,181\,932\,517\,526\,088\,377$
20	123	$10\,633\,823\,966\,279\,326\,983\,230\,456\,482\,242\,771\,737 = 1867 \cdot 5\,695\,674\,325\,805\,745\,572\,164\,143\,804\,093\,611$

При $n = 2007$ это $\delta_{2007} = 2^{2007} + 2007^2$ из 605 цифр! Не станем приводить здесь десятичную запись этого числа.

При $n = 2127$ это простое число $\delta_{2127} = 2^{2127} + 2127^2$ из 642 цифр!

При $n = 3759$ это простое число $\delta_{3759} = 2^{3759} + 3759^2$ из 1133 цифр!

В этом месте мы должны перевести дыхание.

Посмотрим на сайте [28] последовательность под номером A061119, т. е. последовательность простых чисел, представимых в виде $2^n + n^2$. Мы видим, что 19 июля 2017 года Харви Дэйл (Harvey P. Dale) нашёл вышеуказанное 605-значное число. Таким образом, 10 апреля 2021 года мог бы быть поставлен новый рекорд: найдены простые числа вида $2^n + n^2$ из 642 и 1133 цифр! К сожалению, в другой последовательности под номером A064539 мы находим оба показателя 2127 и 3759, а также показатели 29 355, 34 653, 57 285, 99 069. Эти результаты были получены Хьюго Пфертнером 14 ноября 2019 года с использованием программы тестирования на простоту Primeform GW (PFGW).

Мы не можем утверждать, конечное или бесконечное количество простых чисел имеется в последовательности $\{\delta_n\} = \{2^n + n^2\}$. Однако отыскание таких многозначных чисел говорит в пользу того, что в этой последовательности будут ещё встречаться простые числа[2)]. Почему мы это предполагаем? Самое время обратиться к истории.

§ 5. Простые числа Мерсенна

Немного отойдём от нашей «красивой» последовательности $\{2^n+n^2\}$ и посмотрим на другую очень известную последовательность $\{2^n - 1\}$.

Упражнение 6. Если число n составное, то число $2^n - 1$ также составное.

Следовательно, если число $2^n - 1$ простое, то n также простое. Исходя из этого, в последовательности $\{2^n - 1\}$ рассматривается подпоследовательность $\{M_p\} = \{2^p - 1\}$ с простым показателем p. Числа $M_p = 2^p - 1$ называются числами Мерсенна в честь монаха Марена Мерсенна (Marin Mersenne). Он был членом монашеского ордена минимов и сыграл выдающуюся роль как организатор науки своего времени. Он вёл переписку с П. Ферма, Р. Декартом, Б. Паскалем, Х. Гюйгенсом, Дж. Валлисом и другими выдающимися учёными.

Не для каждого простого p число $M_p = 2^p - 1$ будет простым. Например при $p = 11$ получаем $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ — составное число.

[2)] Это неизвестно и для более простых выражений, например, n^2+1 (4-я задача Э. Ландау `https://en.wikipedia.org/wiki/Landau%27s_problems`).

Последовательность простых чисел Мерсенна начинается так (см. [28, A000 668]):

$$3,\ 7,\ 31,\ 127,\ 8191,\ 131\,071,\ 524\,287,$$
$$2\,147\,483\,647,\ 2\,305\,843\,009\,213\,693951,\ \ldots$$

Показатели p простых чисел Мерсенна образуют последовательность (см. [28, A000043])

$$2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 61,\ 89,\ 107,\ 127,\ 521,\ 607,\ \ldots$$

Не обязательно проверять все простые нечётные p, поскольку некоторые числа Мерсенна специального вида всегда являются составными, что вытекает, например, из следующей доказанной Эйлером теоремы:

Теорема 2 (Эйлер). *Пусть числа $p = 4n + 3$ и $q = 2p + 1 = 8n + 7$ — простые*[3]. *Тогда $M_p \equiv 0 \pmod q$.*

Существует эффективный алгоритм проверки чисел Мерсенна на простоту — *критерий Люка* (тест Люка — Лемера). Поэтому простые числа Мерсенна вызывают особый интерес и давно удерживают лидерство как самые большие известные простые числа [29].

Критерий состоит в следующем.

Теорема 3 (критерий Люка или тест Люка — Лемера, [9, с. 96]). *Пусть p — простое нечётное. Число Мерсенна $M_p = 2^p - 1$ простое тогда и только тогда, когда оно делит нацело $(p-1)$-й член рекуррентной последовательности (см.* [28, A003010])

$$S_k = S_{k-1}^2 - 2, \quad S_1 = 4.$$

Начальные члены этой последовательности: $4, 14, 194, 37\,634, \ldots$

Этот критерий простоты был предложен французским математиком Люка в 1878 году. Чуть ранее (без использования компьютера!) Люка доказал простоту числа $M_{127} = 2^{127} - 1$ (см. [20]). В частности, Люка показал, что алгоритм позволяет проверять простоту M_p для простых $p \equiv 1 \pmod 4$. В 1930 году в своей докторской диссертации американский математик Лемер полностью доказал справедливость критерия для всех простых нечётных p.

В 1952 году Робинсон при поддержке Лемера провёл вычисления на компьютере SWAC с использованием теста Люка — Лемера, результатом которого стало открытие простых чисел M_{521} и M_{607}. Позднее в том же году были открыты M_{1279}, M_{2203} и M_{2281}.

---

[3] Если числа p и $2p + 1$ одновременно являются простыми, то меньшее из них называется простым числом Софи Жермен.

Для проверки простоты M_p последовательность чисел $S_1, S_2, \ldots, S_{p-1}$ вычисляется по модулю числа M_p (т. е. вычисляются не сами числа S_k, длина которых растёт экспоненциально, а остатки от деления S_k на M_p, длина которых ограничена p битами). Последнее число в этой последовательности $S_{p-1} \pmod{M_p}$ называется вычетом Люка — Лемера. Таким образом, число Мерсенна M_p является простым тогда и только тогда, когда число p — нечётное простое и вычет Люка — Лемера равен нулю.

Лёгкость реализации теста и рост вычислительных мощностей компьютеров позволили фактически любому человеку заниматься поиском простых чисел Мерсенна. Так, в 1978 году два американских старшеклассника Лора Никель и Курт Нолл[4)] за 3 года работы доказали простоту числа M_{21701}, используя суперкомпьютер CDC Cyber 176 в Калифорнийском университете.

До настоящего времени остаётся открытым вопрос о существовании бесконечного количества простых чисел Мерсенна. Этому вопросу уже более 400 лет. Но, несмотря на это, с упорством и с верой, заложенной ещё монахом Мерсенном, большие простые числа ищутся среди простых чисел Мерсенна.

Самым большим известным простым числом является число Мерсенна, проверенное с помощью теста Люка — Лемера,

$$M_{82589933} = 2^{82589933} - 1.$$

Это число было найдено 7 декабря 2018 года Патриком Ляроше в рамках проекта добровольных вычислений GIMPS. Десятичная запись числа $M_{82589933}$ содержит 24 862 048 цифр.

Всего в настоящее время известно 51 простое число Мерсенна, при этом порядковые номера достоверно установлены только у первых 47 чисел. Неизвестно, существуют ли другие простые числа Мерсенна, меньшие известного рекордного. В таблице 4 приведены простые числа Мерсенна, известные в настоящее время.

Завершим наш исторический экскурс и снова посмотрим на последовательность $\{2^n + n^2\}$.

В настоящее время мы не располагаем доказательством, однако склонны считать, что верна следующая гипотеза.

Гипотеза 1. *В последовательности* $\{\delta_n\} = \{2^n + n^2\}$ *встречается бесконечно много простых чисел.*

Косвенным подтверждением нашей гипотезы является нахождение простого числа $2^{3759} + 3759^2$ из 1133 цифр!

[4)] Лемер преподавал им теорию чисел.

Таблица 4

Открытие простых чисел Мерсенна

№	p — показатель	Знаков в M_p	Год	Первооткрыватель
1	2	1	—	—
2	3	1	—	—
3	5	2	—	—
4	7	3	—	—
5	13	4	1456	неизвестен
6	17	6	1588	Катальди (Cataldi)
7	19	6	1588	Катальди
8	31	10	1772	Эйлер
9	61	19	1883	Первушин
10	89	27	1911	Пауэрс (Powers)
11	107	33	1914	Пауэрс
12	127	39	1876	Люка (Lucas)
13	521	157	1952	Робинсон (Robinson)
14	607	183	1952	Робинсон
15	1279	386	1952	Робинсон
16	2203	664	1952	Робинсон
17	2281	687	1952	Робинсон
18	3217	969	1957	Ризель (Riesel)
19	4253	1281	1961	Гурвиц (Hurwitz)
20	4423	1332	1961	Гурвиц
21	9689	2917	1963	Гиллис (Gillies)
22	9941	2993	1963	Гиллис
23	11213	3376	1963	Гиллис
24	19937	6002	1971	Такерман (Tuckerman)
25	21701	6533	1978	Нолл (Noll), Никель (Nickel)
26	23209	6987	1979	Нолл
27	44497	13395	1979	Нельсон (Nelson), Словинский (Slowinski)
28	86243	25962	1982	Словинский
29	110503	33265	1988	Колквит (Colquitt), Уэлш (Welsh)
30	132049	39751	1983	Словинский
31	216091	65050	1985	Словинский
32	756839	227832	1992	Словинский, Гейдж (Gage) и др.
33	859433	258716	1994	Словинский, Гейдж
34	1 257 787	378 632	1996	Словинский, Гейдж

Окончание таблицы 4

№	p — показатель	Знаков в M_p	Год	Первооткрыватель
35	1 398 269	420 921	1996	Арменгауд (Armengaud), Вольтман (Woltman), и др.
36	2 976 221	895 932	1997	Спенс (Spence), Вольтман, и др. (GIMPS)
37	3 021 377	909 526	1998	Кларксон (Clarkson), Вольтман, Куровский (Kurowski) и др.
38	6 972 593	2 098 960	1999	Хаджратвала (Hajratwala), Вольтман, Куровский и др.
39	13 466 917	4 053 946	2001	Кемерон (Cameron), Вольтман, Куровский и др.
40	20 996 011	6 320 430	2003	Шефер (Shafer), Вольтман, Куровский и др.
41	24 036 583	7 235 733	2004	Финдли (Findley), Вольтман, Куровский и др.
42	25 964 951	7 816 230	2005	Новак (Nowak), Вольтман, Куровский и др.
43	30 402 457	9 152 052	2005	Купер (Cooper), Бун (Boone), Вольтман, Куровский и др.
44	32 582 657	9 808 358	2006	Купер, Бун, Вольтман, Куровский и др.
45	37 156 667	11 185 272	2008	Елвенич (Elvenich), Вольтман, Куровский и др.
46	42 643 801	12 837 064	2009	Стриндмо (Strindmo), Вольтман, Куровский и др.
47	43 112 609	12 978 189	2008	Смит (Smith), Вольтман, Куровский и др.
48?	57 885 161	17 425 170	2013	Купер, Вольтман, Куровский и др.
49?	74 207 281	22 338 618	2016	Купер, Вольтман, Куровский, Блоссер (Blosser) и др.
50?	77 232 917	23 249 425	2017	Пак (Pace), Вольтман, Куровский, Блоссер и др.
51?	82 589 933	24 862 048	2018	Лярош (Laroche), Вольтман, Блоссер и др.

Существенным продвижением в нахождении простых чисел в последовательности $\{2^n + n^2\}$ было бы нахождение критерия, аналогичного критерию Люка, для последовательности простых чисел Мерсенна.

§ 6. Простые числа Каллена

Последовательность $\{n2^n + 1\}$ называется последовательностью Каллена[5)] (см. [28, A002064]). Предполагалось, что все числа в этой последовательности при $n > 1$ будут составными, пока Робинсон не показал, что при $n = 141$ мы получим простое число.

[5)] Названа в честь ирландского священника-иезуита Джеймса Каллена (James Cullen), который проверил, что для $1 < n \leqslant 100$ её члены являются составными числами.

В монографии Кристофера Хооли [22] анонсирован результат, опирающийся на «методы решета». Название эти методы получили от известного метода решета Эратосфена.

Приведём упомянутый результат без доказательства.

Теорема 4 (К. Хооли, [22]). *Пусть $k(x)$ есть количество положительных целых n, не превосходящих x, для которых $n2^n + 1$ является простым числом. Тогда при $x \to +\infty$*

$$k(x) = o(x). \tag{1}$$

Это означает, что если простые числа встречаются в последовательности Каллена, то встречаются они очень редко.

Процитируем ремарку Хооли: «Подобные методы применимы к другим последовательностям, таким, например, как $\{2^n + n^2\}$. Следовательно, можно заключить, что методы решета могут сделать скромный вклад в наши знания об очень редко распределённых последовательностях, хотя, по-видимому, они не приведут при этом к решению наиболее интересных проблем».

Подобную же ремарку со ссылкой на Хооли мы можем найти в [3, с. 255].

К сожалению, в своей монографии Хооли не привёл доказательство этого утверждения для последовательности $\{2^n + n^2\}$. Нам не удалось найти полного доказательства этого утверждения (которое использовало бы методы решета или иные методы) в других доступных нам источниках.

Поэтому сформулируем это утверждение в виде гипотезы.

Гипотеза 2 (К. Хооли). *Пусть $f(x)$ есть количество положительных целых n, не превосходящих x, для которых $2^n + n^2$ является простым числом. Тогда при $x \to +\infty$*

$$f(x) = o(x). \tag{2}$$

Итак, мы имеем ещё одно косвенное подтверждение гипотезы 1. С важным дополнением: простые числа в этой последовательности встречаются крайне редко.

§ 7. Случай $3^n + n^3$

Рассмотрим случай $a = 3$.

Если n нечётно, то сумма $3^n + n^3$ делится на 2. Если n делится на 3, то сумма $3^n + n^3$ делится на 3.

Таблица 5

n	$3^n + n^3$
2	17 (простое)
4	$145 = 5 \cdot 29$
8	$7073 = 11 \cdot 643$
10	$60\,049 = 11 \cdot 53 \cdot 103$
14	$4\,785\,713 = 677 \cdot 7069$
16	$43\,050\,817 = 17 \cdot 2\,532\,401$
20	$3\,486\,792\,401 = 83 \cdot 461 \cdot 91\,127$
22	$31\,381\,070\,257 = 23 \cdot 1\,364\,394\,359$
26	$2\,541\,865\,845\,905 = 5 \cdot 1709 \cdot 297\,468\,209$
28	$22\,876\,792\,476\,913 = 29 \cdot 10\,193 \cdot 77\,391\,829$
32	$1\,853\,020\,188\,884\,609 = 1049 \cdot 1\,766\,463\,478\,441$
34	$16\,677\,181\,699\,705\,873 = 23 \cdot 725\,094\,856\,508\,951$
38	$1\,350\,851\,717\,673\,046\,961 = 307 \cdot 10\,061 \cdot 437\,349\,017\,143$
40	$12\,157\,665\,459\,056\,992\,801 = 41 \cdot 8\,987\,921 \cdot 32\,991\,881\,641$
44	$984\,770\,902\,183\,611\,318\,065 = 5 \cdot 71 \cdot 1\,221\,907 \cdot 2\,270\,223\,954\,329$
46	$8\,862\,938\,119\,652\,501\,193\,265 = 5 \cdot 11 \cdot 47 \cdot 3\,428\,602\,754\,217\,602\,009$
50	$717\,897\,987\,691\,852\,588\,895\,249 = 41 \cdot 17\,509\,707\,016\,874\,453\,387\,689$
52	$6\,461\,081\,889\,226\,673\,299\,072\,849 = 53 \cdot 121\,907\,205\,457\,107\,043\,378\,733$
56	523 347 633 027 360 537 213 687 137 (простое)
58	$4\,710\,128\,697\,246\,244\,834\,921\,798\,801 = 59 \cdot 177\,949\,463 \cdot 295\,176\,373 \cdot 1\,519\,856\,161$

Поэтому в онлайн-калькуляторе проведём вычисления для чётных n, не делящихся на 3, т. е. вида $n = 2(3k \pm 1)$, где $k \in \mathbb{N}$. Данные внесём в таблицу 5.

Кроме уже упоминавшегося числа 17 мы находим ещё одну пару $a = 3$, $n = 56$.

Число $3^{56} + 56^3$ является простым!

К сожалению, вычисления Джонатана Хашпера на домашнем компьютере не дали новых простых чисел при $a = 3$.

§ 8. Числа Лейланда. Случай $7^n + n^7$

В случае $a = 7$ проведём аналогичные рассуждения.

Если n нечётное, то $7^n + n^7$ делится на 2. Если n делится на 7, то $7^n + n^7$ делится на 7. Поэтому вычисления проводим для чисел вида $n = 2(7k + r)$, где $r = 1, 2, 3, 4, 5, 6$.

Таблица 6

n	$7^n + n^7$
4	$18\,785 = 5 \cdot 13 \cdot 17^2$
6	$397\,585 = 5 \cdot 131 \cdot 607$
10	$292\,475\,249 = 11 \cdot 4397 \cdot 6047$
12	$13\,877\,119\,009 = 13 \cdot 1\,067\,470\,693$
16	$33\,233\,199\,005\,057 = 17 \cdot 1\,954\,894\,059\,121$
18	$1\,628\,414\,210\,130\,481 = 19 \cdot 85\,706\,011\,059\,499$
22	$3\,909\,821\,051\,077\,345\,937 = 13 \cdot 23 \cdot 47 \cdot 278\,219\,672\,032\,829$
24	$191\,581\,231\,385\,152\,885\,825 = 5^2 \cdot 341\,333 \cdot 22\,450\,947\,477\,701$
30	$22\,539\,340\,290\,692\,279\,957\,863\,249 = 31 \cdot 727\,075\,493\,248\,138\,063\,156\,879$
34	$54\,116\,956\,037\,952\,111\,721\,483\,010\,993 =$ $= 23^2 \cdot 31 \cdot 43 \cdot 13\,649 \cdot 5\,622\,723\,213\,426\,086\,701$
36	$2\,651\,730\,845\,859\,653\,471\,857\,387\,545\,697 =$ $= 37^2 \cdot 1\,936\,983\,817\,282\,434\,968\,486\,039\,113$
40	$6\,366\,805\,760\,909\,027\,985\,741\,598\,979\,224\,001 =$ $= 37 \cdot 41 \cdot 4\,196\,971\,496\,973\,650\,616\,836\,914\,290\,853$
46	$749\,048\,330\,965\,186\,233\,494\,494\,103\,130\,382\,150\,865 =$ $= 5 \cdot 11 \cdot 47 \cdot 107 \cdot 970\,090\,462\,791\,553 \cdot 2\,791\,600\,584\,558\,224\,939$
48	$36\,703\,368\,217\,294\,125\,441\,230\,211\,032\,620\,728\,531\,073 =$ $= 643 \cdot 3631 \cdot 15\,720\,584\,845\,159\,650\,136\,109\,872\,534\,726\,981$
52	$88\,124\,787\,089\,723\,195\,184\,393\,736\,687\,913\,846\,185\,013\,729 =$ $= 53 \cdot 110\,703\,724\,474\,073 \cdot 15\,019\,655\,750\,344\,554\,442\,695\,759\,941$
54	$4\,318\,114\,567\,396\,436\,564\,035\,293\,097\,707\,729\,426\,477\,458\,833$ (простое)
58	$10\,367\,793\,076\,318\,844\,190\,248\,738\,727\,596\,255\,140\,420\,933\,654\,001 =$ $= 59 \cdot 1\,310\,148\,050\,957 \cdot 44\,316\,771\,096\,751 \cdot 3\,026\,535\,857\,960\,488\,271\,777$

Если $n \equiv 2 \pmod 3$, то $7^n + n^7 \equiv 1^n + 2^7 \equiv 0 \pmod 3$. Значит, в этом случае сумма делится на 3 и является составным числом. Например, $7^2 + 2^7 = 177 = 3 \cdot 59$. Опять используем онлайн-калькулятор и внесём данные в таблицу 6.

Нам везёт (!), мы находим пару $a = 7$, $n = 54$.

Число $7^{54} + 54^7$, состоящее из 46 знаков, является простым!

Вычисления Джонатана Хашпера на домашнем компьютере позволили найти ещё одно простое число при $n = 3076$. А именно, $7^{3076} + 3076^7$ — простое число, состоящее из 2600 десятичных знаков.

Снова заглянем на сайт [28]. Последовательность под номером A094133 состоит из простых чисел, представимых в виде $a^n + n^a$. Члены этой последовательности называются простыми числами Лейланда (Leyland).

Поиски всё больших чисел Лейланда ведутся на суперкомпьютерах, и вряд ли домашний компьютер сможет составить им конкуренцию.

Мы собрали достаточно примеров, поэтому самое время вернуться к теории. В дальнейшем мы предполагаем, что наш читатель знаком с теорией сравнений. Основы теории сравнений можно найти в [7].

§ 9. Малая теорема Ферма как критерий простоты

Норвежский математик О. Оре в своей книге [18] в параграфе о простых числах Мерсенна пишет: «В течение нескольких столетий шла погоня за простыми числами. Многие математики боролись за честь стать открывателем самого большого из известных простых чисел. <…> Теперь эта погоня утихла, она идёт только в одном направлении, оказавшемся удачным».

Однако он ошибся, погоня за простыми числами не утихла и идёт по разным направлениям. Более того, для современной криптографии необходимы очень большие простые числа и их нужно много. Фактически нужно «массовое производство» больших простых чисел. В своё время сборник «Математическое просвещение» опубликовал ряд статей, связанных с криптографией, см. [6, 17, 24].

Сейчас разработано много алгоритмов и методов определения простоты больших чисел. Но простейшим критерием для определения простоты (хотя правильнее было бы сказать непростоты) служит следующая известная

Теорема 5 (малая теорема Ферма, [15, гл. 1, § 1.1, с. 23]). *Пусть a и n — произвольные взаимно простые числа. Тогда если n — простое число, то справедливо сравнение*

$$a^{n-1} \equiv 1 \pmod{n}, \tag{3}$$

т. е. $a^{n-1} - 1$ делится на n.

Итак, если у нас есть число n и мы найдём взаимно простое с ним число a, для которого условие (3) не будет выполнено, то мы можем утверждать, что число n составное.

К сожалению, выполнение условия (3) даже для всех взаимно простых с n чисел a не гарантирует его простоту.

Определение. Число n называется *псевдопростым по основанию a*, если выполнено сравнение (3).

В качестве примера рассмотрим составное число $91 = 7 \cdot 13$ и взаимно простое с ним число 3. Тогда выполнено сравнение

$$3^{90} \equiv (3^6)^{15} \equiv 729^{15} \equiv 1^{15} \equiv 1 \pmod{91}.$$

Это означает, что число 91 является псевдопростым по основанию 3.

Если же мы возьмём другое основание, например 2, то получим

$$2^{90} \equiv (2^{10})^9 \equiv 1024^9 \equiv 23^9 \equiv 12\,167^3 \equiv 64^3 \equiv 64 \pmod{91}.$$

Поскольку по основанию 2 условие (3) не выполнено, мы можем утверждать, что число 91 составное.

Собственно говоря, так действуют современные алгоритмы: берётся несколько оснований и проводится тест. Если хотя бы в одном случае сравнение не выполнено, то проверяемое число является составным.

Однако если сравнение выполнено для всех выбранных нами оснований, то мы не можем утверждать, что проверяемое нами число является простым.

Определение. *Числами Кармайкла* (Carmichael) называются составные числа, которые являются псевдопростыми для всех a, взаимно простых с n.

Такие числа есть: например, $561 = 3 \cdot 11 \cdot 17$, $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, и их бесконечно много.

Теорема 6 (Корселт, [14, § 11.3, с. 272]). *Нечётное натуральное число n является числом Кармайкла, если и только если для каждого его простого делителя p выполнены следующие два условия*:

(1) p^2 *не делит* n;

(2) $p-1$ *делит* $n-1$.

Обобщением малой теоремы Ферма является следующая

Теорема 7 (Эйлер, [16, с. 85]). *Если n взаимно просто с*

$$m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k},$$

где $p_1, \ldots, p_k$ — простые числа и

$$\varphi(m) = (p_1 - 1)p_1^{\alpha_1 - 1} \cdot \ldots \cdot (p_k - 1)p_k^{\alpha_k - 1},$$

то

$$n^{\phi(m)} \equiv 1 \pmod{m}, \tag{4}$$

т. е. $n^{\phi(m)} - 1$ делится на m.

Здесь $\varphi(m)$ — *функция Эйлера*, равная количеству чисел от 1 до m, взаимно простых с m.

Доказательства малой теоремы Ферма и теоремы Эйлера можно найти в разных источниках, в том числе и адаптированных для школьников [8], [7]. Доказательство теоремы Корселта можно найти в [14].

Используя всё вышесказанное, получаем целый ряд примеров, когда сумма $a^n + n^a$ — составное число.

Первый пример. Пусть $p \geqslant 3$ — простое число. Поскольку p нечётно, для любого n имеем

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

Если n простое и $(n, p) = 1$, из малой теоремы Ферма получаем $p^{n-1} \equiv 1 \pmod{n}$.

Следовательно, если числа $p \geqslant 3$ и n простые, $p \neq n$, то

$$(n-1)^p + p^{n-1} \equiv -1 + 1 \equiv 0 \pmod{n}.$$

Например, если взять $n = 11$ и простое число $p \neq 11$, то числа $3^{10} + 10^3$, $5^{10} + 10^5$, $7^{10} + 10^7$, …, $p^{10} + 10^p$ делятся на 11.

Как мы отметили, число $5^{10} + 10^5$ делится на 11, но этот пример не столь интересен, поскольку сразу видно, что это число составное и делится на 5^5. Поэтому в содержательных примерах числа p и $n-1$ должны быть взаимно просты.

Второй пример. Пусть n — число Кармайкла, $n = p_1 p_2 \dots p_k$. Пусть a — нечётное число, взаимно простое с n. Тогда $a^{n-1} \equiv 1 \pmod{n}$, следовательно,

$$a^{n-1} + (n-1)^a \equiv 1 + (-1)^a \equiv 0 \pmod{n}.$$

В частности, числа $13^{560} + 560^{13}$, $19^{560} + 560^{19}$, …, $p^{560} + 560^p$ делятся на 561 при $p \neq 3, 11, 17$. Числа $5^{560} + 560^5$, $7^{560} + 560^7$ также делятся на 561, хотя этот случай не так интересен, поскольку первое делится на 5^5, а второе на 7^7.

Третий пример. Пусть n — псевдопростое число по основанию a. Пусть a — нечётное число, взаимно простое с n.

Рассуждая аналогично предыдущему, получаем

$$a^{n-1} + (n-1)^a \equiv 1 - 1 \equiv 0 \pmod{n}.$$

В частности, числа $11^{90} + 90^{11}$, …, $p^{90} + 90^p$ делятся на 91 при $p \neq 7, 13$. Числа $3^{90} + 90^3$, $5^{90} + 90^5$ также делятся на 91, к тому же первое делится на 3^6, а второе на 5^5.

Итак, мы достаточно хорошо продвинулись в определении того, какие из сумм $a^n + n^a$ могут быть составными числами. Однако методов для нахождения пар с простой суммой не нашли.

§ 10. Символ Лежандра. Квадратичный закон взаимности

Необходимое условие простоты, которое применял Гаусс, основано на свойстве цикличности мультипликативной группы $(\mathbb{Z}/n\mathbb{Z})^\times$ для простых чисел n. Для нечётного простого n извлечём квадратный корень

из левой и правой частей сравнения (3). Мы получим $a^{(n-1)/2} \equiv 1 \pmod{n}$ или $a^{(n-1)/2} \equiv -1 \pmod{n}$ в зависимости от того, является ли a квадратом по модулю n или нет. Эти два сравнения можно записать одной строчкой

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}, \tag{5}$$

где $\left(\frac{a}{n}\right)$ обозначает символ Лежандра.

Пусть a — целое число и p — простое число. *Символ Лежандра* $\left(\frac{a}{p}\right)$ определяется следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \text{ делится на } p; \\ 1, & \text{если } a \text{ является квадратичным вычетом,} \\ & \text{по модулю } p, \text{ т. е. существует такое } x \in \mathbb{Z}, \\ & \text{что } x^2 \equiv a \pmod{p}; \\ -1 & \text{в противном случае.} \end{cases} \tag{6}$$

Часто сравнение 5 называют *критерием Эйлера*.

Чтобы быстро вычислять символ Лежандра, нам понадобится

Теорема 8 (квадратичный закон взаимности, [15, гл. 1, § 1.1, с. 29–30]). *Пусть p и q — различные нечётные простые числа, тогда*:

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \cdot (q-1)/2} \cdot \left(\frac{p}{q}\right). \tag{7}$$

Нам также будут нужны два дополнения к квадратичному закону взаимности:

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}, \tag{8}$$

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}. \tag{9}$$

Если мы не знаем, простое число n или составное, то вместо символа Лежандра используется *символ Якоби* $\left(\frac{a}{p}\right)$, который определён для нечётного положительного числа n и любого целого числа a.

Доказательство квадратичного закона взаимности можно найти в [19] или [15].

Быстрое вычисление символа Лежандра является стандартным упражнением для студентов, изучающих курс теории чисел. В следующем параграфе мы проведём несколько таких вычислений.

§ 11. Тест Люка

Предыдущие тесты могли установить только разложимость того или иного числа. Следующий тест помогает определить его простоту.

Теорема 9 (тест Люка, [14, § 11.1, с. 265]). *Пусть n — нечётное натуральное число и b — натуральное число такое, что $2 \leqslant b \leqslant n-1$. Если для каждого простого делителя p числа $n-1$ справедливы следующие утверждения*: (1) $b^{n-1} \equiv 1 \pmod{n}$; (2) $b^{(n-1)/p} \not\equiv 1 \pmod{n}$, *то n — простое число.*

Заметим, что для успешного применения теста Люка нам нужно знать полное разложение числа $n-1$ на множители. Кроме того, нам должно повезти с выбором b, в противном случае тест может не дать ответ, даже если число простое.

Например, докажем, что число $m = 2^9 + 9^2 = 593$ — простое.

Найдём разложение числа $m-1=2^9+9^2-1=592$ на множители. Имеем $2^9 + 9^2 - 1 = 2^4 \cdot 37$. Для проверки выберем $b = 2$. Чтобы применить тест Люка, мы должны найти вычеты $2^{m-1} = 2^{2^9+9^2-1}$, $2^{(m-1)/2} = 2^{2^3 \cdot 37}$ и $2^{(m-1)/37} = 2^{2^4}$ по модулю $m = 593$.

Постараемся сократить наши вычисления. Сначала найдём вычет для $2^{(m-1)/37} = 2^{2^4}$. Имеем

$$2^{2^4} = 2^{16} = (2^8)^2 = 256^2 \equiv 306 \pmod{593}.$$

Теперь найдём вычет $2^{(m-1)/2^4} = 2^{37}$. Имеем

$$2^{37} = 2^{2^4 \cdot 2+5} = 2^5 \cdot (2^{2^4})^2 \equiv 32 \cdot 306^2 \equiv 516 \pmod{593}.$$

Отсюда

$$2^{(m-1)/2} = 2^{2^3 \cdot 37} = (2^{37})^8 \equiv (516^2)^4 \equiv (592^2)^2 \equiv 1 \pmod{593}.$$

Это означает, что кандидат $b = 2$ не подходит.

Придётся взять $b=3$ и искать вычеты $3^{m-1}=3^{2^9+9^2-1}$, $3^{(m-1)/2}=3^{2^3 \cdot 37}$ и $3^{(m-1)/37} = 3^{2^4}$ по модулю $m = 593$. Поступим аналогично предыдущему: сначала найдём вычет $3^{(m-1)/37} = 3^{2^4}$. Имеем

$$3^{2^4} = 3^{16} = (3^4)^4 = (81^2)^2 \equiv 38^2 \equiv 258 \pmod{593}.$$

Далее,

$$3^{37} = 3^{2^4 \cdot 2+5} = 3^5 \cdot (3^{2^4})^2 \equiv 243 \cdot 258^2 \equiv 384 \pmod{593}.$$

Отсюда

$$3^{(m-1)/2}=3^{2^3 \cdot 37}=(3^{37})^8 \equiv (384^2)^4 \equiv (392^2)^2 \equiv 77^2 \equiv 592 \equiv -1 \pmod{593}.$$

Наконец,

$$3^{m-1} = 3^{2^9+9^2-1} \equiv (-1)^2 \equiv 1 \pmod{593}.$$

Итак, получаем

$$3^{m-1} \equiv 1 \pmod{m},$$
$$3^{(m-1)/2} \not\equiv 1 \pmod{m},$$
$$3^{(m-1)/37} \not\equiv 1 \pmod{m}.$$

Согласно тесту Люка число $m = 2^9 + 9^2 = 593$ — простое.

Можно проверить, что тест также сработает, если в качестве кандидата взять $b = 5$ или $b = 7$.

Упражнение 7. Докажите с помощью теста Люка, что число $2^{15} + 15^2 = 32993$ простое.

Тест Люка легко запрограммировать. Быстрое возведение в степень производится с помощью умножения и возведения в квадрат.

С помощью теста Люка можно обосновать следующий тест на простоту для чисел Ферма. Впервые его предложил Жан Франсуа Теофил Пепэн (Jean François Theophile Pepin).

Теорема 10 (тест Пепэна, [14, § 11.1, с. 266]). *Число Ферма F_k является простым при данном $k > 1$, если и только если*

$$5^{(F_k-1)/2} \equiv -1 \pmod{F_k}. \tag{10}$$

Доказательство. Докажем достаточность. Предположим, что сравнение (10) выполнено. Применим тест Люка. В качестве кандидата берём $b = 5$. Очевидно, что единственным простым делителем числа $F_k - 1 = 2^{2^k}$ является 2. Имеем

$$5^{(F_k-1)/2} \equiv -1 \not\equiv 1 \pmod{F_k}$$

и

$$5^{F_k-1} \equiv (-1)^2 \equiv 1 \pmod{F_k}.$$

Условия теста Люка выполнены, следовательно, F_k — простое число.

Докажем необходимость. Пусть F_k — простое число. Тогда по критерию Эйлера (5) имеем

$$5^{(F_k-1)/2} \equiv \left(\frac{5}{F_k}\right) \pmod{F_k}.$$

Найдём символ Лежандра $\left(\frac{5}{F_k}\right)$, для этого используем квадратичный закон взаимности. Имеем для $k \geqslant 2$:

$$\left(\frac{5}{F_k}\right) = (-1)^{(5-1)/2 \cdot (F_k-1)/2} \cdot \left(\frac{F_k}{5}\right) =$$
$$= \left(\frac{2^{2^k}+1}{5}\right) = \left(\frac{4^{2^{k-1}}+1}{5}\right) = \left(\frac{(-1)^{2^{k-1}}+1}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Итак, если F_k — простое число, то

$$5^{(F_k-1)/2} \equiv -1 \pmod{F_k}.$$

Что и требовалось доказать. □

При проверке на простоту числа $2^9 + 9^2 = 593$ с помощью теста Люка мы увидели, что при выборе кандидата $b = 2$ мы получаем неопределённый результат. Если читатель решал упражнение (7), то он мог также убедиться, что и при проверке числа $2^{15} + 15^2 = 32\,993$ кандидат $b = 2$ снова даст неопределённый результат. Это не случайно.

Предложение 1. *Если число $\delta_n = 2^n + n^2$ является простым, то*

$$\text{а)}\ 2^{(\delta_n-1)/2} \equiv 1 \pmod{\delta_n}; \tag{11}$$

$$\text{б)}\ 3^{(\delta_n-1)/2} \equiv -1 \pmod{\delta_n}. \tag{12}$$

Доказательство. Так как δ_n — простое, получаем, что $n = 6k + 3$, где $k \in \mathbb{Z}\ k \geqslant 0$.

а) Используем критерий Эйлера. Далее найдём символ Лежандра по формуле (8).

$$2^{(\delta_n-1)/2} \equiv \left(\frac{2}{\delta_n}\right) = (-1)^{((2^n+n^2)^2-1)/8} = 1 \pmod{\delta_n}.$$

б) Используем критерий Эйлера и квадратичный закон взаимности. Имеем

$$3^{(\delta_n-1)/2} \equiv \left(\frac{3}{\delta_n}\right) = (-1)^{(3-1)/2\cdot(2^n+n^2-1)/2} \cdot \left(\frac{\delta_n}{3}\right) =$$
$$= \left(\frac{2^n+n^2}{3}\right) = \left(\frac{(-1)^n}{3}\right) = \left(\frac{(-1)}{3}\right) = -1 \pmod{\delta_n}.$$

Что и требовалось доказать. □

Итак, мы показали, что при проверке простоты чисел 2^n+n^2 тестом Люка кандидат $b = 2$ даёт неопределённый ответ.

§ 12. Критерий определения простоты $2^n + n^2$

На основании теста Люка с учётом предложения 1 можно предложить

Критерий определения простоты $2^n + n^2$ для нечётных $n > 3$.

Шаг 1. В качестве кандидатов выбираем небольшие простые b, например $b = 3, 5, 7$; достаточно взять $b \leqslant 100$.

Проверяем, выполняются ли сравнения

$$3^{2^n+n^2-1} \equiv 1 \pmod{2^n+n^2},$$
$$5^{2^n+n^2-1} \equiv 1 \pmod{2^n+n^2},$$
$$7^{2^n+n^2-1} \equiv 1 \pmod{2^n+n^2},$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$

Если хотя бы одно из сравнений не выполнено, то число 2^n+n^2 составное. (Это следует из малой теоремы Ферма.)

Шаг 2. Теперь мы должны разложить число 2^n+n^2-1 на множители. Это число при нечётных $n>3$ делится на 8. Поэтому мы применим усечённый тест Люка — только для одного простого делителя, равного 2.

Проверим, выполняется ли сравнение

$$b^{(2^n+n^2-1)/4} \not\equiv \pm 1 \pmod{2^n+n^2}. \qquad (*)$$

Если сравнение не выполняется, то с большой вероятностью число 2^n+n^2 — простое.

Вообще говоря, по критерию Люка мы должны были бы проверить сравнение

$$b^{(2^n+n^2-1)/2} \not\equiv 1 \pmod{2^n+n^2}. \qquad (**)$$

Но мы применили небольшую хитрость. Поскольку

$$b^{(2^n+n^2-1)/2}-1 = (b^{(2^n+n^2-1)/4}-1)(b^{(2^n+n^2-1)/4}+1),$$

мы можем проверять сравнение $(*)$, у которого меньший показатель, вместо проверки сравнения $(**)$.

§ 13. Случай $a = p-1$

Остался нерассмотренным случай суммы a^n+n^a при условии, что числа a и $n+1$ не являются взаимно простыми.

Пусть $p \geqslant 3$ — простое число. Рассмотрим пару $a=p-1$ и $n=p$.

Можем ли мы что-то сказать о делителях числа $(p-1)^p+p^{p-1}$? Условие взаимной простоты чисел $p-1$ и $p+1$ не выполнено — оба числа чётны. Поэтому применить малую теорему Ферма так, как мы это делали раньше, не удаётся. Сумма $(p-1)^p+p^{p-1}$ не делится ни на $p-1$, ни на p.

Вообще говоря, нам следует рассматривать общий случай суммы $(lp-1)^p+p^{lp-1}$, где l — нечётное число, но остановимся на вышеуказанном частном случае.

Таблица 7

p	$(p-1)^p + p^{p-1}$
3	17 (простое)
5	$1649 = 17 \cdot 97$
7	$397585 = 5 \cdot 131 \cdot 607$
11	$125937424601 = 2531 \cdot 49757971$
13	$130291290501553 = 19 \cdot 6857436342187$
17	$34380909705501969433 7 = 573645313 \cdot 599340898049$
19	$8123626956532489178904 73 = 22156214713 \cdot 36665229425521$
23	$8419259736788826438132968480177 = 103 \cdot 5419 \cdot 214765247 \cdot 70234990225477963$
29	$10166155490042397076886511571194164153939 69 =$ $= 11 \cdot 127 \cdot 200467 \cdot 690280837 \cdot 5258860293889023977022163$
31	$6727352483185380837374536871905139185678862401 =$ $= 137 \cdot 1608214821278413 \cdot 30533708557637524653832992221$
37	$4115218838977518769133856210493722956973810264387642573937 =$ $= 6301 \cdot 26713 \cdot 48040093 \cdot 60035377 \cdot 847714691074239247963794857110780 9$
41	$5160307578612836698510898936820328355118509592722353901054911696 01 =$ $859 \cdot 24103 \cdot 108684413 \cdot 2293211229013793477795401613248443486949238477526 01$
43	$6708842943577578539447301465522222859778574357817542410258174135488537 =$ $= 1300283 \times$ $\times 5159525229182861376675155689586207663853618295261525691144292539$
47	(составное, делится на 5)
53	(составное, делится на 17)
59	(составное, делится на 1039)
61	?
67	(составное, делится на 5)

Призовём на помощь онлайн-калькулятор. Число $(p-1)^p + p^{p-1}$ удаётся разложить на множители для всех простых $p \leqslant 59$ (см. таблицу 7). Поскольку при $p \geqslant 47$ сумма $(p-1)^p + p^{p-1}$ содержит более 70 значащих цифр, в таблице мы указали только наименьший делитель.

