Библиотека
«Математическое просвещение»
Выпуск 1

В. М. Тихомиров

Великие математики прошлого и их великие теоремы

Издательство Московского центра
непрерывного математического образования
Москва • 1999

Аннотация

В брошюре доказываются замечательные теоремы великих математиков прошлого — Архимеда (теорема об объёме шара), Ферма (теорема о представлении простых чисел в виде суммы двух квадратов натуральных чисел), Эйлера (равенство $e^{\pi i} = -1$), Лагранжа (теорема о представлении любого натурального числа в виде суммы четырёх квадратов целых чисел) и Гаусса (теорема о построении циркулем и линейкой правильного семнадцатиугольника).

Текст брошюры представляет собой обработку лекции, прочитанной автором 30 октября 1999 года на Малом мехмате для школьников 9–11 классов.

Тихомиров Владимир Михайлович

Великие математики прошлого
и их великие теоремы

Главный редактор серии *В. М. Тихомиров.*

Редакторы *Р. М. Кузнец*, *Е. Н. Осьмова.* Техн. редактор *М. Ю. Панов.*

Лицензия ЛР №071150 от 11/IV 1995 г. Подписано к печати 18/XI 1999 г. Формат бумаги 60 × 88 $^1/_{16}$. Физич. печ. л. 1,5. Условн. печ. л. 1,5. Уч.-изд. л. 1,38. Тираж 3000 экз.

Издательство Московского центра непрерывного математического образования. 121002, Москва, Г-2, Бол. Власьевский пер., 11.

Предисловие к серии «Библиотека „Математическое просвещение“»

В этом году исполнилось 65 лет с той поры, когда в Москве началась работа со школьниками, интересующимися математикой. В 1934 году был организован первый математический кружок для школьников, стали регулярно читаться лекции для учащихся старших классов, и начали выходить брошюрки серии «Популярная библиотека по математике». В 1935 году состоялась первая Московская математическая олимпиада. Всё это внесло неоценимый вклад в развитие математики в нашей стране.

В чтении лекций и написании популярных брошюр приняли участие крупнейшие учёные, такие как П. С. Александров, И. М. Гельфанд, Б. Н. Делоне, А. Н. Колмогоров, Л. А. Люстерник, Л. С. Понтрягин, С. Л. Соболев, Л. Г. Шнирельман и другие.

После войны лекции для школьников, читавшиеся крупными учёными и педагогами, возобновились, а в 1950 году стала выходить серия «Популярные лекции по математике». Эти лекции издавали основные издательства нашей страны — сначала Государственное издательство технико-теоретической литературы, а затем — сменившая его Главная редакция физико-математической литературы издательства «Наука». Первая книжка серии — «Возвратные последовательности» А. И. Маркушевича — была издана тиражом 10 тыс. экземпляров. Но серия пользовалась всё бо́льшим и бо́льшим спросом, и книжки этой серии стали печатать тиражом 100, 150, 250 тыс. экземпляров.

В начале девяностых годов издательство «Наука» стало испытывать большие финансовые трудности, и издание «Популярные лекции по математике» прекратило своё существование. И сами лекции для школьников в МГУ не читались уже с давних времён.

Осенью этого года по инициативе Малого мехмата были возобновлены лекции для школьников, которые читаются профессорами и преподавателями Московского университета, известными учёными и педагогами Москвы. Лекции проходят по субботам с 16 до 18 часов в аудитории 16–10 главного здания МГУ. Они посвящены и современной математике, и математике прошлого, но всякий раз — выразительным, красивым и содержательным сюжетам.

Избранные лекции предполагается издать в серии «Библиотека „Математическое просвещение“».

Перед вами — первая брошюра этой серии.

Хочу выразить глубокую признательность директору Московского центра непрерывного математического образования И. В. Ященко за организацию издания новой серии и В. Гуровицу, Р. Кузнецу, Е. Осьмовой, М. Панову за тщательную подготовку рукописей серии к печати.

На долю предыдущих серий популярных книжек по математике выпала счастливая судьба: они украшают библиотеки многих и многих математиков разных поколений, в частности, школьников 30–50-х годов. Они не утратили интереса и для них самих и вызывают интерес у их детей и внуков.

Хотелось бы пожелать новой серии такой же счастливой судьбы.

В. М. Тихомиров

Для этой книги из творчества величайших среди великих — Архимеда, Ферма, Эйлера, Лагранжа и Гаусса — я отобрал или те из их высших достижений, которыми они больше всего гордились сами, или же те, благодаря которым они более всего прославились в научном мире. Я постараюсь доказать эти великие теоремы. Какую цель я этим преследую? Отвечу так: я хотел бы вдохновить вас, своих читателей, на бесстрашие. И пусть каждый, поняв замыслы Богов нашей науки, придя в восхищение от глубины этих замыслов, войдёт в храм науки без робости, не с сознанием своего ничтожества, но с жаждой дерзания.

Архимед и его формула для объёма шара

> Я вдруг обнаружил маленькую колонну, вершина которой поднималась из зарослей. На ней были изображены шар и цилиндр, которые я искал. Я тотчас же сказал сопровождавшим меня, что перед нами, несомненно, могильный памятник Архимеда.
>
> *Цицерон*

Архимед (ок. 287–212 до н. э.) — величайший учёный Древнего мира. Имя его овеяно легендами. Мы восклицаем: «Эврика!» — выражая, как Архимед, восторг по поводу своей удачи. Каждый знает, что он может перевернуть весь Мир, если только найдётся надёжная точка опоры. У каждого перед глазами сцена: убийца с обнажённым мечом и сидящий старец, восклицающий: «Не трогай моих чертежей!»

