

Великие математики прошлого и их великие теоремы

В. ТИХОМИРОВ

Лагранж и его теорема о четырех квадратах

Эта теорема 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 огромное, невиданное, ни с чем не сравнимое

Окончание. Начало см. в «Кванте» №2.

число отдельных, конкретных задач, и в большинстве своем каждую задачу он решал своим, особым, индивидуальным приемом. Лагранж же старался отыскать общие закономерности у разнородных явлений, найти потаенные связи между отдельными объектами, вскрыть единство казалось бы несоединимого. Но при всем при том ему принадлежит также и множество замечательных конкретных результатов. Об одном из них – о представлении натуральных чисел в виде суммы четырех 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 зем-

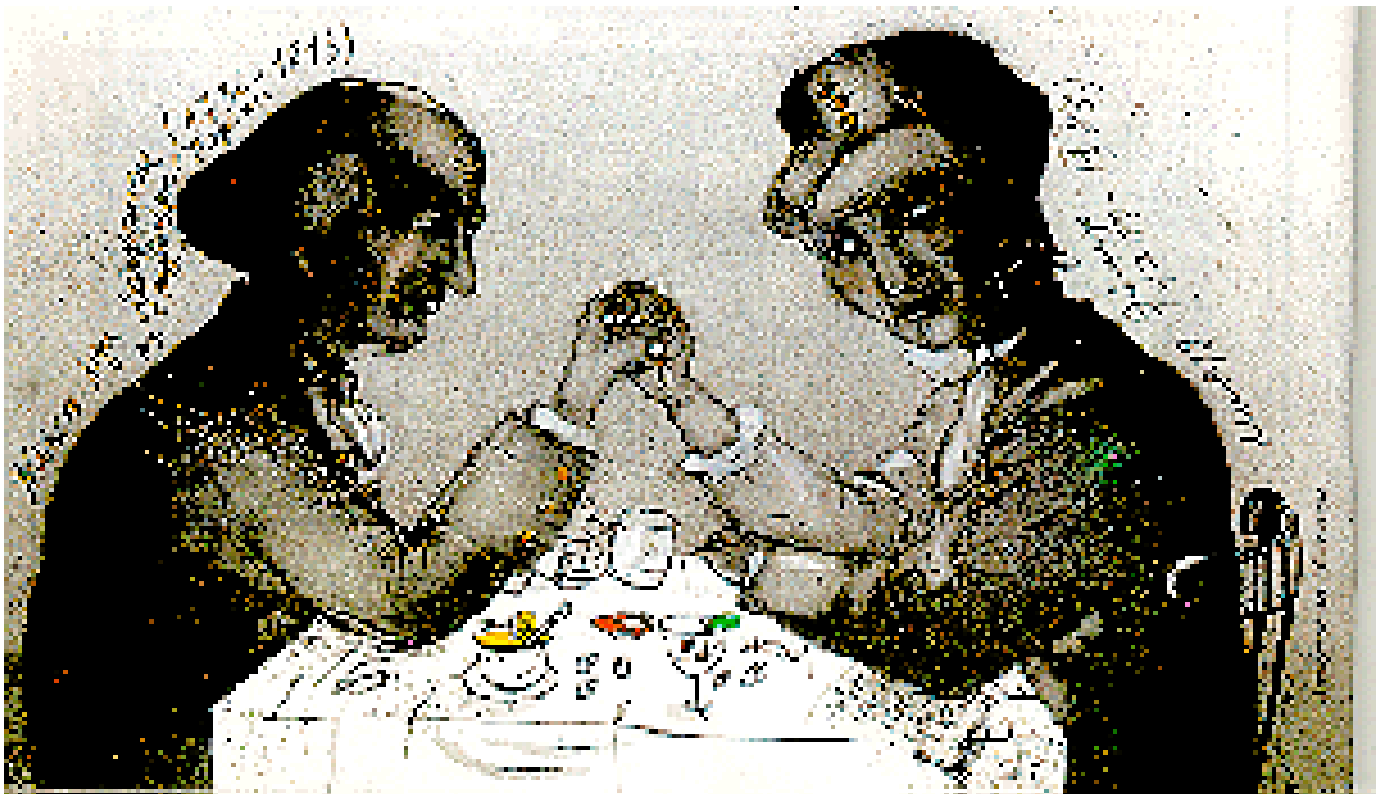
ных благ, глубокой преданностью общим интересам человечества, благородной простотой своих привычек, возвышенностью души и глубокой справедливостью в оценке трудов своих современников».

А теперь перейдем к формулировке и доказательству теоремы Лагранжа.

Теорема 4. Любое натуральное число представимо в виде суммы четырех квадратов целых чисел.

Доказательство. Формула Эйлера

$$\begin{aligned} (a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + t^2) = \\ = (ax + by + cz + dt)^2 + \\ + (ay - bx + ct - dz)^2 + \\ + (az - bt - cx + dy)^2 + \\ + (at + bz - cy - dx)^2 \end{aligned}$$



показывает, что произведение чисел, представимых в виде суммы четырех квадратов, тоже представимо в этом виде. Поэтому достаточно доказать теорему 4 для простых чисел.