В этом случае с помощью онлайн-калькулятора нам не удалось найти новые примеры простых чисел, за исключением 17.

Означает ли этот факт, что число $(p-1)^p + p^{p-1}$ при $p \geqslant 5$ всегда составное, нам неизвестно.

С другой стороны, в качестве упражнений мы предлагаем новые примеры, когда достоверно известно, что сумма является составным числом.

Упражнение 8. Если $p \equiv 7 \pmod{20}$, то $(p-1)^p + p^{p-1} \equiv 0 \pmod 5$. В частности, суммы $46^{47} + 47^{46}$ и $66^{67} + 67^{66}$ делятся на 5.

Таблица 8

r	$(r-1)^r + r^{r-1}$
2	3
3	17
4	$145 = 5 \cdot 29$
5	$1649 = 17 \cdot 97$
6	$23\,401 = 7 \cdot 3343$
7	$397\,585 = 5 \cdot 131 \cdot 607$
8	$7\,861\,953 = 3 \cdot 11 \cdot 19 \cdot 12\,539$
9	$177\,264\,449 = 7523 \cdot 23\,563$
10	$4\,486\,784\,401 = 11 \cdot 407\,889\,491$
11	$125\,937\,424\,601 = 2531 \cdot 49\,757\,971$
12	$3\,881\,436\,747\,409 = 13 \cdot 3631 \cdot 82\,228\,603$
13	$130\,291\,290\,501\,553 = 19 \cdot 6\,857\,436\,342\,187$
14	$4\,731\,091\,158\,953\,433 = 3 \cdot 23 \cdot 61 \cdot 71 \cdot 125\,497 \cdot 126\,151$
15	$184\,761\,021\,583\,202\,849 = 23 \cdot 1571 \cdot 5\,113\,359\,576\,653$
16	$7\,721\,329\,860\,319\,737\,601 = 17 \cdot 1601 \cdot 12\,401 \cdot 22\,876\,793\,153$
17	$343\,809\,097\,055\,019\,694\,337 = 573\,645\,313 \cdot 599\,340\,898\,049$
18	$16\,248\,996\,011\,806\,421\,522\,977 = 19 \cdot 5779 \cdot 147\,985\,865\,445\,728\,377$
19	$812\,362\,695\,653\,248\,917\,890\,473 = 22\,156\,214\,713 \cdot 36\,665\,229\,425\,521$
20	$42\,832\,853\,457\,545\,958\,193\,355\,601 = 3 \cdot 127 \cdot 552\,634\,829 \cdot 203\,429\,428\,717\,049$
21	$2\,375\,370\,429\,446\,951\,548\,637\,196\,401 = 58\,967 \cdot 40\,283\,046\,949\,089\,347\,408\,503$
22	$138\,213\,776\,357\,206\,521\,921\,578\,463\,913 =$ $= 13 \cdot 23 \cdot 316\,031 \cdot 1\,462\,683\,827\,323\,261\,743\,877$
23	$8\,419\,259\,736\,788\,826\,438\,132\,968\,480\,177 =$ $= 103 \cdot 5419 \cdot 214\,765\,247 \cdot 70\,234\,990\,225\,477\,963$
24	$535\,823\,088\,031\,930\,481\,975\,544\,151\,644\,865 =$ $= 5 \cdot 24\,821 \cdot 48\,763\,734\,563 \cdot 88\,539\,116\,795\,595\,251$
25	$35\,562\,372\,323\,207\,319\,916\,133\,576\,686\,141\,249 =$ $= 41\,719 \cdot 852\,426\,288\,338\,822\,117\,407\,741\,716\,871$
26	$2\,457\,219\,879\,258\,280\,669\,724\,058\,501\,120\,110\,001 =$ $= 3 \cdot 7 \cdot 31 \cdot 3019 \cdot 92\,269 \cdot 514\,847 \cdot 1\,072\,817\,117 \cdot 24\,532\,410\,559$
27	$176\,482\,312\,353\,646\,748\,226\,944\,999\,299\,114\,553\,465 =$ $= 5 \cdot 7 \cdot 17 \cdot 113 \cdot 3929 \cdot 211\,229 \cdot 3\,162\,788\,888\,980\,701\,288\,689\,959$

Упражнение 9. Если $p \equiv 2 \pmod{17}$ и $p \equiv 5 \pmod 8$, то $(p-1)^p + p^{p-1} \equiv 0 \pmod{17}$. В частности, сумма $52^{53} + 53^{52}$ делится на 17.

Разложение на множители чисел $(r-1)^r + r^{r-1}$ для $r \leqslant 27$ представлено в таблице 8.

§ 14. Криптосистема с открытым ключом Диффи — Хэллмана

Разложение на простые множители и малая теорема Ферма играют важнейшую роль в современной криптографии, а именно при построении криптосистем с открытым ключом.

В настоящее время криптосистемы с открытым ключом получили широкое распространение. По всей видимости, первым был опубликован протокол обмена ключами Диффи — Хэллмана [2]. Алгоритм (протокол) Диффи — Хэллмана активно использует малую теорему Ферма. Дадим краткое описание этого протокола передачи важной информации, например, коммерческой тайны.

Шаг 1. Софья и Макс вместе выбирают простое число p и целое число a, которое имеет порядок $p-1$ по модулю p, т. е. для которого выполнено следующее условие:

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

при этом $a^k \not\equiv 1 \pmod{p}$ для любого положительного числа $k < p-1$.

Шаг 2. Софья выбирает случайное число $n < p$. Макс выбирает случайное число $m < p$.

Шаг 3. Софья отправляет Максу число, равное остатку от деления a^n на p, т. е. число $a^n \pmod{p}$. Макс отправляет Софье число, равное остатку от деления a^m на p, т. е. число $a^m \pmod{p}$.

Шаг 4. Софья вычисляет секретный ключ: $s = a^{nm} = (a^m)^n \pmod{p}$. Аналогично Макс вычисляет секретный ключ: $s = a^{nm} = (a^n)^m \pmod{p}$.

Шаг 5. Софья использует ключ s для шифрования и отправляет зашифрованное сообщение Максу. Макс расшифровывает сообщение с помощью ключа s.

Третьи лица могут знать оба числа $a^n \pmod{p}$ и $a^m \pmod{p}$, но они не смогут использовать их для достаточно быстрого получения n, m или $a^{nm} \pmod{p}$.

Трудности расшифровки связаны с проблемой определения дискретного логарифма.

§ 15. Алгоритм RSA

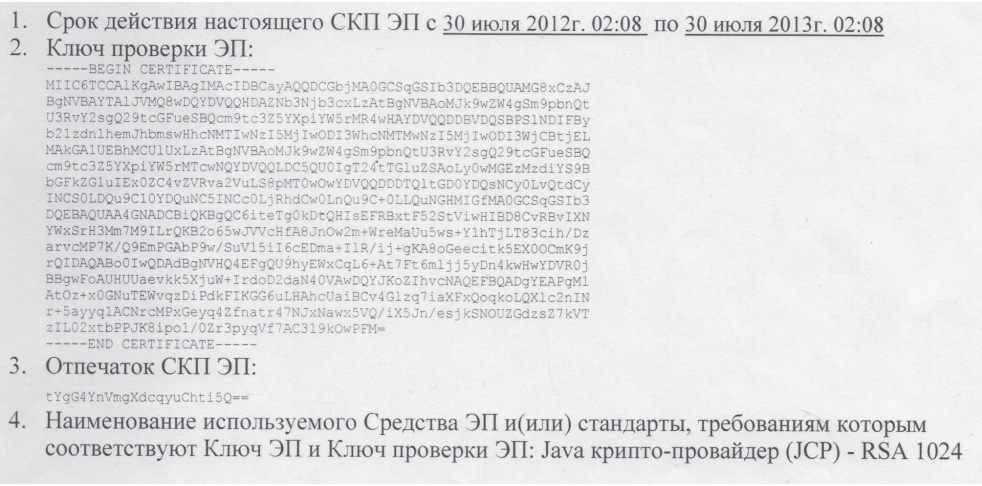
Алгоритм RSA является популярной «криптосистемой с открытым ключом», открытой Л. Адлеманом, Р. Ривестом и А. Шамиром [5].

Предположим, что существует некоторое количество пользователей U_1, U_2, U_3, … Время от времени некоторой паре пользователей необходимо обменяться сообщениями, которые должны оставаться

секретными для всех остальных пользователей. В классической криптосистеме эта пара должна сначала разделить между собой ключи и держать их в секрете. Система с открытым ключом обходит последнее ограничение: для секретного попарного общения достаточно использования лишь доступной всем информации.

Системы с открытым ключом названы так потому, что ключ, используемый при шифровании данных, не является секретным и может быть, например, опубликован в средствах массовой информации. Также несекретным является алгоритм шифрования. Защита данных обеспечивается тем, что для расшифрования необходим другой (секретный) ключ, причём он не может быть определён по открытому ключу зашифрования. Алгоритмы шифрования с открытым ключом называют поэтому несимметричными алгоритмами.

В настоящее время этот алгоритм широко используется в банковской сфере. Например, при открытии банковского счёта владельцу выдаётся сертификат ключа проверки электронной подписи (СКП ЭП). Фрагмент такого сертификата можно увидеть на рис. 2. В правом нижнем углу фрагмента можно увидеть название используемого алгоритма — RSA 1024.



1. Срок действия настоящего СКП ЭП с 30 июля 2012г. 02:08 по 30 июля 2013г. 02:08
2. Ключ проверки ЭП:


```
-----BEGIN CERTIFICATE-----
MIIC6TCCAlKgAwIBAgIMAcIDBCayAQQDCGbjMA0GCSqGSIb3DQEBBQUAMG8xCzAJ
BgNVBAYTAlJVMQ8wDQYDVQQHDAZNb3Njb3cxLzAtBgNVBAoMJk9wZW4gSm9pbnQt
U3RvY2sgQ29tcGFueSBQcm9tc3Z5YXpiYW5rMR4wHAYDVQQDDBVDQSBPSlNDIFBy
b21zdnlhemJhbmswHhcNMTIwNzI5MjIwODI3WhcNMTMwNzI5MjIwODI3WjCBtjEL
MAkGA1UEBhMCUlUxLzAtBgNVBAoMJk9wZW4gSm9pbnQtU3RvY2sgQ29tcGFueSBQ
cm9tc3Z5YXpiYW5rMTcwNQYDVQQLDC5QU0IgT24tTGluZSAoLy0wMGEzMzdiYS9B
bGFkZGluIEx0ZC4vZVRva2VuLS8pMT0wOwYDVQQDDDTQ1tGD0YDQsNCy0LvQtdCy
INCS0LDQu9C10YDQuNC5INCc0LjRhdCw0LnQu9C+0LLQuNGHMIGfMA0GCSqGSIb3
DQEBAQUAA4GNADCBiQKBgQC6iteTg0kDtQHIsEFRBxtF52StViwHIBD8CvRBvIXN
YWxSrH3Mm7M9ILrQKB2o65wJVVcHfA8JnOw2m+WreMaUu5ws+Y1hTjLT83cih/Dz
arvcMP7K/Q9EmPGAbP9w/SuVl5iI6cEDma+I1R/ij+gKA8oGeecitk5EX0OCmK9j
rQIDAQABo0IwQDAdBgNVHQ4EFgQU9hyEWxCqL6+At7Ft6mljj5yDn4kwHwYDVR0j
BBgwFoAUHUUaevkk5XjuW+IrdoD2daN40VAwDQYJKoZIhvcNAQEFBQADgYEAPgM1
AtOz+x0GNuTEWvqzDiPdkFIKGG6uLHAhcUaiBCv4Glzq7iaXFxQoqkoLQXlc2nIN
r+5ayyqlACNrcMPxGeyq4Zfnatr47NJxNawx5VQ/iX5Jn/esjkSNOUZGdzsZ7kVT
zIL02xtbPPJK8ipol/0Zr3pyqVf7AC319kOwPFM=
-----END CERTIFICATE-----
```


3. Отпечаток СКП ЭП:


```
tYgG4YnVmgXdcqyuChti5Q==
```


4. Наименование используемого Средства ЭП и(или) стандарты, требованиям которым соответствуют Ключ ЭП и Ключ проверки ЭП: Java крипто-провайдер (JCP) - RSA 1024

Рис. 2. Фрагмент Сертификата ключа проверки электронной подписи (СКП ЭП)

Согласно методу RSA для генерирования ключей необходимо выполнить следующие действия.

Шаг 1. Каждый пользователь U_i:

а) выбирает два больших простых числа p_i и q_i;

б) находит произведение этих чисел $n_i = p_i \cdot q_i$;

в) выбирает число d_i, взаимно простое с числом $\varphi(n_i)=(p_i-1)(q_i-1)$, где $\varphi(m)$ обозначает функцию Эйлера;

г) определяет число e_i, для которого выполняется условие $e_i d_i \equiv 1 \pmod{\phi(n_i)}$.

Числа d_i и e_i рассматриваются как остатки по модулю $n_i = p_i \cdot q_i$.

Шаг 2. Пары чисел (e_i, n_i) объявляются всем пользователям. Они называются открытым ключом.

Практически невозможно вычислить d_i, зная лишь (e_i, n_i). Так что числа d_i являются секретными данными.

Действительно, эффективный алгоритм нахождения d_i должен был бы также эффективно раскладывать на множители числа n_i, что по предположению является невыполнимо сложным.

Пусть нам известны числа d_i. Тогда $\varphi(n_i)$ делит $e_i d_i - 1$. Если бы мы знали сами числа $\varphi(n_i)$, то могли бы легко найти p_i и q_i, поскольку

$$p_i + q_i = n_i + 1 - \phi(n_i), \quad p_i - q_i = \sqrt{(p_i + q_i)^2 - 4n_i}.$$

Шаг 3. Зашифрованное сообщение представляется последовательностью битов. Предположим, что пользователю U_i необходимо передать это сообщение пользователю U_j. Сначала он разделяет последовательность битов на блоки длины $[\log_2 n_j]$. Затем он рассматривает каждый блок как некоторый остаток $m \pmod{n_j}$ и шифрует его как остаток $b = m^{e_j} \pmod{n_j}$. Таким образом, пара (n_j, e_j) служит шифрующим ключом j-го пользователя (напомним, что она известна всем пользователям).

Шаг 4. Получив зашифрованное сообщение, пользователь U_j дешифрует каждый блок $b \pmod{n_j}$, вычисляя остаток $b = m^{e_j} \pmod{n_j}$ (напомним, что ему известен дешифрующий ключ d_j). Результат легко проверить при помощи малой теоремы Ферма.

Детали этой схемы могут меняться. Например, аналогично можно построить процедуру аутентификации пользователя («электронная подпись») и т. п.

Пример. Рассмотрим алгоритм RSA, основанный на небольших числах p_i и q_i.

Предположим, что у нас есть два пользователя U_1, U_2 и шифрованию подлежит сообщение на русском языке. Буквы сообщения можно представить числами от 0 до 32.

Первый пользователь выбирает $p_1=3$, $q_1=11$ и находит $n_1=3\cdot 11=33$.

Второй пользователь выбирает $p_2=5$, $q_2=7$ и находит $n_2=5\cdot 7=35$.

Согласно описанному алгоритму:

в) первый пользователь в качестве числа d_1, взаимно простого с числом $(p_1-1)(q_1-1)=20$, выбирает число 3; второй пользователь в качестве числа d_2, взаимно простого с числом $(p_2-1)(q_2-1)=24$, выбирает число 5.

г) соотношению $e_1d_1=3e_1\equiv 1 \pmod{20}$ удовлетворяют числа $7, 27, 47, \ldots$, выберем $e_1=7$; соотношению $e_2d_2=5e_2\equiv 1 \pmod{24}$ удовлетворяют числа $5, 29, 53, \ldots$, выберем $e_2=5$.

Итак, открытыми ключами для шифрования являются пары чисел $e_1=7$, $n_1=33$ и $e_2=5$, $n_2=35$. Закрытыми (секретными) ключами — числа $d_1=3$ и $d_2=5$.

Зашифруем слово КВАНТ. Буквам К, В, А, Н и Т сопоставим числа 11, 03, 01, 14 и 19. Для простоты мы нумеруем буквы по порядку, считая Е и Ё одной буквой. Используя открытый ключ, получим криптограмму (Шаг 3), состоящую из чисел:

$C_1=11^5=161\,051 \pmod{35}\equiv 16 \pmod{35}$;
$C_2=3^5=243 \pmod{35}\equiv 33 \pmod{35}$;
$C_3=1^5=1 \pmod{35}\equiv 1 \pmod{35}$;
$C_4=14^5=537\,824 \pmod{35}\equiv 14 \pmod{35}$;
$C_5=19^5=2\,476\,099 \pmod{35}\equiv 24 \pmod{35}$.

Для расшифрования криптограммы $\{16, 33, 01, 14, 24\}$ второй пользователь использует формулу (Шаг 4) и секретный ключ $e_2=5$:

$M_1=16^5=1\,048\,576 \pmod{35}\equiv 11 \pmod{35}$;
$M_2=33^5=39\,135\,393 \pmod{35}\equiv 3 \pmod{35}$;
$M_3=1^5=1 \pmod{35}\equiv 1 \pmod{35}$;
$M_4=14^5=537\,824 \pmod{35}\equiv 14 \pmod{35}$;
$M_5=24^5=7\,962\,624 \pmod{35}\equiv 19 \pmod{35}$.

Как видим, в результате расшифрования получилось исходное сообщение КВАНТ.

Отметим, что на практике применяются настолько большие числа p_i и q_i, что, зная лишь e_i и n_i (открытый ключ), невозможно найти d_i за приемлемое время. Сейчас не только неизвестен достаточно эффективный (полиномиальный) алгоритм разложения большого числа на простые множители, но остаётся открытым и сам вопрос о существовании таких алгоритмов (а следовательно, о возможности взлома систем с открытым ключом в будущем).

Однако нельзя исключить открытие в дальнейшем эффективных алгоритмов определения делителей целых чисел (факторизации), вследствие чего метод шифрования с открытым ключом станет абсолютно

бесполезным. Пока этого не произошло, метод RSA имеет важные преимущества перед другими криптосистемами, такие как очень высокая криптостойкость и простота аппаратной и программной реализации.

§ 16. Краткие комментарии к вычислениям. Тест Бейли — Померанца — Селфриджа — Уогстаффа (BPSW)

Мы упоминали, что для разложения чисел на множители мы использовали онлайн-калькулятор [27].

Программа, написанная студентом Джонатаном Хашпером, подтвердила простоту чисел, найденных онлайн-калькулятором, и, как мы уже упоминали, нашла ещё пять простых чисел:

$$\begin{gathered} 2^{2007}+2007^2, \quad 2^{2127}+2127^2, \quad 2^{3759}+3759^2, \\ 5^{1036}+1036^5, \quad 7^{3076}+3076^7 \end{gathered} \tag{!}$$

Для своей программы Дж. Хашпер использовал тест на простоту Бейли — Померанца — Селфриджа — Уогстаффа. Это алгоритм вероятностной проверки на простоту. Он назван по фамилиям своих создателей — Роберта Бэйли, Карла Померанца, Джона Селфриджа, Сэмюэля Вагстаффа. Более подробно об этом тесте можно прочитать в [4, 26].

Погнавшись за обманчивой простотой школьной задачи, мы шаг за шагом дошли до серьёзных теорем, тестов на простоту и алгоритмов шифрования. С помощью компьютера мы нашли интересные простые числа и придумали аналог теста Люка для них. Появилась гипотеза о бесконечности количества простых чисел вида 2^n+n^2. Мы получили больше вопросов, чем ответов. Но мы надеемся, что часть вопросов будет решена уже в обозримом будущем.

§ 17. Ответы, указания, решения

Решение задач

1. 2) Квадрат числа, не кратного трём, даёт остаток 1 при делении на 3. Следовательно, каждое слагаемое даёт остаток 1, а их сумма делится на 3.

3) Выражение $2^{2145}+3^{2145}=(2^{15})^{143}+(3^{15})^{143}$ делится на $2^{15}+3^{15}$. Далее,

$$2^{15}+3^{15}=(2^5+3^5)(2^{10}-2^5\cdot 3^5+3^{10})=275\cdot 52\,297=25\cdot 11\cdot 7\cdot 31\cdot 241.$$

Отсюда следует делимость на 11, 241 и $341=11\cdot 31$.

2. 1) Имеем

$$2222^{5555} + 5555^{2222} = \\ = (2222^{5555} + 4^{5555}) + (5555^{2222} - 4^{2222}) - (4^{5555} - 4^{2222}).$$

Выражение в первой скобке делится на $2222 + 4 = 2226 = 7 \cdot 318$, следовательно, делится на 7. Выражение во второй скобке делится на $5555 - 4 = 5551 = 7 \cdot 793$, следовательно, делится на 7.

Преобразуем третье выражение:

$$4^{5555} - 4^{2222} = 4^{2222}(64^{1111} - 1).$$

Теперь видно, что третье выражение делится на $64 - 1 = 63$, следовательно, делится на 7.

Поскольку каждое из выражений делится на 7, их сумма также делится на 7.

2) Имеем

$$\begin{aligned} 222^{555} + 555^{222} &= 111^{555} \cdot 2^{555} + 111^{222} \cdot 5^{222} = \\ &= 111^{222}(111^{333} \cdot 2^{555} + 5^{222}) = \\ &= 111^{222}((111^3 \cdot 2^5)^{111} + 25^{111}), \end{aligned}$$

поэтому сумма делится на 111^{222} и на $111^3 \cdot 2^5 + 25 = 43\,764\,217 = 7 \cdot 6\,252\,031$.

3) Имеем

$$30^{239} \equiv (-1)^{239} \equiv -1 \pmod{31}.$$

Поскольку НОД$(239, 31) = 1$ и 31 — простое число, применив малую теорему Ферма, получим $239^{30} \equiv 1 \pmod{31}$. Следовательно,

$$30^{239} + 239^{30} \equiv -1 + 1 \equiv 0 \pmod{31},$$

т. е. сумма делится на 31 и является составным числом.

Замечание. Можно, конечно, представить сумму в виде

$$30^{239} + 239^{30} = (30^{239} + 1^{239}) + (239^{30} - 1^{30}).$$

Понятно, что выражение в первой скобке делится на 31. Разложим выражение во второй скобке на множители:

$$239^{30} - 1^{30} = (239^{15} + 1)(239^{15} - 1).$$

Увидеть без малой теоремы Ферма, что первый сомножитель делится на 31, достаточно трудно, поскольку ни $239 + 1 = 240$, ни $239^3 + 1$, ни $239^5 + 1$ на 31 не делятся.

3. а) Докажем, что выражение $19^{71} + 71^{19} - 90$ делится на 360. Имеем

$$19^{71} + 71^{19} - 90 = 19^{71} - 19 + 71^{19} - 71 = \\ = 19(19^{70} - 1) + 71(71^{18} - 1) = 19(361^{35} - 1) + 71(5041^{9} - 1).$$

Применяя формулы сокращённого умножения, видим, что первое слагаемое делится на $360 = 361 - 1$. Второе слагаемое делится на $5041 - 1 = 5040 = 360 \cdot 14$ и также делится на 360. Значит, сумма делится на 360. Тогда $19^{71} + 71^{19} - 90 = 360m$ для некоторого натурального m. Отсюда следует утверждение задачи.

б) Поступим аналогично. Докажем, что выражение $19^{77} + 77^{19} - 96$ делится на 456. Имеем

$$19^{77} + 77^{19} - 96 = 19^{77} - 19 + 77^{19} - 77 = 19(19^{76} - 1) + 77(77^{18} - 1).$$

Рассмотрим первое слагаемое. Поскольку $456 = 19 \cdot 24$, достаточно доказать, что множитель $19^{76} - 1$ делится на 24. Имеем $19^{76} - 1 = (19^2)^{38} - 1$. Этот множитель делится на $19^2 - 1 = 360 = 24 \cdot 15$, т. е. делится на 24. Следовательно, первое слагаемое делится на 456.

Рассмотрим второй множитель второго слагаемого

$$77^{18} - 1 = (77^2)^9 - 1.$$

Он делится на $77^2 - 1 = (77 - 1)(77 + 1) = 76 \cdot 78 = 456 \cdot 13$, т. е. делится на 456. Следовательно, сумма делится на 456.

Тогда $19^{77} + 77^{19} - 96 = 456n$ для некоторого натурального n. Отсюда следует утверждение задачи.

4. Поскольку p и q — различные простые числа (и, следовательно, взаимно просты), применима малая теорема Ферма. Имеем

$$p^q + q^p \equiv pp^{q-1} \equiv p \pmod q,$$
$$p^q + q^p \equiv qq^{p-1} \equiv q \pmod p.$$

Остаётся применить китайскую теорему об остатках.

6. Для любого $k \in \mathbb{N}$ число $m^4 + 4k^4$ будет составным. См. решение упражнения 1.

Решения упражнений

1. Имеем

$$n^4 + 4m^4 = n^4 + 4n^2m^2 + 4m^4 - 4n^2m^2 = \\ = (n^2 + 2m^2)^2 - (2nm)^2 = (n^2 + 2nm + 2m^2)(n^2 - 2nm + 2m^2).$$

2. а) Последовательность $\{r'_n\}$, где r'_n — остаток от деления n^5 на 3, периодична с периодом 3. Её начальные члены равны $0, 1, 2, 0, 1, 2, \ldots$

Последовательность $\{r''_n\}$, где r''_n — остаток от деления 5^n на 3, периодична с периодом 2. Её начальные члены равны $1, 2, 1, 2, \ldots$ Тогда последовательность $\{r_n\}$, где r_n — остаток от деления $5^n + n^5$ на 3, периодична с периодом 6. Её начальные члены равны $1, 0, 0, 2, 2, 1, 1, \ldots$

Следовательно, остаток от деления $5^n + n^5$ на 3 равен нулю только в случаях $n=6k+1$, $n=6k+2$, где $k\in\mathbb{Z}$, $k \geqslant 0$. Наименьшим будет $n=1$.

б) Последовательность $\{r'_n\}$, где r'_n — остаток от деления n^5 на 7, периодична с периодом 7. Её начальные члены равны $0, 1, 4, 5, 2, 3, 6, \ldots$ Последовательность $\{r''_n\}$, где r''_n — остаток от деления 5^n на 7, периодична с периодом 6. Её начальные члены равны $1, 5, 4, 6, 2, 3, \ldots$ Тогда последовательность $\{r_n\}$, где r_n — остаток от деления $5^n + n^5$ на 7, периодична с периодом 42. Её начальные члены равны $1, 6, 1, 4, 4, 6, 0, \ldots$

Следовательно, остаток от деления $5^n + n^5$ на 7 равен нулю только в случаях $n=42k+6$, $n=42k+10$, $n=42k+15$, $n=42k+23$, $n=42k+25$, $n = 42k + 26$, где $k \in \mathbb{Z}$, $k \geqslant 0$. Наименьшим будет $n = 6$.

в) Последовательность $\{r'_n\}$, где r'_n — остаток от деления n^5 на 11, периодична с периодом 11. Её начальные члены равны $0, 1, 10, 1, 1, 1, \ldots$ Последовательность $\{r''_n\}$, где r''_n — остаток от деления 5^n на 11, периодична с периодом 5. Её начальные члены равны $1, 5, 3, 4, 9, \ldots$ Тогда последовательность $\{r_n\}$, где r_n — остаток от деления $5^n + n^5$ на 11, периодична с периодом 55. Её начальные члены равны $1, 6, 2, 5, 10, 2, 4, \ldots$

Следовательно, остаток от деления $5^n + n^5$ на 11 равен нулю только в случаях $n=55k+10$, $n=55k+30$, $n=55k+35$, $n=55k+40$, $n=55k+50$, где $k \in \mathbb{Z}$, $k \geqslant 0$.

Наименьшим будет $n = 10$.

3. При $p = 2$ подойдёт любое нечётное n. В этом случае $5^n + n^5$ делится на 2.

При $p = 5$ подойдёт любое n, делящееся на 5. В этом случае $5^n + n^5$ делится на 5.

Рассмотрим нечётное простое $p \neq 5$. Поскольку 5 и p взаимно просты, можно применить малую теорему Ферма, получив для $n = p - 1$:

$$5^{p-1} + (p-1)^5 \equiv 1 + (-1)^5 \equiv 0 \pmod{p}.$$

Учтём периодичность последовательности и возьмём теперь

$$n = (p-1)pk + p - 1 = (p-1)(pk+1).$$

Имеем НОД$(n, p) = 1$, откуда

$$5^{(p-1)(pk+1)} + ((p-1)pk + p - 1)^5 \equiv$$
$$\equiv (5^{(p-1)})^{(pk+1)} + (-1)^5 \equiv 1 - 1 \equiv 0 \pmod{p}.$$

Что и требовалось доказать!

4. а) Последовательность $\{r'_n\}$, где r'_n — остаток от деления n^2 на 5, периодична с периодом 5. Её начальные члены равны $0, 1, 4, 4, 1, \ldots$ Последовательность $\{r''_n\}$, где r''_n — остаток от деления 2^n на 5, периодична с периодом 4. Её начальные члены равны $1, 2, 4, 3, \ldots$ Тогда последовательность $\{r_n\}$, где r_n — остаток от деления $2^n + n^2$ на 5, периодична с периодом 20. Её начальные члены равны $1, 3, 3, 2, 2, 2, 0, \ldots$

Следовательно, остаток от деления $2^n + n^2$ на 5 равен нулю только в случаях $n = 20k+6$, $n = 20k+8$, $n = 20k+12$, $n = 20k+14$, где $k \in \mathbb{Z}$, $k \geqslant 0$.

б) Последовательность $\{r'_n\}$, где r'_n — остаток от деления n^2 на 11, периодична с периодом 11. Её начальные члены равны 0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1, … Последовательность $\{r''_n\}$, где r''_n — остаток от деления 2^n на 11, периодична с периодом 10. Её начальные члены равны 1, 2, 4, 8, 5, 10, 9, 7, 3, 6, … Тогда последовательность $\{r_n\}$, где r_n — остаток от деления $2^n + n^2$ на 11, периодична с периодом 110. Её начальные члены равны 1, 3, 8, 6, 10, 2, 1, …

Следовательно, остаток от деления $2^n + n^2$ на 11 равен нулю только в случаях $n = 110k + t$, где $t \in \{29, 41, 45, 57, 59, 65, 83, 91, 93, 97\}$ и $k \in \mathbb{Z}$, $k \geqslant 0$.

5. а) Остатками от деления n^2 на 7 являются числа $\{0, 1, 2, 4\}$. Остатками от деления 2^n на 7 являются числа $\{1, 2, 4\}$. Тогда возможные остатки от деления $2^n + n^2$ на 7 будут $\{1, 2, 3, 4, 5, 6\}$. Следовательно, $2^n + n^2$ не делится на 7 ни для какого натурального n.

б) Рассмотрим простые числа вида $p = 8k - 1$, где $k \in \mathbb{Z}$, $k \geqslant 0$. Таких чисел бесконечно много в силу теоремы Дирихле о простых числах в арифметических прогрессиях. Для таких простых чисел сумма $2^n + n^2$ не делится на p ни для какого натурального n.

6. Пусть $n = pq$ — составное число, где $p \geqslant 2$, $q \geqslant 2$. Тогда $2^n - 1 = 2^{pq} - 1 = (2^q)^p - 1^p$ делится на $2^q - 1$.

7. Докажем с помощью теста Люка, что число

$$m = 2^{15} + 15^2 = 32\,993$$

— простое.

Найдём разложение числа $m - 1 = 2^{15} + 15^2 - 1$ на простые множители. Имеем $2^{15} + 15^2 - 1 = 2^5 \cdot 1031$.

В качестве кандидата возьмём $b = 3$. Нам нужно найти вычеты

$$3^{m-1} = 3^{2^{15}+15^2-1}, \quad 3^{(m-1)/2} = 3^{2^4 \cdot 1031}, \quad 3^{(m-1)/1031} = 3^{2^5}$$

по модулю $m = 32\,993$.

Начнём с вычета $3^{(m-1)/1031} = 3^{2^5}$. Имеем

$$3^{2^5} = 3^{32} = (3^4)^8 = (81^2)^4 \equiv (6561^2)^2 \equiv 23\,849^2 \equiv 8474 \pmod{32\,993}.$$

Далее,

$$3^{1031} = 3^{2^{10}+7} = 3^7 \cdot (3^{32})^{32} \equiv 3^7 \cdot (8474^2)^{16} \equiv 3^7 \cdot (15\,908^2)^8 \equiv$$
$$\equiv 3^7 \cdot (8154^2)^4 \equiv 3^7 \cdot (6821^2)^2 \equiv 3^7 \cdot 5911^2 \equiv 4612 \pmod{32\,993};$$
$$3^{(m-1)/2} = 3^{2^4 \cdot 1031} = (3^{1031})^{16} \equiv (4612^2)^8 \equiv (23\,052^2)^4 \equiv$$
$$\equiv (9446^2)^2 \equiv 13\,844^2 \equiv 32\,992 \equiv -1 \pmod{32\,993}.$$

Наконец,

$$3^{m-1} = 3^{2^{15}+15^2-1} \equiv (-1)^2 \equiv 1 \pmod{32\,993}.$$

Итак,

$$3^{m-1} \equiv 1 \pmod{m},$$
$$3^{(m-1)/2} \not\equiv 1 \pmod{m},$$
$$3^{(m-1)/1031} \not\equiv 1 \pmod{m}.$$

Согласно тесту Люка число $m = 2^{15} + 15^2 = 32\,993$ — простое.

Читатель может убедиться самостоятельно, что для $b = 2$ тест даёт неопределённый ответ.

8. По условию имеем $p = 20k + 7$, где $k \in \mathbb{Z}$, $k \geqslant 0$. Тогда

$$(p-1)^p + p^{p-1} = (20k+6)^{20k+7} + (20k+7)^{20k+6} \equiv 1^{20k+7} + 2^{20k+6} \equiv$$
$$\equiv 1 + 4^{10k+3} \equiv 1 + (-1)^{10k+3} \equiv 1 - 1 \equiv 0 \pmod{5}.$$

9. По условию имеем $p = 17k_1 + 2$ и $p = 8k_2 + 5$, где $k_i \in \mathbb{Z}$, $k_i \geqslant 0$, $i = 1, 2$. Отсюда

$$(p-1)^p + p^{p-1} = (17k_1+1)^p + (17k_1+2)^{p-1} \equiv 1^p + 2^{8k_2+4} \equiv$$
$$\equiv 1 + 16^{2k_2+1} \equiv 1 + (-1)^{2k_2+1} \equiv 1 - 1 \equiv 0 \pmod{17}.$$

Замечание. С помощью китайской теоремы об остатках можно получить, что $p = 136k + 53$, где $k \in \mathbb{Z}$, $k \geqslant 0$.

Список литературы

[1] *Koninck J.-M. de.*, *Mercier A.* 1001 Problemes en Théorie Classique Des Nombres. Problem 165 pp. 30, 160. Paris: Ellipses, 2004.

[2] *Diffie W.*, *Hellman M. E.* New directions in cryptography // IEEE Trans. Inform. Theory. 1976. Vol. 22. P. 644–654.

[3] *Everest G.*, *Poorten A. van der.*, *Shparlinski I.*, *Ward T.* Recurrence Sequences // Amer. Math. Soc., 2003; see esp. p. 255.

[4] *Pomerance C.*, *Selfridge J. L.*, *Wagstaff S. S.*, *Jr.* The pseudoprimes to 25×10^9 // Math. Comp. 1980. Vol. 35, № 151. P. 1003–1026.

[5] *Rivest R.*, *Shamir A.*, *Adleman L.* A method for obtaining digital signatures and public-key cryptosystems (англ.) // Commun. ACM. 1978. Vol. 21, № 2. P. 120–126.

[6] *Варновский Н. П.* Криптография и теория сложности // Математическое просвещение. Сер. 3. Вып. 2. М.: МЦНМО, 1998. С. 71–86.

[7] *Виноградов И. М.* Основы теории чисел. М.: Ленанд, 2022.

[8] *Воробьёв Н. Н.* Признаки делимости. М.: Наука, 1980.

[9] *Горбачёв Н. В.* Сборник олимпиадных задач по математике. М.: МЦНМО, 2010.

[10] *Дайан-Дальмедико Эми.* Софи Жермен // В мире науки. 1992. № 2. С. 60–66.

[11] Задачник Кванта, М663 // Квант. 1981. № 1. С. 26.

[12] Зарубежные математические олимпиады. М.: Наука, 1987.

[13] *Кордемский Б. А.*, *Ахадов А. А.* Удивительный мир чисел: Математические головоломки и задачи для любознательных. М.: Просвещение, 1986.

[14] *Коутинхо С.* Введение в теорию чисел. Алгоритм RSA. М.: Постмаркет, 2001.

[15] *Манин Ю. И.*, *Панчишкин А. А.* Введение в современную теорию чисел. М.: МЦНМО, 2009.

[16] Математика в задачах. М.: МЦНМО, 2009.

[17] *Нестеренко Ю. В.* Алгоритмические проблемы теории чисел // Математическое просвещение. Сер. 3. Вып. 2. М.: МЦНМО, 1998. С. 87–114.

[18] *Оре О.* Приглашение в теорию чисел. М.: Наука, 1980. (Серия «Библиотечка „Квант“»; Вып. 3).

[19] *Прасолов В. В.* Доказательство квадратичного закона взаимности по Золотарёву // Математическое просвещение. Сер. 3. Вып. 4. М.: МЦНМО, 2000. С. 140–144.

[20] *Рудаков А. Н.* Числа Фибоначчи и простота числа $2^{127}-1$ // Математическое просвещение. Сер. 3. Вып. 4. М.: МЦНМО, 2000. С. 127–139.

[21] *Суконник Я. Н.* Математические задачи повышенной трудности. Киев: Радянська школа, 1985.

[22] *Хооли К.* Применения методов решета в теории чисел. М.: Наука, 1987.

[23] *Шклярский Д. О.*, *Ченцов Н. Н.*, *Яглом И. М.* Избранные задачи и теоремы элементарной математики. Арифметика и алгебра. М.: Наука, 1976.

[24] *Ященко В. В.* Основные понятия криптографии // Математическое просвещение. Сер. 3. Вып. 2. М.: МЦНМО, 1998. С. 53–70.

[25] XV Всероссийская олимпиада по математике и физике // Квант. 1989. № 10. С. 67–70.

[26] https://ru.wikipedia.org/wiki/

[27] https://cocalc.com/

[28] http://oeis.org/

[29] https://primes.utm.edu/mersenne/index.html#known

Валерий Михайлович Журавлёв, ПАО «Туполев», Москва
zhuravlevvm@mail.ru

Пётр Исаакович Самовол, Беер-Шева, Израиль
pet12@012.net.il

Геометрия

О построении линейкой центров окружностей*

А. А. Заславский

Глава 26 замечательной книги [1] называется «О необходимости циркуля в построениях элементарной геометрии». Основное содержание этой главы составляет доказательство невозможности построения одной линейкой центра окружности. Невозможность такого построения следует из существования центральной проекции, переводящей окружность в окружность, а центр исходной окружности — в точку, не совпадающую с центром её образа. Действительно, поскольку при такой проекции все прямые переходят в прямые, а точки пересечения прямых друг с другом и исходной окружностью в точки пересечения образов прямых друг с другом и образом окружности, то, проецируя построение центра исходной окружности, мы получили бы построение центра её образа, что не имеет места.