Архимед общепризнанно считается одним из величайших гениев в истории человечества. Его вклад в математику огромен. Именно он придумал формулу для определения площади треугольника по его сторонам (она известна нам как формула Герона). Не кто иной, как Архимед первый дерзнул исчислить размеры окружающего нас Мира. Он определил границы для числа π, доказав, что

$$3\frac{10}{71} < \pi < 3\frac{1}{7}.$$

Вплотную он подошёл к понятию определённого интеграла, опередив человечество почти на два тысячелетия. Ему первому принадлежат точные формулировки законов природы, сохранившиеся в неприкосновенности на все времена. Но более всего он гордился найденной им формулой объёма шара, и в память об этом потомки изобразили шар и цилиндр на его могильном камне.

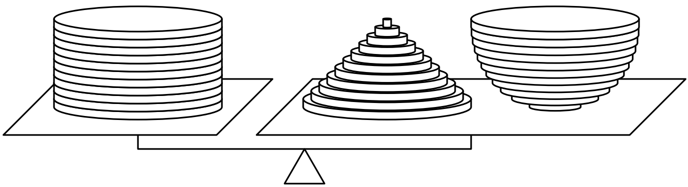
Докажем же, следуя идеям Архимеда, тот результат, который доставил ему высшую творческую радость.

Теорема 1. *Объём шара радиуса* 1 *равен* $\frac{4}{3}\pi$.

Доказательство. Мы будем опираться на следующие две формулы стереометрии: объём цилиндра с радиусом основания R и высотой H равен $\pi R^2 H$, и объём конуса с радиусом основания R и высотой H равен $\dfrac{1}{3}\pi R^2 H$. Эта последняя формула также принадлежит Архимеду.

А теперь перейдём к доказательству. Я надеюсь, вы ещё не забыли детских игрушек, которые называют *пирамидками*. Вот как они устроены: имеются подставка с вертикальной палочкой и набор колечек разного размера. Надо нанизать эти колечки на палочку так, чтобы размеры колечек увеличивались по мере приближения к подставке. Тогда получится фигура, похожая на конус.

Доказательство теоремы Архимеда (по Архимеду) очень легко понять с помощью подобных игрушек. Только надо сделать не одну — коническую, а три разных — цилиндрическую (когда колечки будут иметь радиус 1, сами будут тоненькими-претоненькими, а если собрать их все вместе, то они образуют



цилиндр высоты 1), коническую (из таких же тоненьких колечек, но разных радиусов, из которых можно собрать «почти» конус высоты и радиуса основания, равных 1), и «полушаровую» (опять-таки из таких же тоненьких колечек, из которых можно собрать «почти» полушар радиуса 1). При этом все колечки должны быть сделаны из одинакового материала.

А теперь, вслед за Архимедом, возьмём аптекарские весы с плоскими чашами и поставим на одну чашу собранную из колечек игрушку-цилиндр, а на другую — конус и полушар, причём конус поставим основанием на чашу весов, а полушар — «на голову», чтобы плоское основание полушара было сверху и расположено горизонтально (см. рис. на с. 6).

Пусть высоты колечек одинаковы и равны δ, где δ очень малое число. Подсчитаем, каков объём колечек, находящихся на одной и той же высоте h. У цилиндрического колечка этот объём равен $\pi\delta$, у конического $\pi(1-h)^2\delta$, а у «полушарного» (а как ещё сказать?) $\pi\big(1-(1-h)^2\big)\delta$ (ибо радиус колечка у конуса равен $1-h$, а у полушара, по теореме Пифагора, — $\sqrt{1-(1-h)^2}$). Суммарный объём на каждой из чаш весов оказался одинаковым. Но если δ очень мало, то коническая игрушка будет почти неотличима от конуса, полушаровая — от полушара, а цилиндрическая — всегда цилиндр.

В пределе получаем, что объём полушара радиуса 1 равен объёму цилиндра с радиусом основания и высотой, равными 1, минус объём конуса с радиусом основания и высотой, также равных 1. Откуда и следует теорема 1.

Теорема Ферма—Эйлера о представлении простых чисел в виде суммы двух квадратов

> Быть может, потомство будет признательно мне
> за то, что я показал ему, что Древние знали не всё.
> *Пьер Ферма*

Лишь один математик удостоился того, что имя его стало нарицательным. Если произносится слово «ферматист», значит, речь идёт о человеке, одержимом до безумия какой-то несбыточной идеей. Но это слово ни в какой мере не может быть отнесено к самому Пьеру Ферма (1601–1665), одному из самых светлых умов Франции.

Ферма — человек удивительной судьбы: один из величайших математиков всех времён, он не был, в современной терминологии, «профессиональным» математиком. По профессии Ферма был юристом. Он получил великолепное гуманитарное образование и был выдающимся знатоком искусства и литературы. Всю жизнь он проработал на государственной службе, последние 17 лет был советником местного парламента в Тулузе.

К математике его влекла бескорыстная и возвышенная любовь (это иногда случается с людьми), и именно эта наука дала ему всё, что может дать человеку любовь: упоение красотой, наслаждение и счастье. В те годы не было ещё математических журналов, и Ферма почти ничего не напечатал при жизни. Но он много переписывался со своими современниками, и посредством этой переписки некоторые его достижения становились известными. Пьеру Ферма повезло с детьми: сын обработал архив отца и издал его.

«Я доказал много исключительно красивых теорем», — сказал как-то Ферма. Особенно много красивых фактов удалось ему обнаружить в теории чисел, которую, собственно, он и основал.

В бумагах и в переписке Ферма было сформулировано немало замечательных утверждений, о которых он писал, что располагает их доказательством. И постепенно, год за годом, таких недоказанных утверждений становилось всё меньше и меньше. И наконец, осталось только одно.

