Доказательство трансцендентности числа e

В 1874 году Шарль Эрмит доказал трансцендентность числа e. Здесь мы имеем существенное обобщение классической постановки вопроса; там речь шла только о том, чтобы построить e при помощи циркуля и линейки, а это, как мы знаем, аналитически сводится к тому, чтобы представить e как результат нескольких последовательных извлечений корня квадратного из рациональных чисел. Теперь же доказывается не только то, что это невозможно, но нечто гораздо большее; а именно, показано, что e есть число трансцендентное, т. е. что его вообще нельзя связать с целыми числами никаким алгебраическим соотношением. Другими словами, e не может быть корнем алгебраического уравнения

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = 0, \quad a_0 \neq 0,$$

каковы бы ни были целые коэффициенты $a_o, \cdots, a_n$ и показатель n. Самое существенное здесь — это целые коэффициенты, достаточно было бы, собственно, сказать «рациональные» коэффициенты, потому что, приводя к общему знаменателю и отбрасывая его, мы всегда можем свести уравнение с рациональными коэффициентами к уравнению с целыми коэффициентами. Нам предстоит доказать, что предположение существования равенства

$$a_0 + a_1 e + a_2 e^2 + \ldots + a_n e^n = 0, \quad (1)$$

где $a_0 \neq 0$ и коэффициенты $a_o, \cdots, a_n$ — целые числа, ведет к противоречию; это противоречие обнаружится на самых простых свойствах целых чисел. Нам придется ссылаться из теории чисел только на самые элементарные теоремы о делимости, в частности на то, что каждое целое положительное число можно разложить на простые множители только одним способом, и на то, что существует бесчисленное множество простых чисел.

План доказательства заключается в следующем: мы покажем, как можно находить очень хорошие рациональные приближенные значения для числа e и его степеней, имеющие следующий вид:

$$e = \frac{M_1 + \varepsilon_1}{M}, \quad e^2 = \frac{M_2 + \varepsilon_2}{M}, \quad \ldots, \quad e^n = \frac{M_n + \varepsilon_n}{M}, \quad (2)$$

где $M, M_1, \cdots, M_n$ — целые числа, а $\frac{\varepsilon_1}{M}, \frac{\varepsilon_2}{M}, \cdots, \frac{\varepsilon_n}{M}$ — чрезвычайно малые дроби. Умножая затем обе части равенства (1) на M, мы придадим ему такой вид:

$$(a_0M + a_1M_1 + a_2M_2 + \ldots + a_nM_n) + \\ + (a_1\varepsilon_1 + a_2\varepsilon_2 + \ldots + a_n\varepsilon_n) = 0. \quad (3)$$

Первое слагаемое в левой части является целым числом, и мы докажем, что оно не равно нулю; второе слагаемое нам удастся, выбирая достаточно малые значения для чисел $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n$ сделать правильной дробью. Мы придем, таким образом, к противоречию, заключающемуся в том, что сумма целого отличного от нуля числа $a_0M + a_1M_1 + \cdots + a_nM_n$ и правильной отличной от единицы дроби $a_1\varepsilon_1 + \cdots + a_n\varepsilon_n$ равна нулю; отсюда и будет вытекать невозможность равенства (1).

При этом большую услугу вам окажет следующее предложение: целое число, которое не делится на некоторое определенное число, непременно отлично от нуля (потому что нуль делится на всякое число); именно, мы покажем, что числа $M_1, \cdots, M_n$ делятся на некоторое простое число p, а число a_0M на него заведомо не делится; таким образом, сумма $a_0M + a_1M_1 + \cdots + a_nM_n$ не делится на p и, значит, отлична от нуля.

Главным орудием для осуществления доказательства, идея которого только что намечена, является один определенный интеграл; его впервые в таких рассуждениях стал употреблять Эрмит, и поэтому мы можем назвать его интегралом Эрмита; построить его значило найти ключ ко всему доказательству. Мы увидим, что значение этого интеграла есть целое число, и он определит нужное нам число M:

$$M = \int_0^\infty \frac{z^{p-1}\{(z-1)(z-2)\ldots(z-n)\}^p e^{-z}}{(p-1)!}dz; \quad (4)$$

Здесь n есть степень предполагаемого уравнения (1), а p — некоторое простое число, которое мы определим дальше. При помощи этого интеграла мы найдем также вышеупомянутые приближенные значения (2) для степеней e^ν ($\nu = 1, 2, \cdots, n$); для этого мы разобьем интервал $0 < z < \infty$ на два интервала при помощи числа ν и положим

$$M_\nu = e^\nu \int_\nu^\infty \frac{z^{p-1}\{(z-1)\ldots(z-n)\}^p e^{-z}}{(p-1)!}dz,$$

$$\varepsilon_\nu = e^\nu \int_0^\nu \frac{z^{p-1}\{(z-1)\ldots(z-n)\}^p e^{-z}}{(p-1)!}dz. \quad (4a)$$

Перейдем теперь к самому доказательству.