Г. Радемахер и О. Тёплиц указывают также, что существует центральная проекция, переводящая две непересекающиеся, неконцентрические окружности в окружности, но не сохраняющая центры. Из этого они делают вывод, что центры двух таких окружностей тоже нельзя построить одной линейкой. (В брошюре [2] показано, как построить одной линейкой центры двух пересекающихся, касающихся или концентрических окружностей, а также трёх несоосных окружностей.) В примечании от редактора говорится, что этот вывод некорректен, поскольку центральная проекция не является взаимно однозначным отображением и прямые, пересекающиеся на исходной плоскости, могут про-

* См. задачу 17.5 (вып. 17, с. 196).

ецироваться в параллельные, а тогда мы не сможем спроецировать построение центров (для одной окружности это затруднение легко обойти, поскольку центр и плоскость проекции можно выбрать бесконечно многими способами). Более того, в работе [3] утверждается, что для некоторых (не для всех!) пар непересекающихся окружностей построить центры непересекающихся окружностей одной линейкой можно.

На самом деле, последнее утверждение нуждается в уточнении. В [3] предполагается, что при построении линейкой можно не только проводить прямые через две отмеченные точки и отмечать точки пересечения проведённых линий или случайные точки, но и определять, являются ли две построенные прямые параллельными. Это предположение можно считать оправданным, если построения проводятся в графическом редакторе (например, Geogebra), который по координатам двух точек строит уравнение проходящей через них прямой, а по уравнениям двух прямых находит координаты точки их пересечения или сообщает об отсутствии таковой (впрочем, и в этом случае необходима абсолютная точность вычислений, недостижимая в реальной жизни). Если же речь идёт о построении карандашом на бумаге, то установить, действительно ли две прямые параллельны или мы просто не смогли провести их до точки пересечения, можно не всегда.

Строго говоря, на вопрос о возможности построения одной линейкой центров двух непересекающихся, неконцентрических окружностей нельзя дать однозначного ответа, пока не формализовано понятие «построение одной линейкой». Можно предложить, как минимум, три формализации.

1. Построение проводится на евклидовой плоскости и представляет последовательность следующих операций:

— отметить случайную точку на плоскости, данной или построенной ранее линии;
— провести прямую через две отмеченные точки:
— отметить точку пересечения двух данных или построенных ранее линий, либо убедиться, что такой точки не существует.

В этом случае, как показано в [3], существуют пары окружностей, для которых центры построить можно, и пары окружностей, для которых центры построить нельзя.

2. Построение проводится в ограниченной области евклидовой плоскости и представляет последовательность следующих операций:

— отметить лежащую в данной области случайную точку плоскости, данной или построенной ранее линии;

— построить лежащий в данной области отрезок прямой, соединяющей две отмеченные точки;
— отметить точку пересечения данных или построенных линий, если она лежит в данной области.

Заметим, что «недоступность» точки пересечения двух построенных прямых не препятствует использованию этой точки в дальнейших построениях, поскольку можно построить прямую, соединяющую недоступную и отмеченную точки, а также найти точку пересечения прямой, проходящей через две недоступные точки, с другой прямой. Решения этих задач можно найти в [4].

Очевидно, что в этой формализации мы не можем отличить параллельные прямые от пересекающихся вне данной области. Поэтому приведённое в [1] рассуждение становится корректным и центры непересекающихся окружностей построить нельзя.

3. Построение проводится на проективной плоскости и представляет последовательность следующих операций:

— отметить случайную точку на плоскости, данной или построенной ранее линии;
— провести прямую через две отмеченные точки;
— отметить точку пересечения данных или ранее построенных линий.

При этом мы не можем отличить конечную точку пересечения от бесконечно удалённой.

В этой формализации мы также не можем отличить параллельные прямые от пересекающихся. Соответственно построить центры нельзя.

Заметим, что с практической точки зрения две последние формализации одинаковы: недоступные точки могут оказаться как конечными, так и бесконечно удалёнными.

Можно предположить, что авторы книги [1] имели в виду вторую формализацию, моделирующую процесс построения на бумаге. С другой стороны, в статье [3] используется первая формализация, соответствующая современным компьютерным построениям. Именно этим объясняется различие полученных ответов.

Список литературы

[1] *Радемахер Г., Тёплиц О.* Числа и фигуры. М.: МЦНМО, 2020.

[2] *Смогоржевский А. С.* Линейка в геометрических построениях. М.: Гостехиздат, 1957.

[3] *Akopyan A.*, *Fedorov R.* Two circles and only straightedge. arXiv:1709.02562[mayh.MG].

[4] *Яглом И. М.* Геометрические преобразования. Т. 2. М.: Гостехиздат, 1956.

Алексей Александрович Заславский, ЦЭМИ РАН, МЭИ
alzasl@yandex.ru

Антибиссектрисы: знакомые — незнакомые

В. М. Журавлёв, П. И. Самовол

§ 1. Введение: постановка задачи

В этой заметке мы хотим предложить читателям поразмыслить над следующей задачей про антибиссектрисы[1)].

Задача 1.

(а) *Однозначно ли определяется треугольник по длинам своих антибиссектрис*?

(б) *Для любых ли длин антибиссектрис существует треугольник с такими антибиссектрисами*?

(в) *Можно ли построить треугольник по трём антибиссектрисам циркулем и линейкой*?

Аналогичные задачи для медиан и высот входят в школьные учебники. Задаче для случая биссектрис около 150 лет, и она регулярно упоминается в математической литературе [2, 8]:

Для любых ли длин биссектрис существует треугольник с такими биссектрисами и однозначно ли определяется?

Можно ли построить треугольник по трём биссектрисам циркулем и линейкой?

Для задачи о биссектрисах найдено несколько различных решений, в том числе и доступных школьникам.

[1)] Две точки на стороне треугольника, равноотстоящие от середины этой стороны, называются *изотомическими* (*изотомически сопряжёнными*) точками. Аналогично, две прямые, соединяющие вершину треугольника с изотомическими точками противоположной стороны, называются *изотомическими прямыми* треугольника. Прямые, изотомические с внутренними или внешними биссектрисами треугольника, называются соответственно внутренними или внешними *антибиссектрисами* этого треугольника.

Для случая симедиан задача также решена, хотя она не так известна, как задача про биссектрисы (см. [5]):

Однозначно ли определяется треугольник по длинам своих симедиан?

Для любых ли длин симедиан существует треугольник с такими симедианами?

Можно ли построить треугольник по трём симедианам циркулем и линейкой?

С решением задачи про симедианы можно ознакомиться в [4, 5].

§ 2. Антибиссектрисы — не такие, как все

Известно, что треугольник однозначно определяется по длинам трёх своих медиан. То же утверждение верно для высот, биссектрис и симедиан. Можно ожидать, что это утверждение верно для антибиссектрис. Но так ли это?

В «Математическом просвещении» мы уже рассказывали об антибиссектрисах [3]. Поэтому выберем факты об антибиссектрисах, которые нам понадобятся, и сформулируем их в виде упражнений. Доказательства читатель может найти самостоятельно или ознакомиться с ними в упомянутом источнике.

Используем общепринятые обозначения. Пусть a, b, c — длины сторон треугольника. Через k_a, k_b, k_c обозначим длины антибиссектрис, проведённых к сторонам длины a, b, c соответственно.

Упражнение 1. Докажите, что треугольник является равнобедренным тогда и только тогда, когда две его антибиссектрисы равны.

Упражнение 2. Если $a \geqslant b \geqslant c$, то $k_a \leqslant k_b \leqslant k_c$.

Другими словами, бóльшая антибиссектриса проведена к меньшей стороне.

Упражнение 3. Докажите, что квадрат длины антибиссектрисы можно найти по формуле

$$k_a^2 = b^2 + c^2 - bc - \frac{a^2bc}{(b+c)^2}. \qquad (1)$$

Оказывается, ответ на пункт (а) задачи 1 — отрицательный. По длинам своих антибиссектрис треугольник не определяется однозначно.

Задача 2. Докажите, что существуют два неконгруэнтных треугольника, у которых совпадают длины трёх соответствующих антибиссектрис.

Более того, мы найдём два неравных равнобедренных треугольника, у которых совпадают длины антибиссектрис.

Решение. Рассмотрим равнобедренный треугольник ABC (рис. 1). Пусть $BC = AC = a = b$, $AB = c$ и $a = b \geqslant c$, тогда $k_a = k_b \leqslant k_c$ согласно упражнению 2. Обозначим $\angle ACB = \gamma$ и $t = \sin(\gamma/2)$. Тогда $c = 2at$.

Зафиксируем длину большей антибиссектрисы, положив $k_c = 1$. Будем изменять угол γ от 0 до $\pi/3$, тогда переменная $t = \sin(\gamma/2)$ изменяется от 0 до $1/2$. (При $\gamma = 0$ имеем $t = 0$ и получим вырожденный треугольник.) Длина другой антибиссектрисы будет являться функцией от t. Обозначим $k_a = k_b = y(t)$.

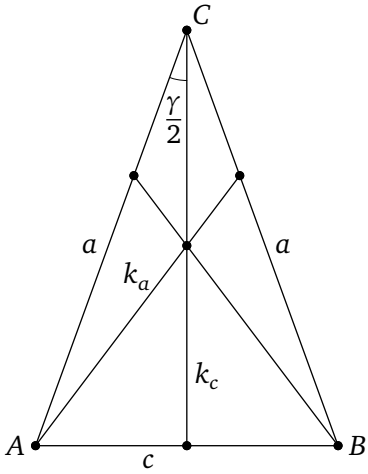


Рис. 1

Из упражнения 3 находим

$$1 = k_c^2 = a^2 - \frac{c^2}{4} = a^2(1 - t^2).$$

Отсюда получаем $a^2 = 1/(1 - t^2)$. Далее,

$$y^2(t) = k_a^2 = k_b^2 = a^2 + c^2 - ac - \frac{a^3 c}{(a+c)^2} =$$

$$= \frac{a^4 + ac^3 + c^4}{(a+c)^2} = a^2 \frac{1 + 8t^3 + 16t^4}{(1+2t)^2} = \frac{1 + 8t^3 + 16t^4}{(1-t^2)(1+2t)^2}.$$

Тогда

$$y(t) = \sqrt{\frac{1 + 8t^3 + 16t^4}{(1-t^2)(1+2t)^2}}.$$

Нетрудно проверить, что $y(0) = 1$, $y(1/2) = 1$. На отрезке $0 \leqslant t \leqslant 1/2$ функция $y(t)$ имеет локальный минимум. Чтобы его найти, можно использовать онлайн-калькулятор `https://www.wolframalpha.com/examples/mathematics/`. С его помощью легко нарисовать график функции (рис. 2), найти её производную, а также найти приближённое значение корня уравнения.

Получаем

$$y'(t) = -\frac{8t^5 - 28t^4 - 40t^3 - 16t^2 - t + 2}{(1-t^2)^2(1+2t)^3} \left(\frac{1 + 8t^3 + 16t^4}{(1-t^2)(1+2t)^2} \right)^{-1/2}.$$

Обозначим через $0 < t_0 < 1/2$ корень уравнения

$$8t^5 - 28t^4 - 40t^3 - 16t^2 - t + 2 = 0.$$

Используя онлайн-калькулятор, получим $t_0 \approx 0{,}25129$, $y(t_0) \approx 0{,}75030$.

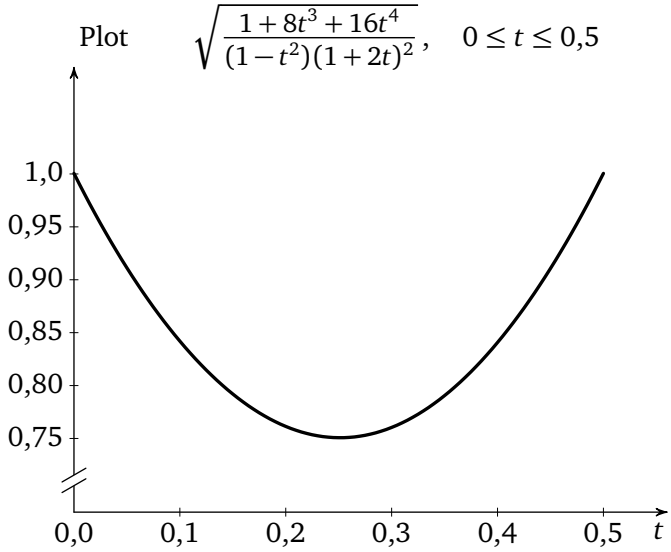


Рис. 2

Теперь ясно, что для любого значения антибиссектрис $y(t_0) < k_a = k_b < 1$ существуют два равнобедренных треугольника, у которых длины антибиссектрис совпадают, но углы разные.

§ 3. Существует ли треугольник с заданными антибиссектрисами?

Известно [2], что для любых положительных чисел l_a, l_b, l_c существует единственный треугольник с биссектрисами, длины которых равны l_a, l_b, l_c.

Для существования треугольника с длинами медиан, равными трём наперёд заданным положительным числам m_a, m_b, m_c, необходимо потребовать, чтобы числа m_a, m_b, m_c удовлетворяли неравенствам треугольника:

$$\begin{cases} m_a + m_b > m_c, \\ m_b + m_c > m_a, \\ m_c + m_a > m_b. \end{cases}$$

Ответ в случае высот и симедиан также известен [2], [5].

В этом разделе нас будет интересовать следующий вопрос: *для каких положительных чисел k_a, k_b, k_c существует треугольник с длинами антибиссектрис k_a, k_b, k_c?*

Не теряя общности, можно считать, что $k_a \leqslant k_b \leqslant k_c$, и положить $k_c = 1$.

Построим двумерную графическую модель. Отметим те точки (x, y) на координатной плоскости, для которых существует треугольник с антибиссектрисами, длины которых равны x, y, 1, причём $0 < x \leqslant y \leqslant 1$. Множеству всех допустимых точек (x, y) будет соответствовать некоторая область. Попытаемся найти уравнения прямых и кривых, ограничивающих эту область.

Мы не смогли получить явное уравнение одной из частей границы. Попробуем задать эту кривую параметрически.

В качестве параметров рассмотрим длины сторон треугольника a, b, c. Используем формулу (1) для квадрата длины антибиссектрисы:

$$\begin{cases} x^2 = k_a^2 = b^2 + c^2 - bc - \dfrac{a^2bc}{(b+c)^2}, \\ y^2 = k_b^2 = a^2 + c^2 - ac - \dfrac{b^2ac}{(a+c)^2}, \\ 1 = k_c^2 = a^2 + b^2 - ab - \dfrac{c^2ab}{(a+b)^2}. \end{cases} \tag{2}$$

Поскольку в нашей модели $0 < x \leqslant y \leqslant 1$, согласно упражнению 2 имеем $a \geqslant b \geqslant c$.

С параметрами a, b, c не очень удобно работать, поскольку трудно определить границы их изменения. Введём два новых параметра, положив $u = b/a$ и $v = c/a$. Поскольку a — наибольшая сторона, имеем $0 < v \leqslant u \leqslant 1$. Поскольку a, b, c удовлетворяют неравенству треугольника, имеем $a < b + c \leqslant 2b$, следовательно, $1/2 < b/a = u \leqslant 1$.

Разделим обе части каждого из уравнений системы (2) на a^2. Получаем

$$\begin{cases} \dfrac{x^2}{a^2} = u^2 + v^2 - uv - \dfrac{uv}{(u+v)^2}, \\ \dfrac{y^2}{a^2} = 1 + v^2 - v - \dfrac{u^2v}{(1+v)^2}, \\ \dfrac{1}{a^2} = 1 + u^2 - u - \dfrac{v^2u}{(1+u)^2}. \end{cases}$$

Далее,

$$\begin{cases} x = \sqrt{\dfrac{u^2 + v^2 - uv - uv/(u+v)^2}{1 + u^2 - u - v^2u/(1+u)^2}}, \\ y = \sqrt{\dfrac{1 + v^2 - v - u^2v/(1+v)^2}{1 + u^2 - u - v^2u/(1+u)^2}}. \end{cases} \tag{3}$$

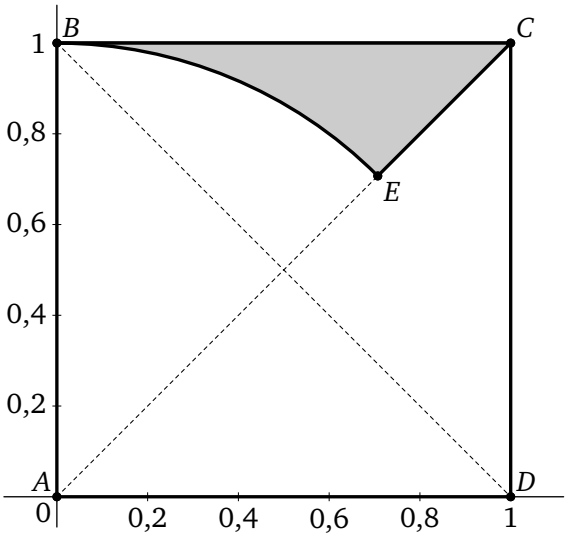


Рис. 3

Таким образом, при $1/2 < u \leqslant 1$ и $0 < v \leqslant u$ мы находим координаты точки (x, y). Тем самым определяется область в квадрате $ABCD$ (рис. 3).

Одну часть границы области найдём, если возьмём $u = v$. Тогда $b = c$ и для $1/2 < v = u \leqslant 1$ имеем параметризацию

$$\begin{cases} x = \sqrt{\dfrac{v^2 - 1/4}{1 + v^2 - v - v^3/(1+v)^2}}, \\ y = 1. \end{cases}$$

Получаем сторону BC квадрата.

Если взять $u = 1$, то $a = b$ и для $0 < v \leqslant 1$ получаем ещё одну часть границы с параметризацией

$$x = y = \sqrt{\frac{1 + v^2 - v - v/(1+v)^2}{1 - v^2/4}}.$$

Это отрезок EC, лежащий на диагонали квадрата.

Из второго уравнения системы (3) мы можем получить оценку снизу на длину средней антибиссектрисы. Поскольку $1/2 < u \leqslant 1$, выполнены неравенства

$$\sqrt{1 + u^2 - u - \frac{v^2 u}{(1+u)^2}} < \sqrt{1 + u^2 - u} \leqslant 1.$$

С другой стороны, для $1/2 < u \leqslant 1$ имеем

$$\sqrt{1+v^2-v-\frac{u^2v}{(1+v)^2}} > \sqrt{1+v^2-v-\frac{v}{(1+v)^2}}.$$

Функция

$$f(v) = \sqrt{1+v^2-v-\frac{v}{(1+v)^2}}$$

на промежутке $0 < v \leqslant 1$ является дифференцируемой и имеет минимум. Решив уравнение $f'(v) = 0$, найдём, что $\min f(v) > 0{,}72$. Тогда

$$y = \frac{\sqrt{1+v^2-v-u^2v/(1+v)^2}}{\sqrt{1+u^2-u-v^2u/(1+u)^2}} > 0{,}72.$$

Итак, для всех значений параметров $1/2 < u \leqslant 1$ и $0 < v \leqslant u$ имеем $y > 0,72$. Вспомним, что в нашей модели мы рассматривали треугольники с точностью до подобия, при этом длина наибольшей антибиссектрисы равнялась 1. Следовательно, верно

Предложение. *Пусть a, b, c — длины сторон треугольника, где $a \geqslant b \geqslant c$. Тогда для длин большей антибиссектрисы k_c и средней антибиссектрисы k_b выполнено неравенство $0{,}72k_c \leqslant k_b$.*

Неизвестно, можно ли константу 0,72 из предложения улучшить до константы 0,75030, найденной в § 2 для равнобедренных треугольников.

§ 4. Антибиссектрисы: построение циркулем и линейкой

Первоначально авторам заметки было неизвестно, можно ли построить треугольник циркулем и линейкой по длинам трёх его антибиссектрис. Следующая теорема даёт ответ на этот вопрос.

Теорема. *Задача построения треугольника по заданным длинам его антибиссектрис неразрешима с помощью циркуля и линейки.*

Прежде чем излагать доказательство теоремы, напомним, что если кубический многочлен с рациональными коэффициентами неприводим над полем рациональных чисел (т. е. у него нет рационального корня), то его корни непостроимы с помощью циркуля и линейки. В задаче, вероятно сформулированной Брокаром, о невозможности построения треугольника с помощью циркуля и линейки по длинам трёх его биссектрис возникает кубический многочлен. Доказательство невозможности построения треугольника с помощью циркуля и ли-

нейки по длинам трёх его симедиан также сводится к неприводимости кубического многочлена.

Что же не так с антибиссектрисами? Дело в том, что мы приходим к уравнению четвёртой степени. В брошюре [6] находим фразу: «Можно привести пример многочлена четвёртой степени, корни которого нельзя построить циркулем и линейкой». Это наш случай.

Напомним, что если имеется приведённое уравнение четвёртой степени: $x^4 + ax^2 + bx + c = 0$, то кубическое уравнение относительно переменной y: $y^3 - 2ay^2 + (a^2 - 4c)y + b^2 = 0$ будет его резольвентой.

Доказательство теоремы. Рассмотрим равнобедренный треугольник ABC (рис. 1). Пусть $BC = AC = a = b$, $AB = c \leqslant a$, тогда $k_a = k_b \leqslant k_c$. Обозначим $\angle ACB = \gamma$ и $t = \sin(\gamma/2)$. Тогда $c = 2at$.

Пусть длины двух антибиссектрис равны $k_a = k_b = \sqrt{3}/2$, а длина третьей равна $k_c = 1$ (рис. 1). Тогда

$$1 = k_c^2 = a^2 - \frac{c^2}{4} = a^2(1 - t^2),$$

$$\frac{3}{4} = k_a^2 = k_b^2 = a^2 + c^2 - ac - \frac{a^3c}{(a+c)^2} = \frac{a^4 + ac^3 + c^4}{(a+c)^2} = a^2\frac{1 + 8t^3 + 16t^4}{(1+2t)^2},$$

$$\frac{3}{4} = \frac{1 + 8t^3 + 16t^4}{(1+2t)^2(1-t^2)}.$$

Получаем уравнение 4-й степени: $76t^4 + 44t^3 - 9t^2 - 12t + 1 = 0$.

Если бы мы построили наш равнобедренный треугольник, то мы также смогли бы построить отрезок длины $t = \sin(\gamma/2)$, т. е. мы могли бы построить корень уравнения четвёртой степени.

Будем решать уравнение четвёртой степени методом Феррари.

Домножив обе части уравнения на $27\,436 = 2^2 \cdot 19^3$ и сделав замену переменных $u = 38t$, получим уравнение

$$u^4 + 22u^3 - 171u^2 - 8664u + 27\,436 = 0.$$

Сделаем замену переменных $u = x - 11/2$, наше уравнение четвёртой степени приведётся к каноническому виду

$$x^4 - \frac{705x^2}{2} - 5452x + \frac{1\,074\,721}{16} = 0.$$

Теперь найдём резольвенту этого уравнения: получаем

$$y^3 + 705y^2 - 144\,424y + 29\,724\,304 = 0.$$

Докажем, что у резольвенты нет рациональных решений. Пусть корнем уравнения будет рациональное число $y = p/q$, где p, q — целые

взаимно простые числа, $q > 0$. Тогда

$$p^3 = q(-705p^2 + 144\,424pq - 29\,724\,304q^2). \qquad (4)$$

Поскольку p, q — взаимно простые числа, получаем $q = 1$. Но уравнение (4) не имеет решений в целых числах. Следовательно, левая часть резольвенты — кубический многочлен, неприводимый над $\mathbb{Q}$. Это означает, что корни исходного многочлена четвёртой степени непостроимы с помощью циркуля и линейки.

Следовательно, с помощью циркуля и линейки мы не сможем построить треугольник, длины двух антибиссектрис которого равны $\sqrt{3}/2$, а длина третьей равна 1. Теорема доказана. □

Список литературы

[1] *Ефремов Д.* Новая геометрия треугольника. Одесса: Матезис, 1902.

[2] *Жуков А.*, *Акулич И.* Однозначно ли определяется треугольник? // Квант. 2003. № 1. С. 29–31.

[3] *Журавлёв В. М.*, *Самовол П. И.* Об одной задаче о биссектрисах и точках Брокара // Математическое просвещение. Сер. 3. Вып. 18. М.: МЦНМО, 2014. С. 217–229.

[4] *Журавлёв В. М.*, *Самовол П. И.* Печать Соломона. Опыты математического творчества. М.: Лори, 2021.

[5] *Журавлёв В.*, *Самовол П.* Этюд о симедианах // Квант. 2013. № 5–6. С. 33–40.

[6] *Кириченко В.* Построения циркулем и линейкой и теория Галуа // Летняя школа «Современная математика». Дубна, 2005.

[7] *Манин Ю. И.* О разрешимости задач на построение с помощью циркуля и линейки // Энциклопедия элементарной математики. Кн. 4. М.: Физматлит, 1963. С. 205–227.

[8] Математическое просвещение. Сер. 3. Вып. 27. М.: МЦНМО, 2021. С. 234. Задача 5.

Валерий Михайлович Журавлёв, ПАО «Туполев», Москва

zhuravlevvm@mail.ru

Пётр Исаакович Самовол, Беер-Шева, Израиль

pet12@012.net.il

Комбинаторика

Простые доказательства оценок чисел Рамсея и уклонения

А. Я. Бучаев, А. Б. Скопенков

Эта заметка возникла в ходе обсуждений на семинарах по курсу А. М. Райгородского на ФИВТ МФТИ. Благодарим за полезные обсуждения Д. А. Колупаева, Г. М. Кучерявого, А. А. Печенкина, А. М. Райгородского и анонимного рецензента[1)]

Мы приводим простые доказательства теоремы 1 Эрдёша о нижней оценке чисел Рамсея и теоремы 2 об оценке уклонения (см. формулировки ниже). Для понимания формулировок и доказательств не требуется знаний, выходящих за пределы школьной программы (кроме неравенства ($*$) в конце доказательства леммы 1, для которого требуется разложение экспоненты в ряд). По сути наше изложение аналогично [AS, § 1.1], [R10, § 3.2, § 4.2]. Однако оно проще для восприятия, поскольку не использует ненужного здесь вероятностного языка (см. подробнее замечание 1). Для доказательства существования «хорошего» объекта подсчитывается, что «плохих» объектов меньше, чем всех. Кроме того, теоремы излагаются без технических усложнений, дающих незначительно более сильные оценки (таким образом, обычно теоремой Эрдёша и теоремой об оценке уклонения называются не теоремы 1 и 2, а немного более сильные утверждения). Также мы постарались хорошо структурировать доказательство теоремы 2 (т. е. разбить его на шаги, в частности, выделить красивую лемму 1).

Мы начинаем с олимпиадных задач, являющихся частными случаями указанных теорем.

[1)] Полную обновляемую версию см. на `https://arxiv.org/abs/2107.13831`.

Задача 1. (a) Среди любых 51 из 10 миллионов китежан имеется двое знакомых. Обязательно ли найдётся 51 китежанин, любые два из которых знакомы?

(b) Любые два из 1000 учёных переписываются по одной из четырёх тем: географии, геологии, топографии и топологии. Обязательно ли найдутся 12 учёных, любые два из которых переписываются по одной и той же теме?

(c) Среди 1000 членов хурала выбрано несколько комиссий, в каждой из которых 3 человека. Обязательно ли найдётся 10 членов хурала, из которых либо любые 3 образуют комиссию, либо любые 3 не образуют?

Ответы — нет. Они являются частным случаем следующих теорем.

Назовём *n-кликой* (*n-антикликой*) полный (пустой) подграф на n вершинах данного графа. Для фиксированного l назовём *n-гиперклика* семейство всех l-элементных подмножеств данного подмножества из n элементов.

Теорема 1 (Эрдёш). (a) *Для любого n существует граф на $2^{\lfloor (n-2)/2 \rfloor}$ вершинах, не имеющий ни n-клики, ни n-антиклики.*

(b) *Для любых n, k в полном графе на $k^{\lfloor (n-2)/2 \rfloor}$ вершинах существует раскраска рёбер в k цветов, для которой нет одноцветной n-клики.*

(c) *Для любых n, k, l в множестве из $k^{\lfloor (n-l+1)^{l-1}/l! \rfloor}$ элементов существует раскраска всех l-элементных подмножеств в k цветов, в которой нет одноцветной n-гиперклики.*

Следующая задача является частным случаем теоремы 2 об оценке уклонения для $n = 1000$, $s = 300$ и $a = 150$ (поскольку $2^{150^2} > 2^{10 \cdot 2000} > 600^{2000}$).

Задача 2 [PT]. 1000 пионеров города Новые Васюки вышли на парад. Известно, что пионеры ходят в 300 кружков. Докажите, что Остап Бендер может раздать пионерам пилотки двух цветов (красные и синие) так, чтобы среди представителей одного кружка разность (по модулю) между количествами пионеров в красных пилотках и в синих пилотках не превосходила 150.

Теорема 2 (об оценке уклонения). *Пусть $M_1, \ldots, M_s$ — семейство подмножеств множества $[n] := \{1, \ldots, n\}$. Если $2^{a^2} \geqslant (2s)^{2n}$, то существует раскраска множества $[n]$ в красный и синий цвета, для которой при любом $k \in [s]$ количества красных и синих элементов в M_k отличаются менее чем на a.*

Доказательство ответов «нет» в задачах 1(a), (c). (a) Рассмотрим граф знакомств китежан. Назовём граф с вершинами $1, 2, \ldots, 10^7$ *рамсеевским*, если в нём есть либо 51-клика, либо 51-антиклика. Для доказательства существования нерамсеевского графа достаточно показать, что рамсеевских графов меньше, чем всех графов с вершинами $1, 2, \ldots, 10^7$. Количество последних равно $N := 2^{10^7(10^7-1)/2}$. Клику на данной 51 вершине можно продолжить до $N/2^{51\cdot 50/2}$ графов с вершинами $1, 2, \ldots, 10^7$. Аналогичное справедливо для антиклики. Количество 51-элементных подмножеств 10^7-элементного множества равно

$$\binom{10^7}{51} < (10^7)^{51} = 10^{357}.$$

Поэтому количество рамсеевских графов меньше, чем

$$2 \cdot 10^{357} \frac{N}{2^{51\cdot 25}} < \frac{N \cdot 10^{357}}{2^{10\cdot 5\cdot 25}} < \frac{N \cdot 10^{357}}{10^{3\cdot 5\cdot 25}} = N \cdot 10^{357-375} < N.$$

(c) Назовём семейство трехчеловечных комиссий (среди 1000 членов хурала) *рамсеевским*, если в нём есть либо 10-гиперклика, либо 10-антигиперклика (10-антигиперкликой называются 10 человек, никакая тройка из которых не является комиссией). Для доказательства существования нерамсеевского семейства трехчеловечных комиссий достаточно показать, что рамсеевских семейств меньше, чем всех семейств. Количество последних равно $N := 2^{\binom{1000}{3}}$. Гиперклику размера 10 данного подмножества из 10 членов хурала можно продолжить до $N/2^{\binom{10}{3}}$ семейств трехчеловечных комиссий. Антигиперклику размера 10 данного подмножества из 10 членов хурала можно продолжить до $N/2^{\binom{10}{3}}$ семейств трехчеловечных комиссий. Количество 10-элементных подмножеств 1000-элементного множества равно

$$\binom{1000}{10} < (1000)^{10} < 2^{100}.$$

Поэтому количество рамсеевских семейств трехчеловечных комиссий меньше, чем

$$2 \cdot 2^{100} \frac{N}{2^{\binom{10}{3}}} = \frac{N \cdot 2^{101}}{2^{120}} < N. \qquad \square$$

Ответ «нет» в задаче 1(b) и теорема 1 Эрдёша доказываются аналогично. В частности, в начале доказательства теоремы 1(a) берём $r := 2^{\lfloor (n-2)/2 \rfloor}$, тогда

$$\binom{r}{n} < r^n \leqslant 2^{(n^2-n-2)/2} \quad \text{при } n \geqslant 2.$$

Перейдём к доказательству теоремы 2 *об оценке уклонения* (и, тем самым, к решению задачи 2). Для подмножества M множества $[n]$

и раскраски x множества $[n]$ в два цвета обозначим через $\Delta_M(x)$ (*уклонение*) разность между количествами элементов первого и второго цвета в M.

Лемма 1. *Для любых $a > 0$ и подмножества M множества $[n]$ количество раскрасок x, для которых $\Delta_M(x) \geqslant a$, меньше $2^{n-a^2/(2n)}$.*

Доказательство теоремы 2. Применим лемму 1 к любому $k \in [s]$. Получим, что количество раскрасок x, для которых $\Delta_{M_k}(x) \geqslant a$, меньше $2^{n-a^2/(2n)} \leqslant 2^n/(2s)$. В силу симметрии количество раскрасок x, для которых $\Delta_{M_k}(x) \leqslant -a$, также меньше $2^n/(2s)$. Поэтому количество (k-«плохих») раскрасок x, для которых $|\Delta_{M_k}(x)| \geqslant a$, меньше $2^n/s$. Тогда количество («плохих») раскрасок x, для которых найдётся такое $k \in [s]$, что $|\Delta_{M_k}(x)| \geqslant a$, меньше $s2^n/s = 2^n$. Следовательно, найдётся «хорошая» раскраска. □

В доказательстве леммы 1 используется следующий очевидный, но крайне полезный факт.

Лемма 2 (неравенство Маркова). *Для любых $w_1, \ldots, w_s > 0$ количество тех i, для которых $w_i \geqslant 1$, не превосходит $w_1 + \ldots + w_s$.*

Более общо, для любых $a, w_1, \ldots, w_s > 0$ количество тех i, для которых $w_i \geqslant a$, не превосходит $(w_1 + \ldots + w_s)/a$. □

Доказательство леммы 1. Ввиду неравенства Маркова (лемма 2) для любого $\lambda > 0$ имеем

$$|\{x\colon \Delta_M(x) \geqslant a\}| = |\{x\colon \lambda\Delta_M(x) \geqslant \lambda a\}| = \\ = |\{x\colon e^{\lambda\Delta_M(x)} \geqslant e^{\lambda a}\}| \leqslant e^{-\lambda a}\sum_x e^{\lambda\Delta_M(x)}.$$

Раскраску подмножества $A \subset [n]$ в два цвета будем считать отображением $A \to \{-1, 1\}$. Тогда

$$\sum_{x\in\{-1,1\}^{[n]}} e^{\lambda\Delta_M(x)} = \sum_{x\in\{-1,1\}^{[n]}} \prod_{j\in M} e^{\lambda x(j)} = \\ = 2^{n-|M|}\sum_{y\in\{-1,1\}^M}\prod_{j\in M} e^{\lambda y(j)} = 2^{n-|M|}(e^\lambda + e^{-\lambda})^{|M|}.$$

Здесь

- первое равенство верно, поскольку $\Delta_M(x) = \sum_{j\in M} x(j)$;
- второе равенство верно, поскольку каждую раскраску подмножества M в два цвета можно продолжить до $2^{n-|M|}$ раскрасок множества $[n]$.

- третье равенство верно, поскольку при раскрытии скобок в правой части получается левая часть.

  Поэтому

$$|\{x\colon \Delta_M(x) \geqslant a\}| \leqslant e^{-\lambda a} 2^n \left(\frac{e^\lambda + e^{-\lambda}}{2}\right)^{|M|} \overset{(*)}{<} 2^n e^{|M|\lambda^2/2 - \lambda a} \leqslant$$
$$\leqslant 2^n e^{n\lambda^2/2 - \lambda a} \overset{(**)}{=} 2^n e^{-a^2/(2n)} < 2^{n - a^2/(2n)}.$$

Здесь

- неравенство $(*)$ верно, поскольку

$$e^\lambda + e^{-\lambda} = \sum_{k=0}^{\infty} \frac{\lambda^k}{k!} + \sum_{k=0}^{\infty} \frac{(-1)^k \lambda^k}{k!} = 2\sum_{k=0}^{\infty} \frac{\lambda^{2k}}{(2k)!} < 2\sum_{k=0}^{\infty} \frac{\lambda^{2k}}{2^k k!} = 2e^{\lambda^2/2}.$$

- равенство $(**)$ получается подстановкой $\lambda = a/n$. □

Замечание 1. Часто для доказательства существования «хорошего» объекта *подсчитывается*, что «плохих» объектов меньше, чем всех. Такие доказательства существования можно излагать на вероятностном языке (т. е. построив дискретное вероятностное пространство с равновероятными элементарными событиями). К сожалению, такое изложение недоступно для многих студентов. Ибо многие не в состоянии сформулировать необходимое для доказательства определение (дискретного) вероятностного пространства. А многим не хватает математической культуры даже для осознания того, что такого пространства нет в формулировке теоремы, поэтому его построение — часть доказательства («дополнительное построение»).

Тем не менее, развивать вероятностную интуицию крайне полезно. Применение дискретных вероятностных пространств с элементарными событиями, уже не являющимися равновероятными, — мощный метод комбинаторики, *вероятностный метод* [AS, R10]. В качестве пропедевтики вероятностного метода полезны доказательства существования, использующие подсчёт (подобно вышеприведённым). После их изучения разумно потренироваться излагать эти доказательства на вероятностном языке [GDI, решения к п. 1.6 «подсчёт двумя способами»]. (Точно так же, как в начале освоения теории Галуа разумно потренироваться излагать на её языке уже известные решения квадратного уравнения и уравнений 3-й и 4-й степени.) Другие примеры естественного выращивания вероятностного языка приведены, например, в [ZSS, § 22], [IRS], [GDI, § 6.2].

Хотя подсчёт «плохих» объектов позволяет обойтись без вероятностного языка, сущностные (т. е. не связанные с языком изложения) элементы доказательства при обоих изложениях одни и те же.

Список литературы

[AS] *Алон Н.*, *Спенсер Дж.* Вероятностный метод. М.: Бином. Лаборатория знаний, 2011.

[GDI] *Глибичук А. А.*, *Дайняк А. Б.*, *Ильинский Д. Г.*, *Купавский А. Б.*, *Райгородский А. М.*, *Скопенков А. Б.*, *Чернов А. А.* Элементы дискретной математики в задачах. М.: МЦНМО, 2016. http://www.mccme.ru/circles/oim/discrbook.pdf.

[IRS] *Ильинский Д. Г.*, *Райгородский А. М.*, *Скопенков А. Б.* Независимость и доказательства существования в комбинаторике // Математическое просвещение. Сер. 3. Вып. 19. М.: МЦНМО, 2015. С. 164–177. http://arxiv.org/abs/1411.3171.

[PT] *Полянский А. А.*, *Тарасов П. Б.* Избранные задачи экзамена по дискретному анализу // Математическое просвещение. Сер. 3. Вып. 21. М.: МЦНМО, 2017. С. 205–209.

[R10] *Райгородский А. М.* Вероятность и алгебра в комбинаторике. М.: МЦНМО, 2010.

[ZSS] Элементы математики в задачах: через олимпиады и кружки к профессии Сборник под редакцией А. Заславского, А. Скопенкова и М. Скопенкова. М.: МЦНМО, 2018. http://www.mccme.ru/circles/oim/materials/sturm.pdf.

Абдулкадыр Яхьяевич Бучаев, МФТИ
buchaev.aia@phystech.edu

Аркадий Борисович Скопенков, МФТИ, НМУ
https://users.mccme.ru/skopenko

Подсчёт нетранзитивных троек в методе парных сравнений

П. П. Рябов

§ 1. Введение

В социально-экономических приложениях существенная часть информации может быть получена только от экспертов и требует специальных методов анализа. Одним из самых старых методов экспертных оценок являются парные сравнения. В этом методе мы считаем, что эксперт из любых двух объектов может выбрать более предпочтительный или объявить, что эти объекты эквивалентны. Метод парных сравнений используются также при проведении соревнований (круговые турниры, далее в работе «турниры») и при анализе предпочтений индивида. В статье мы будем пользоваться турнирной терминологией.

Наличие полной информации о встречах позволяет делать выводы независимо от порядка игр участников, однако не решает проблему итогового упорядочивания. Например, для турнира без ничьих может найтись нетранзитивная тройка игроков a, b и c: a выиграл у b, b — у c, а c — у a. Тогда, как бы мы ни упорядочили игроков a, b и c в итоговой таблице, результат будет вызывать сомнения. Среди турниров без ничьих турнир, в котором отсутствуют нетранзитивные тройки, определён однозначно. Мы будем называть такой турнир **упорядоченным**.