Хорошо известно, что квадраты некоторых чисел можно разложить в сумму двух квадратов. Таков египетский треугольник со сторонами 3, 4 и 5: $3^2 + 4^2 = 5^2$. Можно описать все целочисленные решения уравнения $x^2 + y^2 = z^2$. Это было сделано Диофантом, греческим математиком, жившим (вероятно) в III веке нашей эры, во второй книге его трактата «Арифметика» (до нас дошли 6 книг из 13). На полях около решения Диофанта Ферма написал: «Нельзя разложить куб на два куба, ни квадрато-квадрат (т. е. четвёртую степень числа) на два квадрато-квадрата, ни вообще никакую степень выше квадрата и до бесконечности нельзя разложить на две степени с тем же показателем. Я открыл этому поистине чудесное доказательство, но эти поля для него слишком узки». Иначе говоря, уравнение $x^n + y^n = z^n$ при натуральном $n > 2$ в целых числах неразрешимо.

В бумагах Ферма было найдено доказательство этого утверждения для $n = 4$ (это единственное подробное доказательство теоремы из теории чисел, обнаруженное в бумагах

Ферма). Для $n = 3$ теорему Ферма доказал Эйлер в 1768 году. В течение XIX века для доказательства теоремы Ферма были предприняты огромные усилия. Особенных успехов добился немецкий математик Куммер. После его работ теорема Ферма оказалась доказанной для всех простых n (а доказать её только для них), меньших 100, кроме 37, 59 и 97. В нашем веке теорема Ферма была доказана для простых чисел, меньших 100 000, но окончательное решение так и не было найдено.

В 1908 году любитель математики Вольфскель завещал 100 000 марок тому, кто докажет теорему Ферма. Это стало бедствием для математиков многих стран. Потекли сотни и тысячи писем с доказательствами теоремы Ферма. Как правило, они содержали элементарные ошибки, но на их нахождение тратились немалые силы многих математиков.

Во время Первой мировой войны эта премия обесценилась. Поток псевдодоказательств сократился, но не иссяк.

И уже казалось, что эта проблема перейдёт через новую грань веков, но всё-таки пять лет тому назад английский математик Уайлс «залатал последнюю дыру» в своём доказательстве этой великой теоремы, с которым он впервые предстал перед математическим миром в 1993 году.

Мир признал: Великая теорема Ферма доказана!

Однако, тем, кто интересуется математикой, имя Ферма говорит очень многое независимо от его Великой теоремы. Он был, без всякого сомнения, одним из самых проницательных умов своего времени — времени Гигантов. Его по праву считают основоположником теории чисел, он внёс огромный вклад в зарождающиеся новые направления, определившие последующее развитие науки: математический анализ и аналитическую геометрию. Мы признательны Ферма за то, что он приоткрыл для нас мир, полный красоты и загадочности.

Следующая теорема, несомненно, принадлежит к числу высших достижений математики XVII–XVIII веков.

Взгляните на несколько первых нечётных простых чисел:

$$3, \quad 5, \quad 7, \quad 11, \quad 13, \quad 17, \quad 19, \quad \ldots$$

Числа 5, 13, 17 представимы в виде суммы двух квадратов: $5 = 2^2 + 1^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, а остальные числа (3, 7, 11, 19) этим свойством не обладают. Можно ли объяснить этот феномен? Ответ на этот вопрос даёт

Теорема 2. *Для того чтобы нечётное простое число было представимо в виде суммы двух квадратов, необходимо и достаточно, чтобы оно при делении на* 4 *давало в остатке* 1.

Немного истории

На Рождество 1640 года в письме от 25 декабря Пьер Ферма извещал знаменитого Мерсенна, друга Декарта и главного посредника в переписке учёных того времени, о том, что «всякое простое число, которое при делении на четыре даёт единицу, единственным способом представимо как сумма двух квадратов».

В ту пору математических журналов ещё не существовало, информацией обменивались в письмах, и как правило, результаты лишь анонсировались, но не сопровождались детальными доказательствами.

Правда, спустя почти двадцать лет после письма Мерсенну в письме к Каркави, отправленном в августе 1659 года, Ферма приоткрывает замысел доказательства сформулированной выше теоремы. Он пишет, что основная идея доказательства состоит в *методе спуска*, позволяющем из предположения, что для какого-то простого числа вида $4n+1$ заключение теоремы неверно, получить, что оно неверно и для меньшего числа того же и т. д., пока мы не доберёмся до числа 5, когда окончательно придём к противоречию.

Первые доказательства, которые впоследствии были опубликованы, найдены Эйлером между 1742 и 1747 годами. Причём, желая утвердить приоритет Ферма, к которому он испытывал чувства глубочайшего уважения, Эйлер придумал доказательство, соответствующее описанному выше замыслу Ферма.

Воздавая должное обоим великим учёным (об Эйлере речь ещё впереди), мы называем эту теорему *теоремой Ферма—Эйлера*.

Есть свойство, присущее почти всякому прекрасному математическому результату, равно как и почти всякой неприступной и прекрасной горной вершине: его можно штурмовать с разных сторон, и все пути доставляют наслаждение тому, кто не устрашится ими последовать.

В своей статье в «Кванте» [2] я привёл три совершенно различных доказательства. Одно из них (принадлежащее Лагранжу) было придумано в XVIII веке, другое — Германа Минковского — в XIX веке, а третье — нашим современником Даном Цагиром. Но здесь нет возможности воспроизвести их все, и я ограничусь лишь первым из названных.

Доказательство Лагранжа

Это доказательство опирается на следующую *лемму Вильсона*: если p — простое число, то число $(p-1)!+1$ делится на p.

Чтобы не отвлекаться на доказательство этого вспомогательного факта, продемонстрирую лишь основную идею этого доказательства на примере простого числа 13. Для любого числа x, $2 \leqslant x \leqslant 11$, найдётся такое число y, $2 \leqslant y \leqslant 11$, что $x \cdot y$ при делении на 13 даёт в остатке 1. Действительно,

$$(13-1)! = 12! = (2\cdot 7)(3\cdot 9)(4\cdot 10)(5\cdot 8)(6\cdot 11)\cdot 12,$$

и при этом все произведения в скобках при делении на 13 дают в остатке 1, а значит, 12! при делении на 13 даст в остатке 12, откуда (для выбранного нами числа 13) следует утверждение леммы Вильсона.