Очевидно, $2 = 1^2 + 1^2 + 0^2 + 0^2$. Пусть p – нечетное простое число.

Лемма. *Существуют такие целые числа x и y , что $x^2 + y^2 + 1$ кратно p .*

Доказательство леммы. Рассмотрим числа $0^2, 1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$.

Если какие-то два из них дают один и тот же остаток при делении на p , т.е. если $x^2 \equiv y^2 \pmod{p}$, где $0 \leq x < y \leq (p-1)/2$, то $x^2 - y^2 = (x-y)(x+y)$ кратно p . Но ни разность $x-y$, ни сумма $x+y$ не кратна p .

Итак, рассматриваемые числа дают *разные* остатки при делении на p . Рассмотрим теперь еще $(p+1)/2$ чисел: $-1 - 0^2, -1 - 1^2, -1 - 2^2, \dots$

$\dots, -1 - \left(\frac{p-1}{2}\right)^2$. Они тоже дают *разные* остатки. Поскольку остатков от деления на p существует p штук, а в каждом из рассматриваемых нами множеств $(p+1)/2$ элементов, то хотя бы одно из чисел вида x^2 дает при делении на p такой же остаток, как и некоторое число вида $-1 - y^2$. При этом

$$x^2 \equiv -1 - y^2 \pmod{p},$$

что и требовалось доказать:

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}.$$

Числа x и y , как мы помним, не превосходят $(p-1)/2$; поэтому

$$x^2 + y^2 + 1 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 < p^2.$$

При этом

$$x^2 + y^2 + 1 = pm,$$

где $m < p$.

Мы хотим доказать, что число p представимо в виде суммы четырех квадратов целых чисел. Давайте рассмотрим *наименьшее* натуральное число m , для которого существуют такие целые числа x, y, z, t , что

$$x^2 + y^2 + z^2 + t^2 = pm.$$

Как мы уже знаем, $m < p$. Докажем, что $m = 1$. Для этого применим изобретенный Пьером Ферма метод

бесконечного спуска: предположим, что $m > 1$, и докажем, что в таком случае m – не наименьшее.

Пусть для начала m четно. Тогда либо все числа x, y, z, t четны, либо все они нечетны, либо два из них (для определенности, пусть это x и y) четны, а два (z и t) нечетны. В любом случае формула

$$\begin{aligned} & \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \\ & + \left(\frac{z+t}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2 = \\ & = \frac{x^2 + y^2 + z^2 + t^2}{2} = \frac{pm}{2} \end{aligned}$$

показывает, что m – не наименьшее возможное.

Пусть теперь m нечетно. Рассмотрим остатки a, b, c, d от деления чисел x, y, z, t на m . Хотя бы один из них отличен от 0: в противном случае сумма квадратов $pm = x^2 + y^2 + z^2 + t^2$ делилась бы на m^2 и (простое!) число p делилось бы на m .

Можно считать, что числа a, b, c, d не превосходят $(m-1)/2$. (Если, например, величина a окажется равна $(m+1)/2$ или больше, то можно заменить x на противоположное ему число $-x$. При этом вместо a получим остаток $m - a \leq m - \frac{m+1}{2} = \frac{m-1}{2}$.)

Обозначим $n = a^2 + b^2 + c^2 + d^2$.

Так как

$$\begin{aligned} n &= a^2 + b^2 + c^2 + d^2 \equiv \\ &\equiv x^2 + y^2 + z^2 + t^2 = pm \equiv 0 \pmod{m}, \end{aligned}$$

то $n \equiv 0 \pmod{m}$, так что $n = ml$, где l – натуральное число. Поскольку все числа a, b, c, d меньше $m/2$, имеем

$$\begin{aligned} ml = a^2 + b^2 + c^2 + d^2 < \\ < 4(m/2)^2 = m^2. \end{aligned}$$

Следовательно, $l < m$.

Применим формулу Эйлера:

$$\begin{aligned} & (ax + by + cz + dt)^2 + \\ & + (ay - bx + ct - dz)^2 + \\ & + (az - bt - cx + dy)^2 + \\ & + (at + bz - cy - dx)^2 = \\ & = (a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + t^2) = \\ & = npm = m^2 pl. \end{aligned}$$

Как мы помним, $x \equiv a, y \equiv b, z \equiv c$ и $t \equiv d \pmod{m}$. Поэтому

$$\begin{aligned} ax + by + cz + dt &\equiv \\ &\equiv x^2 + y^2 + z^2 + t^2 = pm \equiv 0, \\ ay - bx + ct - dz &\equiv \\ &\equiv xy - yx + zt - tz = 0, \\ az - bt - cx + dy &\equiv \\ &\equiv xz - yt - zx + ty = 0, \\ at + bz - cy - dx &\equiv \\ &\equiv xt + yz - zy - tx = 0. \end{aligned}$$

Итак, все числа $ax + by + cz + dt, ay - bx + ct - dz, az - bt - cx + dy$ и $at + bz - cy - dx$ кратны m ; формула

$$\begin{aligned} pl = & \left(\frac{ax + by + cz + dt}{m}\right)^2 + \\ & + \left(\frac{ay - bx + ct - dz}{m}\right)^2 + \\ & + \left(\frac{az - bt - cx + dy}{m}\right)^2 + \\ & + \left(\frac{at + bz - cy - dx}{m}\right)^2 \end{aligned}$$

представляет число pl в виде суммы четырех квадратов целых чисел. Таким образом, число m не является наименьшим возможным. Теорема Лагранжа доказана.