Существуют разные метрики для сравнения турнира с упорядоченным. В данной статье для сравнения используется число нетранзитивных троек. Проблема такого сравнения заключается в сложности подсчёта этих троек при очень большом числе участников. Г. Дэвид [1, с. 20] вывел формулу для турнира без ничьих, позволяющую подсчитать число нетранзитивных троек через число побед каждого участника. Если в турнире допускаются ничьи, упорядоченный турнир можно определить по-разному (мы рассмотрим транзитивные и полутранзитивные турниры). А. Заславский [3, 4] обобщил формулу

Г. Дэвида для сравнения турнира с транзитивным турниром, но коэффициенты в формуле оказались плохо интерпретируемы. В этой статье мы покажем, почему нет другой линейной формулы для сравнения турнира с транзитивным и почему не существует линейной формулы для сравнения турнира с полутранзитивным.

§ 2. Определения

Сопоставим игрокам вершины графа. Если игрок a выиграл у b, то направим ребро из b в a. Если игроки сыграли вничью, то ребро будет направлено к обеим вершинам.

Обозначим через a_j число троек A_j в турнире. Пусть в турнире участвовало n игроков. Число побед, поражений и ничьих игрока i $(1 \leqslant i \leqslant n)$ обозначим через v_i, l_i и d_i соответственно.

На рис. 1 указаны всевозможные результаты встреч трёх игроков. Символом A_j, $1 \leqslant j \leqslant 7$, будем обозначать вид тройки.

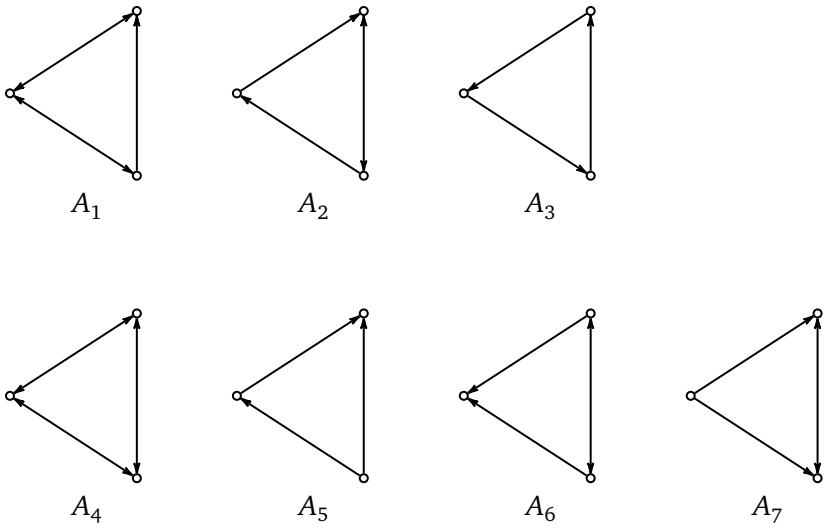


Рис. 1

Определение 1. **Полутранзитивным турниром** называется турнир, в котором не существует игроков $v_1, \ldots, v_k$ таких, что игрок v_1 выиграл или сыграл вничью с v_2, игрок v_2 выиграл или сыграл вничью с v_3, и т. д., игрок v_k выиграл или сыграл вничью с v_1 (при этом среди указанных игр не более одной ничьей).

Определение 2. **Транзитивным турниром** будем называть турнир, в котором отсутствуют тройки игроков A_1, A_2 и A_3.

Замечание. Упорядоченные турниры можно определять и с помощью циклов. **Транзитивным турниром** называется турнир, в котором не существует игроков $v_1, \dots, v_k$ таких, что игрок v_1 выиграл или сыграл вничью с v_2, игрок v_2 выиграл или сыграл вничью с v_3, и т. д., игрок v_k выиграл или сыграл вничью с v_1. При этом хотя бы одна из данных игр отлична от ничейной. **Полутранзитивным турниром** называется турнир, в котором не существует игроков $v_1, \dots, v_k$ таких, что игрок v_1 выиграл у v_2, игрок v_2 выиграл у v_3, и т. д., игрок v_k выиграл у v_1. Эквивалентность определений доказана в [3]. Однако для сравнения турнира с упорядоченными гораздо легче считать число троек A_1, A_2, A_3, чем число циклов неопределённой длины.

§ 3. Основной результат

Для турнира без ничьих Г. Дэвид вывел следующую формулу [1, с. 20]:

$$\frac{n(n-1)(2n-1)}{12} - \frac{1}{2}\sum_{i=1}^{n} v_i^2 = a_3.$$

А. Заславский обобщил формулу Г. Дэвида для турниров с ничьими [3, 4].

$$6a_3 + 3a_2 + a_1 = \frac{(n^3-n) - \sum_{i=1}^{n} d_i(d_i+2) - 3\sum_{i=1}^{n}(v_i - l_i)^2}{4}.$$

Покажем, что в любой формуле, связывающей линейную комбинацию числа троек A_1, A_2 и A_3 с числом побед/ничьих/поражений каждого игрока, коэффициенты при a_1, a_2 и a_3 определены однозначно с точностью до умножения на константу.

Теорема 1. *Для турнира с n участниками верны следующие равенства*:

$$\sum_{i=1}^{n}(v_i l_i) = a_2 + a_5 + 3a_3,$$

$$\sum_{i=1}^{n}(v_i d_i) = a_1 + a_2 + 2a_7,$$

$$\sum_{i=1}^{n}(d_i l_i) - \frac{n(n-1)(n-2)}{6} = a_6 - a_3 - a_4 - a_5 - a_7,$$

$$\sum_{i=1}^{n}(2v_i^2 + d_i) - (n-1)n = 4a_5 + 4a_6,$$

$$\sum_{i=1}^{n}(2l_i^2 + d_i) - (n-1)n = 4a_5 + 4a_7.$$

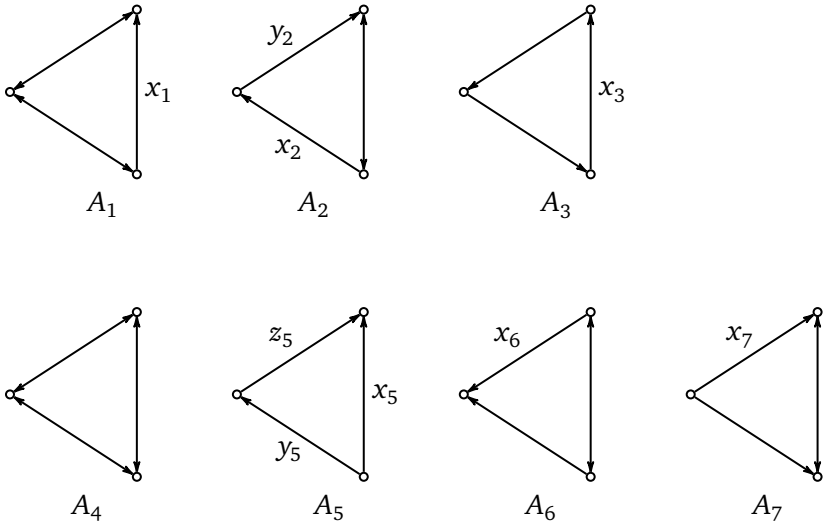


Рис. 2

Доказательство. Рассмотрим произвольный турнир, в котором не все партии закончились вничью. В этом турнире возьмём двух игроков a и b таких, что игрок a выиграл у b, и заменим результат их встречи на ничейный. Подсчитаем, как изменится число различных троек в турнире и число побед, поражений и ничьих каждого игрока. На рис. 2 числа x_i, y_j, $i = 1, 2, 3, 5, 6, 7$, $j = 2, 5$ и z_5 обозначают количество троек данного вида с ребром ab (в тройках A_2 и A_5 рёбра неравнозначны, поэтому важно учитывать, где расположено ребро ab; в тройку A_4 не могут одновременно входить игроки a и b). Через $\triangle$ обозначим изменение величины при замене результата игры на ничейный (из нового значения мы вычитаем первоначальное). Далее приведены формулы изменения числа троек каждого вида в турнире при замене результата игры между a и b на ничейный.

$$\begin{aligned}
\triangle a_1 &= -x_1 + x_2 + y_2 + x_6 + x_7,\\
\triangle a_2 &= -x_2 - y_2 + x_3 + x_5,\\
\triangle a_3 &= -x_3,\\
\triangle a_4 &= x_1,\\
\triangle a_5 &= -x_5 - y_5 - z_5,\\
\triangle a_6 &= y_5 - x_6,\\
\triangle a_7 &= z_5 - x_7.
\end{aligned} \tag{1}$$

Через число троек с ребром ab также можно выразить число побед v_a, v_b, поражений l_a, l_b и ничьих d_a, d_b игроков a и b до замены

результата их встречи:

$$\begin{aligned} v_a &= x_5 + z_5 + x_6 + 1, & v_b &= y_2 + x_3 + z_5, \\ l_a &= x_2 + x_3 + y_5, & l_b &= x_5 + y_5 + x_7 + 1, \\ d_a &= x_1 + y_2 + x_7, & d_b &= x_1 + x_2 + x_6. \end{aligned} \tag{2}$$

После замены результата встречи на ничью число побед у a уменьшилось на единицу, число ничьих увеличилось на единицу, число поражений не изменилось; у игрока b число поражений уменьшилось на единицу, число ничьих увеличилось на единицу, количество побед не изменилось. Теперь, используя формулы (2), запишем равенства:

$$\begin{aligned} &\triangle(v_a^2) = -1 - 2x_5 - 2z_5 - 2x_6, && \triangle(v_b^2) = 0, \\ &\triangle(l_a^2) = 0, && \triangle(l_b^2) = -1 - 2x_5 - 2y_5 - 2x_7, \\ &\triangle(d_a^2) = 1 + 2x_1 + 2y_2 + 2x_7, && \triangle(d_b^2) = 1 + 2x_1 + 2x_2 + 2x_6, \\ &\triangle(d_a l_a) = x_2 + x_3 + y_5, && \triangle(d_b l_b) = x_5 + y_5 + x_7 - x_1 - x_2 - x_6, \\ &\triangle(v_a d_a) = -x_1 - y_2 - x_7 + x_5 + z_5 + x_6, && \triangle(v_b d_b) = y_2 + x_3 + z_5, \\ &\triangle(v_a l_a) = -x_2 - x_3 - y_5, && \triangle(v_b l_b) = -y_2 - x_3 - z_5, \\ &\triangle(d_a) = 1, && \triangle(d_b) = 1. \end{aligned}$$

Поскольку результаты остальных участников турнира не поменялись, верны следующие формулы:

$$\begin{aligned} &\triangle\left(\sum_{i=1}^{n} v_i^2\right) = -1 - 2x_5 - 2z_5 - 2x_6, \\ &\triangle\left(\sum_{i=1}^{n} l_i^2\right) = -1 - 2x_5 - 2y_5 - 2x_7. \\ &\triangle\left(\sum_{i=1}^{n} d_i^2\right) = 2 + 4x_1 + 2x_2 + 2y_2 + 2x_6 + 2x_7, \\ &\triangle\left(\sum_{i=1}^{n} d_i l_i\right) = x_3 + x_5 - x_1 - x_6 + x_7 + 2y_5, \\ &\triangle\left(\sum_{i=1}^{n} v_i d_i\right) = -x_1 + x_3 - x_7 + x_5 + 2z_5 + x_6, \\ &\triangle\left(\sum_{i=1}^{n} v_i l_i\right) = -x_2 - y_2 - 2x_3 - y_5 - z_5, \\ &\triangle\left(\sum_{i=1}^{n} d_i\right) = 2. \end{aligned} \tag{3}$$

Приравнивая (1) и (3), получаем равенства:

$$\triangle\left(\sum_{i=1}^{n} v_i l_i\right) = -x_2 - y_2 - 2x_3 - y_5 - z_5 = \triangle a_2 + \triangle a_5 + 3\triangle a_3,$$

$$\triangle\left(\sum_{i=1}^{n} (v_i d_i)\right) = -x_1 + x_3 - x_7 + x_5 + 2z_5 + x_6 = \triangle a_1 + \triangle a_2 + 2\triangle a_7,$$

$$\triangle\left(\sum_{i=1}^{n} (d_i l_i)\right) = x_3 + x_5 - x_1 - x_6 + x_7 + 2y_5 = \triangle a_6 - \triangle a_3 - \triangle a_4 - \triangle a_5 - \triangle a_7,$$

$$\triangle\left(\sum_{i=1}^{n} (2v_i^2 + d_i)\right) = -4x_5 - 4z_5 - 4x_6 = 4\triangle a_5 + 4\triangle a_6,$$

$$\triangle\left(\sum_{i=1}^{n} (2l_i^2 + d_i)\right) = -4x_5 - 4y_5 - 4x_7 = 4\triangle a_5 + 4\triangle a_7.$$

Заменяя победы и поражения на ничьи, получаем турнир целиком из ничейных игр. В нём выполнено равенство

$$\sum_{i=1}^{n} d_i = n(n-1),$$

а число троек A_4 равно $n(n-1)(n-2)/6$. Отсюда нетрудно видеть, что правая и левая части формул из условия теоремы меняются одинаково при замене результатов игр на ничейные, а в турнире из ничьих имеют одинаковые значения. □

Замечание. Выражения величины $\triangle$ через v_i, l_i и d_i не единственные. Для любого i выполняется равенство $v_i + d_i + l_i = n - 1$.

Рассмотрим $a_1, \ldots, a_7$ как векторы. Тогда векторы

$$a_2 + a_5 + 3a_3, \quad a_1 + a_2 + 2a_7, \quad a_6 - a_3 - a_4 - a_5 - a_7, \quad 4a_5 + 4a_6 \quad \text{и} \quad 4a_5 + 4a_7$$

образуют пятимерное векторное подпространство V в семимерном векторном пространстве W, порождённом линейными комбинациями из $\{a_j\}$, $1 \leqslant j \leqslant 7$.

Теорема 2. *Пусть число участников турнира не меньше* 6. *Тогда все линейные комбинации элементов* a_j, $1 \leqslant j \leqslant 7$, *значения которых можно определить при любых возможных количествах побед/поражений/ничьих каждого игрока, лежат в* V.

Доказательство. Покажем, что при числе участников турнира $n \geqslant 6$ невозможно получить информацию о количествах троек вида A_2 и A_3

и любой их линейной комбинации. Для этого рассмотрим два турнира: в одном все игроки сыграли вничью, кроме четвёрки игроков, которые сыграли как показано на рис. 3 слева, а во втором все участники сыграли вничью, кроме четырёх игроков, которые сыграли, как показано на рис. 3 справа. Для обоих турниров множества, образованные тройками из чисел побед, поражений, ничьих каждого игрока, совпадают. Однако в первом турнире нет троек A_2 и 2 тройки A_3, а во втором 2 тройки A_2 и 1 тройка A_3. Следовательно, единственная линейная комбинация, о которой можно получить информацию, это $a_2 + 2a_3$.

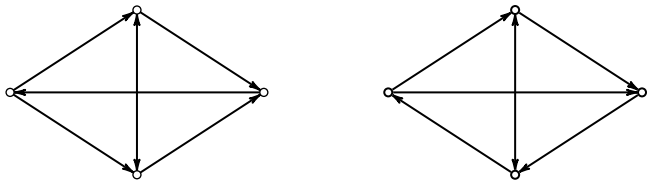


Рис. 3

Рассмотрим другую пару турниров, в каждом из которых все игроки сыграли вничью, кроме шестёрки игроков, игры которых, отличные от ничейных, показаны на рис. 4 (слева — в первом турнире, справа — во втором). В первом турнире нет троек A_3 и есть 6 троек A_2, во втором нет троек A_2 и есть 2 тройки A_3. Множества образованные тройками из чисел побед, ничьих, поражений каждого игрока, для обоих турниров совпадают. Поэтому о комбинации $a_2 + 2a_3$ также не всегда возможно получить информацию.

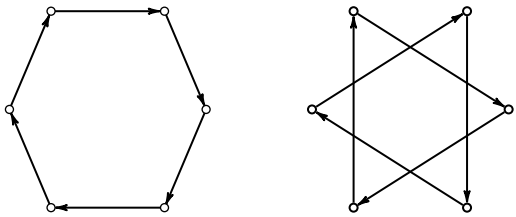


Рис. 4

Линейные комбинации, о которых можно получить информацию, образуют векторное подпространство. Размерность пространства $\{a_2, a_3\}$ равна двум; $\dim W = 7$. Следовательно, векторное пространство, о котором можно получить информацию, имеет размерность не больше 5. Однако $\dim V = 5$. Следовательно, ни для одной линейной комбинации, не лежащей в V, мы не сможем однозначно определить значения при

любых возможных количествах побед/поражений/ничьих каждого игрока. □

Замечание. Если число участников турнира меньше шести, то по числу побед/ничьих/поражений каждого игрока можно всегда узнать, например, число троек A_4.

Следствие 1. *Не существует формулы, связывающей линейную комбинацию числа троек A_2 и A_3 с числом побед/ничьих/поражений каждого игрока.*

Следствие 2. *В любой формуле, связывающей линейную комбинацию числа троек A_1, A_2 и A_3 с числом побед/ничьих/поражений каждого игрока, коэффициенты при a_1, a_2 и a_3 относятся как* $1:3:6$.

Благодарности

Автор благодарен своему научному руководителю А. А. Заславскому за ценные наставления и замечания.

Список литературы

[1] *Дэвид Г.* Метод парных сравнений. М.: Статистика, 1978.

[2] *Заславский А. А.* Геометрия парных сравнений // Автоматика и телемеханика. 2007. № 3. С. 181–186.

[3] *Заславский А. А.*, *Френкин Б. Р.* Математика турниров. М.: МЦНМО, 2009.

[4] *Заславский А. А.*, *Шевлякова А. Н.* Геометрический метод анализа парных сравнений. Результаты вычислительного эксперимента // Вестник МЭИ. 2010. № 6. С. 5–12.

[5] *Заславский А. А.* О логичных и нелогичных турнирах // Квант. 1997. № 5. С. 11–13.

Павел Павлович Рябов, ВШЭ, Москва

pavel_ryabov_98@mail.ru

Нам пишут

Письмо в редакцию

А. И. Бикеев

В статье «Реализуемость дисков с ленточками на ленте Мёбиуса» («Математическое просвещение», вып. 28, с. 150-158) допущены неточности в формулировке леммы 1. Правильная формулировка следующая:

Лемма 1. *Пусть M — симметричная матрица над $\mathbb{Z}_2$. Тогда следующие условия эквивалентны.*

1. *Изменением некоторых элементов на главной диагонали можно из матрицы M получить матрицу, ранг которой не превосходит* 1.
2. *Можно сделать такую одинаковую перестановку строк и столбцов*[1] *матрицы M и изменить некоторые элементы на главной диагонали таким образом, что в верхнем левом углу полученной матрицы будет стоять подматрица, заполненная единицами, а остальные элементы будут равны нулю.*
3. *Нельзя сделать такую одинаковую перестановку строк и столбцов матрицы M, что в верхнем левом углу полученной матрицы будет стоять подматрица вида*

$$P = \begin{pmatrix} * & 1 & 1 \\ 1 & * & 0 \\ 1 & 0 & * \end{pmatrix} \quad \text{или} \quad Q = \begin{pmatrix} * & 1 & 0 & 0 \\ 1 & * & 0 & 0 \\ 0 & 0 & * & 1 \\ 0 & 0 & 1 & * \end{pmatrix},$$

где через $*$ обозначены произвольные (возможно, различные) элементы из $\mathbb{Z}_2$.

[1] Это означает, что строки и столбцы занумерованы подряд числами от 1 до n и некоторая перестановка σ чисел от 1 до n применена и к строкам, и к столбцам.

Новые условия 2 и 3 являются исправлением прежних условий 3 и 4. Соответственно, две фразы перед леммой нужно читать следующим образом:

«Равносильность (1) $\Leftrightarrow$ (2) очевидна. Импликация (2) $\Rightarrow$ (3) следует из того, что при любой расстановке нулей и единиц на главной диагонали матрицы P или Q по крайней мере две строки полученной матрицы будут ненулевыми и различными. Импликация (3) $\Rightarrow$ (2) фактически доказана при доказательстве импликации (4) $\Rightarrow$ (3) теоремы 3».

Артур Игоревич Бикеев, МФТИ
bikeev99@mail.ru

По мотивам задачника

Постоянная Эйлера

Л. Радзивиловский

В «Математическом просвещении», сер. 3, вып. 18, с. 258, опубликована

Задача 18.11. Найдите $\int_0^1 \ln(-\ln x)\,dx$. (*Фольклор*)

Интеграл выглядит не очень устрашающе, но его тяжело решить, не зная одной темы, о которой мы и расскажем. Более подробную информацию можно найти в [1, 2].

Если загнать интеграл в Wolfram Alpha или какую-нибудь другую подходящую программу, получится довольно короткий ответ.

Попробуем поиграть с этим интегралом: например, подставим $t = -\ln x$ и получим

$$\int_0^\infty e^{-t} \cdot \ln t\,dt. \tag{1}$$

Можно попробовать ещё другие подстановки или взять по частям, но это не приведёт нас к ответу. Но если мы изучим одну тему, то легко решим этот интеграл.

В некоторых работах Эйлера появляется такое интересное число:

$$\gamma = \lim_{n\to\infty}\left(1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} - \ln n\right).$$

Можно было бы вместо $\ln n$ написать в этой формуле $\ln(n+1)$, поскольку разница между $\ln(n+1)$ и $\ln n$ стремится к нулю при росте n. Тогда это число можно представлять себе, как тёмно-серую площадь на рис. 1: то, что находится над графиком $1/x$ и под «лестницей».

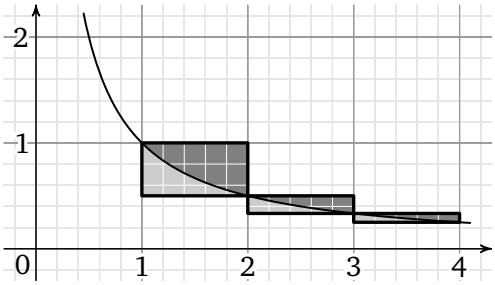


Рис. 1

Если бы мы добавили светло-серую площадь (то, что под графиком функции, но над нижней лестницей), получилась бы последовательность прямоугольников, из которых складывается квадрат единичной площади. Однако тёмно-серая часть чуть больше, чем светло-серая, поэтому γ чуть больше половины. Эйлер неоднократно пытался вычислить γ и связать её с другими известными константами. Он подсчитал γ с 15 знаками после запятой: $\gamma \approx 0{,}577215664901533$; но ему не удалось выразить γ через другие известные константы. До сих пор неизвестно, рационально γ или иррационально, алгебраично или трансцендентно.

Иногда γ называют *константой Маскерони*. В те дни было принято называть знаменитые константы именем человека, подсчитавшего константу с наибольшей точностью. Маскерони объявил 32 десятичных цифры для γ, из них первые 19 были правильные; с точки зрения математиков XVIII века это оправдывает переименование константы в честь Маскерони.

Эйлер доказал несколько красивых формул, связанных с γ.

Например:

$$\gamma = \lim_{n\to\infty} \sum_{k=1}^{n} \left(\frac{1}{k} - \ln\left(\frac{k+1}{k}\right)\right) =$$

$$= \lim_{n\to\infty} \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k} + \frac{1}{2k^2} - \frac{1}{3k^3} + \frac{1}{4k^4} - \ldots\right) =$$

$$= \frac{\zeta(2)}{2} - \frac{\zeta(3)}{3} + \frac{\zeta(4)}{4} - \ldots$$

(доказательство того, что здесь можно менять порядок суммирования, остаётся читателю в качестве упражнения).

Эйлеру неоднократно удавалось найти разумное продолжение функции, изначально заданной на натуральных числах, на все действительные (или даже все комплексные) числа.

Самым знаменитым примером, наверное, является понятие факториала. Для всякого натурального числа

$$n! = \int_0^1 (-\ln x)^n \, dx = \int_0^\infty e^{-t} t^n \, dt.$$

Я не знаю, какая из этих двух формул красивее, но они связаны заменой переменных: $t = -\ln x$. В каждый из этих интегралов можно подставить любое действительное $n > -1$ и получить определение факториала для нецелого числа. Интегрированием по частям легко доказать, что

$$\int_0^\infty e^{-t} t^n \, dt = n \int_0^\infty e^{-t} t^{n-1} \, dt,$$

а значит, можно пользоваться формулой $(n-1)! = n!/n$ и распространить понятие интеграла на все действительные числа, кроме целых отрицательных: $(-1)! = 0!/0 = \infty$. Аналогично можно распространить понятие факториала на все комплексные числа, кроме целых отрицательных.

Обычно, когда пишут $n!$, имеется в виду, что n — натуральное число, а для нецелых чисел используется Г-функция:

$$\Gamma(z) = \int_0^1 (-\ln x)^{z-1} \, dx = \int_0^\infty e^{-t} t^{z-1} \, dt,$$

что обобщает не $z!$, а $(z-1)!$. Интеграл сходится при $\operatorname{Re} z > 0$, а в левой полуплоскости можно доопределить Г, многократно применяя функциональное уравнение: $\Gamma(z+1) = z \cdot \Gamma(z)$. Получается мероморфная функция с полюсами в неположительных целых числах.

Другой пример, важный для нашего рассказа, — это гармонические числа. Положим

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}.$$

Как определить эту величину для нецелых чисел?

Рассмотрим такую сумму:

$$H_n = \sum_{k=1}^{\infty} \left(\frac{1}{k} - \frac{1}{k+n} \right).$$

Если мы просуммируем много слагаемых, останется H_n минус n очень маленьких слагаемых. Значит, эта величина стремится к H_n. Но в новую формулу можно подставить и нецелое n, и получится формула,

работающая почти для всех чисел. Действительно,

$$\frac{1}{k}-\frac{1}{k+z}=\frac{z}{k(k+z)},$$

и эта величина убывает квадратично, а значит, сумма таких слагаемых сходится. Заметим также, что

$$\frac{1}{k}=\int_0^1 x^{k-1}\,dx.$$

Положим

$$H_z=\sum_{k=1}^{\infty}\Big(\frac{1}{k}-\frac{1}{k+z}\Big),$$

и тогда

$$H_z=\sum_{k=1}^{\infty}\Big(\frac{1}{k}-\frac{1}{k+z}\Big)=\sum_{k=1}^{\infty}\int_0^1(x^{k-1}-x^{k-1+z})\,dz=$$

$$=\sum_{k=1}^{\infty}\int_0^1(x^{k-1}-x^{k-1+z})\,dz=\int_0^1(1-x^z)\sum_{k=1}^{\infty}x^{k-1}dz=\int_0^1\frac{1-x^z}{1-x}\,dz.$$

Итак, у нас есть обобщение H_n на нецелые числа, и у этого обобщения есть даже две красивых формулировки:

$$\sum_{k=1}^{\infty}\Big(\frac{1}{k}-\frac{1}{k+z}\Big)\quad\text{и}\quad\int_0^1\frac{1-x^z}{1-x}\,dz.$$

Разумеется, можно было бы определить другие функции, которые совпадают с данной последовательностью на натуральных числах, например добавив к тем функциям, которые мы построили, $\sin\pi x$ или, скажем, $\sin\pi x\cdot e^{x^8}$, но наверное читатель согласится с тем, что конструкции Эйлера очень естественны и разумны. Есть несколько теорем на тему о том, что Г-функция — «лучшее» из всех возможных обобщений факториала. Наиболее известная из этих теорем, возможно, —

Теорема Бора — Моллерупа. *Функция f из положительных чисел в положительные числа, удовлетворяющая следующим трём условиям, существует и единственна*:

- $f(1)=1$;
- $f(z+1)=z\cdot f(z)$;
- *f логарифмически выпукла.*

Это и есть Г.

Мы приведём доказательство теоремы Бора — Моллерупа, потому что из доказательства легко получится важная для нас формула. Но перед этим хочется напомнить, что такое логарифмическая выпуклость, и пояснить, почему разумно требовать именно логарифмической выпуклости.

Последовательность действительных чисел называется выпуклой, если с каждым шагом мы добавляем всё больше и больше. Другими словами, $a_{n+1} - a_n \geqslant a_n - a_{n-1}$. Например, n^2 — выпуклая последовательность.

Последовательность называется логарифмически выпуклой, если она положительна и её логарифмы образуют выпуклую последовательность. Другими словами, с каждым шагом мы умножаем на всё большее и большее число, т. е. $a_{n+1}/a_n \geqslant a_n/a_{n-1}$. Хороший пример выпуклой последовательности — это $a_n = n!$.

Теперь о функциях. Есть много определений выпуклой функции, мы введём такое определение, которое легко будет проверить. Наверное, читатель знает другие определения выпуклой функции; хорошим упражнением будет доказать, что они эквивалентны нашему определению.

Будем говорить, что функция f (на всей действительной прямой, либо на открытом интервале, конечном или бесконечном) выпукла, если, во-первых, она непрерывна, а во-вторых,

$$f\left(\frac{x_1+x_2}{2}\right) \leqslant \frac{f(x_1)+f(x_2)}{2} \quad \text{для любых } x_1, x_2.$$

Будем говорить, что функция g логарифмически выпукла, если она положительна и её логарифм — выпуклая функция.

Вместо этого можно было бы сказать, что g непрерывна и

$$0 < g\left(\frac{x_1+x_2}{2}\right) \leqslant \sqrt{g(x_1)g(x_2)} \quad \text{для произвольных } x_1, x_2.$$

Докажем простую, но полезную лемму:

Лемма. *Пусть f, g — логарифмически выпуклые функции. Тогда $f+g$ — тоже логарифмически выпуклая функция.*

Доказательство. Понятно, что $f+g$ тоже непрерывна и положительна; остаётся доказать неравенство.

Мы можем использовать два неравенства:

$$f\left(\frac{x_1+x_2}{2}\right) \leqslant \sqrt{f(x_1)f(x_2)}, \quad g\left(\frac{x_1+x_2}{2}\right) \leqslant \sqrt{g(x_1)g(x_2)}.$$

Обозначим для краткости:

$$a_1 = f(x_1), \quad a_2 = f(x_2), \quad b_1 = g(x_1), \quad b_2 = g(x_2).$$

Тогда по неравенству Коши — Буняковского — Шварца

$$f\left(\frac{x_1+x_2}{2}\right)+g\left(\frac{x_1+x_2}{2}\right)\leqslant\sqrt{a_1a_2}+\sqrt{b_1b_2}\leqslant\sqrt{(a_1+b_1)(a_2+b_2)}.$$

Что и требовалось доказать. □

Доказательство теоремы Бора — Моллерупа. Итак, сумма двух логарифмически выпуклых функций логарифмически выпукла. То же можно сказать про сумму трёх или большего количества функций. Переходя к пределу, легко вывести, что если есть семейство функций $f_t(x)$, логарифмически выпуклых для каждого t, и неотрицательная функция $\varphi(t)$, то интеграл $\int\varphi(t)f_t(x)\,dt$ (если он сходится) задаёт логарифмически выпуклую функцию.

Отсюда понятно, что функция

$$\Gamma(x)=\int\limits_0^\infty e^{-t}t^{x-1}\,dt$$

логарифмически выпукла, поскольку t^x логарифмически выпукла (её логарифм линеен). В теореме Бора — Моллерупа это уже доказывает существование, поскольку у нас есть пример нужной функции. Остаётся единственность.

Хочется надеяться, что после сказанного формулировка теоремы Бора — Моллерупа звучит довольно естественно: мы пытаемся расширить логарифмически выпуклую последовательность на нецелые числа, естественно потребовать логарифмическую выпуклость.

Итак, докажем единственность. Сначала сформулируем основные идеи. При помощи функционального уравнения $f(z+1)=z\cdot f(z)$ мы можем двигать числа на целое число единиц, поэтому достаточно доказать единственность для $z\in(0,1)$. Но чем дальше мы передвинем число вправо, тем более жёсткими будут ограничения. Например, если $2<z<3$, то при сдвиге вправо нужно умножить его на что-то между 2 и 3, т. е. диапазон — в полтора раза, а если $100<z<101$, то нужно умножить на что-то между 100 и 101, т. е. ошибка не превышает 1 %. А если мы сдвинем число ещё дальше вправо, то диапазон будет ещё уже.

Для всякой выпуклой функции g легко доказать (или увидеть геометрически) такое неравенство. Пусть $x_1<x_2<x_3$ отличны от x. Пусть k_i — наклон хорды, соединяющей точку $(x_i,g(x_i))$ с точкой $(x,g(x))$. Другими словами,

$$k_i=\frac{g(x_i)-g(x)}{x_i-x}.$$

Тогда $k_1<k_2<k_3$.

В теореме Бора — Моллерупа речь идёт о логарифмически выпуклой функции f, значит, $\ln f$ выпукла. Пусть n — натуральное число. Положим $x = n$, $x_1 = n-1$, $x_2 = n+z$, $x_3 = n+1$, где $0 < z < 1$. Тогда

$$\frac{\ln f(n) - \ln f(n-1)}{n-(n-1)} \leqslant \frac{\ln f(n+z) - \ln f(n)}{n+z-n} \leqslant \frac{\ln f(n+1) - \ln f(n)}{n+1-n},$$

в силу первых двух условий из формулировки теоремы

$$\ln(n-1) \leqslant \frac{1}{z} \ln \frac{f(n+z)}{(n-1)!} \leqslant \ln n,$$

$$(n-1)^z \leqslant \frac{f(n+z)}{(n-1)!} \leqslant n^z,$$

$$(n-1)^z \leqslant \frac{f(z) \cdot z(z+1) \cdot \ldots \cdot (z+n-1)}{(n-1)!} \leqslant n^z.$$

В левом неравенстве заменим $n-1$ на n и получим

$$\frac{f(z) \cdot z(z+1) \cdot \ldots \cdot (z+n-1)}{(n-1)!} \leqslant n^z \leqslant \frac{f(z) \cdot z(z+1) \cdot \ldots \cdot (z+n)}{n!}.$$

При увеличении n отношение между правой и левой частью неравенства $(z+n)/n$ стремится к единице. Значит, отношение между правой и средней частями тоже стремится к единице. Поэтому при $0 < z < 1$

$$f(z) = \lim_{n\to\infty} \frac{n^z \cdot n!}{z(z+1) \cdot \ldots \cdot (z+n)}.$$

Таким образом, при $0 < z < 1$ мы получили явную формулу для f, поэтому f определена однозначно. Этим теорема Бора — Моллерупа доказана. □

Но мы получили не только доказательство теоремы; мы получили явную (причём красивую) формулу для Γ:

$$\Gamma(z) = \lim_{n\to\infty} \frac{n^z \cdot n!}{z(z+1) \cdot \ldots \cdot (z+n)}. \tag{2}$$

Доказали мы её только при $0 < z < 1$, но она может быть легко обобщена на все остальные действительные числа. Достаточно заметить, что эта формула верна для z тогда и только тогда, когда она верна для $z+1$. Действительно,

$$\Gamma(z+1) = z \cdot \Gamma(z) = z \lim_{n\to\infty} \frac{n^z \cdot n!}{z(z+1) \cdot \ldots \cdot (z+n)} = \lim_{n\to\infty} \frac{n^{z+1} \cdot (n-1)!}{(z+1) \cdot \ldots \cdot (z+n)}.$$

А это та же самая формула с $z+1$ вместо z и $n-1$ вместо n.

Итак, мы доказали формулу (2), теперь будем её «причёсывать». Имеем

$$\frac{1}{\Gamma(z)} = \lim_{n\to\infty} n^{-z}\cdot z\cdot(1+z)\Big(1+\frac{z}{2}\Big)\cdot\ldots\cdot\Big(1+\frac{z}{n}\Big). \tag{3}$$

Пару слов о бесконечных произведениях. Пусть у нас есть произведение вида $\prod_{k=1}^{\infty}(1+a_i)$, где $a_i \neq 1$ и $a_i \to 0$. Такое произведение называется сходящимся, если последовательность $\prod_{k=1}^{n}(1+a_i)$ сходится к числу, отличному от 0. Есть простой критерий: произведение является сходящимся, если $\sum_{k=1}^{\infty} a_i$ сходится. Чтобы его доказать, нужно взять логарифм и воспользоваться тем, что $a \approx \ln(1+a)$ при $a \approx 0$. Согласно этому критерию произведение $\prod_{k=1}^{n}(1+z/k)$ расходится при всяком $z \neq 0$. Вейерштрасс хорошо умел «подправлять» такие произведения, делать из них сходящиеся. Например, мы знаем, что $e^z \approx 1+z$. Значит,

$$\prod_{k=1}^{\infty}\frac{1+z/k}{e^{z/k}}$$

является сходящимся произведением, поскольку

$$\frac{1+z/k}{e^{z/k}} = 1+O\Big(\frac{1}{k^2}\Big).$$

Перепишем формулу (3) по-другому, «причесав» её в стиле Вейерштрасса:

$$\frac{1}{\Gamma(z)} = \lim_{n\to\infty} n^{-z}\cdot e^{z+\frac{z}{2}+\frac{z}{3}+\ldots+\frac{z}{n}}\cdot z\cdot\frac{1+z}{e^z}\cdot\frac{1+z/2}{e^{z/2}}\cdot\frac{1+z/3}{e^{z/3}}\cdot\ldots\cdot\frac{1+z/n}{e^{z/n}}.$$

Последнюю серию в этом произведении можно выделить как отдельный — сходящийся — предел:

$$\frac{1}{\Gamma(z)} = \lim_{n\to\infty} e^{z\left(1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n}-\ln n\right)}\cdot z\cdot\prod_{k=1}^{\infty}\frac{1+z/k}{e^{z/k}},$$

$$\frac{1}{\Gamma(z)} = e^{\gamma z}\cdot z\cdot\prod_{k=1}^{\infty}\frac{1+z/k}{e^{z/k}}. \tag{5}$$

Это *формула Вейерштрасса*. Посмотрим на эту формулу и восхитимся ею. В чём суть? Мы уже упомянули, что у Γ имеются полюса в неположительных целых числах. Значит, у $1/\Gamma$ в этих точках — серия нулей. Мы можем сказать, что это как бы многочлен, но с бесконечной серией корней. Многочлен мы попытались бы разложить на линейные множители; тут мы захотели тоже написать бесконечное произведение, но получили, что оно расходится. Затем пришёл Вейерштрасс и добавил поправки для сходимости, и получилось почти то, что надо, но затем абсолютно мистическим образом сбоку появилось $e^{\gamma z}$, где γ — то самое!

Ещё один инструмент, который нам понадобится, это логарифмическая производная. Её можно определить двумя способами: $(\ln f(z))'$ или $f'(z)/f(z)$, и это одно и тоже. Замечательно, что в комплексных числах логарифм определён не очень хорошо (с точностью до добавки в $2\pi in$, причём иногда эту добавку нельзя выбрать во всех точках), а вот логарифмическая производная всегда работает. Как и логарифм, логарифмическая производная переводит произведение в сумму:

$$\frac{(fg)'}{fg} = \frac{f'}{f} + \frac{g'}{g}, \quad \frac{(f/g)'}{f/g} = \frac{f'}{f} - \frac{g'}{g}$$

(возможно, это самый удобный способ записать формулу Лейбница).

Например, если мы возьмём функциональное уравнение Γ и обозначим через $\psi(z) = \Gamma'(z)/\Gamma(z)$ его логарифмическую производную, то из $\Gamma(z+1) = z \cdot \Gamma(z)$ получается $\psi(z+1) = 1/z + \psi(z)$. Читатель может догадаться, что $\psi(z+1)$ чем-то похоже на H_z, но это не та же самая функция, она отличается на… Впрочем, не будем забегать вперёд.

В чём логарифмическая производная нам действительно сильно поможет, это в том, чтобы продифференцировать Γ. У нас есть замечательная формула Вейерштрасса (5), но это огромное произведение, а дифференцировать длинное произведение не так просто. А вот логарифмическую производную очень легко:

$$-\psi(z) = \gamma + \frac{1}{z} + \sum_{k=1}^{\infty}\Big(\frac{1/k}{1+z/k} - \frac{1}{k}\Big),$$

$$-\psi(z) = \gamma + \frac{1}{z} + \sum_{k=1}^{\infty}\Big(\frac{1}{k+z} - \frac{1}{k}\Big).$$

Стоп. Эту формулу

$$\sum_{k=1}^{\infty}\Big(\frac{1}{k+z} - \frac{1}{k}\Big)$$

мы где-то видели. Это же $-H_z$.

Слишком много минусов (и у ψ, и у H_z), давайте поменяем знак:

$$\psi(z) = H_z - \frac{1}{z} - \gamma, \quad \psi(z) = H_{z-1} - \gamma.$$

Это уже очень красиво, но давайте получим отсюда ещё несколько выводов.