Из леммы Вильсона извлечём такое следствие: если $p = 4n+1$, где n — натуральное число, то $\big((2n)!\big)^2+1$ делится на p. Действительно, из леммы Вильсона следует, что $(4n)!+1$ делится на p, и теперь необходимое утверждение вытекает из следующей выкладки:

$$\begin{aligned}(4n)!+1 &= (2n)!\,(2n+1)\cdot\ldots\cdot(4n)+1 =\\ &= (2n)!\,(p-2n)(p-2n-1)\cdot\ldots\cdot(p-1)+1 =\\ &= (2n)!\,(-1)^{2n}(2n)!+pk+1 \equiv \big((2n)!\big)^2+1 \pmod p.\end{aligned}$$

Обозначим $(2n)!$ через N. Мы доказали, что $N^2 \equiv -1 \pmod p$.

Теперь нам предстоит преодолеть основную трудность. Рассмотрим все пары целых чисел (m, s), такие что $0 \leqslant m \leqslant \leqslant [\sqrt{p}]$, $0 \leqslant s \leqslant [\sqrt{p}]$, через $[\sqrt{p}]$ обозначена целая часть числа $\sqrt{p}$ — наибольшее целое число, не превосходящее $\sqrt{p}$. Число таких пар $([\sqrt{p}]+1)^2 > p$. Значит, по крайней мере для двух *различных* пар (m_1, s_1) и (m_2, s_2) остатки от деления $m_1 + Ns_1$ и $m_2 + Ns_2$ на p одинаковы, т. е. число $a + Nb$, где $a = m_1 - m_2$, $b = s_1 - s_2$, будет делиться на p. При этом $|a| \leqslant [\sqrt{p}]$, $|b| \leqslant [\sqrt{p}]$. Но тогда число $a^2 - N^2b^2 = = (a + Nb)(a - Nb)$ делится на p, и значит, учитывая, что $N^2 \equiv -1 \pmod p$, получим, что $a^2 + b^2$ делится на p, т. е. $a^2 + b^2 = rp$, где r — натуральное число ($r \neq 0$, ибо иначе пары были бы одинаковы). С другой стороны, $a^2 + b^2 \leqslant 2[\sqrt{p}]^2 < < 2p$, т. е. $r = 1$, и значит, $a^2 + b^2 = p$. Теорема 2 доказана.

Вопрос о представлении чисел в виде суммы двух квадратов исчерпывается следующим утверждением:

Натуральное число представимо в виде суммы двух квадратов целых чисел тогда и только тогда, когда все простые сомножители вида $4k + 3$ входят в разложение этого числа на простые сомножители с чётными показателями. (См. [3, с. 45].)

Теорема Ферма—Эйлера очень красиво доказывается, если использовать теорию делимости целых коплексных чисел $n + mi$, n, m — целые (см. об этом в замечательной книге [4, с. 28–29]).

Эйлер и его формула $e^{\pi i} = -1$

Его [Эйлера] творчество изумительно и в науке беспримерно.

А. Н. Крылов

Однажды, когда я учился в восьмом классе, мой друг и одноклассник написал мне формулу Эйлера, которой я посвящаю этот раздел. Тогда я уже знал, что e — это число: две целых, семь десятых, год рождения Толстого, год рождения Толстого и дальше — другие десятичные знаки, запоминать которые уже необязательно ($e = 2{,}718281828\ldots$). Я знал также, что

$$e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n .$$

Разумеется, я имел представление о числе π, о том, что такое степень и, слышал о том, что i — это какое-то мистическое число, квадрат которого равен -1. Формула Эйлера потрясла меня, как, пожалуй, ничто математическое не потрясало ни до, ни после. Эта формула восхищала не одного меня. Наш знаменитый академик, математик и кораблестроитель Алексей Николаевич Крылов, слова которого я поставил эпиграфом к этому разделу, видел в этой формуле символ единства всей математики, ибо в ней «-1 представляет арифметику, i — алгебру, π — геометрию и e — анализ».

Можно очень многое сказать о творце этой формулы Леонарде Эйлере (1707–1783) — гениальном математике, физике, механике и астрономе, прожившем значительную часть своей жизни в России и похороненном в Санкт-Петербурге.

Леонард Эйлер — один из величайших тружеников в истории науки. Ему принадлежит 865 исследований по самым разнообразным проблемам. В 1909 году швейцарское естественнонаучное общество приступило к изданию полного собрания сочинений Эйлера. С тех пор прошёл срок, бо́льший, чем вся жизнь Эйлера, издано около семидесяти томов его сочинений, а издание ещё не закончено.

Переписка Эйлера занимает свыше 3000 писем. Уже одно это — свидетельство необыкновенного нравственного облика учёного: дурным людям писем не пишут. Все учёные, современники Эйлера, делились с ним плодами своих размышлений, просили высказать своё суждение по интересующим их проблемам и всегда находили отклик и поддержку.

Необыкновенные щедрость и благородство Эйлера отразились в известной шутке, касающейся самого определения — кого следует называть математиком. Определение математика (согласно этой шутке) индуктивно. Основание индукции составляет утверждение: Эйлер — математик. И далее:

математиком называется человек, которого математик называет математиком.*

Душевная красота Эйлера отразилась во множестве его поступков. В предыдущем разделе я рассказывал о том, как Эйлер старался утвердить приоритет Ферма. Когда молодой Лагранж (о нём речь впереди) посвятил Эйлера в свои исследования в области вариационного исчисления, Эйлер направил ему письмо (от 2 декабря 1759 года, Лагранжу было тогда 23 года), и я не могу не привести его слова, слова высокого духовного благородства.