Гаусс и его теорема о семнадцатигульнике

Подобно Архимеду Гаусс выразил желание, чтобы на его могиле был увековечен семнадцатигульник.

Г.Вебер

Так же как в литературе Гомер, Данте, Шекспир, Гете, 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, чье имя, как и имя Архимеда, овеяно легендами. Многие его высказывания вошли в поговорку. Часто вспоминают его девиз: «Nil actum reputans si quid superesset agendum»¹. В этой личности сплелись могучий интеллект, сильный характер и любознательность естествоиспытателя. При жиз-

¹ *Что не завершено, не сделано вовсе (лат.).*

ни Гаусс был признан величайшим и коронован титулом «*Mathematicorum Princeps*»².

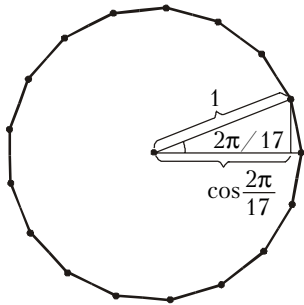
«Математическая деятельность Гаусса, — писал Феликс Клейн, — началась одним крупным открытием, которое привело его к твердому убеждению навсегда посвятить себя науке... 30 марта 1796 года ему — девятнадцатилетнему — удалось показать, что правильный семнадцатиугольник может быть построен с помощью циркуля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

Потомки постарались выполнить завещание великого ученого. Они воздвигли ему памятник (на родине, в Брауншвейге), который стоит на постаменте, являющемся правильным семнадцатиугольником. Но если не знать этого, то и 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. Для построения правильного семнадцатиугольника, вписанного в окружность радиуса 1, достаточно построить отрезок длины $\cos \frac{2\pi}{17}$ (см. рисунок). Дальнейшая последовательность действий не вы-



зывает трудностей. Однако для этого построения нам потребуются некоторые соотношения между комплексными числами.

Обозначим через ε один из комплексных корней семнадцатой степени из единицы:

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

Введем обозначения:

$$z_1 = \varepsilon + \varepsilon^{-1}, \quad z_2 = \varepsilon^4 + \varepsilon^{-4},$$

$$y_1 = z_1 + z_2,$$

$$y_2 = \varepsilon^2 + \varepsilon^{-2} + \varepsilon^8 + \varepsilon^{-8},$$

$$y_3 = z_1 z_2,$$

$$y_4 = (\varepsilon^2 + \varepsilon^{-2})(\varepsilon^8 + \varepsilon^{-8}),$$

$$x_1 = y_1 + y_2, \quad x_2 = y_3 + y_4.$$

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

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

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

Лемма 1. $\varepsilon^k = \varepsilon^{17+k}$ при целых k .

Действительно,

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

Лемма 2. $\sum_{k=0}^{16} \varepsilon^k = 0$.

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

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

Отсюда следует, что

$$\sum_{k=1}^{16} \varepsilon^k = \left(\sum_{k=0}^{16} \varepsilon^k \right) - \varepsilon^0 = 0 - 1 = -1,$$

т.е. $\sum_{k=1}^8 (\varepsilon^k + \varepsilon^{-k}) = -1$.

Лемма 3. $y_1 y_2 = y_3 y_4 = -1$.

Действительно,

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

$$+ \varepsilon^4 + \varepsilon^{-12} = \sum_{k=1}^8 (\varepsilon^k + \varepsilon^{-k}) = -1.$$

Аналогично, $y_3 y_4 = -1$.

Лемма 4. $x_1 + x_2 = -1$, $x_1 x_2 = -4$. (Доказательство предоставляем читателю.)

Напомним, что если заданы отрезки длины 1, $|p|$ и $|q|$, то циркулем и линейкой можно построить отрезок, длина которого равна абсолютной величине корня квадратного уравнения $x^2 + px + q = 0$.

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 $\cos \frac{2\pi}{17}$:

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

Впоследствии было доказано, что правильный n -угольник можно построить циркулем и линейкой тогда и только тогда, когда $n = 2^k F_1 F_2 \dots F_k$, где все F_i — различные 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

$$2^{2^5} + 1 = 4294967297$$

имеет простым делителем 641. В наш компьютерный век стало возможным исследовать на простоту достаточно большие числа, но пока ни одного простого числа Ферма, кроме 3, 5, 17, 257 и 65537, не найдено.

² Король математиков (лат.).