Например, чему равно $\Gamma'(1)$? Очень просто: $H_0 = H_1 - 1 = 0$, а значит,

$$\frac{\Gamma'(1)}{\Gamma(1)} = H_0 - \gamma = -\gamma.$$

Но $\Gamma(1)=1$, значит, $\Gamma'(1)=-\gamma$. Читатель может аналогично вычислить $\Gamma'(2)$, $\Gamma'(1/2)$ и т. д. и везде будет выплывать γ (при подсчёте последнего может понадобиться $\Gamma(1/2)$, это связано с красивым интегралом Гаусса $\int_{-\infty}^{\infty} e^{-x^2}\,dx$).

Мы почти готовы вычислить интеграл (1), с которого начали наш разговор; но перед этим давайте попробуем продифференцировать Γ «руками», без всех этих хитростей:

$$\Gamma'(z) = \frac{d}{dz}\int\limits_0^\infty e^{-x}x^{z-1}\,dx = \int\limits_0^\infty e^{-x}\cdot\ln x\cdot x^{z-1}\,dx.$$

Давайте подставим для примера $z=1$:

$$\Gamma'(1) = \int\limits_0^\infty e^{-x}\cdot\ln x\,dx.$$

Но мы же знаем, что это $-\gamma$. Это и есть ответ.

Читатель получит настоящее удовольствие, если подсчитает до конца, без всяких там «ну понятно, что можно доделать»,

$$\int\limits_0^\infty e^{-x}\cdot\sqrt{x}\cdot\ln x\,dx.$$

Там будет и π, и $\ln 2$, и конечно же γ.

Список литературы

[1] *Artin E.* Einführung in die Theorie der Gammafunktion. Leipzig: Teubner. 1931.

[2] *Lagarias J.* Euler's constant: Euler's work and modern developments // Bull. AMS. 2013. Vol. 50, № 4. P. 527–628.

Л. Радзивиловский, Тель-Авивский университет (Израиль)
levr78@hotmail.com

Пентагональная теорема Эйлера

Ф. В. Петров

§ 1. Введение

Пентагональная теорема

$$(1-x)(1-x^2)(1-x^3)\ldots = \sum_{n=-\infty}^{\infty}(-1)^n x^{n(3n-1)/2} = \\ = 1-x-x^2+x^5+x^7-x^{12}-x^{15}+\ldots \quad (1)$$

была сначала высказана в качестве гипотезы ([1], представлено в 1741 году) а затем доказана Леонардом Эйлером [4]. Обе статьи опубликованы в Комментариях Петербургской академии наук, в которой Эйлер проработал в общей сложности более 30 лет. Здесь и далее мы ссылаемся на работы и переписку Эйлера по обзору Джордана Белла [10], проделавшего в том числе большую работу по переводу с латыни. Ряд исторических сведений почерпнут из замечательного обзора Игоря Пака [11]. Из популярной математической литературы на русском языке, посвящённой пентагональной теореме, отметим [7].

Это удивительно красивое тождество оказалось и очень важным для развития математики. Оно наряду с другими работами Эйлера положило начало области, которую сейчас называют теорией разбиений, в которой особенно прославился другой гениальный математик — Сриниваса Рамануджан. Обобщения этого тождества возникают при изучении предметов самых разных — от бесконечномерных алгебр Ли до суперструн.

Мы обсудим некоторые доказательства пентагональной теоремы, начав с оригинального рассуждения Эйлера, а также её приложения и обобщения.

Статья содержит решение задачи 26.3″ («Математическое просвещение», вып. 29, с. 268).

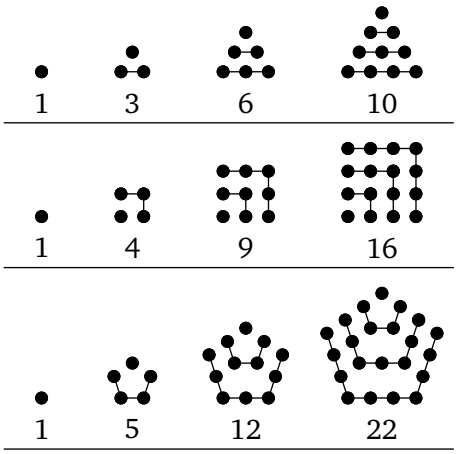
Но прежде того обсудим, как следует понимать (1). Есть два подхода. Во-первых, можно считать, что x — вещественное или комплексное число и $|x|<1$. Тогда обе части (1) сходятся и речь идёт о равенстве бесконечной суммы (которая в данном случае не зависит от порядка слагаемых) бесконечному произведению. Другой подход к (1) не апеллирует к анализу. А именно, можно зафиксировать показатель m и определить коэффициент бесконечного произведения $(1-x)(1-x^2)(1-x^3)\ldots$ при одночлене x^m, перемножив лишь первые m сомножителей. Домножение на каждую следующую скобку не меняет этого коэффициента, что делает такое определение естественным. Тождество (1) говорит, что коэффициент при x^m окажется равным $(-1)^n$, если $m=n(3n-1)/2$ при некотором целом n, и равным 0 в противном случае. Таким образом, тождество (1) можно понимать как серию утверждений о коэффициентах *многочленов*.

В теории разбиений продуктивно используются оба подхода. Оправдание некоторых преобразований с бесконечными суммами и произведениями требует в обоих случаях рутинной проверки, которая в настоящей статье опускается.

Устоявшееся название «пентагональная теорема» связано с тем, что числа

$$\frac{n(3n-1)}{2}=1+4+\ldots+(3n-2)$$

называют пятиугольными — по аналогии с треугольными $n(n+1)/2=$ $=1+2+\ldots+n$ и квадратными $n^2=1+3+5+\ldots+(2n-1)$ числами (см. рисунок). Впрочем, при отрицательном $n=-k$ мы получаем числа вида $k(3k+1)/2$, которые пятиугольными уже не называются.



§ 2. Доказательство Эйлера

Последуем старому совету Пьера-Симона Лапласа: *читайте Эйлера, читайте Эйлера — он наш общий учитель*.

На протяжении десяти лет Эйлер постоянно возвращался к пентагональной теореме в своей переписке с Даниилом и Николаем Бернулли, д'Аламбером и Гольдбахом. Доказательство, которое мы сейчас обсудим, приводится Эйлером в письме Гольдбаху от 9 июня 1750 года.

Эйлер начинает со следующего общего тождества:

$$(1-\alpha)(1-\beta)(1-\gamma)(1-\delta)\ldots = \\ = 1-\alpha-\beta(1-\alpha)-\gamma(1-\alpha)(1-\beta)-\ldots, \quad (2)$$

которое доказывается непосредственно. Переписывая произведение

$$s := (1-x)(1-x^2)(1-x^3)\ldots,$$

с помощью (2) получаем

$$s = 1-x-x^2(1-x)-x^3(1-x)(1-x^2)\ldots = 1-x-Ax^2,$$

где

$$A = 1-x+x(1-x)(1-x^2)+x^2(1-x)(1-x^2)(1-x^3)+\ldots$$

Раскрываем везде скобку $1-x$, получаем

$$\begin{aligned} A = 1 &-x+x(1-x^2) -x^2(1-x^2)+x^2(1-x^2)(1-x^3)- \\ &-x^3(1-x^2)(1-x^3)+x^3(1-x^2)(1-x^3)(1-x^4)-\ldots = \\ &= 1-x^3-x^5(1-x^2)-x^7(1-x^2)(1-x^3)-\ldots = 1-x^3-Bx^5, \end{aligned}$$

где

$$B = 1-x^2+x^2(1-x^2)(1-x^3)+x^4(1-x^2)(1-x^3)(1-x^4)+\ldots$$

Продолжаем в том же духе: раскрываем везде скобку $1-x^2$ и группируем пары слагаемых, которые кратны одной и той же степени x. Получаем

$$B = 1-x^5-Cx^8,$$

где

$$C = 1-x^3+x^3(1-x^3)(1-x^4)+x^6(1-x^3)(1-x^4)(1-x^5)+\ldots$$

Аналогично

$$C = 1-x^7-Dx^{11}, \quad D = 1-x^9-Ex^{14} \quad \text{и т. д.}$$

Теперь несложно получить (1). Имеем

$$\begin{aligned} s &= 1 - x - Ax^2, \\ A &= 1 - x^3 - Bx^5, \\ B &= 1 - x^5 - Cx^8, \\ C &= 1 - x^7 - Dx^{11}, \\ &\dots\dots\dots\dots\dots\dots \end{aligned} \tag{3}$$

Умножая второе уравнение на $-x^2$, третье на x^7, четвёртое на $-x^{15}$ и т. д. и складывая (чтобы сократились члены с буквами $A, B, C \dots$) получаем

$$s = 1 - x - x^2(1 - x^3) + x^7(1 - x^5) - x^{15}(1 - x^7) + \dots,$$

что равносильно (1).

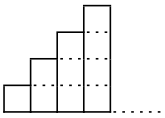
§ 3. Вероятность

Приведённое доказательство коротко и понятно, исключительно нетривиально (что подтверждается хотя бы тем, сколько времени заняло у Эйлера найти его), и хочется понять, что стоит за этим жонглированием формулами. Изложим то же доказательство без формул, но с картинками.

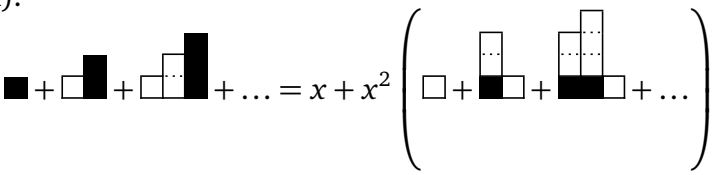
Начнём с тождества (2). Оно имеет ясный вероятностный смысл: если $\alpha, \beta, \gamma, \dots$ — вероятности независимых событий, то

$$(1 - \alpha)(1 - \beta)(1 - \gamma) \dots$$

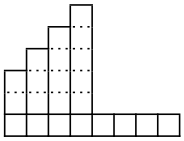
— вероятность того, что ни одно из них не происходит. Она равна 1 минус (вероятность того, что произошло первое событие) минус (вероятность того, что первое событие не произошло, но произошло второе) минус (вероятность того, что первые два события не произошли, но произошло третье) минус (и т. д.) В нашей ситуации $\alpha = x$, $\beta = x^2$, $\gamma = x^3$, … Соответствующий случайный процесс можно реализовать так: рассмотрим бесконечную клетчатую плоскость. Пусть $0 < x < 1$ и в каждом квадрате с вероятностью $1 - x$ (и независимо от остальных квадратов) вырастает ёлочка. Тогда $s = (1 - x)(1 - x^2) \dots$ — это вероятность того, что *в каждом из выделенных на рисунке прямоугольников* 1×1, 1×2, 1×3, … *есть хотя бы одна ёлочка.*



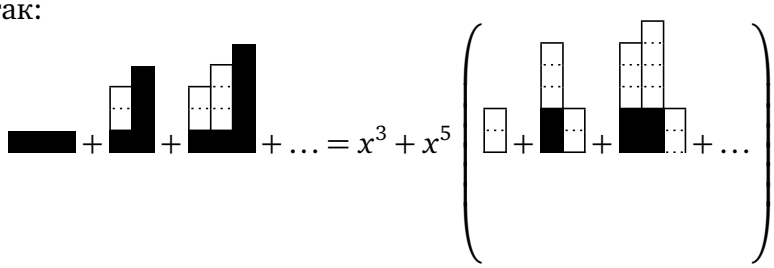
Следовательно, $1-s$ есть вероятность того, что по крайней мере в одном из выделенных прямоугольников нет ёлочки. В том, что написано далее, фигура, составленная из чёрных и белых прямоугольников, означает вероятность такого события: каждый чёрный прямоугольник не содержит ёлочек, а каждый белый содержит хотя бы одну ёлочку (см. рисунок).

$1-s=$  $= x+x^2\Big($ $+\dots\Big)$.

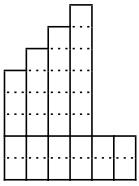
Получаем $1-s=x+x^2A$, где A после нашего перекладывания прямоугольников интерпретируется как вероятность такого события: *находим первую ёлочку в нижней строке, тогда все выделенные прямоугольники* 1×2, 1×3, … *слева от неё содержат хотя бы по одной ёлочке.*



Таким образом, $1-A$ есть вероятность того, что в некотором столбце выделенный прямоугольник, а также часть первой строки вплоть до этого прямоугольника, не содержат ёлочек. Это опять же можно перерисовать так:

$1-A=$  $= x^3+x^5\Big($ $+\dots\Big)$,

т. е. $1-A=x^3+x^5B$, где B есть вероятность такого события: *находим первую ёлочку в нижних двух строках, тогда все выделенные прямоугольники* 1×3, 1×4, … *слева от неё содержат хотя бы по одной ёлочке.*



Продолжая в таком духе, получаем (3).

§ 4. Биекция

Раскроем скобки в выражении $(1-x)(1-x^2)(1-x^3)\ldots$ Мы получим сумму всевозможных слагаемых вида

$$(-1)^m x^{c_1+c_2+\ldots+c_m},$$

где $c_1 < c_2 < \ldots < c_m$ — целые положительные числа.

Будем говорить, что числа $c_1, \ldots, c_m$ образуют слагаемые *разбиения* числа $N = c_1 + \ldots + c_m$. Таким образом, коэффициент при данном одночлене x^N оказывается равен *разности между количеством разбиений N на чётное количество попарно различных слагаемых и на нечётное количество попарно различных слагаемых*.

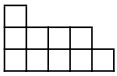
Тождество (1) говорит, что эта разность равна $(-1)^n$, если $N = n(3n+1)/2$ для некоторого целого n, и равна 0 в противном случае.

То есть разбиений на чётное и на нечётное количество слагаемых должно быть поровну или «почти поровну», если N имеет указанный вид. Естественно желание установить биекцию (или, соответственно, «почти биекцию») между теми и другими разбиениями. Это было сделано американским математиком Фабианом Франклином в 1881 году Приведём его доказательство.

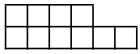
Попробуем разбить все разбиения числа N на пары так, чтобы разбиения в каждой паре имели разное по чётности количество слагаемых. Если $N = n(3n \pm 1)/2$ и разбиение на слагаемые имеет вид $(n+1) + \ldots + 2n$ или $n + \ldots + (2n-1)$, выделим это разбиение и разобьём на пары все остальные. Если же N не имеет такого вида, разобьём на пары просто все разбиения числа N. Пусть x — наибольшее слагаемое разбиения и пусть оно содержит слагаемые x, $x-1$, …, $x-t+1$, но не содержит $x-t$. Пусть, далее, s — наименьшее слагаемое разбиения. Если $s \leqslant t$, то выкинем из разбиения слагаемое s и прибавим по 1 к слагаемым от $x-s+1$ до x. Если $s > t$, вычтем по 1 из слагаемых от $x-t+1$ до x и добавим слагаемое t. Это соответствие между разбиениями разбивает их на пары, и в каждой паре количества слагаемых отличаются на 1. Заметим, что первое из наших соответствий не работает только в случае $x-t+1 = s = t$ (в этом случае следовало бы увеличивать выкидываемое слагаемое). Второе соответствие не работает только в случае $s = t+1 = x-t+1$ (в этом случае в новом разбиении получаются два равных слагаемых). Но как раз такие разбиения мы заблаговременно выделяли.

Соответствие Франклина становится особенно наглядным, если каждому разбиению сопоставлять *диаграмму Юнга* — фигуру, состав-

ленную из единичных квадратиков, в которой слагаемым соответствуют длины строк. Например, разбиению $10 = 5 + 4 + 1$ соответствует диаграмма

 .

Тогда s — количество клеток в самой короткой строчке, а t — в диагонали, ведущей из самой правой клетки нижней строчки на северо-запад. Если $s \leqslant t$, мы убираем самую короткую строчку и увеличиваем за счёт неё s самых длинных строк. Если же $s > t$, мы укорачиваем t самых длинных строк на 1 каждую и добавляем строку длины t. В приведённом примере $s = 1 < 2 = t$, так что мы получаем парное разбиение $10 = 6 + 4$ с диаграммой

 .

Решите следующую задачу, предлагавшуюся Финляндией в 1979 году на Международную олимпиаду.

Набор целых положительных чисел $(a_1, a_2, \ldots, a_n)$, удовлетворяющий равенству $a_1 + 2a_2 + \ldots + na_n = 1979$, назовём чётным, если n чётно, и нечётным, если n нечётно. Докажите, что чётных и нечётных наборов поровну.

В каком году их было не поровну?

§ 5. Число разбиений

Рассмотрим произведение

$$\begin{aligned}\frac{1}{1-x}\cdot\frac{1}{1-x^2}\cdot\frac{1}{1-x^3}\cdot\ldots &= \\ = (1+x+x^2+\ldots)(1+x^2+x^4+\ldots)(1+x^3+x^6+\ldots)\ldots &= \\ = 1+x+2x^2+3x^3+5x^4+\ldots &= \\ = p(0)+p(1)x+p(2)x^2+p(3)x^3+\ldots \quad (4)\end{aligned}$$

Мы воспользовались разложением дроби $1/(1-y)$ в геометрическую прогрессию $1 + y + y^2 + y^3 + \ldots$ при $y = x, x^2, \ldots$ Раскрывая скобки, получаем, что коэффициент $p(n)$ при x^n равен числу способов представить n в виде

$$n = k_1 + 2k_2 + 3k_3 + \ldots \qquad (5)$$

с целыми неотрицательными $k_1, k_2, \ldots$ Такому представлению соответствует разбиение числа n на натуральные слагаемые (не обязательно

различные): k_1 единиц, k_2 двоек, k_3 троек и т. д. — и наоборот, каждому разбиению соответствует представление (5). Разбиениям, как и в предыдущем разделе, соответствуют диаграммы Юнга — только теперь длины строк могут совпадать.

Комбинируя (1) и (4), получаем

$$\begin{aligned} 1 &= (p(0)+p(1)x+p(2)x^2+\ldots)(1-x)(1-x^2)(1-x^3)\ldots = \\ &= (p(0)+p(1)x+p(2)x^2+\ldots)(1-x-x^2+x^5+x^7-\ldots). \end{aligned} \tag{6}$$

Раскрывая скобки и приравнивая коэффициент при x^n, $n>0$, получаем рекуррентное соотношение на числа $p(n)$:

$$p(n)-p(n-1)-p(n-2)+p(n-5)+p(n-7)-\ldots=0. \tag{7}$$

Это тождество было получено Эйлером в работе [2].

Соотношение (7) позволяет быстро искать значения $p(n)$ вручную или на компьютере (отметим, что Эйлер в [2] вычислил с помощью (7) таблицу значений $p(n)$ вплоть до $n=30$, а та же задача для как можно большего n была предложена участникам самой первой всесоюзной олимпиады по программированию в 1988 году).

Но понять что-нибудь о росте значений $p(n)$ при больших n с помощью (7) проблематично. Априори совершенно не очевидно даже, что последовательность, задаваемая начальным условием и рекуррентным соотношением (7), принимает положительные значения.

Тем не менее, асимптотика числа разбиений, полученная Харди и Рамануджаном, непосредственно связана с пентагональной теоремой. Число разбиений растёт как

$$p(n) \sim \frac{1}{4\sqrt{3}\,n} e^{\pi\sqrt{2n/3}} \tag{8}$$

(обозначение $a \sim b$ означает, что частное $a:b$ стремится к 1), но формула (8) становится гораздо точнее и открывает путь к полному асимптотическому разложению, если вместо n использовать $n-1/24$:

$$p(n) \sim \frac{1}{2\pi\sqrt{2}} \left(\frac{\pi}{\sqrt{6}\left(n-\frac{1}{24}\right)} - \frac{1}{2\left(n-\frac{1}{24}\right)^{3/2}} \right) \exp\left(\pi\sqrt{\frac{2}{3}\left(n-\frac{1}{24}\right)} \right). \tag{9}$$

Чтобы продемонстрировать, насколько формула (9) точнее, чем (8), приведём значения при $n=200$: $p(200)=3\,972\,999\,029\,388$, правая часть (8) при $n=200$ даёт значение $4\,100\,251\,432\,187$, а правая часть (9) — значение $3\,972\,998\,993\,185$.

Почему 1/24? Связь не очевидна, но на самом деле потому, что

$$\frac{n(3n+1)}{2}+\frac{1}{24}=\frac{3}{2}\left(n+\frac{1}{6}\right)^2,$$

а значит, при умножении на $x^{1/24}$ в показателях суммы в правой части (1) выделяются полные квадраты:

$$\left(\sum_{n=0}^{\infty}p(n)x^{n-1/24}\right)^{-1}=x^{1/24}\prod_{k=1}^{\infty}(1-x^k)=\sum_{n=-\infty}^{\infty}(-1)^n x^{\frac{3}{2}(n+1/6)^2}.$$

Функция в правой части удовлетворяет неочевидному функциональному уравнению, которое позволяет с хорошей точностью находить её значения вблизи $x=1$, а они в свою очередь связаны с ростом $p(n)$.

§ 6. Сумма делителей

Тождество Лейбница для производной произведения

$$(fg)'=f'g+g'f=fg\left(\frac{f'}{f}+\frac{g'}{g}\right)$$

допускает при некоторых условиях обобщение

$$(f_1f_2\ldots)'=\left(\frac{f_1'}{f_1}+\frac{f_2'}{f_2}+\ldots\right)f_1f_2\ldots$$

на случай произведения бесконечного количества сомножителей. Эти условия выполнены для левой части (1), так что

$$\sum_{n=-\infty}^{\infty}(-1)^n\frac{n(3n+1)}{2}x^{n(3n+1)/2}=x\left(\sum_{n=-\infty}^{\infty}(-1)^n x^{n(3n+1)/2}\right)'=$$
$$=x\left(\prod_{k=1}^{\infty}(1-x^k)\right)'=-\left(\sum_{k=1}^{\infty}\frac{kx^k}{1-x^k}\right)\left(\prod_{k=1}^{\infty}(1-x^k)\right)=$$
$$=-\left(\sum_{k=1}^{\infty}\frac{kx^k}{1-x^k}\right)\left(\sum_{n=-\infty}^{\infty}(-1)^n x^{n(3n+1)/2}\right).$$

Для первого сомножителя в правой части имеем

$$\sum_{k=1}^{\infty}\frac{kx^k}{1-x^k}=\sum_{k=1}^{\infty}kx^k(1+x^k+x^{2k}+x^{3k}+\ldots)=$$
$$=\sum_{k=1}^{\infty}k\sum_{m=1}^{\infty}x^{mk}=\sum_{n=1}^{\infty}\sum_{k|n}kx^n=\sum_{n=1}^{\infty}\sigma(n)x^n,$$

где $\sigma(n)$ — сумма всех натуральных делителей числа n. Таким образом,

$$\sum_{n=-\infty}^{\infty}(-1)^n\frac{n(3n+1)}{2}x^{n(3n+1)/2}=-\left(\sum_{n=1}^{\infty}\sigma(n)x^n\right)\left(\sum_{n=-\infty}^{\infty}(-1)^n x^{n(3n+1)/2}\right). \tag{10}$$

Перепишем (10) в виде

$$\sum_{n=-\infty}^{\infty}(-1)^n\frac{n(3n+1)}{2}x^{n(3n+1)/2}+\left(\sum_{n=1}^{\infty}\sigma(n)x^n\right)\left(\sum_{n=-\infty}^{\infty}(-1)^n x^{n(3n+1)/2}\right)=0$$

и раскроем скобки. Приравнивая нулю коэффициент при x^N, получаем

$$\sigma(N)-\sigma(N-1)-\sigma(N-2)+\sigma(N-5)+\sigma(N-7)-\ldots=0, \tag{11}$$

где надо полагать $\sigma(N-N)=N$, если такое слагаемое возникнет (т. е. если N имеет вид $N=n(3n+1)/2$ с целым n).

Тождество (11) было также получено Эйлером [3, 4] ещё до доказательства пентагональной теоремы (но с её помощью — собственно, его рассуждение приведено выше). Эйлер находил его весьма примечательным, охотно соглашались с ним Гольдбах и д'Аламбер. Действительно, сам факт, что суммы делителей чисел N, $N-1$, $N-2$, $N-5$, … связаны нетривиальным соотношением, ошеломляет.

§ 7. Тройное тождество Якоби

Замечательным обобщением пентагональной теоремы является *тройное тождество Якоби* [5] (раньше, чем Якоби, его открыл Гаусс, но не опубликовал):

$$\prod_{n=1}^{\infty}(1-zq^{n-1})(1-z^{-1}q^n)(1-q^n)=\sum_{m=-\infty}^{\infty}(-1)^m q^{m(m-1)/2}z^m. \tag{12}$$

Здесь следует понимать обе части как степенные ряды по q, коэффициенты которых суть многочлены Лорана от переменной z (т. е. многочлены от z, z^{-1}). Поскольку q везде содержится только в положительных степенях, мы, как и раньше, можем определить в левой части коэффициент при любой степени q.

Пентагональная теорема получается, если подставить $q=x^3$, $z=x$.

Приведём два доказательства тройного тождества Якоби — алгебраическое и комбинаторное.

Начнём с комбинаторного, которое принадлежит Джеймсу Джозефу Сильвестру [6] и впоследствии неоднократно переоткрывалось. Как

показал Ричард Борчердс (см. книгу Питера Кэмерона [8]), к эквивалентному доказательству можно прийти из физических соображений, изучая электроны в море Дирака.

Прежде всего, заменим z на $-z$ и умножим обе части (12) на

$$\prod_{n=1}^{\infty}(1-q^n)^{-1} = \sum_{k=0}^{\infty} p(k)q^k.$$

Получим равносильное тождество

$$\prod_{n=1}^{\infty}(1+zq^{n-1})(1+z^{-1}q^n) = \left(\sum_{k=1}^{\infty} p(k)q^k\right)\left(\sum_{m=-\infty}^{\infty} q^{m(m-1)/2}z^m\right). \qquad (13)$$

Раскроем скобки в произведении $\prod(1+zq^{n-1})$, получаем

$$\prod_{n=1}^{\infty}(1+zq^{n-1}) = \sum_{\lambda} z^{\ell(\lambda)}q^{|\lambda|},$$

где λ пробегает все разбиения λ: $0 \leqslant c_1 < c_2 < \ldots < c_m$ целых неотрицательных чисел на попарно различные целые неотрицательные слагаемые, $m = \ell(\lambda)$ — количество слагаемых, $c_1 + \ldots + c_m = |\lambda|$ — их сумма. Аналогично

$$\prod_{n=1}^{\infty}(1+z^{-1}q^n) = \sum_{\mu} z^{-\ell(\mu)}q^{|\mu|},$$

но μ пробегает все разбиения (в том числе пустое) на различные целые *положительные* слагаемые. Таким образом, левая часть (13) есть

$$\sum_{\lambda,\mu} z^{\ell(\lambda)-\ell(\mu)}q^{|\lambda|+|\mu|}.$$

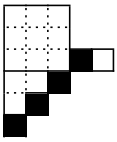
Теперь раскроем скобки в правой части (13) и обратим внимание на члены с фиксированным показателем при z. Получим, что при всяком целом m надо доказать равенство

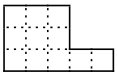
$$\sum_{\lambda,\mu\colon \ell(\lambda)-\ell(\mu)=m} q^{|\lambda|+|\mu|} = \sum_{k=0}^{\infty} p(k)q^{k+m(m-1)/2} = \sum_{\sigma} q^{|\sigma|+m(m-1)/2}, \qquad (14)$$

где суммирование производится по всем диаграммам Юнга σ с $|\sigma|$ клетками. Пусть $m \geqslant 0$ (случай $m < 0$ аналогичен). Опишем наше соответствие, сопоставляющее диаграмме σ пару разбиений λ, μ и тем доказывающее (14). Увеличим диаграмму σ, пририсовав к ней снизу треугольник из $m(m-1)/2$ клеток: $m-1$ клеток к первому столбцу,

$m-2$ ко второму столбцу и т. д. Это множество клеток, вообще говоря, уже не является диаграммой Юнга, но оно содержит $|\sigma|+m(m-1)/2$ клеток, их мы и собираемся разбивать на λ и μ. Закрасим m клеток на диагональной прямой под дорисованным треугольником, а также клетки этой же прямой, попадающие в диаграмму σ.

В разбиение λ возьмём для каждой закрашенной клетки количество клеток увеличенной диаграммы, лежащих строго выше закрашенной клетки в том же столбце. В разбиение μ возьмём для каждой закрашенной клетки самой диаграммы σ количество клеток диаграммы σ, лежащих в той же строке нестрого правее, чем эта закрашенная клетка.



Например, на этом рисунке $m=3, \sigma=$  . Получается $\lambda=\{5,4,3,0\}$, $\mu=\{2\}$. Несложно видеть, что построено взаимно однозначно соответствие, доказывающее (14), а с ним (13) и (12).

Алгебраическое доказательство приводится в следующем разделе.

§ 8. q-биномиальная теорема

Важную роль в комбинаторике играют так называемые q-тождества. Будем называть **q-аналогом** натурального числа n многочлен от буквы q:

$$(n)_q = 1+q+q^2+\ldots q^{n-1} = \frac{1-q^n}{1-q}.$$

Будем называть q-аналогом факториала $n!$ произведение

$$(n)_q! = (1)_q \cdot (2)_q \cdot \ldots \cdot (n)_q.$$

Обозначим также

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{(n)_q!}{(k)_q!(n-k)_q!}.$$

При $q=1$ получаются обычные факториалы и биномиальные коэффициенты.

q-Аналогом биномиальной теоремы является следующая *q-биномиальная теорема*:

$$(x-y)(x-qy)(x-q^2y)\ldots(x-q^{n-1}y)=\sum_{k=0}^{n}(-1)^k q^{k(k-1)/2}\begin{bmatrix} n \\ k \end{bmatrix} x^{n-k}y^k. \quad (15)$$

Доказать (15) можно, например, индукцией по n (для перехода от n к $n+1$ надо умножить обе части на $x-q^n y$, раскрыть справа скобки и упростить коэффициенты). Это доказательство несложное, но оно не раскрывает суть.

Другой способ доказательства (15) состоит в применении *комбинаторной теоремы о нулях* Н. Алона. Последняя утверждает (ограничимся случаем двух переменных, чтобы не вводить новые обозначения), что если многочлен $F(x,y)$ степени не выше n принимает нулевые значения во всех точках «прямоугольника» $A\times B$, где $|A|=n-k+1$, $|B|=k+1$ то и его коэффициент при $x^{n-k}y^k$ равен нулю (здесь A,B — подмножества поля, над которым задан многочлен, в нашем случае поля рациональных функций от q). Про комбинаторную теорему о нулях и её применения можно прочитать в статье Алона [9]. Применяя эту теорему к многочлену

$$\begin{aligned}F(x,y) = (x-y)(x-qy)(x-q^2y)\dots(x-q^{n-1}y) + \\ + (-1)^{k+1}q^{k(k-1)/2}\begin{bmatrix} n \\ k \end{bmatrix}(x-1)(x-q)(x-q^2)\dots\times \\ \times(x-q^{n-k+1})(y-1)(y-q^{-1})\dots(y-q^{1-k}),\end{aligned}$$

который обнуляется на множестве

$$\{1,q,q^2,\dots,q^{n-k}\}\times\{1,q^{-1},q^{-2},\dots,q^{-k}\}$$

(проверьте это), получаем, что коэффициент при $x^{n-k}y^k$ многочлена F равен нулю, а следовательно, у многочлена

$$(x-y)(x-qy)(x-q^2y)\dots(x-q^{n-1}y)$$

он равен $(-1)^k q^{k(k-1)/2}\begin{bmatrix} n \\ k \end{bmatrix}$, что и утверждает (15).

Теперь покажем, как (15) влечёт (12).

Зафиксируем большое число N. Подставим в (15) $n=2N$, $x=z^{-1}$, $y=q^{-N}$. Получим

$$\begin{aligned}\prod_{i=1}^{N}(z^{-1}-q^{i-1})(z^{-1}-q^{-i}) = (x-y)\dots(x-q^{2N-1}y) = \\ = \sum_{k=0}^{2N}(-1)^k q^{k(k-1)/2}\begin{bmatrix} 2N \\ k \end{bmatrix}q^{-Nk}z^{-(2N-k)}.\end{aligned}$$

Домножим на $(-1)^N z^N q^{N(N+1)/2}$, тогда левая часть превратится в

$$\prod_{i=1}^{N}(1-q^{i-1}z)(1-q^i z^{-1}).$$

Справа переобозначим $k-N=m$. Получим

$$\prod_{i=1}^{N}(1-q^{i-1}z)(1-q^{i}z^{-1})=\sum_{m=-N}^{N}(-1)^{m}\begin{bmatrix}2N\\N+m\end{bmatrix}q^{m(m-1)/2}z^{m}.$$

Теперь устремим N к бесконечности. Заметим, что левая часть будет стремиться (в том смысле, что коэффициент при каждой степени q будет стабилизироваться) к

$$\prod_{i=1}^{\infty}(1-q^{i-1}z)(1-q^{i}z^{-1}).$$

Слагаемые справа при $|m|>N/2$ будут стремиться, очевидно, к 0 (каждое по отдельности и всё в сумме). Для прочих слагаемых q-биномиальный коэффициент

$$\begin{bmatrix}2N\\N+m\end{bmatrix}=\prod_{i=1}^{N+m}\frac{1-q^{2N+1-i}}{1-q^{i}}$$

стремится к $\prod_{i=1}^{\infty}\dfrac{1}{1-q^{i}}$. Окончательно, переходя к пределу, получаем

$$\prod_{i=1}^{\infty}(1-q^{i-1}z)(1-q^{i}z^{-1})=\prod_{i=1}^{\infty}\frac{1}{1-q^{i}}\sum_{m=-\infty}^{\infty}(-1)^{m}q^{m(m-1)/2}z^{m},$$

что и требовалось.

Список литературы

[1] *Euler L.* Observationes analyticae variae de combinationibus // Commentarii academiae scientiarum imperialis Petropolitanae. 1741–1743. Vol. 13. P. 64–93.

[2] *Euler L.* De partitione numerorum // Novi commentarii academiae scientiarum imperialis Petropolitanae. 1750–1751. Vol. 3. P. 125–169.

[3] *Euler L.* Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs // Bibliothèque impartiale. 1751. Vol. 3. P. 10–31.

[4] *Euler L.* Demonstratio theorematis circa ordinem in summis divisorum observatum // Novi commentarii academiae scientiarum imperialis Petropolitanae. 1760. Vol. 5. P. 75–83.

[5] *Jacobi C. G. J.* Fundamenta nova theoriae functionum ellipticarum. Königsberg: Borntraeger, 1829. Переиздано в Cambridge University Press (2012).

[6] *Sylvester J. J.*, *Franklin F.* A constructive theory of partitions, arranged in three acts, an interact and an exodion // Amer. J. Math. 1882. Vol. 5, № 1. P. 251–330.

[7] *Фукс Д.* О раскрытии скобок, об Эйлере, Гауссе, Макдональде и об упущенных возможностях // Квант. 1981. № 8. С. 12–20.

[8] *Cameron P. J.* Combinatorics: Topics, Techniques, Algorithms. Cambridge University Press, 1994.

[9] *Alon N.* Combinatorial Nullstellensatz // Combin. Probab. Comput. 1999. Vol. 8. P. 7–29.

[10] *Bell J.* Euler and the Pentagonal Number Theorem. `https://arxiv.org/abs/math/0510054`.

[11] *Pak I.* Partition bijections, a survey // The Ramanujan Journal. 2006. Vol. 12, № 1. P. 5–75.

Фёдор Владимирович Петров, СПбГУ
`fedyapetrov@gmail.com`

Задачи о линейных рекуррентах

А. Я. Канель-Белов

В «Математическом просвещении», сер. 3, вып. 12, с. 236, опубликована

Задача 12.12 (теорема Сколема — Малера — Леха[1]). *Линейной рекуррентой порядка n* называется такая последовательность $\{u_k\}$, что при всех k

$$a_0 u_{k+n} + a_1 u_{k+n-1} + \ldots + a_n u_k \equiv 0,$$

где a_i — некоторые константы, не все равные нулю одновременно. *Нулём* 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.

(*Предложил А. Я. Канель*)

Понятие линейной рекурренты играет важную роль во многих математических задачах. Первоначальные сведения о линейных рекуррентах содержатся в брошюре [4].

I. Напомним классический факт:

Теорема 1. *Дана линейная рекуррента $A = \{a_n\}$ порядка k, где*

$$a_{n+k} = b_1 a_{n+k-1} + \ldots + b_k a_n. \tag{1}$$

Тогда её общий член a_n имеет вид

$$a_n = \sum_i \lambda_i^n P_i(n), \tag{2}$$

где λ_i — корень характеристического уравнения

$$x^k = b_1 x^{k-1} + \ldots + b_k$$

некоторой кратности k_i, а P_i — многочлен степени не выше $k_i - 1$.

[1] Сколем [9] доказал эту теорему для рациональных чисел, Малер [8] — для алгебраических, Лех [7] — для любого поля характеристики 0.

Доказательство основано на следующих соображениях. Пусть τ — *оператор сдвига*, переводящий последовательность с n-м членом a_n в последовательность с n-м членом a_{n+1}. Тогда наша линейная рекуррента $A = \{a_n\}$ удовлетворяет условию

$$(\tau^k - b_1\tau^{k-1} - \ldots - b_k)A = 0.$$

Оператор $Q = \tau^k - b_1\tau^{k-1} - \ldots - b_k$ можно представить в виде

$$Q = \tau^k - b_1\tau^{k-1} - \ldots - b_k = \prod_{i=1}^{m}(\tau - \lambda_i)^{k_i}.$$

Как известно, аннулятор такого оператора состоит из последовательностей, удовлетворяющих условию (2).

С другой стороны, линейная рекуррента порядка k однозначно задаётся своими первыми k членами, которые можно выбрать произвольным образом. Поэтому пространство последовательностей, удовлетворяющих равенству (1), имеет размерность k. Но пространство последовательностей, удовлетворяющих равенству (2), имеет ту же размерность k, так что эти пространства совпадают. Теорема доказана. □

Упражнение. Пусть $\{a_n\}$ — линейная рекуррента, как в теореме 1. Тогда её *производящая функция* $f(x) = \sum_{n=0}^{\infty} a_n x^n$ имеет вид $f(x) = P(x)/Q(x)$, где $\deg(P) < \deg(Q)$, $Q(x)$ — характеристический многочлен для $\{a_n\}$.

Замечание 1. Аналогичное утверждение (с похожим доказательством) есть в матанализе. Рассмотрим дифференциальное уравнение с постоянными коэффициентами:

$$a_0 y^{(n)} + a_1 y^{(n-1)} + \ldots + a_n y = 0.$$

Тогда его решение имеет вид

$$y = \sum_i e^{\lambda_i x} P_i(x), \tag{3}$$

где λ_i — корень *характеристического уравнения*

$$x^k = b_1 x^{k-1} + \ldots + b_k$$

некоторой кратности k_i, а P_i — многочлен степени не выше $k_i - 1$.

В доказательстве теоремы 1, равно как и её родственника в теории дифференциальных уравнений, применяется идея *линейной суперпозиции*. Например, при исследовании линейных дифференциальных уравнений с ненулевой правой частью используется *функция Грина*.

Поясним её физический смысл. Пусть нам надо исследовать напряжение $T(y)$, $y \in B$, при граничной нагрузке $P(x)$, где $x \in S$ — точка поверхности. Рассматривается случай, когда нагрузка P сосредоточена в одной точке x (т. е. является дельта-функцией), находят напряжение $G(y, x)$, а потом суммируют с весами, пропорциональными значениям функции P, т. е. получают соотношение вида

$$T(y) = \int\limits_x G(y, x)P(x).$$

Замечание 2. Приведём подборку олимпиадных задач, где эта идея также работает.