«Твоё аналитическое решение изопериметрической проблемы содержит, насколько я вижу, всё, что только можно желать в этой области, и я чрезвычайно рад, что эта теория, которой после моих первых попыток я занимался едва ли не один, доведена до величайшего совершенства. Важность вопроса побудила меня к тому, что я с помощью твоего освещения сам вывел аналитическое решение; я, однако, решил скрывать это, пока ты не опубликуешь свои результаты, так как я никоим образом не хочу отнимать часть заслуженной тобою славы».

Теорема 3. $e^{\pi i} = -1$.

Доказательство. **3.1.** При доказательстве мы будем использовать следующую формулу (она носит название *бином Ньютона*):

$$(a+b)^n = a^n + C_n^1 a^{n-1} b + C_n^2 a^{n-2} b^2 + C_n^3 a^{n-3} b^3 + \ldots \\ \ldots + C_n^{n-2} a^2 b^{n-2} + C_n^{n-1} a^{n-1} b + b^n,$$

где n — натуральное число, $C_n^k = \dfrac{n!}{k!\,(n-k)!}$.

* При этом, можно быть почти уверенным, что человек, сделавший в математике что-то содержательное, будет математиком в смысле этого определения. Но если в качестве основания брать других учёных, то нельзя исключить случая, когда список математиков состоял бы только из одного лица...

3.2. Как известно,

$$e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n.$$

Применим формулу бинома Ньютона:

$$\left(1+\frac{1}{n}\right)^n = 1+\frac{n}{1!}\cdot\frac{1}{n}+\frac{n(n-1)}{2!}\cdot\frac{1}{n^2}+\frac{n(n-1)(n-2)}{3!}\cdot\frac{1}{n^3}+\ldots$$

(здесь мы выписали только несколько первых членов разложения).

Перейдём в обеих частях равенства к пределу при $n \to \infty$ и получим следующее *разложение в ряд*:

$$e = 1+\frac{1}{1!}+\frac{1}{2!}+\frac{1}{3!}+\ldots$$

Конечно, с точки зрения современного математика, этот предельный переход необходимо строго обосновать. Но во времена Эйлера к вопросу о правомерности преобразований подходили довольно свободно. Сам Эйлер в подобных случаях поступал очень смело и практически всегда оказывался прав.

Рассуждая аналогично, можно получить разложение

$$e^x = \lim_{n\to\infty}\left(1+\frac{x}{n}\right)^n = 1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\ldots = \sum_{k=0}^{\infty}\frac{x^k}{k!}.$$

Это разложение впервые было получено именно Эйлером, и в его честь число e получило своё обозначение: e есть первая буква фамилии Euler.

Функция e^x обладает многими замечательными свойствами. В частности, все её производные в точке 0 равны 1.

3.3. Воспользуемся *формулой Тейлора*

$$f(x) = f(0)+\frac{f'(0)}{1!}x+\frac{f''(0)}{2!}x^2+\frac{f'''(0)}{3!}x^3+\ldots,$$

чтобы разложить в ряд функции $\sin x$ и $\cos x$.

Поскольку $(\sin x)' = \cos x$, $(\cos x)' = -\sin x$, получаем, что

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \ldots, \qquad \cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \ldots$$

3.4. Гениальная идея Эйлера состоит в том, что формулу для e^x можно применять не только к действительным, но и к комплексным числам:

$$e^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \frac{z^4}{4!} + \frac{z^5}{5!} + \ldots,$$

где z — произвольное комплексное число.

Подставим в эту формулу $z = \pi i$ (где i — мнимая единица, т. е. $i^2 = -1$):

$$\begin{aligned} e^{\pi i} &= 1 + \pi i + \frac{(\pi i)^2}{2!} + \frac{(\pi i)^3}{3!} + \frac{(\pi i)^4}{4!} + \frac{(\pi i)^5}{5!} + \ldots = \\ &= 1 + \pi i - \frac{\pi^2}{2!} - \frac{\pi^3}{3!} i + \frac{\pi^4}{4!} + \frac{\pi^5}{5!} i - \ldots = \\ &= \left(1 - \frac{\pi^2}{2!} + \frac{\pi^4}{4!} - \ldots\right) + i\left(\pi - \frac{\pi^3}{3!} + \frac{\pi^5}{5!} - \ldots\right) = \\ &= \cos\pi + i\sin\pi = -1. \end{aligned}$$

Теорема 3 доказана.

Позднее, когда появилась строгая теория рядов, подобные выводы, восходящие к Эйлеру, были подтверждены, а все преобразования признаны законными.

Лагранж и его теорема о четырёх квадратах

Эта теорема [о четырёх квадратах] до сих пор входит в число величайших достижений математики.

М. Кац, С. Улам

Жозеф Луи Лагранж (1736–1813) родился в Турине, а умер и похоронен в Париже. В его жилах текла французская и итальянская кровь, и поэтому обе нации могут гордиться человеком, который (по словам Талейрана) сделал своим гением честь всему человечеству.

По своим научным установкам Лагранж отличался от своего старшего великого современника — Леонарда Эйлера. Эйлер в течение своей жизни решал и решил огромнейшее, невиданное, ни с чем не сравнимое число отдельных, конкретных задач, и в большинстве своём каждую задачу он решал своим, особым, индивидуальным приёмом. Лагранж же старался отыскать общие закономерности у разнородных явлений, найти потаённые связи между отдельными объектами, вскрыть единство казалось бы несоединимого. Но при всём при том ему принадлежит также и множество замечательных конкретных результатов. Об одном из них — о представлении натуральных чисел в виде суммы четырёх квадратов — и будет сейчас рассказано.

Лагранж остался в благодарной памяти всего человечества как светлая, благородная личность. Вот как характеризует его Фурье: «Лагранж был столько же философ, сколько математик. Он доказал это своей жизнью, умеренностью желаний земных благ, глубокой преданностью общим интересам человечества, благородной простотой своих привычек, возвышенностью души и глубокой справедливостью в оценке трудов своих современников».

А теперь перейдём к формулировке и доказательству теоремы Лагранжа.

Теорема 4. *Всякое натуральное число есть сумма четырёх квадратов целых чисел.*

Доказательство. **4.1. Лемма.** Произведение чисел, представимых в виде суммы четырёх квадратов, есть сумма четырёх квадратов.

Доказательство леммы.

$$
\begin{aligned}
&(n_1^2+n_2^2+n_3^2+n_4^2)(m_1^2+m_2^2+m_3^2+m_4^2) = \\
&\qquad = (n_1m_1+n_2m_2+n_3m_3+n_4m_4)^2 + \\
&\qquad + (-n_1m_2+n_2m_1-n_3m_4+n_4m_3)^2 + \\
&\qquad + (-n_1m_3+n_3m_1-n_4m_2+n_2m_4)^2 + \\
&\qquad\qquad + (-n_1m_4+n_4m_1-n_2m_3+n_3m_2)^2.
\end{aligned}
$$

Лемма 4.1 доказана.

4.2. Лемма. Для любого простого числа $p > 2$ найдётся число $m \in \mathbb{N}$, $m < p$, такое что $mp = a^2 + b^2 + c^2$, $a, b, c \in \mathbb{Z}$.

Доказательство леммы. Рассмотрим два множества чисел:

$$K = \left\{0,\ 1,\ 4,\ \ldots,\ \left(\frac{p-1}{2}\right)^2\right\},$$

$$L = \left\{-1-0,\ -1-1,\ -1-4,\ \ldots,\ -1-\left(\frac{p-1}{2}\right)^2\right\}.$$

В каждом из множеств числа попарно не сравнимы по модулю p. В самом деле, возьмём $k_1^2 \neq k_2^2$ из множества K (или, эквивалентно, $-1-k_1^2 \neq -1-k_2^2$ из множества L), где $0 \leqslant k_1 \leqslant \left(\frac{p-1}{2}\right)$, $0 \leqslant k_2 \leqslant \left(\frac{p-1}{2}\right)$. Если $k_1^2 \equiv k_2^2 \pmod p$, то $(k_1+k_2)(k_1-k_2) \equiv 0 \pmod p$. Но $0 < k_1 + k_2 < p$ и $0 < |k_1 - k_2| < p$, поскольку $k_1 < \frac{p}{2}$, $k_2 < \frac{p}{2}$ и $k_1 \neq k_2$. Противоречие.

Всего в этих двух множествах $p+1$ чисел, следовательно, среди них найдутся сравнимые по модулю p, т. е. такие числа $\varkappa^2$ из первого множества и $-1-\lambda^2$ из второго, что

$$\varkappa^2 \equiv -1-\lambda^2 \pmod p.$$

Откуда $\varkappa^2 + \lambda^2 + 1 = mp$ для некоторого $m \in \mathbb{N}$.

Теперь, поскольку $\varkappa < \frac{p}{2}$ и $\lambda < \frac{p}{2}$, получаем $mp = \varkappa^2 + \lambda^2 + 1 < \frac{p^2}{4} + \frac{p^2}{4} + 1 < p^2$, а значит, $m < p$. Лемма 4.2 доказана.

4.3. Докажем, что любое простое число представимо в виде суммы четырёх квадратов целых чисел. Для $p = 2$ имеем $2 = 1^2 + 1^2 + 0^2 + 0^2$. Для $p > 2$, по предыдущей лемме, найдётся такое $m < p$, что число mp можно представить в виде $mp = n_1^2 + n_2^2 + n_3^2 + n_4^2$ (n_4 можно положить равным 0). Выберем теперь *минимальное* натуальное m, обладающее таким свойством. Покажем, что оно равно 1.

Пусть m чётно. Тогда либо все n_i имеют одинаковую чётность, либо среди них есть два чётных и два нечётных (нумерация этих чисел не важна, поэтому пусть $n_1 \equiv n_2 \pmod 2$, а $n_3 \equiv n_4 \pmod 2$). В обоих случаях числа

$$\frac{n_1+n_2}{2}, \quad \frac{n_1-n_2}{2}, \quad \frac{n_3+n_4}{2}, \quad \frac{n_3-n_4}{2}$$

являются целыми. Имеем:

$$\left(\frac{n_1+n_2}{2}\right)^2 + \left(\frac{n_1-n_2}{2}\right)^2 + \left(\frac{n_3+n_4}{2}\right)^2 + \left(\frac{n_3-n_4}{2}\right)^2 = \\ = \frac{n_1^2+n_2^2+n_3^2+n_4^2}{2} = \frac{m}{2}p,$$

значит, $\frac{m}{2}p$ также представляется в виде суммы четырёх квадратов целых чисел. Но $\frac{m}{2} < m$, а m, по предположению, минимальное число с таким свойством. Противоречие.

Пусть m нечётно. Тогда числа n_i можно представить в виде $n_i = q_i m + m_i$ (q_i, $m_i \in \mathbb{Z}$), причём $|m_i| < \frac{m}{2}$. Тогда

$$mp = n_1^2+n_2^2+n_3^2+n_4^2 = sm + m_1^2+m_2^2+m_3^2+m_4^2,$$

где s — некоторое целое число. Следовательно, $m_1^2+m_2^2+ m_3^2+m_4^2 = nm$, где n — неотрицательное целое число. Если $n = 0$, то $m_i = 0$, $n_i = q_i m$ для всех i, и тогда $mp = n_1^2+n_2^2+ n_3^2+n_4^2 = m^2k$, где k — натуральное, т. е. $p = mk$, $m < p$, а это означает, что $m = 1$. Предположим теперь, что $n \geqslant 1$.