1. В клетки шахматной доски записаны числа от 1 до 64 (в первой горизонтали слева направо идут числа от 1 до 8, во второй — от 9 до 16, и т. д.). Перед некоторыми числами поставлены плюсы, перед остальными — минусы, так что в каждой вертикали и в каждой горизонтали 4 плюса и 4 минуса. Докажите, что сумма всех чисел равна нулю.
2. По кругу расставлены 128 натуральных чисел. За один ход между всеми соседними числами записывают их сумму, а старые числа стирают. Докажите, что через несколько ходов все числа будут делиться на 128.
3. В вершинах правильного 100-угольника расставлены целые числа. Каждую минуту каждое из чисел заменяется на свою разность с числом, следующим за ним по часовой стрелке. Докажите, что через 5 минут сумма чисел в вершинах любого правильного 20-угольника с вершинами в вершинах нашего 100-угольника будет делиться на 5.
4. Правильный треугольник разбит прямыми, параллельными его сторонам, на равные между собой правильные треугольники. Один из маленьких треугольников чёрный, остальные — белые. Разрешается перекрашивать одновременно все треугольники, пересекаемые прямой, параллельной любой стороне исходного треугольника. Всегда ли можно с помощью нескольких таких перекрашиваний добиться того, чтобы все маленькие треугольники стали белыми?
5. В правильном десятиугольнике проведены все диагонали. Возле каждой вершины и каждой точки пересечения диагоналей поставлено число +1 (рассматриваются только сами диагонали, а не их продолжения). Разрешается одновременно изменить все знаки на одной стороне или одной диагонали. Можно ли с помощью нескольких таких операций изменить все знаки на противоположные?

6. Стороны правильного треугольника разделены на n частей. Через получившиеся точки проведены прямые, параллельные сторонам. Внутри получившихся треугольников записаны ± 1 так, что каждое число внутри исходного треугольника равно произведению соседей (по сторонам маленького треугольника). Покажите, что в треугольниках при вершинах записаны одинаковые числа.
7. а) Рассмотрим множество непрерывных функций на отрезке $[0, 2n]$, таких, что $F(0) = 0$ и на любом интервале $(k, k+1)$, где k целое, производная равна либо $+1$, либо -1. Каких функций больше: неотрицательных или таких, что $F(2n) = 0$?
   б) Как подсчитать число таких функций, что $-n/3 < F(x) < n/3$? (См. задачи 11.7, вып. 11, с. 163, и 11.7′, вып. 26, с. 269, а также их решения, вып. 27, с. 251–254).
8. Бесконечная в обе стороны полоса клетчатой бумаги состоит из чёрных и белых клеток. Каждую секунду клетка, имеющая чётное число чёрных соседей, становится белой, а имеющая нечётное число чёрных соседей — чёрной. Докажите, что:
   а) если через 2^n секунд исходная раскраска повторится, то она периодична с периодом $3 \cdot 2^n$;
   б) исходная раскраска периодически повторяется тогда и только тогда, когда она сама периодична (т. е. периодичность во времени равносильна периодичности в пространстве).
   в) Что можно сказать о полосе произвольной ширины? Или о всей клетчатой плоскости?
9. В каждой вершине пятиугольника записано некоторое число, меньшее 1000, причём сумма всех этих чисел равна 0. Каждое число заменяется полусуммой соседних чисел, и эта операция проводится 1000 раз. Докажите, что после этого каждое из чисел будет меньше 1.
10. На плоскости дано 239 прямых общего положения. Докажите, что в областях, на которые эти прямые разбивают плоскость, можно расставить ненулевые целые числа так, чтобы для каждой из прямых было выполнено следующее условие: сумма чисел в каждой из полуплоскостей, определяемых этой прямой, равна нулю.
11. Правильный $4k$-угольник разрезан на параллелограммы. Докажите, что среди них не менее k прямоугольников. Найдите их общую площадь, если сторона $4k$-угольника равна a.

II. Приведём теперь несколько полезных фактов про линейные рекурренты.

Предложение 2. *Пусть линейная рекуррента удовлетворяет системе линейных рекуррентных соотношений порядков k_i:*

$$b_0^{(i)} a_n + b_1^{(i)} a_{n-1} + \ldots + b_{k_i}^{(i)} a_{n-k_i} = 0, \quad i = 1, \ldots, s.$$

Тогда все эти соотношения следуют из одного:

$$c_0 a_n + b_1 a_{n-1} + \ldots + c_k a_{n-k} = 0.$$

Если коэффициенты исходной системы рациональны, то и коэффициенты c_i тоже рациональны.

Доказательство. Рассмотрим характеристические многочлены

$$P_i(x) = b_0^{(i)} x^{k_i} + b_1^{(i)} x^{k_i - 1} + \ldots + b_{k_i}^{(i)} = 0, \quad i = 1, \ldots, s.$$

Заметим следующее.

1. Если линейная рекуррента удовлетворяет характеристическому уравнению с многочленом P, то для любого многочлена Q она удовлетворяет характеристическому уравнению с многочленом PQ.
2. Если линейная рекуррента удовлетворяет характеристическим уравнениям с многочленами P_1, P_2, то для любых коэффициентов λ_1, λ_2 она удовлетворяет характеристическому уравнению с многочленом $\lambda_1 P_1 + \lambda_2 P_2$.
3. И, следовательно, если линейная рекуррента удовлетворяет характеристическим уравнениям с многочленами P_1, P_2, то для любых многочленов Q_1, Q_2 она удовлетворяет характеристическому уравнению с многочленом $Q_1 P_1 + Q_2 P_2$.

Действительно, соотношения можно естественным образом умножать на константы и складывать. Соответствующие операции производятся и с характеристическими многочленами. Кроме того, соотношение можно *сдвигать*, т. е. переходить от соотношения

$$d_0 a_n + d_1 a_{n-1} + \ldots + d_m a_{n-m} = 0$$

к его следствию

$$d_0 a_{n+1} + d_1 a_{n-1} + \ldots + d_m a_{n-m+1} = 0.$$

Этому переходу отвечает умножение характеристического многочлена на переменную x. Осуществляя сдвиги последовательно, мы можем умножать характеристический полином и на x^k.

Остаётся отметить, что (как и у целых чисел) наибольший общий делитель D системы многочленов P_i от одного переменного есть их линейная комбинация $D = \sum_i Q_i P_i$ для некоторых многочленов Q_i. Предложение доказано. □

Предложение 3. *Если все члены линейной рекурренты рациональны, то и все коэффициенты d_i задающего её соотношения*

$$d_0 a_n + d_1 a_{n-1} + \ldots + d_m a_{n-m} = 0$$

тоже рациональны.

Первое доказательство. В силу предыдущего предложения достаточно рассмотреть соотношение минимальной степени. Условие, что *фиксированная последовательность* $\{a_n\}$ удовлетворяет соотношению

$$d_0 a_n + d_1 a_{n-1} + \ldots + d_m a_{n-m} = 0,$$

можно записать как (бесконечную) систему линейных уравнений с коэффициентами из множества $\{a_n\}$ (где d_i — неизвестные, a_i — коэффициенты). Предложение вытекает из следующей леммы:

Лемма 4. (*а*) *Любая система линейных уравнений от конечного числа переменных равносильна своей конечной подсистеме.*

(*б*) *Пусть дана* (*вообще говоря бесконечная*) *система линейных уравнений с рациональными коэффициентами. Если она имеет ненулевое решение, то она имеет и ненулевое рациональное решение.*

Доказательство. (а) Рассмотрим первое уравнение, выразим одну из неизвестных через другие и подставим в остальные уравнения. Те уравнения, в которых все коэффициенты окажутся нулевыми, вычеркнем. Далее берём любое из оставшихся уравнений и опять выразим какую-либо неизвестную через другие, и т. д. Поскольку число неизвестных конечно, процесс остановится на некотором шаге. Система равносильна совокупности тех уравнений, которые мы использовали для выражения неизвестных.

Замечание. То же верно и для системы полиномиальных уравнений. *Теорема Гильберта о базисе* утверждает, что любая система полиномиальных уравнений произвольной степени от ограниченного числа переменных равносильна конечной подсистеме. См. решение задачи 4.12 (выпуск 18, с. 265), а также задачу 11.12 (выпуск 11, с. 164).

(б) В силу п. (а) достаточно рассмотреть систему из конечного числа уравнений. Как и при решении п. (а), последовательно исключаем переменные. При этом рациональность коэффициентов сохраняется. В конце концов мы избавимся от всех уравнений, но так как по условию система имеет ненулевое решение, при этом останутся *свободные параметры*, т. е. неизвестные, через которые остальные выражаются как линейные функции с рациональными коэффициентами. Остаётся

придать этим свободным параметрам ненулевые рациональные значения. Лемма доказана, а вместе с ней и предложение 3. □

□

Упражнение. В стаде 101 корова. Любые 100 из них можно разделить на два стада по 50 коров так, что общие веса стад будут равны. Докажите, что веса всех коров равны.

Упражнение. Решите задачу сперва для целых, потом для рациональных, потом для вещественных весов.

Второе доказательство. Выберем базис $\{e_i\}$ в векторном пространстве V над $\mathbb{Q}$, порождённом коэффициентами d_i нашей линейной рекурренты

$$d_0a_n + d_1a_{n-1} + \ldots + d_ma_{n-m} = 0.$$

Раскладывая выражение $d_0a_n + d_1a_{n-1} + \ldots + d_ma_{n-m}$ по базису $\{e_i\}$, мы получаем набор коэффициентов при базисных векторах e_i. Поскольку все a_i рациональны, а векторы линейно независимы над $\mathbb{Q}$, сумма коэффициентов при каждом таком e_i должна равняться нулю, т. е.

$$d_0^{(i)}a_n + d_1^{(i)}a_{n-1} + \ldots + d_m^{(i)}a_{n-m} = 0, \tag{4}$$

где $d_j^{(i)}$ есть i-я координата числа d_j, рассматриваемого как вектор из V. Таким образом, рекуррентное соотношение

$$d_0a_n + d_1a_{n-1} + \ldots + d_ma_{n-m} = 0$$

равносильно системе линейных рекуррентных соотношений (4). А эта система в свою очередь, в силу предложения 2, равносильна одному линейному соотношению с рациональными коэффициентами. Предложение доказано. □

Лемма 5. *Рассмотрим линейную рекурренту, заданную соотношением*

$$d_0a_n + d_1a_{n-1} + \ldots + d_ma_{n-m} = 0 \tag{5}$$

минимальной степени. С каждым n свяжем вектор $f_n = (a_n, \ldots, a_{n-m+1})$. Пусть имеет место равенство

$$\sum_i \lambda_i f_i = 0. \tag{6}$$

Тогда при любом k справедливо равенство

$$\sum_i \lambda_i f_{i+k} = 0. \tag{7}$$

Доказательство. Поскольку равенство (5) устойчиво относительно сдвигов (справедливо для всех n), из него следует и соотношение

$$d_0 f_n + d_1 f_{n-1} + \ldots + d_m f_{n-m} = 0. \tag{8}$$

Преобразуя выражение (6) с помощью соотношения (8), мы получим соотношение, в котором индексы i при всех f_i меньше m. А тогда, в силу минимальности m и, как следствие, линейной независимости f_i, $i = 1, \ldots, m-1$, все они окажутся нулями. Поскольку процесс преобразования остаётся тем же при сдвиге нумерации, аналогичное преобразование выражения (7) также приведёт к нулевому результату, что и доказывает лемму 5. □

Существует несколько другое доказательство леммы 5, основанное на том, что все соотношения между f_i следуют из соотношения (5), а подстановка $f_i \to f_{i+1}$, отвечающая сдвигу, сохраняет эти соотношения.

Нам потребуется ещё одна

Лемма 6. *В любой системе целочисленных m-мерных векторов $\{f_i\}$ можно указать конечную подсистему $\{f_j\}$ такую, что каждый вектор f_i будет целочисленной линейной комбинацией векторов из $\{f_j\}$.*

Доказательство. Проведём индукцию по m. Пусть $m = 1$, т. е. векторы — это целые числа. Пусть d — их НОД. Тогда в системе существует такая конечная совокупность элементов, что d является их целочисленной линейной комбинацией. Но тогда и любой элемент системы представляется в виде целочисленной линейной комбинации этих элементов.

Пусть $m > 1$ и для меньших размерностей лемма верна. Пусть НОД первых координат векторов системы равен d'. Найдётся конечная подсистема векторов, через первые координаты которых d' выражается в виде целочисленной линейной комбинации. Вычитая из каждого вектора исходной системы эту комбинацию, умноженную на подходящий коэффициент, получим систему, в которой первая координата каждого вектора равна нулю. По предположению индукции векторы этой системы выражаются через их конечную подсистему. А эта подсистема выражается через конечную совокупность векторов исходной системы, что и требовалось.

Лемма доказана. □

Замечания. (а) Верен аналог леммы при замене чисел на многочлены. При этом вместо целочисленной комбинации многочленов $P_i(x)$ следует рассматривать полиномиальную комбинацию $\sum P_i(x) Q_i(x)$.

(б) Для линейных комбинаций с неотрицательными коэффициентами аналогичное утверждение для одномерного случая имеет место (упражнение), а для многомерного — нет (тоже упражнение).

Предложение 7. *Если все члены линейной рекурренты целые, то в некотором задающем её минимальном соотношении*

$$d_0 a_n + d_1 a_{n-1} + \ldots + d_m a_{n-m} = 0$$

все коэффициенты d_i тоже целые и при этом $d_0 = 1$.

Доказательство. Коэффициенты d_i можно считать взаимно простыми в совокупности. Рассмотрим систему векторов $\{f_i\}$ (см. лемму 5). Применив лемму 6, найдём конечную подсистему $\{f_j\}$, $j < M$, через которую выражаются все f_i, в том числе f_M. Итак, имеет место равенство

$$f_M = \sum_{i=1}^{M-1} \lambda_j f_j.$$

Ввиду леммы 5 получаем при всех k:

$$f_{M+k} = \sum_{i=1+k}^{M-1+k} \lambda_j f_j.$$

Это означает, что наша линейная рекуррента обладает соотношением нужного типа:

$$a_{n+M} = \sum_{i=1}^{M} a_{n+M-i} c_i. \tag{9}$$

При этом характеристический многочлен для минимального соотношения

$$d_0 a_n + d_1 a_{n-1} + \ldots + d_m a_{n-m} = 0$$

делит характеристический многочлен для соотношения (9). Поскольку старший коэффициент последнего равен единице, а старший член произведения есть произведение старших членов, коэффициент d_0 тоже равен единице. Предложение 7 доказано. □

Рассмотрим линейную рекурренту

$$d_0 a_n + d_1 a_{n-1} + \ldots + d_m a_{n-m} = 0.$$

Пусть $a_k^{(\lambda)} = \lambda^k a_k$. Тогда

$$d_0 a_n^{(\lambda)} + \lambda \cdot d_1 a_{n-1}^{(\lambda)} + \ldots + \lambda^m \cdot d_m a_{n-m}^{(\lambda)} = 0,$$

так что характеристические многочлены для последовательностей $\{a_n\}$ и $\{a_n^{(\lambda)}\}$ будут равны соответственно

$$P(x) = d_0x^n + d_1x^{n-1} + \ldots + \cdot d_m$$

и

$$P_\lambda(x) = d_0x^n + \lambda \cdot d_1x^{n-1} + \ldots + \lambda^m \cdot d_m$$

и корни многочлена P_λ получаются из корней многочлена P умножением на λ.

Из наших рассмотрений следует

Предложение 8. *Дана целочисленная линейная рекуррента*

$$A\colon\ a_n + d_1a_{n-1} + \ldots + d_ma_{n-m} = 0.$$

Пусть p — простое число. Тогда при некотором рациональном μ линейная рекуррента $A^\mu\colon a_n^\mu = p^{n\mu}a_n$ задаётся соотношением

$$A^\mu\colon\ a_n^\mu + d_1^\mu a_{n-1} + \ldots + d_m^\mu a_{n-m} = 0,$$

где ${d_k}^\mu = d_k\mu^k$. При этом можно подобрать такое μ, для которого:

- *хотя бы один коэффициент d_i^μ является целым числом, не делящимся на p;*
- *все нецелые коэффициенты d_i^μ представимы в виде произведения целого числа на p в положительной рациональной степени.* □

III. Под *прополкой с шагом m* последовательности $\{a_n\}$ будем понимать последовательность $\{w_{m,k} = a_{m\cdot k+q_0}\}$, где k пробегает целые числа, а q_0 фиксированное целое. Прополка также является линейной рекуррентой, и при переходе к прополке собственные числа характеристического уравнения возведутся в m-ю степень, а кратность их не уменьшится, ибо

$$w_{m,k} = \sum_i P_i(m\cdot k + q_0)\lambda_i^{q_0}(\lambda_i^m)^k = \sum_i Q_i(k)\delta_i^k,$$

где

$$\delta_i = \lambda_i^m, \quad Q_i(x) = \lambda_i^{q_0}P_i(m\cdot x + q_0), \quad \deg(Q_i) = \deg(P_i).$$

При подходящем m (равном количеству ненулевых элементов факторкольца по модулю p) они будут сравнимы с 1 по модулю p.

При этом возможно уменьшение степени Q_i после сокращения членов, но это не может происходить при всех q_0, ибо полный набор всех таких прополок с фиксированным шагом m однозначно определяет исходную линейную рекурренту.

Будем считать, что выполнено следующее.

1. Числа λ_i не являются корнями из единицы, кроме случая $\lambda_i = 1$.
2. Отношение λ_i/λ_j не есть корень из единицы при всех $i \neq j$.
3. Любая прополка является линейной рекуррентой порядка строго больше 1.

Предложение 9. (*а*) *Пусть p — простое число, $A = \{a_n\}$ — целочисленная линейная рекуррента, хотя бы два коэффициента которой не делятся на p и при этом один из её членов не делится на p. Тогда в ней найдётся прополка, все члены которой не делятся на p.*

(*б*) *Пусть p — простое число, $A = \{a_n\}$ — линейная рекуррента, члены и коэффициенты которой принадлежат $\mathbb{Z}[p^{1/n}]$, хотя бы два коэффициента не делятся на p и при этом один из её членов не делится на $p^{1/n}$. Тогда в ней найдётся прополка, все члены которой не делятся на $p^{1/n}$.*

Доказательство. Утверждение сводится к следующему очевидному факту: дана линейная рекуррента над $\mathbb{Z}_p$ хотя бы с двумя ненулевыми коэффициентами и хотя бы одним ненулевым членом. Тогда члены в ней повторяются периодически и найдётся прополка, состоящая из ненулевых членов. □

Из вышеприведённого следует

Предложение 10. *Дана ненулевая линейная рекуррента с соотношением*

$$A\colon\ a_n + d_1 a_{n-1} + \ldots + d_m a_{n-m} = 0.$$

Тогда для любого простого p найдётся её прополка вида $W\colon w_{k,n} = a_{k\cdot n+r}$ и целочисленная линейная рекуррента $C = \{c_n\}$, все члены которой взаимно просты с p, причём

$$w_{k,n} = D \cdot p^{q\cdot n} c_n, \quad D \in \mathbb{Z},\ q \geqslant 0,\ q \in \mathbb{Z}^+.$$

Если при этом все характеристические корни A не равны собственному корню из единицы, их отношения не являются корнями из единицы и их хотя бы два, то тем же свойством обладает и линейная рекуррента $\{b_n\}$.

IV. Вернёмся к задаче 12.12. Проведём подготовительную работу.

1. Среди коэффициентов a_i выберем *базис трансцендентности*, т. е. максимальное множество M алгебраически независимых в совокупности элементов. Любой другой коэффициент a_j выражается как корень некоторого неприводимого многочлена P_j с коэффициентами из $\mathbb{Q}[M]$. Выберем простое число p, достаточно большое в следующем смысле:

можно выбрать M так, что каждый многочлен P_j взаимно прост со своей производной и все его ненулевые коэффициенты остаются ненулевыми по модулю p.

Некоторые способы выбора базиса неэквивалентны, ибо есть соотношения на a_j, выполняющиеся при одном выборе базиса и не выполняющиеся при другом. Мы берём такое большое p, чтобы все эти неэквивалентности сохранить.

Замечание. Для читателя, знакомого с нестандартным анализом, достаточно сказать: выберем бесконечно большое простое число p и значения a_k, которые не имеют алгебраических зависимостей конечной степени с рациональными коэффициентами. Рекомендуем читателю книгу [5].

Рассмотрим теперь расширение $\mathbb{F}_q$, $q = p^\ell$, поля вычетов $\mathbb{Z}_p$, содержащее все выбранные коэффициенты. Построим расширение кольца *целых p-адических чисел*, связанное с $\mathbb{F}_q$. Известно, что поле $\mathbb{F}_q$ порождается одним элементом x степени ℓ над $\mathbb{Z}_p$. Это значит, что для некоторого неприводимого многочлена Q с коэффициентами из $\mathbb{Z}_p$ выполняется равенство $Q(x) = 0$. При этом Q — многочлен со старшим коэффициентом единица, не имеющий общих делителей со своей производной (можно считать $p > \ell$, поэтому $Q'(x) \neq 0$).

Коэффициенты многочлена Q равны остаткам от деления на p коэффициентов некоторого целочисленного многочлена $\widehat{Q}$ со старшим коэффициентом 1. Рассмотрим расширение кольца p-адических чисел элементом $\widehat{x}$ таким, что $\widehat{Q}(\widehat{x}) = 0$. Далее рассмотрим формальные степенные ряды

$$\sum_{i=0}^{\deg(Q)-1} \sum_{j=0}^{\infty} c_{ij} x^i p^j$$

с целыми c_{ij}. На них естественным образом определяются операции *сложения* и *умножения*, создающие структуру кольца R. Его редукция по модулю p есть $\mathbb{F}_q$. Это кольцо R по своим свойствам очень похоже на кольцо целых p-адических чисел, т. е. кольцо рядов $\sum_{k=0}^{\infty} c_k p^k$ с целыми c_k.

Теперь возьмём в качестве $a_i \in M$ произвольные элементы из R (с остатками $\bar{a}_i$ от деления на p), а в качестве остальных a_j — корни соответствующих многочленов P_j. Покажем, что они лежат в R. Для этого применим метод последовательных приближений.

В обычном вещественном анализе есть *метод Ньютона* построения корней. Пусть f — функция, z — её корень, $f'(z) \neq 0$. Возьмём

точку x, достаточно близкую к z, и из точки $(x, f(x))$ проведём касательную к графику функции f. Её пересечение с осью OX даст точку

$$x_1 = x - \frac{f(x)}{f'(x)},$$

являющуюся следующим приближением к z, и т. д. Пренебрегая изменением производной на маленьком отрезке $[z, x]$, имеем:

$$x_1 = x - \frac{f(x)}{f'(z)}.$$

Если z близко к x, то процесс достаточно быстро сойдётся к корню z функции f.

Аналогичный факт справедлив и для сравнений:

Лемма Гензеля. *Пусть* $Q(x) \equiv 0 \pmod p, Q'(x) \not\equiv 0 \pmod p$. *Тогда для любого* k *найдётся по модулю* p^k *единственное* y_k *такое, что* $Q(y_k) \equiv 0 \pmod{p^k}$.

Тем самым существует единственное решение уравнения $Q(y) = 0$ *в* p*-адических числах такое, что* $y \equiv x \pmod p$.

Предоставляем читателю доказать лемму Гензеля и её очевидное обобщение для кольца R.

Мы добились того, что все коэффициенты линейной рекурренты принадлежат кольцу R, причём $\bar{a}_0 \neq 0$, так что $a_0^{-1} \in R$. Поделив на a_0, можно считать, что $a_0 = 1$.

Переходя от последовательности к её прополкам, можно считать, что *все коэффициенты линейной рекурренты лежат в кольце* R, *а все корни характеристического уравнения сравнимы с единицей по модулю* p.

V. *О* p*-адической экспоненте и степенных рядах.* Следующее утверждение родственно лемме Гензеля.

Теорема 11. *Пусть* p — *простое число,* $a \equiv 1 \pmod{p^k}$, *но* $a \not\equiv 1 \pmod{p^{k+1}}$. *Тогда* $a^p \equiv 1 \pmod{p^k}$, *но при этом* $a^p \not\equiv 1 \pmod{p^{k+2}}$, *кроме случая* $p = 2$, $k = 1$.

Пример. Пусть $p = 2$, $a = 9$, $k = 3$. Тогда $a^p = a^2 = 81 \equiv 1 \pmod 8$, но $a^2 \not\equiv 1 \pmod{32}$.

Данное утверждение активно используется в олимпиадной практике. См. задачу 3.10 («Математическое просвещение», сер. 3, вып. 3, с. 233, авторы А. Ерошин и А. Белов; решение см. [3]). Приведём несколько полезных упражнений.

1. При каких n величина $2^n - 1$ делится на 5^{100}?
2. При каких n величина $5^n - 1$ делится на 2^{100}?

3. Пусть $p > 2$, n натуральное. Докажите, что среди остатков по модулю p^n, взаимно простых с p, есть *первообразный корень по модулю* p^n, т. е. такой, что остальные являются его степенями.
4. Пусть $n > 2$. Докажите, что среди остатков по модулю 2^n нет первообразного корня.
5. Укажите такое n, что в десятичном разложении числа 5^n имеется 1000 нулей, идущих подряд. Аналогичные вопросы про девятки и про степени двойки.

Над кольцом p-адических чисел можно рассматривать степенные ряды и элементарные функции. *Близость* означает, что разность делится на высокую степень p, понятие *сходимости* определяется естественным образом. В этой топологии множество p-адических чисел компактно. *Экспонента*, *синус*, *косинус* и т. п. определяются через степенные ряды

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}, \quad \sin x = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{n!}, \quad \cos x = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{n!}.$$

Эти ряды сходятся при x, делящемся на p, если $p > 2$ (при $p = 2$ надо потребовать, чтобы x делился на $4 = p^2$) и удовлетворяют тем же функциональным соотношениям, что в вещественном случае. Например, докажем, что $e^{x+y} = e^x e^y$. Распишем e^{x+y}, e^x, e^y в виде рядов и раскроем скобки. Если коэффициенты в разности $e^{x+y} - e^x e^y$ сократятся, то функциональное соотношение установлено. Если нет, то они не сократятся и для привычных нам вещественных экспонент. Но тогда равенство $e^{x+y} = e^x e^y$ не имеет места и в нашем вещественном мире, что неверно. Аналогично устанавливаются теоремы сложения для синуса и косинуса.

VI. Решение задачи 12.12. Мы закончили подготовительную работу. Как отмечено в конце п. IV, линейная рекуррента состоит из прополок, каждая из которых имеет корни характеристического уравнения, сравнимые с единицей по модулю p, а общий вид её члена согласно теореме 1 представляет собой сумму произведений полинома на экспоненту, т. е. является аналитической функцией. Если у неё конечное число нулей, то задача решена.

Если же число нулей бесконечно, то у них есть предельная точка Z, являющаяся целым p-адическим числом. Теперь заметим, что если x делится на p, то ряд для бинома Ньютона $(1 + x)^z$ сходится при всех p-адических z и определяет аналитическую функцию. Аналогичное верно в кольце R и его расширениях. Значит, ряд Тейлора

для общего члена прополки в окрестности точки Z сходится при всех целых p-адических n, причём к нулю, поскольку Z — предельная точка нулей. Но тогда коэффициенты ряда нулевые, что означает, что его сумма — тождественный нуль.

Мы разбили линейную рекурренту на конечное число прополок, в каждой из которых либо конечное множество нулей, либо все члены нулевые, что и доказывает утверждение задачи.

Замечание 1. Если основное поле конечно или, более общо, состоит из алгебраических элементов, то последовательность нулей линейной рекурренты периодична (возможно, с предпериодом). Если же основное поле имеет положительную характеристику $p>0$ и содержит трансцендентный элемент t, то утверждение задачи перестаёт быть верным.

Пусть, например, $a_n=(t+1)^n-t^n-1$. Тогда $a_n=0 \Leftrightarrow n=p^k$, $k\in\mathbb{N}$. В этом случае множество нулей устроено следующим образом. Рассмотрим такие n, что $a_n=0$. Разложив n в p-ичной системе счисления, рассмотрим множество таких n как множество слов над алфавитом $A=\{0,1,\ldots,p-1\}$. Это *регулярный язык*. Иными словами, имеется конечный граф с начальной O и финальной T вершинами, рёбра которого помечены буквами из A, причём каждому пути из O в T отвечает p-ичная запись числа n, для которого $a_n=0$. В этом случае существует алгоритм, распознающий принадлежность произвольного натурального n множеству нулей. См. [6].

Замечание 2. Линейную рекурренту можно рассматривать как экспоненциально-полиномиальную функцию от одной переменной. Для большего числа переменных, как показала Джулия Робинсон, проблема наличия нуля алгоритмически неразрешима. С другой стороны, если основания экспонент лежат в поле характеристики $p>0$, то ситуация меняется. Пусть F — экспоненциально-полиномиальная функция от k переменных. С набором $(n_1,\ldots,n_k)$ свяжем слово над алфавитом A^k из p^k символов, состоящее из последних цифр чисел $n_1,\ldots,n_k$, предпоследних и т. д. Множеству наборов $(n_1,\ldots,n_k)$ таких, что $F(n_1,\ldots,n_k)=0$, отвечает регулярный язык, и искомый алгоритм существует. См. [6].

VII. Задача 20.4 («Математическое просвещение», сер. 3, вып. 28, с. 236). Последовательность $\{a_n\}$ называется *линейной рекуррентой порядка* k, если для некоторых $b_1,\ldots,b_k$ при всех $n\geqslant k$ выполняется равенство $b_0a_n+b_1a_{n-1}+\ldots+b_ka_{n-k}=0$. Пусть $b_0=1$, $a_i,b_i\in\mathbb{Z}$ при всех i. Докажите, что либо последовательность $\{a_n\}$ содержит член,

имеющий не менее 2016 различных простых делителей, либо множество натуральных чисел разбивается на непересекающиеся арифметические прогрессии, на каждой из которых наша рекуррента пропорциональна геометрической прогрессии. (*А. Я. Канель-Белов*)

Решение задачи 20.4. Пусть рекуррента не распадается на последовательности, пропорциональные геометрическим прогрессиям. Применяя процесс, описанный в предложении 10, найдём прополку вида $B\colon b_n = a_{k\cdot n+r}$, где

$$b_n = D \cdot \prod_i p_i^{q_i \cdot n} c_n, \quad q_i \geqslant 0,\ q_i \in \mathbb{Z},$$

$\{p_i\}$ есть набор всех простых делителей коэффициентов рекурренты, числа c_n не делятся на p_i при всех i, n и $D \in \mathbb{Z}$. Пусть s — натуральное число. Существует простое $P > p_i\ \forall\, i$, делящее c_s, а значит, и $a_{k\cdot s+r}$. Поскольку P не делит характеристические коэффициенты a_i, остатки по модулю P периодически повторяются без предпериода, и мы можем взять прополку как в A, так и в C, состоящую из членов, не делящихся на P. Применив предложение 10, построим прополку

$$B_n^1 = P \cdot D_1 \cdot \prod_i p_i^{q_i \cdot n} P^j c_n^1 = a_{k_1 \cdot n + r_1},$$

где c_n^1 не делятся на p_i, а также на P. Продолжая процесс дальше, на s-м шаге получим прополку

$$B_n^s = \prod_{j=1}^{s} P_j \cdot D_s \cdot \prod_i p_i^{q_{i,s} \cdot n} \prod_{j=1}^{s} P_j^{q'_{j,s}} c_n^s = a_{k_s \cdot n + r_s}.$$

Она состоит из членов, имеющих не менее s различных простых делителей. Поскольку s может быть сколь угодно большим, задача решена.

Замечание. Предложение 7 используется в следующей теореме.

Теорема Пизо. *Если $\alpha > 1$ — алгебраическое число, то следующие свойства равносильны.*

- *Дробная часть числа $\{\alpha^n\}$ стремится к константе при $n \to \infty$.*
- *Число α есть число Пизо, т. е. является корнем уравнения $P(x) = 0$ с целыми коэффициентами и со старшим коэффициентом 1, причём $|\alpha| > 1$, а все остальные корни многочлена P по модулю строго меньше единицы.*

Числам Пизо был посвящён проект на 12 Летней конференции Международного математического Турнира городов в 2000 году, см. [10].

Позднее А. А. Егоров по мотивам этого проекта опубликовал две статьи в «Кванте» [1], [2]. Предложение 7 обсуждается в [2].

Про дробные части степеней трансцендентных чисел мало что известно. Не установлено, может ли предел дробной части степеней вообще существовать (кроме тривиального случая $|\alpha| < 1$). Известно только, что множество чисел, превосходящих единицу, дробная часть которых имеет предел, не более чем счётно. (См. задачу 24.9, вып. 24, с. 176; решение, вып. 27, с. 260–262.)

Список литературы

[1] *Егоров А.* Числа Пизо // Квант. 2005. № 5. С. 8–13.

[2] *Егоров А.* Числа Пизо (окончание) // Квант. 2005. № 6. С. 9–13.

[3] *Ерошин А. Е.* Периодические десятичные дроби // Математическое просвещение. Сер. 3. Вып. 8. М.: МЦНМО, 2004. С. 239–245.

[4] *Маркушевич А. И.* Возвратные последовательности. М.: Наука, 1983.

[5] *Успенский В. А.* Что такое нестандартный анализ? М.: Наука, 1987.

[6] *Chilikov A. A.*, *Belov A. Ya.* Exponential Diophantine equations in rings of positive characteristic // Journal of knot theory and its ramifications. 2020. Vol. 29, № 2.

[7] *Lech C.* A Note on Recurring Series // Ark. Mat. 1953. Vol. 2. P. 417–421.

[8] *Mahler K.* Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen // Proc. Akad. Wetensch. Amsterdam. 1935. Vol. 38. S. 50–60.

[9] *Skolem Th.* Einige Sätze uber gewisse Reihenentwicklungen und Exponentiale Beziehungen mit Anwendung auf diophantische Gleichungen. Oslo Vid. akad. Skrifter, I(6). 1933.

[10] `https://www.turgor.ru/lktg/2000/index.php`.

Алексей Яковлевич Канель-Белов, университет Бар-Илана (Израиль)
`kanel@mccme.ru`

Задача о треугольнике с заданными длинами биссектрис

Н. Н. Осипов

Излагается история задачи о нахождении треугольника по трём его биссектрисам. Доказывается (разными способами) теорема о том, что для любых трёх положительных чисел существует единственный с точностью до изометрии треугольник, длинами биссектрис которого являются эти числа. Обсуждается вопрос о построении циркулем и линейкой треугольника по заданным его биссектрисам.

Вместо введения

В «Математическом просвещении» (2021, вып. 27, раздел «Задачник») была опубликована следующая задача.

Задача 27.5. а) Для любых ли длин биссектрис существует треугольник с такими биссектрисами и однозначно ли определяется?

б) Можно ли построить треугольник по трём биссектрисам циркулем и линейкой?

Второй пункт этой задачи составители «Задачника» совершенно справедливо отнесли к фольклору, а вот с авторством первого пункта (здесь автор не указан), по-видимому, возникли вопросы. Что, впрочем, неудивительно, так как этот пункт задачи имеет собственную историю. Настоящая заметка, в частности, имеет целью познакомить читателя с некоторыми фактами, связанными с п. (а) задачи 27.5, которые, насколько известно автору, ранее не публиковались на русском языке[1)].

Прежде чем обсуждать саму задачу 27.5, скажем несколько слов о двух аналогичных, но более простых задачах, в которых вместо биссектрис речь идёт о медианах и высотах треугольника соответственно.

Работа поддержана Красноярским математическим центром, финансируемым Минобрнауки РФ (Соглашение 075-02-2022-876).

[1)] Здесь автору очень помогла короткая статья [25], случайно обнаруженная в Интернете. Более подробно история вопроса освещена в статье [19].

Треугольник с заданными длинами медиан m_a, m_b, m_c существует тогда и только тогда, когда тройка чисел (m_a, m_b, m_c) удовлетворяет *неравенствам треугольника*:

$$m_a + m_b > m_c, \quad m_b + m_c > m_a, \quad m_c + m_a > m_b.$$

Что касается треугольника с предписанными длинами высот h_a, h_b, h_c, то он существует, если и только если неравенства треугольника выполнены для тройки чисел $(h_a^{-1}, h_b^{-1}, h_c^{-1})$. В обоих случаях, если искомый треугольник существует, то он единствен с точностью до изометрии. Более того, этот треугольник возможно построить циркулем и линейкой. Автор надеется, что читатель знаком с этими довольно известными фактами, которые вполне можно предлагать как отдельные задачи на занятии математического кружка или даже рассказывать на обычных уроках по элементарной геометрии в школе[2)].

Вопрос о существовании и единственности треугольника с заданными длинами биссектрис является более тонким и, скорее, алгебро-аналитическим, чем геометрическим. Наиболее полное (из доступных автору) описание истории этого вопроса приведено в диссертации Ричарда Бейкера начала XX века [14]. В частности, в разделе «The History of the Problem» Бейкер пишет:

> *The problem of constructing a triangle when the lengths of the bisectors of the angles are given has been an outstanding problem among geometers probably from the time of Pascal and certainly from the time of Euler.*
>
> *Brocard has summed up the literature, dealing almost entirely with special cases, of which the most extensive treatment appears to be the solution of the problem when one angle is a right angle due to Marcus Baker*[3)].

Особенно примечателен последний абзац раздела:

> *The problem must have an extensive domestic history in the schools: P. Barbarin charges that E. Catalan was among those who have proposed*

[2)] Тема построения треугольника по каким-нибудь трём его элементам является, пожалуй, одной из самых популярных тем в школьной геометрии. Внушительная коллекция таких задач на построение есть, например, в книге [9] (см. раздел «Упражнения и дополнительные замечания к главе 1»).

[3)] Задача построения треугольника с заданными длинами биссектрис его углов была широко известна среди геометров, вероятно, со времени Паскаля и, несомненно, со времени Эйлера.

Брокар просуммировал соответствующую литературу, в которой почти всегда рассматривались частные случаи. Среди них наиболее значительным продвижением оказалось решение задачи при наличии прямого угла, принадлежащее Маркусу Бейкеру.

it as an elementary exercise, and from a Russian scholar the writer learns that it has been there extensively used in the schools as a standard setback for ambitious young geometers[4)].

С данным утверждением трудно не согласиться: сам по себе вопрос (особенно после того, как случай с медианами и высотами уже рассмотрен) представляется настолько естественным, что проигнорировать его практически невозможно[5)]. И это только подтверждается публикациями [4, 5, 20] на рубеже XXI века, в которых данный вопрос вновь был поставлен и заново решён, причём разными способами.

Следует отметить, что Бейкер в своей диссертации [14] исследует более серьёзные вопросы (на которых здесь мы не будем останавливаться), связанные с задачей о нахождении треугольника по его биссектрисам, но мимоходом сообщает и ответ на наш вопрос.

А именно, справедлива следующая теорема.

Теорема (Бейкер, 1911). *Для любых трёх положительных чисел l_a, l_b, l_c существует треугольник ABC, длины биссектрис AA_1, BB_1, CC_1 которого суть эти числа: $|AA_1| = l_a$, $|BB_1| = l_b$, $|CC_1| = l_c$. Более того, треугольник ABC определён однозначно с точностью до изометрии.*

Доказательство этого утверждения, которое Бейкер даже не формулирует в виде отдельной теоремы, приводится в разделе «Reality of the Roots for Real Angle-Bisectors» части I диссертации (см. [14, с. 13]). Возможно, данное Бейкером доказательство не столь подробно и понятно по сравнению с более поздними элементарными доказательствами из статей [4, 5], но оно содержит главный ингредиент — явно выписанную функцию

$$F(t) = \frac{1-2t}{t(1-t)^2},$$

с помощью которой оказалось удобно выражать связь между длинами биссектрис и длинами сторон искомого треугольника.

В разделе 1 мы для сравнения приведём существенно другое доказательство теоремы Бейкера (следуя статье [20]), основанное на клас-

---

4) Очевидно, задача имеет обширную историю использования в школах: П. Барбарен утверждает, что Э. Каталан был среди тех, кто предлагал её как элементарное упражнение, а из российского источника автор знает, что там эта задача широко использовалась в школах как стандартное испытание для честолюбивых молодых геометров.

5) Во всяком случае, автор в свои аспирантские годы, параллельно занимаясь со школьниками разной олимпиадной математикой, с удовольствием для себя решил эту задачу (см. далее раздел 2) и был уверен, что это какой-то пусть малоизвестный, но всё же фольклор.

сической *теореме Брауэра о неподвижной точке* (см., например, [26], а также [13, § 1.1] и [1, гл. 3, § 4]), а в разделе 2 представим авторское элементарное доказательство, которое по сути есть переоткрытое доказательство самого Бейкера. Оба доказательства так или иначе используют известные формулы, связывающие длины биссектрис l_a, l_b, l_c с длинами сторон $a = |BC|$, $b = |CA|$, $c = |AB|$ треугольника:

$$l_c^2 = ab\left(1 - \frac{c^2}{(a+b)^2}\right) \tag{0.1}$$

и аналогично для l_a^2 и l_b^2 (см., например, [11, задача 12.37]).