Из леммы 4.1 получаем:

$$(n_1^2+n_2^2+n_3^2+n_4^2)(m_1^2+m_2^2+m_3^2+m_4^2) = s_1^2+s_2^2+s_3^2+s_4^2,$$

где

$$\begin{aligned}
s_1 &= n_1m_1+n_2m_2+n_3m_3+n_4m_4,\\
s_2 &= -n_1m_2+n_2m_1-n_3m_4+n_4m_3,\\
s_3 &= -n_1m_3+n_3m_1-n_4m_2+n_2m_4,\\
s_4 &= -n_1m_4+n_4m_1-n_2m_3+n_3m_2.
\end{aligned}$$

По определению, $m_i \equiv n_i \pmod{m}$, т. е. $s_1 \equiv m_1^2 + m_2^2 + m_3^2 + m_4^2 \equiv 0 \pmod{m}$ и, значит, $\frac{s_1}{m} \in \mathbb{Z}$. Аналогично доказывается, что $\frac{s_i}{m} \in \mathbb{Z}$ при $i = 2, 3, 4$. Но тогда $\left(\text{в силу неравенств } |m_i| < \frac{m}{2}\right)$ получаем: $nm = m_1^2 + m_2^2 + m_3^2 + m_4^2 < m^2$, т. е. $n < m$, и в итоге

$$mp \cdot nm = s_1^2 + s_2^2 + s_3^2 + s_4^2,$$

откуда

$$np = \left(\frac{s_1}{m}\right)^2 + \left(\frac{s_2}{m}\right)^2 + \left(\frac{s_3}{m}\right)^2 + \left(\frac{s_4}{m}\right)^2,$$

что противоречит минимальности m.

Итак, всякое простое число можно представить в виде суммы четырёх квадратов целых чисел. Тогда, по лемме 4.1, и любое составное число представимо в таком виде. Наконец, $1 = 1^2 + 0^2 + 0^2 + 0^2$. Теорема 4 доказана.

После теоремы Ферма—Эйлера мы описали все числа, представимые в виде суммы двух квадратов. Теорема Лагранжа утверждает, что все натуральные числа представимы в виде суммы четырёх квадратов. Числа, представимые в виде суммы трёх квадратов описал Гаусс в 1801 году. О нём — следующий рассказ.

Гаусс и его теорема о семнадцатиугольнике

> Подобно Архимеду Гаусс выразил желание, чтобы на его могиле был увековечен семнадцатиугольник.
>
> *Г. Вебер*

Так же как в литературе Гомер, Данте, Шекспир, Гёте, Толстой и Достоевский, так в математическом естествознании Архимед, Ньютон, Эйлер, Гаусс, Риман и Пуанкаре — высочайшие вершины, соединение гениальности и всеохватности.

Карл Фридрих Гаусс (1777–1855) — математик, чьё имя, как и имя Архимеда, овеяно легендами. Многие его высказывания вошли в поговорку. Часто вспоминают его девиз:

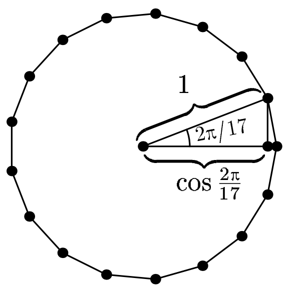
«Nilactum reputans si quid superesset agendum»*. В этой личности счастливо сплелись могучий интеллект, сильный характер и любознательность естествоиспытателя. При жизни Гаусс был признан величайшим и коронован титулом «Mathematicorum Princeps»**. Хвала его гению и блистательный обзор творчества Гаусса содержится в книге [3].

«Математическая деятельность Гаусса, — пишет Феликс Клейн, — началась одним крупным открытием, которое привело его к твёрдому убеждению навсегда посвятить себя науке... 30 марта 1796 года ему — девятнадцатилетнему — удалось показать, что правильный семнадцатиугольник может быть построен с помощью циркуля и линейки», т. е. совершить прорыв в проблеме, где не было никакого прогресса в течение свыше 2000 лет.

Потомки постарались выполнить завещание великого учёного. Они воздвигли ему памятник (на родине, в Брауншвейге), который стоит на постаменте, являющемся правильным семнадцатиугольником. Но если не знать этого, то и не заметишь: правильный семнадцатиугольник почти неотличим от круга.

Теорема 5. *Правильный семнадцатиугольник может быть построен с помощью циркуля и линейки.*

Приводимое доказательство — лишь незначительная обработка доказательства самого Гаусса.



Доказательство. **5.1.** Для построения правильного семнадцатиугольника, вписанного в окружность радиуса 1, достаточно построить отрезок длины $\cos\dfrac{2\pi}{17}$ (см. рис.). Дальнейшая последовательность действий не вызывает трудностей. Однако для этого построения нам потребуются некоторые соотношения в комплексных числах.

* Что не завершено, не сделано вовсе (*лат.*).

** Король математиков (*лат.*).

5.2. Обозначим через ε один из комплексных корень семнадцатой степени из единицы:

$$\varepsilon = \sqrt[17]{1} = e^{2\pi i/17} = \cos\frac{2\pi}{17} + i\sin\frac{2\pi}{17}.$$

Введём обозначения:

$$z_1 = \varepsilon + \varepsilon^{-1}, \qquad \zeta_1 = \varepsilon^2 + \varepsilon^{-2}, \qquad y_1 = z_1 + z_2,$$
$$z_2 = \varepsilon^4 + \varepsilon^{-4}, \qquad \zeta_2 = \varepsilon^8 + \varepsilon^{-8}, \qquad y_3 = z_1 z_2,$$
$$y_2 = \zeta_1 + \zeta_2, \qquad x_1 = y_1 + y_2,$$
$$y_4 = \zeta_1\zeta_2, \qquad x_2 = y_3 + y_4.$$

Заметим, что все эти числа действительные. В самом деле,

$$\varepsilon^k + \varepsilon^{-k} = \left(\cos\frac{2\pi k}{17} + i\sin\frac{2\pi k}{17}\right) + \left(\cos\frac{-2\pi k}{17} + i\sin\frac{-2\pi k}{17}\right) = 2\cos\frac{2\pi k}{17}.$$

Поскольку $z_1 = 2\cos\frac{2\pi}{17}$, нам достаточно построить отрезок длины z_1.