В частности, имеем

$$l_c^2 - l_b^2 = \frac{a(b-c)(a+b+c)(a^3 + (b+c)a^2 + 3bca + b^2c + bc^2)}{(a+b)^2(a+c)^2},$$

откуда следует равносильность неравенств $b > c$ и $l_b < l_c$ (против большей стороны лежит меньшая биссектриса). Ясно также, что $l_b = l_c$ тогда и только тогда, когда $b = c$ (*теорема Штейнера — Лемуса*).

В § 3 мы обратимся к п. б) задачи 27.5 и покажем, что, вообще говоря, нельзя построить циркулем и линейкой треугольник по заданным его биссектрисам. Поскольку этот факт, скорее всего, читателю хорошо известен (ибо в Интернете имеется довольно много публикаций на эту тему, например [23, 25]), мы приведём пару близких, но менее известных утверждений. Отметим, что ещё одна близкая задача — о построении циркулем и линейкой треугольника по заданным основаниям его биссектрис — была решена относительно недавно (см. статьи [12, 22]). Ответ прежний: вообще говоря, такое построение невозможно. Для доказательства подобных утверждений удобно привлекать системы компьютерной алгебры (например, Maple [27]), поскольку тогда появляется возможность рассуждать прямолинейно за счёт манипулирования довольно громоздкими выражениями (типичный пример: упражнение 3 в конце статьи).

Задача о нахождении треугольника по биссектрисам номинально относится к геометрии, поэтому имеет смысл упомянуть статью [21], в которой чисто геометрическими средствами[6)] доказывается единственность (с точностью до изометрии) треугольника, имеющего заданные биссектрисы.

[6)] Цитата из [21]: «…the proof does not use trigonometry, analysis and the formulas for triangle angle bisector length, but only synthetic reasoning» («…доказательство не использует тригонометрию, анализ и формулы для длин биссектрис углов треугольника, но лишь синтетические рассуждения»).

§ 1. Доказательство с помощью теоремы Брауэра о неподвижной точке

Введём обозначения

$$x = \frac{b+c-a}{2}, \quad y = \frac{a+c-b}{2}, \quad z = \frac{a+b-c}{2}$$

и перепишем формулу (0.1) в следующем эквивалентном виде:

$$z = \frac{\sqrt{l_c^2+x^2}-x}{2} + \frac{\sqrt{l_c^2+y^2}-y}{2}. \tag{1.1}$$

Покажем, например, как из формулы (0.1) следует формула (1.1). Имеем

$$\sqrt{l_c^2+x^2} = \frac{(a+b)^2-c(a-b)}{2(a+b)}, \quad \sqrt{l_c^2+y^2} = \frac{(a+b)^2-c(b-a)}{2(a+b)},$$

так что

$$\frac{\sqrt{l_c^2+x^2}-x}{2} + \frac{\sqrt{l_c^2+y^2}-y}{2} = \frac{a+b-c}{2} = z.$$

Для доказательства теоремы Бейкера достаточно доказать следующее утверждение: система уравнений

$$\begin{cases} x = \dfrac{\sqrt{l_a^2+y^2}-y}{2} + \dfrac{\sqrt{l_a^2+z^2}-z}{2}, \\ y = \dfrac{\sqrt{l_b^2+z^2}-z}{2} + \dfrac{\sqrt{l_b^2+x^2}-x}{2}, \\ z = \dfrac{\sqrt{l_c^2+x^2}-x}{2} + \dfrac{\sqrt{l_c^2+y^2}-y}{2} \end{cases} \tag{1.2}$$

имеет единственное решение (x, y, z) в положительных числах. Действительно, тогда длины сторон искомого треугольника могут быть найдены по формулам

$$a = y+z, \quad b = z+x, \quad c = x+y.$$

Рассмотрим отображение Φ, заданное формулой

$$\Phi(x,y,z) = \big(\varphi(l_a,y)+\varphi(l_a,z), \varphi(l_b,z)+\varphi(l_b,x), \varphi(l_c,x)+\varphi(l_c,y)\big),$$

где $\varphi(u,v) = (\sqrt{u^2+v^2}-v)/2$. Утверждение об однозначной разрешимости системы уравнений (1.2) в положительных числах x, y, z равносильно утверждению о существовании у отображения Φ единственной неподвижной точки (x^*, y^*, z^*) с положительными координатами. Пусть Π — прямоугольный параллелепипед

$$\big\{(x,y,z) \in \mathbb{R}^3 \colon 0 \leqslant x \leqslant l_a,\ 0 \leqslant y \leqslant l_b,\ 0 \leqslant z \leqslant l_c\big\}.$$

Поскольку при любых $u \geqslant 0$ и $v \geqslant 0$ справедливы неравенства

$$0 \leqslant \varphi(u, v) \leqslant \frac{u}{2},$$

образ П при отображении Φ содержится в П: $\Phi(\Pi) \subset \Pi$. Очевидно, отображение Φ непрерывно. Поскольку П — компактное выпуклое множество в $\mathbb{R}^3$, по теореме Брауэра в П существует неподвижная точка отображения Φ. Легко видеть, что координаты этой точки (x^*, y^*, z^*) обязаны быть положительными (если, например, $x = 0$, то $\varphi(l_a, y) = \varphi(l_a, z) = 0$ и, как следствие, $l_a = 0$, что невозможно). Кроме того, неподвижная точка с положительными координатами может быть только одна. Последнее вытекает из неравенства

$$\|\Phi(x, y, z) - \Phi(x', y', z')\| < \|(x, y, z) - (x', y', z')\|, \tag{1.3}$$

где $(x, y, z) \neq (x', y', z')$ — две точки с положительными координатами и

$$\|(u, v, w)\| = |u| + |v| + |w|.$$

Докажем неравенство (1.3). Пусть

$$(X, Y, Z) = \Phi(x, y, z), \quad (X', Y', Z') = \Phi(x', y', z').$$

Оценим $|X - X'|$, $|Y - Y'|$ и $|Z - Z'|$:

$$|X - X'| = |\varphi(l_a, y) + \varphi(l_a, z) - \varphi(l_a, y') - \varphi(l_a, z')| \leqslant$$
$$\leqslant |\varphi(l_a, y) - \varphi(l_a, y')| + |\varphi(l_a, z) - \varphi(l_a, z')| < \frac{|y - y'| + |z - z'|}{2}$$

и аналогично для $|Y - Y'|$ и $|Z - Z'|$. Здесь мы воспользовались неравенством

$$|\varphi(u, v_1) - \varphi(u, v_2)| < \frac{|v_1 - v_2|}{2}, \tag{1.4}$$

справедливым для любых положительных чисел u, v_1 и v_2 с условием $v_1 \neq v_2$.

Неравенство (1.4) следует из *формулы конечных приращений*, применённой к функции $f(v) = \varphi(u, v)$ на отрезке $[v_1, v_2]$. Действительно, имеем

$$|f'(v)| = \left| \frac{\sqrt{u^2 + v^2} - v}{2\sqrt{u^2 + v^2}} \right| < \frac{1}{2},$$

поэтому

$$|f(v_1) - f(v_2)| = |f'(v)| \cdot |v_1 - v_2| < \frac{|v_1 - v_2|}{2}.$$

Также неравенство (1.4) можно доказать, интерпретируя $\varphi(u, v)$ как половину разности между длинами гипотенузы и одного из катетов прямоугольного треугольника.

Складывая теперь оценки для $|X-X'|$, $|Y-Y'|$ и $|Z-Z'|$, получим

$$\|(X,Y,Z)-(X',Y',Z')\| < \|(x,y,z)-(x',y',z')\|,$$

что и требовалось.

Итак, доказано, что система (1.2) имеет единственное решение (x^*, y^*, z^*) в положительных числах. Учитывая неравенство (1.3), для поиска этого единственного решения можно воспользоваться общей идеей — искать его приближение *методом итераций*, т. е. рассматривая последовательность точек $\{P_j = (x_j, y_j, z_j)\}$, заданную рекуррентным правилом

$$P_{j+1} = \Phi(P_j), \quad j = 0, 1, 2, \ldots,$$

при каком-нибудь начальном приближении $P_0 \in \Pi$. Конечно, предварительно потребуется обосновать существование предела такой последовательности $\{P_j\}$. Можно использовать метод сжимающих отображений, см. [6, гл. II, § 4]. Подробное доказательство см. в [19].

§ 2. Элементарное доказательство

Мы будем доказывать прямое утверждение: система уравнений и неравенств

$$\begin{cases} l_a^2 = bc\left(1-\dfrac{a^2}{(b+c)^2}\right), \\ l_b^2 = ca\left(1-\dfrac{b^2}{(c+a)^2}\right), \\ l_c^2 = ab\left(1-\dfrac{c^2}{(a+b)^2}\right), \\ a+b>c, \quad b+c>a, \quad c+a>b \end{cases} \tag{2.1}$$

имеет единственное решение в положительных числах a, b, c.

Введём обозначения

$$P = a+b+c, \quad F(t) = \frac{1-2t}{t(1-t)^2}, \quad \lambda = \frac{l_b^2}{l_a^2}, \quad \mu = \frac{l_c^2}{l_a^2}$$

и перепишем систему (2.1) в следующем равносильном виде:

$$\begin{cases} bc\left(1-\dfrac{a^2}{(b+c)^2}\right) = l_a^2, \\ F\left(\dfrac{b}{P}\right) = \lambda F\left(\dfrac{a}{P}\right), \\ F\left(\dfrac{c}{P}\right) = \mu F\left(\dfrac{a}{P}\right), \\ a+b>c, \quad b+c>a, \quad c+a>b. \end{cases} \tag{2.2}$$

Удобно рассмотреть вспомогательную систему

$$\begin{cases} F(b_1) = \lambda F(a_1), \\ F(c_1) = \mu F(a_1), \\ a_1 + b_1 + c_1 = 1, \\ 0 < a_1, b_1, c_1 < 1/2 \end{cases} \tag{2.3}$$

с новыми неизвестными $a_1 = a/P$, $b_1 = b/P$, $c_1 = c/P$. Покажем, что она имеет единственное решение, которое мы обозначим через (a_1^*, b_1^*, c_1^*). Тем самым искомый треугольник будет найден с точностью до подобия.

Действительно, функция $T = F(t)$ является непрерывной и убывающей при $t \in (0; 1/2)$ (это можно проверить, вычислив производную $F'(t)$). Значит, она имеет обратную функцию $t = G(T)$, которая является непрерывной и убывающей при $T \in (0; \infty)$.

Более того, с помощью *формулы Кардано* (см., например, [2, с. 129]) можно получить следующую явную формулу:

$$G(T) = \frac{R_+(T) + R_-(T) + 4}{6}, \tag{2.4}$$

где

$$R_\pm(T) = \frac{1}{T}\sqrt[3]{-8T^3 - 36T^2 \pm 12T\sqrt{12T^3 - 39T^2 + 96T}}.$$

Формулу (2.4) можно использовать при приближённом решении уравнения (2.5) (см. далее).

Очевидно, система (2.3) равносильна системе

$$\begin{cases} b_1 = G(\lambda F(a_1)), \\ c_1 = G(\mu F(a_1)), \\ a_1 + G(\lambda F(a_1)) + G(\mu F(a_1)) = 1, \\ 0 < a_1 < 1/2 \end{cases}$$

(неравенства $0 < b_1, c_1 < 1/2$ выполнены автоматически, так как $G(T) \in$ $\in (0; 1/2)$ при любом $T > 0$). Поскольку уравнение

$$a_1 + G(\lambda F(a_1)) + G(\mu F(a_1)) = 1$$

имеет единственное решение $a_1 = a_1^*$ в интервале $(0; 1/2)$, система (2.3) также имеет единственное решение. Именно здесь нам потребуется не совсем элементарный, но интуитивно очень простой (по сравнению с теоремой Брауэра о неподвижной точке) факт — *теорема*

о промежуточном значении непрерывной функции. Действительно, функция

$$f(t) = t + G(\lambda F(t)) + G(\mu F(t))$$

непрерывна и возрастает при $t \in (0; 1/2)$, при этом

$$\lim_{t\to 0} f(t) = 0 < 1, \quad \lim_{t\to 1/2} f(t) = \frac{3}{2} > 1.$$

Следовательно, существует единственное значение $t = a_1^*$, при котором значение функции равно 1. Найдя это a_1^*, затем находим $b_1^* = G(\lambda F(a_1^*))$ и $c_1^* = G(\mu F(a_1^*))$.

Теперь осталось заметить, что система (2.2) равносильна системе

$$\begin{cases} bc\left(1 - \dfrac{a^2}{(b+c)^2}\right) = l_a^2, \\ \dfrac{a}{P} = a_1^*, \\ \dfrac{b}{P} = b_1^*, \\ \dfrac{c}{P} = c_1^*, \end{cases}$$

которая имеет единственное решение. В самом деле, подставив $a = Pa_1^*$, $b = Pb_1^*$, $c = Pc_1^*$ в первое уравнение, найдём

$$P = \frac{l_a(1 - a_1^*)}{\sqrt{b_1^* c_1^* (1 - 2a_1^*)}},$$

после чего однозначно определим и сами a, b, c.

В заключение обсудим вопрос о приближённом вычислении a_1^*. Удобно решать не уравнение $f(t) = 1$, а уравнение

$$G(T) + G(\lambda T) + G(\mu T) = 1, \tag{2.5}$$

где $T = F(t)$. Его единственное решение $T^* = F(a_1^*)$ легко локализовать в предположении, что $l_a = \min\{l_a, l_b, l_c\}$. Тогда $\lambda \geqslant 1$ и $\mu \geqslant 1$, так что

$$1 = G(T^*) + G(\lambda T^*) + G(\mu T^*) \leqslant 3G(T^*),$$

т. е. $G(T^*) \geqslant 1/3$. Отсюда $T^* \leqslant F(1/3) = 9/4$, причём независимо от значений λ и μ.

Таким образом, уравнение (2.5) достаточно решить на интервале $(0; 9/4]$. Располагая явной формулой (2.4) для вычисления значений функции G и применяя какой-нибудь приближённый метод (например, банальный метод деления пополам), мы сможем найти T^* и затем $a_1^* = G(T^*)$ с любой наперёд заданной точностью.

§ 3. О невозможности построения циркулем и линейкой

Обратимся теперь к п. б) задачи 27.5: можно ли построить циркулем и линейкой треугольник по трём его биссектрисам?

По-видимому, впервые данный вопрос был поставлен в 1875 году Брокаром [17]. В 1896 году П. Барбарен [16] показал, что в общем случае задача сводится к решению в квадратных радикалах некоторого алгебраического уравнения довольно большой степени[7]. В частном случае — когда две из трёх данных биссектрис имеют равные длины — задачу удаётся свести к решению всего лишь кубического уравнения, что открывает лёгкий путь к доказательству невозможности искомого построения в общем случае.

В русскоязычной литературе обоснование невозможности построения циркулем и линейкой треугольника по трём биссектрисам можно найти, по крайней мере, в двух источниках: в статье Ю. И. Манина [8] из «Энциклопедии элементарной математики» 1963 года, а также в книге М. М. Постникова «Теория Галуа» [10]. Отметим, что уже в начале XX века общий метод доказательства невозможности различных построений с помощью циркуля и линейки был хорошо известен. Этот метод практически целиком базируется на алгебраической теории расширений полей. Более подробно с ним можно познакомиться по цитированным выше книгам (см. также часть 1 главы III книги [7]).

Сформулируем один удобный факт, который часто эксплуатируется при доказательстве невозможности построения чего-либо циркулем и линейкой (в частности, этого факта вполне хватает при анализе на разрешимость классических задач об удвоении куба, трисекции угла, построении правильного 7-угольника и т. д.).

Теорема. *Если кубическое уравнение с рациональными коэффициентами не имеет рациональных корней, то ни один из его корней не может быть построен с помощью циркуля и линейки, исходя из поля рациональных чисел.*

Здесь фразу «исходя из поля рациональных чисел» нужно понимать так: помимо циркуля и линейки, в нашем распоряжении есть также некоторый отрезок единичной длины. Доказательство этой теоремы изложено, например, в § 3 главы III книги [7].

Теперь в случае, когда две из трёх данных биссектрис равны по длине, мы легко сможем обосновать невозможность построения тре-

[7] Этот результат также был анонсирован в [15].

угольника циркулем и линейкой. Далее мы дадим совсем прямолинейное доказательство (по сравнению с известными доказательствами из книг [8, 10]).

Действительно, пусть $l_c = l_b$. Тогда, как уже отмечалось, $c = b$, т. е. треугольник обязан быть равнобедренным. Таким образом, имеем систему

$$\begin{cases} l_a^2 = b^2 - \dfrac{a^2}{4}, \\ l_b^2 = ab\left(1 - \dfrac{b^2}{(a+b)^2}\right) \end{cases}$$

для определения основания a и боковой стороны b. Исключив b, получим

$$\left(16l_a^2 - 4l_b^2\right)a^6 + \left(9l_b^4 + 64l_a^4 - 32l_a^2l_b^2\right)a^4 + \\ + \left(-64l_a^4l_b^2 - 24l_b^4l_a^2\right)a^2 + 16l_a^4l_b^4 = 0. \qquad (3.1)$$

Если $l_b \neq 2l_a$, то корни уравнения (3.1), вообще говоря, не могут быть построены циркулем и линейкой. Вот конкретный пример, когда такое построение невозможно: $l_a = 1$ и $l_b = 3$. В самом деле, для $u = a^2$ получается кубическое уравнение

$$20u^3 - 505u^2 + 2520u - 1296 = 0,$$

которое, как нетрудно проверить, не имеет рациональных корней. (При $l_b = 2l_a$ получим равнобедренный треугольник с углом 36° при основании; построение такого треугольника сводится к построению правильного 5-угольника и потому возможно циркулем и линейкой.)

При произвольных l_a, l_b, l_c такой чисто алгебраический подход, связанный с последовательным исключением неизвестных из системы уравнений (2.1) с помощью *результанта*[8)], приведёт к уравнению 20-й степени (см. по этому поводу [24]). Например, при $l_a = 1$, $l_b = 2$, $l_c = 3$ получим

$$2\,043\,740\,160a^{20} - 87\,748\,669\,440a^{18} + 1\,421\,635\,969\,280a^{16} - \\ - 10\,783\,995\,413\,376a^{14} + 37\,981\,175\,081\,076a^{12} - 42\,210\,536\,672\,727a^{10} - \\ - 83\,380\,498\,450\,560a^8 + 250\,870\,367\,172\,096a^6 - 178\,821\,038\,555\,136a^4 - \\ - 1\,495\,906\,320\,384a^2 + 20\,061\,226\,008\,576 = 0.$$

Отметим, однако, что для нахождения истинного значения $a \approx 3{,}607$ это не очень удобно: полученное уравнение имеет много посторонних положительных корней.

---

8) Об этом методе решения систем алгебраических уравнений см., например, § 3 главы III в учебном пособии [2].

Приведём ещё один пример задачи на построение, которую в общем случае невозможно решить циркулем и линейкой.

Предложение 1. *Равнобедренный треугольник нельзя построить циркулем и линейкой, зная боковую сторону b и биссектрису l, проведённую к боковой стороне.*

Доказательство. Обозначив основание равнобедренного треугольника через a и положив $l = 1$, получим уравнение

$$ba^3 + (2b^2 - 1)a^2 - 2ba - b^2 = 0. \tag{3.2}$$

Нетрудно убедиться, что при некоторых рациональных $b > 0$ кубическое относительно a уравнение (3.2) не имеет рациональных корней. Например, при $b = 1$ уравнение

$$a^3 + a^2 - 2a - 1 = 0 \tag{3.3}$$

имеет иррациональные «тригонометрические» корни

$$2\cos\frac{2\pi}{7}, \quad 2\cos\frac{4\pi}{7}, \quad 2\cos\frac{6\pi}{7}.$$

При этом только $a = 2\cos(2\pi/7)$ соответствует реальному треугольнику[9]. □

Вместе с тем, уравнение (3.2) допускает *рациональную параметризацию*:

$$a = \frac{t^2 - 1}{t}, \quad b = \frac{t^2 - 1}{t^3 - 2t}. \tag{3.4}$$

Как следствие, в случае $l = 1$ для бесконечно многих рациональных $b > 0$ построение циркулем и линейкой искомого равнобедренного треугольника всё-таки возможно. Читателю предлагается доказать, что искомый треугольник будет существовать только при $b > 3/4$, что соответствует требованию $\sqrt{2} < t < 2$.

Может показаться, что построение треугольника циркулем и линейкой в случае, когда среди известных элементов треугольника есть биссектрисы, всегда невозможно, но это не так.

---

[9] Наверное, стоит напомнить, что уравнение (3.3) непосредственно связано с задачей построения правильного 7-угольника. Действительно, для комплексных корней 7-й степени из единицы имеем уравнение

$$z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0,$$

которое заменой $a = z + 1/z$ приводится к виду (3.3). В частности, получим $a = 2\cos(2\pi k/7)$, поскольку $z = e^{2\pi i k/7}$.

Предложение 2. *Равнобедренный треугольник можно построить циркулем и линейкой, зная основание a и биссектрису l, проведённую к боковой стороне.*

Доказательство. Действительно, уравнение для определения неизвестной боковой стороны b имеет вид

$$(2a^2 - l^2)b^2 + (a^3 - 2l^2a)b - l^2a^2 = 0. \tag{3.5}$$

В отличие от уравнения (3.2), уравнение (3.5) является квадратным, а положительные корни квадратных уравнений с известными коэффициентами можно построить циркулем и линейкой. □

В заключение читателю предлагается решить несколько упражнений.

Упражнение 1. Опишите все равнобедренные треугольники, у которых длины всех сторон и всех биссектрис суть целые числа[10)].

План решения. 1. Используя параметризацию (3.4), опишите все тройки (a, b, l) натуральных чисел, удовлетворяющих уравнению (3.5) и неравенству $a < 2b$.

2. Среди найденных троек (a, b, l) выделите те, для которых $h = \sqrt{b^2 - a^2/4}$ есть целое число. □

Упражнение 2. Для любых двух положительных чисел l_a, l_b существует единственный прямоугольный треугольник, у которого длины биссектрис, проведённых к катетам, равны этим числам.

План решения. 0. Пусть a, b — катеты, c — гипотенуза. Нужно доказать, что система

$$\begin{cases} l_a^2 = bc\left(1 - \dfrac{a^2}{(b+c)^2}\right), \\ l_b^2 = ac\left(1 - \dfrac{b^2}{(a+c)^2}\right), \\ a^2 + b^2 = c^2 \end{cases}$$

имеет единственное решение в положительных числах a, b, c.

1. Получите формулы

$$a = \frac{l_b\left(l_b + \sqrt{l_b^2 + 8c^2}\right)}{4c}, \quad b = \frac{l_a\left(l_a + \sqrt{l_a^2 + 8c^2}\right)}{4c}. \tag{3.6}$$

---

10) Это задача, решение которой известно (см., например, [18], где даётся обзор диссертации Р. Бухгольца «On triangles with rational altitudes, angle bisectors or medians», посвящённой подобным вопросам).

2. Подставьте (3.6) в уравнение $a^2/c^2 + b^2/c^2 = 1$ и докажите, что оно имеет единственный положительный корень относительно c. □

Из упражнения 2 следует, что у прямоугольного треугольника длины двух биссектрис могут быть целочисленными. Вместе с тем, из формул

$$l_a l_b = \frac{abc(a+b+c)}{(a+c)(b+c)} \cdot \sqrt{2}, \quad l_c = \frac{ab}{a+b} \cdot \sqrt{2}$$

следует, что у *пифагорова треугольника*[11)] лишь одна из биссектрис, проведённых к катетам, может иметь целую длину, а длина биссектрисы, проведённой к гипотенузе, всегда иррациональна. Как найти пифагоров треугольник с одной целочисленной биссектрисой, было описано ещё у Диофанта в его «Арифметике» (см. [3, задача VI_{16}]).

Упражнение 3. Существует ли прямоугольный треугольник, у которого длины всех биссектрис являются целыми числами?

Ответ. Не существует. □

В связи с упражнением 3 отметим, что длины биссектрис прямоугольного треугольника связаны уравнением

$$\begin{aligned}\left(l_a^2 + l_b^2 - l_a l_b \sqrt{2}\right)\left(l_a^2 + l_b^2 + 2 l_a l_b \sqrt{2}\right)^2 t^3 - \\ - 3 l_a^2 l_b^2 \left(l_a^4 + l_b^4 - l_a^2 l_b^2 - l_a l_b \left(l_a^2 + l_b^2\right)\sqrt{2}\right) t^2 + \\ + 3 l_a^4 l_b^4 \left(l_a^2 + l_b^2 - 2 l_a l_b \sqrt{2}\right) t - l_a^6 l_b^6 = 0,\end{aligned}$$

где $t = l_c^2$. Читателю предлагается убедиться (например, с помощью Maple), что при любых положительных l_a, l_b данное уравнение имеет единственный положительный корень $t < \min\{l_a^2, l_b^2\}$[12)]. В частности, при $l_a = 1$, $l_b = \sqrt{2}$ получим уравнение

$$49t^3 + 18t^2 - 12t - 8 = 0$$

без рациональных корней. Это означает, что прямоугольный треугольник нельзя построить циркулем и линейкой по биссектрисам, проведённым к катетам.

Благодарности

Автор благодарит А. В. Спивака за полезные обсуждения по теме статьи.

[11)] То есть прямоугольного треугольника с целочисленными длинами сторон.

[12)] Тем самым, это уравнение характеризует наборы (l_a, l_b, l_c) возможных длин биссектрис прямоугольного треугольника.

Список литературы

[1] *Александров П. С.*, *Пасынков Б. А.* Введение в теорию размерности. М.: Физматлит, 1973.

[2] *Винберг Э. Б.* Алгебра многочленов. М.: Просвещение, 1980.

[3] *Диофант Александрийский*. Арифметика и книга о многоугольных числах / Редакция и комментарии И. Г. Башмаковой. М.: Наука, 1974.

[4] *Жуков А.*, *Акулич И.* Однозначно ли определяется треугольник? // Квант. 2003. № 1. С. 29–31.

[5] *Жуков А. В.*, *Осипов Н. Н.*, *Спивак А. В.* Длины биссектрис треугольника // Новая школьная энциклопедия. (Небесные тела. Астрономия. Числа и фигуры. Математика.) М.: Мир книги, Росмэн, 2005. С. 484–485.

[6] *Колмогоров А. Н.*, *Фомин С. В.* Элементы теории функций и функционального анализа. М.: Физматлит, 1976.

[7] *Курант Р.*, *Роббинс Г.* Что такое математика? М.: МЦНМО, 2019.

[8] *Манин Ю. И.* О разрешимости задач на построение с помощью циркуля и линейки // Энциклопедия элементарной математики. Книга IV. Геометрия. М.: Физматлит, 1963. С. 205–227.

[9] *Пойа Д.* Математическое открытие. М.: Наука, 1976.

[10] *Постников М. М.* Теория Галуа. М.: Изд-во «Факториал Пресс», 2013.

[11] *Прасолов В. В.* Задачи по планиметрии. М.: МЦНМО, 2019.

[12] *Устинов А. В.* Можно ли построить треугольник по основаниям биссектрис? // Потенциал. Математика. Физика. Информатика. 2013. № 10. С. 41–50.

[13] *Хатчер А.* Алгебраическая топология. М.: МЦНМО, 2011.

[14] *Baker R. P.* The Problem of The Angle-Bisectors. Chicago: University of Chicago Press, 1911.

[15] *Barbarin P.* Résumé d'un mémoire sur la détermination d'un triangle au moyen des longueurs de ses bissectrices // Bulletin de la S. M. F. 1894. Vol. 22. P. 76–80.

[16] *Barbarin P.* Triangles dont les bissectrices ont des longueurs données // Mathesis. 1896. Vol. 16. P. 143–150.

[17] *Brocard H.* Question 58 // Nouvelle Correspondance Math. 1875. Vol. 1. P. 208.

[18] *Buchholz R. H.* On triangles with rational altitudes, angle bisectors or medians // Bull. Austral. Math. Soc. 1992. Vol. 45. P. 525–526.

[19] *Dinca G.*, *Mawhin J.* A constructive fixed point approach to the existence of a triangle with prescribed angle bisector lengths // Bull. Belg. Math. Soc. Simon Stevin. 2010. Vol. 17. P. 333–341.

[20] *Mironescu P.*, *Panaitopol L.* The existence of a triangle with prescribed angle bisector lengths // Amer. Math. Monthly. 1994. Vol. 101, № 1. P. 58–60.

[21] *Oxman V.* A Purely Geometric Proof of the Uniqueness of a Triangle with Prescribed Angle Bisectors // Forum Geometricorum. 2008. Vol. 8. P. 197–200.

[22] *Ustinov A. V.* On the Construction of a Triangle from the Feet of its Angle Bisectors // Forum Geometricorum. 2009. Vol. 9. P. 279–280.

[23] `https://www.mccme.ru/ask/qa/bissect.html`.

[24] `https://www.mccme.ru/ask/qa/bissect1.html`.

[25] `https://www.cut-the-knot.org/triangle/TriangleFromBisectors.shtml`.

[26] `https://en.wikipedia.org/wiki/Brouwer_fixed-point_theorem`.

[27] `https://www.maplesoft.com`.

Николай Николаевич Осипов, Сибирский федеральный университет (Красноярск)

`nnosipov@rambler.ru`

Несколько задач о треугольниках Понселе

А. А. Заславский

В «Математическом просвещении» (выпуск 13, с. 179) была опубликована следующая задача (см. решение: выпуск 21, с. 278–282).

Задача 13.5. Известно, что в любом треугольнике расстояние между центрами O и I описанной и вписанной окружностей выражается через их радиусы R и r с помощью *формулы Эйлера*: $OI^2 = R^2 - 2Rr$. Докажите обобщение этой формулы: если в треугольник вписан эллипс с фокусами F_1, F_2 и малой осью ℓ, то

$$R^2\ell^2 = (R^2 - OF_1^2)(R^2 - OF_2^2). \qquad (1)$$

(*А. А. Заславский*)

В данной заметке приводятся решения двух других задач, продолжающих этот сюжет.

Задача 13.5′ (выпуск 28, с. 242–243). Треугольник вписан в окружность радиуса R и описан около эллипса с тем же центром и полуосями a, b.

(а) Докажите, что $R = a + b$.

(б) Найдите расстояние между центром описанной окружности и ортоцентром треугольника. (*А. А. Заславский*)

Решение. (а) Пусть $a > b$. Тогда в формуле (1) $\ell = 2b$ и $OF_1^2 = OF_2^2 = a^2 - b^2$. Следовательно, $a^2 = (R - b)^2$. Поскольку $R > b$, получаем искомое равенство.

(б) Ответ. $|a - b|$.

Будем считать, что $R = 1$ и описанная окружность треугольника является единичной окружностью комплексной плоскости. Пусть A, B, C, f_1, f_2 — комплексные числа, соответствующие вершинам треугольника и фокусам эллипса. Фокусы изогонально сопряжены относительно треугольника, поэтому, как заметил Морли, имеет место равенство (см. решение задачи 13.5 или [1], «Изогонально сопряжённые точки»)

$$f_1 + f_2 + \overline{f_1 f_2}ABC = A + B + C.$$

Но $f_1 + f_2 = 0$, значит,

$$f_1^2 = f_2^2 = -f_1 f_2, \quad f_{1,2} = \pm\sqrt{-(AB + BC + CA)}$$

и

$$OF_i^2 = \sqrt{\frac{(AB + BC + CA)(A + B + C)}{ABC}}.$$

С другой стороны, поскольку центру описанной окружности соответствует 0, ортоцентру H соответствует комплексное число $A + B + C$. Так как $|A| = |B| = |C| = 1$, имеем

$$OH^2 = (A + B + C)(\bar{A} + \bar{B} + \bar{C}) = (A + B + C)\left(\frac{1}{A} + \frac{1}{B} + \frac{1}{C}\right).$$

Следовательно,

$$OH = \sqrt{\frac{(AB + BC + CA)(A + B + C)}{ABC}}.$$

Таким образом,

$$OH = \frac{OF_i^2}{R} = a^2 - b^2 = |a - b|,$$

поскольку $a + b = 1$ в силу п. (а).

Примечания.

1. Из п. (а) и задачи 42 в [2] вытекает следующее свойство. Построим окружность с центром в вершине треугольника, касающуюся эллипса внешним образом. Тогда общие внешние касательные к этой окружности и эллипсу параллельны (рис. 1).

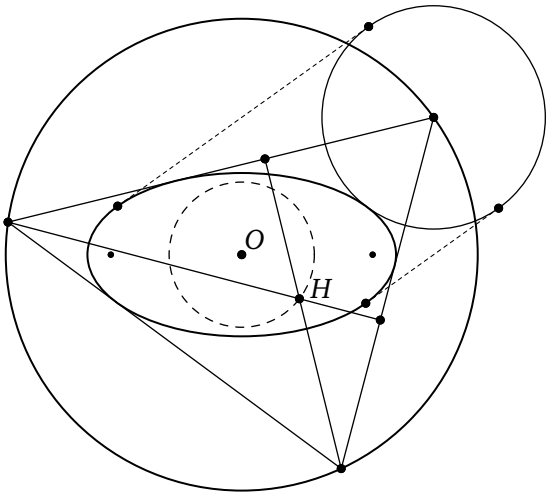


Рис. 1

2. Согласно теореме Понселе треугольник можно «вращать» между описанной окружностью и вписанным эллипсом. Пункт (б) показывает, что при этом вращении ортоцентр треугольника движется по окружности с центром O. Это утверждение является частным случаем задачи А. В. Акопяна [3]. Решение этой задачи, найденное А. Скутиным, приведено в [4].

Задача 13.5″ (выпуск 28, с. 243). Треугольник описан около окружности радиуса r и вписан в эллипс с тем же центром и полуосями a, b.

(а) Докажите, что $\frac{1}{r} = \frac{1}{a} + \frac{1}{b}$.

(б) Найдите радиус описанной окружности треугольника.

Решение. (а) При полярном преобразовании относительно вписанной окружности эллипс перейдёт в эллипс с тем же центром и полуосями r^2/a, r^2/b, а вершины треугольника в три прямые, касающиеся этого эллипса и пересекающиеся на окружности. Поэтому искомое равенство следует из п. (а) предыдущей задачи.

(б) Ответ. $\frac{a+b}{2}$.

Пусть A, B, C — вершины данного треугольника; I — центр его вписанной окружности; A', B', C' — точки её касания со сторонами BC, CA, AB; H' — ортоцентр треугольника $A'B'C'$. Из п. (б) предыдущей задачи получаем, что $IH' = r^2|a-b|/ab = ab|a-b|/(a+b)^2$. Известно, что $IH' : OI = r : R$ (треугольник, образованный вторыми точками пересечения прямых $A'H'$, $B'H'$, $C'H'$ с окружностью, гомотетичен треугольнику ABC, а H' — центр его вписанной окружности). Кроме того, по формуле Эйлера $OI^2 = R^2 - 2Rr$. Из этих соотношений находим $R = (a+b)/2$, $OI = |a-b|/2$.

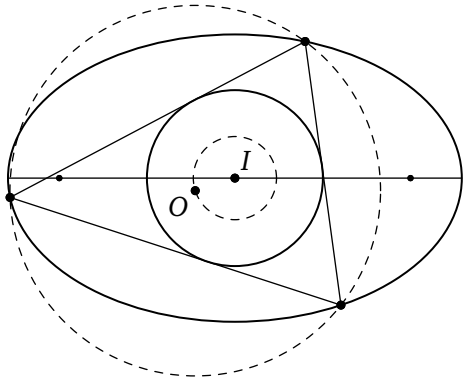


Рис. 2

Примечание. Пункт (б) означает, что при вращении треугольника между описанным эллипсом и вписанной окружностью центр его описанной окружности движется по окружности с центром I, а её радиус остаётся постоянным (рис. 2). Это равносильно следующему факту, замеченному Д. Резником: сумма радиусов вневписанных окружностей треугольника не меняется при его вращении (эта сумма равна $r + 4R$). Другие наблюдения Д. Резника приведены в [5].

Список литературы

[1] *Прасолов В. В.* Рассказы о числах, многочленах и фигурах. М.: МЦНМО, 2019.

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

[3] *Akopyan A.* Rotation of isogonal point // Journal of Classical Geometry. Vol. 1. Problem Section. P. 74. https://jcgeometry.org/Articles/Volume1/JCG2012V1pp72-74.pdf.

[4] *Skutin A.* On rotation of a isogonal point // Journal of Classical Geometry. Vol. 2. P. 66–67. https://jcgeometry.org/Articles/Volume2/JCG2013V2pp66-67.pdf.

[5] https://www.youtube.com/watch?v=wvNUdJbyHZA.

Алексей Александрович Заславский, ЦЭМИ РАН, МЭИ
alzasl@yandex.ru

Задачник

(составители А. Я. Канель-Белов, И. В. Митрофанов)

Условия задач

В этом разделе вниманию читателей предлагается подборка задач разной степени сложности, в основном трудных. Надеемся, что эти задачи окажутся интересными для читателей «Математического просвещения», в том числе для сильных школьников, интересующихся математикой.

Мы обращаемся с просьбой ко всем читателям, имеющим собственные подборки таких задач, присылать их в редакцию. Мы с удовольствием будем публиковать свежие авторские задачи.

В скобках после условия задачи указывается автор (уточнения со стороны читателей приветствуются).

На базе решения трудной задачи неоднократно появлялась научная статья (в том числе у школьника), а также доклад на конференции (школьной или взрослой). Так что призываем присылать решения опубликованных задач. Составители задачника помогут с публикациями и докладами на конференциях.

1. Даны две окружности C_1 радиуса r_1 и C_2 радиуса r_2. Рассматривается множество середин отрезков с концами на C_1 и C_2 соответственно. Какова его площадь? (*Л. Радзивиловский*)

2. Докажите, что для любых $0 < x < 1$ и $m, n \in \mathbb{N}$ имеет место неравенство
$$(1-x^n)^m + (1-x^m)^n > 1. \qquad (\textit{Фольклор})$$

3. Из n стержней (возможно, различной длины), скреплённых шарнирами, составлен выпуклый n-угольник.

   (а) Докажите, что эту конструкцию можно сделать жёсткой с помощью не более чем $n-2$ нитей.

(б) Каково минимальное число нитей для невыпуклого n-угольника? (*А. Я. Канель-Белов*)

4. (а) Изначально на доске нет чисел. Можно поставить две единицы, а если стоят два числа, равных n, то их можно заменить на $n-1$ и $n+1$. Какое минимальное число таких операций потребуется для создания числа 2021?

   (б) Изначально на доске нет чисел. Можно поставить две единицы, а если стоят два числа, равных n, то их можно заменить на $n-k$ и $n+k$ при некотором целом k, но так, чтобы отрицательных чисел не было. Какое минимальное число таких операций потребуется для создания числа 2022? (*А. Я. Канель-Белов*)

5. Пространственный четырёхугольник касается шара. Докажите, что точки касания лежат в одной плоскости. (*Фольклор*)

6. Дана выпуклая (т. е. такая, что множество точек над графиком выпукло) функция $f(x)$, определённая на всей вещественной прямой. Обозначим через U множество всех точек плоскости между графиками функций $f(x)$ и $f(x)+1$ (включая точки, лежащие на графиках). Докажите, что внутри U можно расположить отрезок любой конечной длины. (*Е. Рябов*)

7. Единичный диск покрыт (возможно, пересекающимися) треугольниками, не вылезающими за его пределы. Может ли сумма длин их периметров быть конечной? (*Л. Радзивиловский*)

8. Рассмотрим множество Ω трёхэлементных подмножеств множества $\{1,\ldots,n\}$. Пусть m — минимальное число цветов, в которые можно раскрасить Ω так, чтобы тройки $\{a,b,c\}$ и $\{b,c,d\}$ при $1\leqslant a<b<c<d\leqslant n$ были раскрашены в разные цвета. Докажите, что

$$\frac{1}{100}\cdot\ln\ln n\leqslant m\leqslant 100\cdot\ln\ln n.$$ (*Д. Черкашин*)

9. Дан произвольный треугольник ABC. Пусть O, H — центр его описанной окружности и его ортоцентр соответственно, а P — произвольная точка плоскости.

   (а) Докажите, что касательные к окружностям (AOP), (BOP), (COP) в точках A, B, C конкурентны тогда и только тогда, когда P лежит на гиперболе $ABCOH$.

   (б) Пусть теперь точка P лежит на гиперболе $ABCOH$. Обозначим через A_1 точку пересечения касательной к окружности (ABC) со стороной BC, а через A_2 — точку пересечения прямых $A_1B_1C_1$ и AP. Аналогично определим точки B_1, B_2 и C_1, C_2. Тогда радикальный

центр окружностей (AA_1A_2), (BB_1B_2) и (CC_1C_2) — это точка пересечения прямых OP и $A_1B_1C_1$.

(в) Если P совпадает с точкой Лемуана L треугольника ABC, то окружности из п. (б) соосны и пересекаются на окружности (ABC).

(*А. Жужлев, А. Шевцов*)

10. *Матрицей Маркова* называется квадратная матрица $A=(a_{ij})_{1\leqslant i,j\leqslant n}$, такая, что 1) $a_{ij}\geqslant 0$ для любых i, j; 2) $\sum_{j=1}^{n} a_{ij}=1$ для любого $1\leqslant i\leqslant n$. Пусть $A=(a_{ij})$ — матрица Маркова порядка $n\geqslant 18$. Тогда из неё можно получить циклическими перестановками элементов строк такую матрицу Маркова $B=(b_{ij})$, что

$$\sum_{i=1}^{n} b_{ij} < 2, \quad 1\leqslant j\leqslant n.$$

(*К. Э. Каибханов*)

11. (а) Пусть n — натуральное число. Сколько различных решений $(a,b,c,d)\in\mathbb{Z}^4$ имеет уравнение $a^2+b^2+c^2+d^2=2^n$?

(б)* Покажите, что для простого нечётного p уравнение

$$x^2+y^2+z^2+t^2=4p$$

имеет $24(p+1)$ различных решений в целых числах. (*Фольклор*)

12. Дана непрерывная функция $f\colon [0,1]\to[0,1]$. Её *k-я итерация* $f_k(x)$ — это $f(f(\ldots(x)\ldots))$ (k раз). Известно, что $f_3(x)=x$, но $f(x)\neq x$ при некотором x. Докажите, что тогда для любого k существует такое $y\in[0,1]$, что $f_k(y)=y$, но $f_m(y)\neq y$ при всех $1\leqslant m<k$.

(*Теорема Шарковского*)

13. (а) На плоскости отмечено несколько клеток. Отмеченную клетку назовём *граничной*, если она граничит по стороне с неотмеченной. Имеется n отмеченных граничных клеток. Каково максимальное возможное число всех отмеченных клеток?

(б) Аналогичный вопрос для кубической решётки (*граничная клетка* имеет общую грань с неотмеченной). (*А. Я. Канель-Белов*)

14. Введём отношение эквивалентности на матрицах второго порядка с единичным определителем: $A\simeq B$, если AB^{-1} — целочисленная матрица. Докажите, что множество классов такой эквивалентности изоморфно дополнению трёхмерного пространства до узла трилистника. (*Фольклор*)

15. Периодическую последовательность символов можно задавать запретами, которые показывают, какие последовательности симво-

лов не могут в ней появляться. Например, последовательность $aabaabaab\ldots$ задаётся тремя запретами b^2, bab, a^3.

(а) Дана последовательность периода n. Скольких запретов заведомо будет достаточно?

(б) Периодическая последовательность над n-буквенным алфавитом задана запретами длины k. Каков её максимально возможный период?

(в) Докажите, что последовательность периода n нельзя задать меньше чем $\log_2(n)$ запретами.

(г) Докажите, что есть последовательности периода n, которые можно задать k запретами, где u_k — первое число Фибоначчи, не меньшее чем n. (*А. Я. Канель-Белов*)

Дополнение и комментарии к задачнику

Хорошая задача ценна своими связями. Наиболее содержательные из них открывают новые сюжеты и темы, в рамках которых возникают новые задачи, открываются новые грани. Именно поэтому их решение обогащает и оказывается столь полезным, помимо чисто интеллектуальной тренировки.

Эстетическое чувство позволяет ощутить богатство связей и естественность задачи. Оно так важно в том числе и по этой причине. Значение математика определяется произведением его «пробивной силы» на эстетическое чувство (впрочем, эти две вещи взаимозависимы).

При публикации дополнения к задачнику нам прежде всего важны эти связи. Разумеется, содержательные и важные связи могут найтись как с классикой, так и с сюжетами, которые находятся в процессе исследования и ещё не получили изящной формулировки.

В выпуске 1 (с. 193, см. решение: выпуск 6, с. 137–139) опубликована

Задача 1.1. Могут ли 1000 ладей в пространстве заматовать короля? (*Фольклор*)

Развитием сюжета служит

Задача 1.1′. *Имеется бесконечная клетчатая плоскость и хромая ладья на ней.* (*Ход хромой ладьи — в клетку, соседнюю по стороне.*) *Также имеется программа, которая выставляет между соседними по стороне клетками перегородки и к моменту времени t не может выставить больше чем $t \cdot c$ перегородок, где c — константа* (*то есть программа может и выставлять перегородки регулярно, и долгое время не ставить, но к моменту времени t должно быть выставлено не больше $t \cdot c$ перегородок*). *Программа написана заранее и не может реагировать на то, как будет ходить ладья. Более того, ладья знает программу и знает, когда и куда будут выставляться перегородки.*

(а) *Докажите, что при $c \leqslant 1$ ладья заведомо сможет ходить вечно.*

(б) *Докажите, что при $c > 2$ можно написать программу, которая поймает ладью, если программе известно изначальное местоположение ладьи.*

(в) *Решите пункт* (б) *без условия о том, что программе известно изначальное местоположение ладьи.* (*М. Матдинов, Ф. Ивлев*)

Замечание. Есть гипотеза, что при $c = 2$ (а значит, и при $c < 2$) ладья сможет ходить сколь угодно долго, даже если программе известно изначальное положение ладьи.

В выпуске 8 (с. 246, см. решение: выпуск 9, с. 215–217) опубликована

Задача 8.5. Для иррационального $\alpha > 1$ обозначим

$$N(\alpha) = \{[n\alpha] \mid n \in N\}.$$

При каких k найдутся такие $\alpha_1, \ldots, \alpha_k$, что множества $N(\alpha_1), \ldots, N(\alpha_k)$ задают разбиение натурального ряда?

(*А. А. Заславский, А. В. Спивак*)

С ней связана (выпуск 29, с. 263)

Задача 8.5′. Закрашены k вершин правильного n-угольника P. Закраска называется почти равномерной, если для любого натурального m верно следующее условие: если $M1$ — множество m расположенных подряд вершин и $M2$ — другое такое множество, то количество закрашенных вершин в $M1$ отличается от количества закрашенных вершин в $M2$ не больше, чем на 1. Доказать, что для любых натуральных n и k ($k < n$) почти равномерная закраска существует и что она единственна с точностью до поворотов закрашенного множества.

(*М. Л. Концевич*)

В продолжение темы:

Задача 8.5″. (а) *Опишите все бесконечные апериодические слова над алфавитом из k символов со следующим свойством: в любых двух подсловах одинаковой длины количество символов каждого сорта отличается не более чем на* 1.

(б) *Опишите все бесконечные апериодические слова над алфавитом из k символов такие, что для некоторых C и N_0 при всех $n > N_0$ количество подслов длины n равно $n + C$.*

(*А. Я. Канель-Белов, А. Л. Чернятьев*)

Задача 8.5‴. *Пусть n — фиксированное число. Укажите все такие A, что числа $[A], [2A], \ldots, [NA]$ все различны и $[1/A], [2/A], \ldots, [N/A]$ тоже различны.* (*Фольклор*)

В выпуске 11 опубликована (с. 163, см. решение: выпуск 14, с. 279)

Задача 11.6. Обозначим через $s(n)$ сумму цифр числа n. Ограничена ли последовательность $s(n)/s(n^2)$? (*Э. Туркевич*)

Ответ отрицательный, и решение проходит при всех целых $k > 1$. В этой связи возникает

Задача 11.6′. (а) *Пусть k — целое число, $k > 1$. Ограничена ли последовательность $s(n^k)/s(n)$?*

(б) *Решите уравнение в целых числах*: $s(n^4) = s(n)^4$.

(*А. Я. Канель-Белов*)

В выпуске 13 (с. 181) опубликована

Задача 13.12. Докажите, что следующие числа могут начинаться с любой комбинации цифр: (а) 2^{n^2}; (б) $2^{2^n 3^k}$.

(в) Докажите, что множество $A \subset \mathbb{R}$ чисел таких, что последовательность первых цифр c^{2^n} $(c \in A)$ периодична, счётно, а множество $B \subset \mathbb{R}$ чисел таких, что последовательность первых цифр c^{10^n} $(c \in B)$ периодична, несчётно. (*А. Канель*)

С ней связана (выпуск 29, с. 264)

Задача 13.12′. (а) Пусть $\alpha \notin \mathbb{Q}$. Докажите, что множество дробных частей $\{\alpha \cdot n\}$, где $n \in \mathbb{N}$, всюду плотно и равномерно распределено на единичном отрезке. (*Фольклор*)

(б) Лемма Кронекера. Пусть α_i, $i = 1, \ldots, k$, линейно независимы над $\mathbb{Q}$. Докажите, что множество векторов из дробных частей $\{\alpha_1 \cdot n\}$, $\ldots$, $\{\alpha_k \cdot n\}$, где $n \in \mathbb{N}$, всюду плотно и равномерно распределено в единичном кубе.

Лемма Вейля. Пусть многочлены P_i, $i = 1, \ldots, k$, линейно независимы над $\mathbb{Q}$ по модулю многочленов с рациональными коэффициентами и констант. Докажите, что множество векторов из дробных частей $\{P_1(n)\}, \ldots, \{P_k(n)\}$, где $n \in \mathbb{N}$:

(в) всюду плотно;

(г) равномерно распределено в единичном кубе.

В одном из доказательств леммы Вейля используется следующая

Задача 13.12″. (а) *В таблице $n \times n$ записаны числа $a_{ij} = b_i b_j$. Главная диагональ $((1,1) - (n,n))$ покрыта неперекрывающимися квадратами равного размера, стороны которых параллельны сторонам таблицы, а главные диагонали лежат на главной диагонали большого квадрата. Может ли среднее арифметическое чисел, попавших в эти квадраты, быть строго больше среднего арифметического чисел таблицы?*

(*б*) *Тот же вопрос, если условие равенства размеров убрать.*

(*А. Я. Канель-Белов*)

В выпуске 14 (с. 273, поправка: выпуск 15, с. 235, см. решение: выпуск 15, с. 219–228) опубликована

Задача 14.8. Дан треугольник ABC. A_1, B_1, C_1 — точки касания сторон BC, AC, AB с вписанной окружностью соответственно. A_0, B_0, C_0 — середины сторон. Обозначим точку пересечения прямых A_0B_0 и A_1B_1 через C'. Аналогично определяются точки A' и B'. Докажите, что прямые A_1A', B_1B' и C_1C' пересекаются в точке Фейербаха. (*Ф. Ивлев*)

По мотивам этой задачи придумалась следующая

Задача 14.8′. *Докажите, что касательная к вписанной окружности треугольника в точке Фейербаха касается также вписанного эллипса Штейнера* (*касающегося сторон в их серединах*).

(*А. А. Заславский*)

В выпуске 16 опубликована (с. 231)

Задача 16.7. В единичный шар вписано тело T, все рёбра которого имеют длину не более 10^{-3}, а площадь его поверхности больше 10^3. Докажите, что у него не менее 10^9 граней. (*А. Я. Белов*)

Ей предшествовала классическая задача:

Задача 16.7′. *В единичный шар вписано тело T. Может ли площадь его поверхности быть сколь угодно большой?* (*«Сапог Шварца»*)

В выпуске 20 опубликована (с. 251)

Задача 20.9. (а) Матрица A называется *нормальной*, если $AA^* = A^*A$, где A^* — матрица, транспонированная к матрице A. Какова максимальная размерность векторного подпространства комплексных $(n \times n)$-матриц, все элементы которого нормальны?

(*Международная студенческая олимпиада*, 2015)

(б) Какова максимальная размерность подпространства попарно коммутирующих комплексных $(n \times n)$-матриц? (*Э. Б. Винберг*)

В продолжение сюжета:

Задача 20.9′. *Матрица A называется* идемпотентной *если $A^2 = A$. Дано k идемпотентных матриц $A_1, \ldots, A_k$ порядка n таких, что $A_iA_j = -A_jA_i$ при $i \neq j$. Докажите, что ранг одной из них не превосходит n/k.* (*Данила Белоусов, Новосибирск*)

В выпуске 26 (с. 267) опубликована

Задача 26.8. Пусть 2019 точек случайно, независимо и равномерно распределены на единичном диске $\{(x, y) \in \mathbb{R}^2 \colon x^2 + y^2 \leqslant 1\}$,

и пусть C есть их выпуклая оболочка. Какая вероятность больше: что C — треугольник или что C — четырёхугольник? (*Ф. В. Петров*)

В продолжение вероятностной темы:

Задача 26.8′. *В круге случайно и равномерно выбрали n синих точек и k красных точек. Каково матожидание количества вершин пересечения выпуклой оболочки красных точек и выпуклой оболочки синих точек?* (*Число вершин пустого множества считается равным нулю.*) (*Ф. В. Петров*)

В выпуске 28 (с. 233, см. решение: этот выпуск, с. 239–240) опубликована

Задача 28.2. Любой ли трёхгранный угол имеет сечение, являющееся правильным треугольником? (*Фольклор*)

Развитием темы служит

Задача 28.2′. *Всегда ли возможно, перегнув произвольный треугольник по средним линиям, получить тетраэдр* (*не обязательно правильный*)? (*Фольклор*)

В выпуске 29 (с. 258) опубликована

Задача 29.15. (а) Рассматривается последовательность первых цифр степеней двойки 1248136125 … Каково количество различных подслов длины 13?

(б) Рассматривается последовательность W первых цифр вида 2^{n^2}: 1215636 … Докажите, что существует такой многочлен $P(k)$, что для всех достаточно больших k количество всех различных подслов в W длины k есть в точности $P(k)$. (*А. Я. Канель-Белов*)

Продолжением темы служит

Задача 29.15′. *Рассматривается последовательность W первых цифр степеней двойки* 1248136125 ….

(а) *Докажите, что последовательность непериодична.*

(б) *Докажите, что существует такая константа N, что фрагмент* 1248136125 *встречается в* любом *подслове из W длины N.*

(в) *Докажите, что любое подслово из W, если его записать в обратном порядке, встречается как подслово в последовательности первых цифр степеней пятёрки.*

(г) *Опишите слова, которые могут встречаться бесконечно много раз в последовательности первых цифр числа вида $c_1(c_2n)!$.*

(*А. Я. Канель-Белов*)

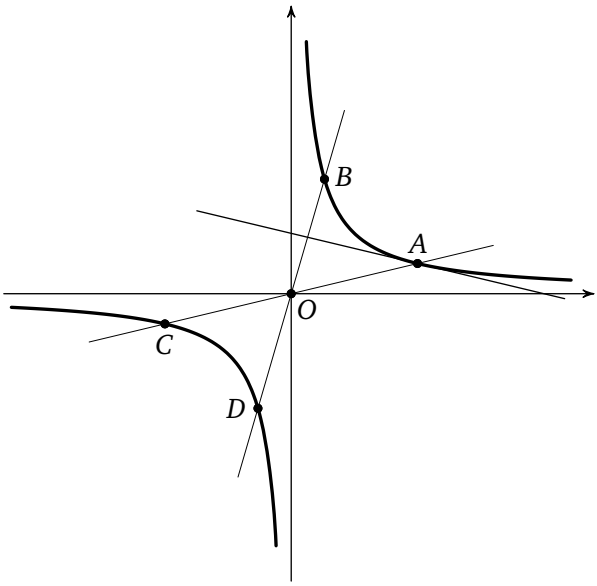
Решения задач из прошлых выпусков

15.3. Условие. Гипербола $H = \{(x, y) : xy = 1\}$ повёрнута на угол α относительно начала координат $(0; 0)$; получилась гипербола H_α. Найдите угол между их касательными в точках пересечения H и H_α.

(*А. В. Акопян*, *D. Schleicher*)

Ответ. $180^\circ - 2\alpha$.

Решение. Возьмём точку A на гиперболе. При повороте она может перейти в одну из точек на гиперболе, находящихся на том же расстоянии от начала координат (см. рисунок). Так как при повороте на 180° гипербола переходит сама в себя, достаточно рассмотреть только случай, когда совмещаются точки A и B, т. е. $\angle AOB = \alpha$. Обозначим через φ острый угол между OA и касательной к гиперболе в точке A. Из симметрии относительно прямой $x = y$ следует, что острый угол между



прямой OB и касательной в точке B также равен φ и противоположно ориентирован, поэтому ответ равен 2φ. Осталось выразить φ через α.

Пусть $y = kx$ — уравнение прямой OA. Тогда $(1/\sqrt{k}, \sqrt{k})$ — координаты точки A. Подставляя $x = 1/\sqrt{k}$ в формулу для производной $y' = -1/x^2$, получаем, что угловой коэффициент касательной в точке A равен $-k$, а значит, касательная и прямая OA образуют равные углы с осью OX.

Угол между Ox и прямой OA равен (из симметрии) $(90^\circ - \alpha)/2 = 45^\circ - \alpha/2$, поэтому $\varphi = \angle 90^\circ - \alpha$ и ответ равен $180^\circ - 2\alpha$.

(*И. В. Митрофанов*)

16.8. Условие. Даны два подмножества в $\mathbb{Z}_2^n$: A и B. Известно, что $|A| + |B| > 2^k$. Докажите, что $|A + B| \geqslant 2^k$. (Здесь $A + B$ — это сумма Минковского двух множеств.) (*Д. Г. Фон-дер-Флаасс*)

Решение. Будем доказывать утверждение задачи индукцией по k. База $k = 1$ очевидна.

Будем говорить, что координата *разделяет* множество двоичных векторов, если в этом множестве есть как векторы, у которых эта координата равна 0, так и векторы, у которых она равна 1. Если среди координат нет такой, которая разделяет и A и B, то координаты делятся на два типа: одинаковые для любого вектора из A и одинаковые для любого вектора из B. Тогда все суммы Минковского попарно разные, а значит, их количество равно $|A| \cdot |B| \geqslant 1 \cdot 2^k = 2^k$.

Теперь предположим, что одна из координат (не умаляя общности, первая) разделяет как A, так и B. Обозначим A_0 множество всех векторов из A, у которых первая координата равна 0. Аналогично определим A_1, B_0 и B_1.

Либо $|A_0| + |B_0| > 2^{k-1}$, либо $|A_1| + |B_1| > 2^{k-1}$. Аналогично либо $|A_0| + |B_1| > 2^{k-1}$, либо $|A_1| + |B_0| > 2^{k-1}$. Не умаляя общности, пусть

$$|A_0| + |B_0| > 2^{k-1}, \quad |A_0| + |B_1| > 2^{k-1}.$$

По предположению индукции $|A_0 + B_0| \geqslant 2^{k-1}$ и $|A_0 + B_1| \geqslant 2^{k-1}$. Далее, у всех векторов из $A_0 + B_0$ первая координата равна 0, а у векторов из $A_0 + B_1$ она равна 1, поэтому эти две суммы Минковского не пересекаются и $|A + B| \geqslant |A_0 + B_0| + |A_0 + B_1| \geqslant 2^k$.

(*И. В. Митрофанов*)

28.2. Условие. Любой ли трёхгранный угол имеет сечение, являющееся правильным треугольником? (*Фольклор*)

Ответ. Не любой.

Решение. Предположим, что любой трёхгранный угол имеет сечение, являющееся правильным треугольником. Можно считать (применив гомотетию), что сторона этого треугольника равна 1. Тогда можно также считать, что для всех трёхгранных углов это один и тот же треугольник ABC.

Рассмотрим замыкание M множества точек, из которых стороны AB и AC видны под углами, не меньшими $\pi - \varepsilon$, где ε — заданное положительное число. Ясно, что $A \in M$.

Возьмём трёхгранный угол, в котором AB и AC принадлежат плоским углам, равным $\pi - \varepsilon$, а третий плоский угол равен ε. Тогда вершина трёхгранного угла O принадлежит M.

Устремим теперь ε к нулю. Множество M в пределе сводится к точке A. Значит, $O \to A$. Так как отрезок BC виден из O под углом ε, из A он должен быть виден под нулевым углом, что неверно.

Замечание. На самом деле наше рассуждение показывает, что для любого треугольника найдётся трёхгранный угол, не имеющий подобного ему сечения. (*А. Я. Канель-Белов, Б. Р. Френкин*)

Указатель условий, решений и статей по мотивам задач из «Математического просвещения»

(число перед запятой — номер выпуска,
число после запятой — номер страницы)

Задача	Условие	Решение или статья по мотивам	Задача	Условие	Решение или статья по мотивам
1.1	1, 193	6, 137–139	4.1	4, 215	6, 149–150
1.2	1, 193	5, 218	4.2	4, 215	7, 193
1.3	1, 193	4, 218	4.3	4, 215	7, 193–194
1.4	1, 193	5, 218–221	4.4	4, 216	7, 194
1.5	1, 194	6, 139–140	4.5	4, 216	6, 150
1.6	1, 194	5, 221–223; 10, 274	4.6	4, 216	6, 150–151
1.7	1, 194	4, 219	4.7	4, 216	6, 151–152
1.8	1, 194	4, 220	4.8	4, 216	5, 228–229
1.9	1, 194	5, 223–225	4.9	4, 217	8, 237–238
1.10	1, 194	4, 220; 5, 225–227;	4.10	4, 217	7, 194–195
		24, 181–184	4.11	4, 217	8, 249–252; 15, 212–218
2.1	2, 216	4, 221	4.12	4, 217	18, 263–269
2.2	2, 216	5, 227–228	5.1	5, 216	6, 152–153
2.3	2, 216	4, 221	5.2	6, 135	7, 195–196
2.4	2, 217	4, 221–222	5.3	5, 216	6, 153
2.5	2, 217	4, 222	5.4	5, 216–217	7, 196–198
2.6	2, 217	4, 222–223	5.5	5, 217	8, 252–254
2.7	2, 217	6, 140–142	5.6	5, 217	14, 275–276
2.8	2, 217	6, 2–145; 18, 259–261	5.7	5, 217	6, 153
2.9	2, 217	6, 145–147	5.8	5, 217	7, 198
2.10	6, 135	8, 248–249	5.9	5, 217	10, 232–235, 236–242;
3.1	3, 232	4, 223			11, 145–148
3.2	3, 232	4, 223–224	5.10	5, 217	8, 254
3.3	3, 232	5, 227–228; 19, 241–247	6.1	6, 133	8, 255
3.4	3, 232	4, 224	6.2	6, 133	9, 225
3.5	3, 233	4, 225; 18, 262	6.3	6, 133	9, 225–226
3.6	3, 233	7, 190–193	6.4	6, 133	9, 226–227
3.7	3, 233	6, 147–148	6.5	6, 133–134	
3.8	3, 233	6, 148–149	6.6	6, 134	8, 255–256
3.9	8, 247	15, 206–211	6.7	6, 134	11, 165–166
3.10	3, 233	8, 239–245	6.8	6, 134	8, 256–257
3.11	3, 233	8, 186–221	6.9	6, 134	8, 222–228; 229–236

Задача	Условие	Решение или статья по мотивам	Задача	Условие	Решение или статья по мотивам
6.10	6, 134	20, 252–253	10.10	10, 280	11, 149–158
6.11	6, 134	9, 227–229; 17, 198–199	10.11	10, 280	
6.12	6, 134	8, 258–259	10.12	10, 280	28, 251–254
7.1	7, 187	9, 229	11.1	11, 162	13, 186; 14, 278
7.2	7, 187	8, 259–260	11.2	11, 162	13, 186–189
7.3	7, 187	9, 229; 10, 274; 10, 275	11.3	11, 162	17, 199
7.4	7, 187	9, 229–230	11.4	11, 162–163	23, 221–223
7.5	7, 187–188		11.5	11, 163	23, 223–224
7.6	7, 188	16, 233–235	11.6	11, 163	14, 279
7.7	7, 188	21, 276–278	11.7	11, 163	27, 251–253
7.8	7, 188	13, 182–184	11.8	11, 163	
7.9	7, 189	9, 230–232	11.9	11, 163	21, 278
7.10	11, 164		11.10	11, 164	17, 199–200
7.11	7, 189	9, 232–233	11.11	11, 164	
7.12	7, 189	11, 166–168	11.12	11, 164	
8.1	8, 246	13, 184	12.1	12, 235	15, 236–237; 17, 187–188
8.2	8, 246	10, 281	12.2	12, 235	
8.3	8, 246	10, 281–282; 22, 237	12.3	12, 235	16, 236; 17, 200
8.4	8, 246	10, 243–264, 282–284	12.4	12, 235	14, 279–280
8.5	8, 246	9, 215–217	12.5	12, 236	
8.6	8, 246	22, 237–239	12.6	12, 236	20, 254–256
8.7	8, 247		12.7	12, 236	16, 236–237
8.8	8, 247	9, 233	12.8	12, 236	14, 256–269
8.9	8, 247	11, 168–169	12.9	12, 236	20, 256–258
8.10	8, 247	26, 279	12.10	12, 236	13, 189–190
8.11	8, 247	22, 239–240	12.11	12, 236	
8.12	8, 247	20, 238–242	12.12	12, 236	
9.1	9, 223	14, 276–277	13.1	13, 179	14, 280–281
9.2	9, 223	13, 184–185	13.2	13, 179	14, 270–271; 14, 281
9.3	9, 223	26, 280–281	13.3	13, 179	15, 237
9.4	9, 223	10, 284–285	13.4	13, 179	23, 224–225
9.5	9, 223	14, 277	13.5	13, 179	21, 278–282
9.6	9, 223–224	12, 237–238	13.6	13, 179–180	20, 258–263
9.7	9, 224	28, 249–251	13.7	13, 180	23, 226
9.8	9, 224	12, 238	13.8	24, 177	29, 275–279
9.9	9, 224	11, 169–172	13.9	13, 180	19, 249–253
9.10	9, 224	10, 265–272	13.10	13, 181	20, 215–227
9.11	9, 224	27, 249–251	13.11	13, 181	22, 242–243
10.1	10, 278	13, 185–186	13.12	13, 181	
10.2	10, 278	11, 172	14.1	14, 272	28, 254–255
10.3	10, 278		14.2	14, 272	
10.4	10, 278–279	11, 173–174	14.3	14, 272	15, 237–239
10.5	10, 279	14, 240–255	14.4	14, 272	28, 255–256
10.6	10, 279	12, 238–239	14.5	14, 272	15, 239–240
10.7	10, 279	24, 186–188	14.6	14, 273	15, 240–241
10.8	10, 279	22, 241–242	14.7	15, 235	15, 241–244
10.9	10, 279	14, 277–278	14.8	15, 235	15, 219–228

Задача	Условие	Решение или статья по мотивам	Задача	Условие	Решение или статья по мотивам
14.9	14, 273	16, 237–239	18.9	18, 257	
14.10	14, 273		18.10	18, 258	19, 266–267
14.11	14, 274	24, 189–193	18.11	18, 258	
14.12	14, 274	15, 229–230	18.12	18, 258	
15.1	15, 232	23, 226–229; 24, 200–201	19.1	19, 257	
15.2	15, 232	23, 229	19.2	19, 257	21, 282–283
15.3	15, 232	30, 238–239	19.3	19, 257	20, 265–267
15.4	15, 232	23, 230–231	19.4	19, 258	
15.5	15, 233	20, 263	19.5	19, 258	
15.6	15, 233		19.6	19, 258	24, 195–197
15.7	15, 233		19.7	19, 258	20, 267
15.8	15, 233		19.8	19, 258	
15.9	15, 233	24, 193–195	19.9	19, 258	20, 267–268
15.10	15, 234	17, 200–202	19.10	19, 258	
15.11	15, 234		19.11	19, 258	
15.12	15, 234		19.12	19, 259	
16.1	16, 230	18, 269	20.1	20, 249	21, 283–284
16.2	16, 230	17, 202–203	20.2	20, 249	21, 235–264
16.3	16, 230	20, 263–264	20.3	20, 250	
16.4	16, 230	19, 260	20.4	28, 236	
16.5	16, 230		20.5	20, 250	23, 232–233
16.6	16, 231	17, 192–195	20.6	20, 250	21, 219–223
16.7	16, 231		20.7	20, 250	
16.8	16, 231	30, 239	20.8	20, 250–251	
16.9	16, 231	19, 260–262	20.9	20, 251	
16.10	16, 231		20.10	20, 251	22, 244–248
16.11	16, 231	17, 203–207	20.11	20, 251	
16.12	16, 232		20.12	20, 251	
17.1	17, 196	20, 264–265	21.1	21, 271	22, 248–249
17.2	17, 196	23, 231–232; 25, 179–180	21.2	21, 271	22, 249–251; 26, 259
17.3	17, 196	22, 243–244	21.3	21, 272	22, 220–228
17.4	17, 196	25, 180	21.4	21, 272	23, 233–234
17.5	17, 196	30, 137–140	21.5	21, 272	28, 256–259
17.6	25, 169	26, 281–282	21.6(а)	21, 272	22, 251–252
17.7	17, 197		21.6(б)	21, 272–273	
17.8	17, 197		21.7	21, 273	
17.9	17, 197	25, 182–185	21.8	21, 273	
17.10	17, 197	19, 263	21.9	21, 273	22, 252–254
17.11	17, 197	20, 228-237	21.10	21, 273	
17.12	17, 197		21.11	21, 273	
18.1	18, 255		21.12	21, 273	
18.2	18, 255–256	19, 264	22.1	22, 231	23, 235
18.3	18, 256		22.2	22, 231–232	23, 235–236
18.4	18, 256		22.3	22, 232	24, 197–198
18.5	18, 257		22.4	22, 232	23, 236–238
18.6	18, 257		22.5(а), (б)	26, 259–262	
18.7	18, 257	19, 264–266	22.5(в)	22, 232	26, 282–284
18.8	18, 257	19, 254–256	22.6	22, 232	

Задача	Условие	Решение или статья по мотивам	Задача	Условие	Решение или статья по мотивам
22.7	22, 233		26.7	26, 266	
22.8	22, 233		26.8	26, 267	
22.9	22, 233		26.9	26, 267	
22.10	22, 233	29, 272–273	26.10	26, 267	
22.11	22, 233		26.11	26, 267	
22.12	22, 233		26.12	26, 267	
23.1	23, 215	24, 168–174	27.1	27, 233	
23.2	23, 215		27.2	27, 233–234	28, 261
23.3	23, 215–216	28, 259–260	27.3	27, 234	28, 261–262
23.4	23, 216		27.4	27, 234	
23.5	23, 216		27.5	27, 234	
23.6	23, 216		27.6	27, 234	
23.7	23, 216	24, 198–199	27.7	27, 234	
23.8	23, 216		27.8	27, 235	
23.9	23, 216	24, 199–200	27.9	27, 235	
23.10	23, 216		27.10	27, 235	
23.11	23, 217		27.11	27, 236	
23.12	23, 217		27.12	27, 236	
24.1	24, 175	25, 185	28.1	28, 233	
24.2	24, 175–176		28.2	28, 233	30, 239–240
24.3	24, 176		28.3	28, 233–234	
24.4	24, 176		28.4	28, 234	
24.5	24, 176		28.5	28, 234	
24.6	24, 176	25, 186–187	28.6	28, 234	
24.7	24, 176		28.7	28, 234–235	
24.8	24, 176	25, 187–189	28.8	28, 235	
24.9	24, 176	27, 260–262	28.9	28, 235	
24.10	24, 177	25, 189–190	28.10	28, 235	
24.11	24, 177	29, 280–282	28.11	28, 235	
24.12	24, 177		28.12	28, 235	
25.1	25, 167	26, 284	28.13	28, 235	
25.2	25,167	27, 175–176	28.14	28, 236	
25.3	25, 168		28.15	28, 236	
25.4	25, 168	26, 249–257	29.1	29, 255–256	
25.5	25, 168		29.2	29, 256	
25.6(а), (б)	25, 168-169	29, 282–285	29.3	29, 256	
25.6(в)	27, 236	29, 285	29.4	29, 256	
25.7	25, 169	27, 262–263	29.5	29, 256	
25.8	25, 169		29.6	29, 256	
25.9	25, 169		29.7	29, 256–257	
25.10	25, 169		29.8	29, 257	
25.11	25, 169	28, 219–232	29.9	29, 257	
25.12	25, 169		29.10	29, 257	
26.1	26, 265	27, 263–265	29.11	29, 257	
26.2	26, 265		29.12	29, 258	
26.3	26, 265–266		29.13	29, 258	
26.4	26, 266	27, 266–269	29.14	29, 258	
26.5	26, 266	27, 182–185	29.15	29, 258	
26.6	26, 266	27, 186–192			

Указатель к Дополнению и комментариям к задачнику «Математического просвещения»

(число перед запятой — номер выпуска,
число после запятой — номер страницы)

Задача	Условие	Решение или статья по мотивам	Задача	Условие	Решение или статья по мотивам
1.1′	30, 233–234		8.5‴	30, 234	
1.2′	22, 234	26, 276	8.8′	27, 240	
1.2″	25, 170	26, 276–279	8.11′	23, 218	29, 273–275
1.3′	29, 259		9.5′	27, 240	
1.5′	27, 238		10.9′	28, 240	
1.8′	27, 238		10.9″	28, 240	
2.3′	28, 237		10.10′	28, 241	
2.4′	22, 234		10.11′	22, 235	
2.4″	22, 234	29, 272	10.11″	22, 235	
2.5′	29, 260		10.11‴	22, 236	
2.7′	28, 238		10.12′	28, 241	
3.1′	28, 238–239		11.4′	23, 218	24, 188–189
3.2′	27, 239		11.4″	24, 178	
3.3′	25, 171		11.4‴	24, 178	25, 177–178
3.5′	26, 268		11.6′	30, 235	14, 279
3.5″	28, 239		11.7′	26, 269	27, 253–254
3.8′	22, 235		11.7″	29, 263	
4.8′	28, 239		11.9′	23, 219	25, 178–179
4.8″	29, 261		11.11′	26, 269	
4.10′	27, 239		12.1′	27, 241	
4.10″	29, 262		13.2′	27, 241	
5.5′	23, 217		13.3′	26, 269	
5.5″	27, 239		13.5′	28, 242–243	30, 233–234
5.9′	29, 262		13.5″	28, 243	30, 234–236
6.1′	23, 217	25, 176–177	13.6′	27, 242	
6.1″	27, 240		13.6″	28, 243	
6.9′	21, 275	24, 185–186	13.10′	24, 179	27, 254–258
7.1′	28, 240		13.10″	27, 242	
8.5′	29, 263		13.12′	29, 264	
8.5″	30, 234		13.12″	30, 235	

Задача	Условие	Решение или статья по мотивам	Задача	Условие	Решение или статья по мотивам
14.6′	23, 219	24, 189	23.6″	27, 246	
14.8′	30, 236		23.10′	24, 180	29, 279–280
14.9′	26, 270		23.10″	24, 180	
14.12′	23, 220	27, 258	23.10‴	27, 247	
15.1′	26, 270		24.2′	28, 245	
15.2′	25, 171		24.2″	29, 266	
15.4′	22, 236		24.6′	29, 266–267	
16.4′	26, 271	27, 259	24.9′	28, 246	
16.7′	30, 236		25.1′	27, 247–248	28, 260
16.12′	27, 243		25.2′	27, 176	27, 176–177
17.1′	27, 243		25.2″	26, 273	27, 177
17.4′	23, 220	25, 180–182	25.10′	28, 246	
17.5′	24, 179–180		26.1′	28, 246–247	
17.7′	29, 265		26.1″	29, 267	
17.9′	26, 271		26.3′	29, 268	
18.1′	23, 220		26.3″	29, 268	30, 177–191
18.3′	26, 272		26.4′ (а)	27, 248	
19.3′	26, 272		26.4′ (б)	28, 236	
19.5′	25, 171		26.6′	26, 274	
20.4′	26, 272	28, 256	26.8′	30, 237	
20.8′	29, 265		26.12′	26, 274	
20.9′	30, 236		26.12″	26, 274	
21.5′	28, 244		27.3′	28, 247	
21.11′	28, 244		27.3″	29, 268	
22.4′	28, 244–245		27.4′	28, 248	29, 244–254
22.5′	26, 273	27, 259–260	27.10′	28, 248	
22.5″ (а)	27, 245	28, 259	28.2′	30, 237	
22.5″ (б)	27, 245		28.6′	29, 269	
22.12′	23, 220		28.7′	29, 270–271	
23.2′ (а)	25, 172		28.13′	29, 271	
23.4′	24, 180	25, 163–166;	29.15′ (а)	30, 237	
		29, 232–238	29.15′ (б)	30, 237	
23.4″	25, 172		29.15′ (в)	30, 237	
23.6′	27, 245–246		29.15′ (г)	30, 237	

Опечатки, замеченные в выпуске 29

Страница,	строка	Напечатано	Следует читать
93	4 сверху	Эрнст	Эрнест
93	4 снизу	российской	советской
232	11 сверху	M1254	M1524
260	16 снизу	$3.5'$	$3.5''$
260	10 снизу	$3.5''$	3.5(3)
260	5 снизу	$3.5'''$	3.5(4)
263	2 снизу	$13.6''$	13.6(3)
272	4 снизу	2.10	22.10

Поправка

Как обратил внимание Д. В. Фомин, в 28-м выпуске на с. 32 имеется ошибочная сноска 39. На самом деле В. И. Рыжик был уволен из 239-й школы без связи с упомянутым там случаем, к которому он не имел отношения.

Информация для авторов

1. Сборник «Математическое просвещение» предназначен для широкого круга научных работников, преподавателей, учащихся и всех, кто интересуется математикой. Издание публикует материалы по различным областям математики, а также по проблемам её истории и преподавания, интересные и доступные указанной аудитории.

2. Сборник «Математическое просвещение» не публикует существенно новые научные результаты, оценка которых доступна лишь специалистам в соответствующей области. Не публикуются также материалы по текущим вопросам преподавания математики в учебных заведениях.

3. Материалы принимаются по электронной почте на адрес `matpros@yandex.ru` в виде двух файлов (`pdf` и `tex`) с дополнительными файлами рисунков и т. п., если требуется. Допускается присылка статей, набранных в `Word`.

4. Просим обратить внимание, что материалы принимаются в чёрно-белом исполнении.

5. Просим авторов кратко пояснять в начале статьи, в чём её цель и почему тема статьи представляет интерес.

6. Редакция благодарна авторам за оформление ссылок на литературу как в предыдущих выпусках, см. `http://www.mccme.ru/free-books/matpros.html`

7. В конце статьи необходимо указать для каждого из авторов:

— фамилию, имя, а также отчество (если есть) полностью,

— место работы/обучения,

— электронный адрес для публикации.

8. Авторы задач вместе с условием представляют письменное решение (хотя бы набросок).

9. Авторы опубликованных статей имеют право на 2 экземпляра сборника каждый, просим обращаться по адресу `matpros@yandex.ru`

Научно-популярное издание

Математическое просвещение. Третья серия. Выпуск 30

Издательство Московского центра
непрерывного математического образования

119002, Москва, Большой Власьевский пер., 11. Тел. (499) 241–08–04.

Отпечатано в ООО «Типография „Миттель-Пресс“».
г. Москва, ул. Руставели, д. 14, стр. 6.
Тел./факс +7 (495) 619–08–30, 647–01–89.
E-mail: mittelpress@mail.ru

Подписано в печать 21.11.2022 г. Формат $70\times100\,{}^{1}/_{16}$. Бумага офсетная.
Печать офсетная. Печ. л. 15,5. Тираж 600 экз. Заказ №

В соответствии с Федеральным законом № 436-ФЗ
от 29 декабря 2010 года издание маркируется знаком 6+

Книги издательства МЦНМО можно приобрести
в магазине «Математическая книга»,
Москва, Большой Власьевский пер., 11. Тел. (495) 745–80–31.
E-mail: biblio@mccme.ru, http://biblio.mccme.ru