5.3. Лемма. $\varepsilon^k = \varepsilon^{17+k}$ при целых k.

Доказательство леммы. Действительно,

$$\varepsilon^{17+k} = \cos\frac{2\pi(17+k)}{17} + i\sin\frac{2\pi(17+k)}{17} = \cos\left(2\pi + \frac{2\pi k}{17}\right) + i\sin\left(2\pi + \frac{2\pi k}{17}\right) = \cos\frac{2\pi k}{17} + i\sin\frac{2\pi k}{17} = \varepsilon^k.$$

5.4. Лемма. $\sum\limits_{k=0}^{16} \varepsilon^k = 0.$

Доказательство леммы. По формуле суммы геометрической прогрессии (которая, конечно, верна и для комплексных чисел) получаем:

$$\sum_{k=0}^{16} \varepsilon^k = \frac{\varepsilon^{17}-1}{\varepsilon-1} = 0.$$

Следствие. $\sum\limits_{k=1}^{16} \varepsilon^k = -1.$

Доказательство следствия. $\sum\limits_{k=1}^{16} \varepsilon^k = \left(\sum\limits_{k=0}^{16} \varepsilon^k\right) - \varepsilon^0 = 0 - 1 = -1.$

Следствие. $\sum\limits_{k=1}^{8} (\varepsilon^k + \varepsilon^{-k}) = -1.$

5.5. Лемма. $y_1 y_2 = y_3 y_4 = -1.$

Доказательство леммы.

$$\begin{aligned} y_1 y_2 &= (\varepsilon + \varepsilon^{-1} + \varepsilon^4 + \varepsilon^{-4})(\varepsilon^2 + \varepsilon^{-2} + \varepsilon^8 + \varepsilon^{-8}) = \\ &= \varepsilon^3 + \varepsilon^{-1} + \varepsilon^9 + \varepsilon^{-7} + \varepsilon^1 + \varepsilon^{-3} + \varepsilon^7 + \varepsilon^{-9} + \varepsilon^6 + \\ &\qquad + \varepsilon^2 + \varepsilon^{12} + \varepsilon^{-4} + \varepsilon^{-2} + \varepsilon^{-6} + \varepsilon^4 + \varepsilon^{-12} = \\ &= \sum_{k=1}^{8} (\varepsilon^k + \varepsilon^{-k}) = -1. \end{aligned}$$

Аналогичная выкладка показывает, что $y_3 y_4 = -1$.

5.6. Лемма. $x_1 + x_2 = -1$, $x_1 x_2 = -4$.

5.7. Напомним, что если заданы отрезки длины 1, $|p|$, и $|q|$, то циркулем и линейкой можно построить отрезки, длины которых равны абсолютной величине корней квадратного уравнения $x^2 + px + q = 0$ (если корни этого уравнения действительны).

Поскольку $x_1 + x_2 = -1$, $x_1 x_2 = -4$, то по теореме Виета x_1 и x_2 — корни уравнения $x^2 + x - 4 = 0$, а значит, мы можем построить отрезки длины $|x_1|$ и $|x_2|$.

Теперь, так как $y_1 + y_2 = x_1$ и $y_1 y_2 = -1$, можно построить отрезки длины $|y_1|$ и $|y_2|$. Из равенств $y_3 + y_4 = x_2$ и $y_3 y_4 = -1$ получаем отрезки длины $|y_3|$ и $|y_4|$. И наконец, используя равенства $z_1 + z_2 = y_1$ и $z_1 z_2 = y_3$, мы можем построить отрезок длины z_1, а следовательно, и правильный семнадцатиугольник.

Воспользовавшись этим рассуждением, можно получить следующее выражение для $\cos\frac{2\pi}{17}$:

$$\cos\frac{2\pi}{17} = \frac{1}{16}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+\right.$$
$$\left.+\sqrt{68+12\sqrt{17}-16\sqrt{34+2\sqrt{17}}-2\left(1-\sqrt{17}\right)\sqrt{34-2\sqrt{17}}}\right).$$

Впоследствии было доказано, что правильный n-угольник можно построить циркулем и линейкой тогда и только тогда, когда $n = 2^k F_1 F_2 \cdot \ldots \cdot F_k$, где все F_i — простые числа вида $2^{2^s}+1$ (числа Ферма). У Ферма было подозрение, что все числа вида $2^{2^s}+1$ — простые. Эйлер опроверг это утверждение, указав, что число

$$2^{2^5}+1 = 4\,294\,967\,297$$

имеет простым делителем 641. В наш компьютерный век стало возможным исследовать на простоту достаточно большие числа, но пока ни одного простого числа Ферма, кроме 5, 17, 257 и 65 537, не найдено.

Литература

[1] *Клейн Ф.* Лекции о развитии математики в XIX столетии. М.: Наука, 1989.

[2] *Тихомиров В. М.* Теорема Ферма—Эйлера о двух квадратах. Квант, №10, 1991.

[3] *Чандрасекхаран К.* Введение в аналитическую теорию чисел. М.: Мир, 1974.

[4] *Шнирельман Л. Г.* Простые числа. М.: ГИТТЛ, 1940.