1. Исходным пунктом является формула, хорошо известная из элементарной теории функции Г:

$$\int_0^\infty z^{\rho-1}e^{-z}\,dz = \Gamma(\rho).$$

Нам придется применять эту формулу только в предположении, что p есть число целое; в этом случае $\Gamma(\rho) = (\rho - 1)!$, и я сейчас это докажу. При помощи интегрирования по частям найдем

$$\int_0^\infty z^{\rho-1}e^{-z}\,dz = [-z^{\rho-1}e^{-z}]_0^\infty + \int_0^\infty (\rho-1)\,z^{\rho-2}e^{-z}\,dz = \\ = (\rho-1)\int_0^\infty z^{\rho-2}e^{-z}\,dz.$$

Второй множитель в правой части представляет собой интеграл того же вида, но только в нем показатель при z на единицу меньше; применяя это преобразование несколько раз, мы дойдем при ρ целом до z^1 а так как $\int_0^\infty e^{-z}\,dz = 0$ то мы получим окончательно

$$\int_0^\infty z^{\rho-1}e^{-z}\,dz = (\rho-1)(\rho-2)\cdot\ldots\cdot 3\cdot 2\cdot 1 = (\rho-1)!. \quad (5)$$

При целом ρ этот интеграл есть, таким образом, целое число, которое очень быстро возрастает с возрастанием ρ.

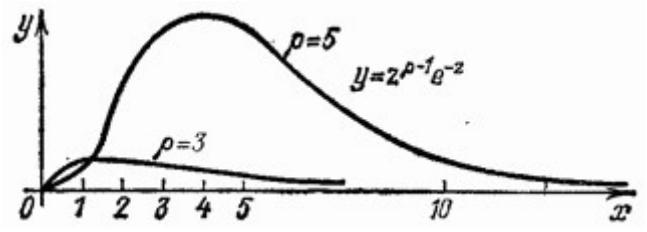

Рис. 1

Чтобы сделать этот результат геометрически наглядным, изобразим графически ход изменения функции $z^{\rho-1}e^{-z}$ для различных значений ρ (рис. 1); значение интеграла будет равно площади фигуры, заключенной между кривой и осью z и простирающейся до бесконечности.

Чем больше ρ, тем теснее кривая примыкает к оси абсцисс вблизи точки $z = 0$, но зато тем круче она идет вверх, начиная от точки $z = 1$; затем она достигает, каково бы ни было ρ, максимума при $z = \rho - 1$ причем с возрастанием ρ этот максимум увеличивается и перемещается вправо; начиная от этой точки получает преобладающее значение множитель e^{-z}, кривая начинает падать и, наконец, опять очень близко подходит к оси абсцисс. Теперь понятно, что площадь — наш интеграл — всегда остается конечной, но с возрастанием ρ сильно возрастает.

2. Пользуясь доказанной формулой, мы теперь легко найдем значение интеграла Эрмита (4). Если мы в числителе раскроем скобки и расположим подынтегральную функцию по убывающим степеням z:

$$\{(z-1)(z-2)\dots(z-n)\}^p = \{z^n - \dots + (-1)^n n!\}^p = \\ = z^{np} - \dots + (-1)^n (n!)^p \ ^{153})$$

(здесь выписаны члены только с высшей и низшей, т. е. нулевой, степенью z), то этот интеграл примет вид

$$M = \frac{(-1)^n (n!)^p}{(p-1)!} \int_0^\infty z^{p-1} e^{-z}\, dz + \sum_{\rho=p+1}^{p+np} \frac{C_\rho}{(p-1)!} \int_0^\infty z^{\rho-1} e^{-z}\, dz;$$

здесь C_ρ — постоянные и притом целые числа, которые получаются при указанном выше раскрытии скобок в многочлене. Применяя формулу (5) к каждому из полученных интегралов, мы получим

$$M = (-1)^n (n!)^p + \sum_{\rho=p+1}^{p+np} C_\rho \frac{(\rho-1)!}{(p-1)!}.$$

Все значения индекса суммирования ρ больше p, и, значит, отношения $\frac{(\rho-1)!}{(p-1)!}$ — целые числа, содержащие, кроме того, множитель p; если его вынести за скобку, то мы получим

$$M = (-1)^n (n!)^p + \\ + p\{C_{p+1} + C_{p+2}(p+1) + C_{p+3}(p+1)(p+2) + \dots\}.$$

Отсюда мы видим, что M делится или не делится на p в зависимости от того, делится или не делится на p первое слагаемое $(-1)^n (n!)^p$. Но так как p есть число простое, то это слагаемое заведомо не будет делиться на p, если p не входит в состав ни одного из его сомножителей $1, 2, \cdots, n$, а это заведомо будет

иметь место, если $p > n$. Этому условию удовлетворяет бесчисленное множество простых чисел; выбрав любое из них, мы достигнем того, что $(-1)^n(n!)^p$, а значит, и M, заведомо не будет делиться на p.

Так как, по предположению, $a_0 \neq 0$, то нам легко сделать так, чтобы и a_0 не делилось на p; для этого достаточно только выбрать p большим, чем a_0 что, как следует из сказанного выше, конечно, возможно. Но тогда

произведение a_0M также не делится на p, и мы достигли, таким образом, нашей первой цели.

3. Исследуем теперь числа M_ν $(\nu = 1, 2, \cdots, n)$, определенные равенствами (4а). Внесем множитель e^ν под знак интеграла и введем новую переменную $\zeta = z - \nu$ принимающую значения от 0 до ∞, когда z изменяется от ν до ∞; тогда мы получим

$$M_\nu = \int_0^\infty \frac{(\zeta+\nu)^{p-1}\{(\zeta+\nu-1)(\zeta+\nu-2)\ldots\zeta\ldots(\zeta+\nu-n)\}^p e^{-\zeta}}{(p-1)!} d\zeta \quad (154).$$

Это интеграл того же вида, что и рассмотренный ранее интеграл M, и мы можем здесь применить аналогичные преобразования. Раскрыв скобки в числителе подынтегральной функции, мы получим сумму степеней переменной ζ с целыми коэффициентами, причем низшая из этих степеней есть ζ^p. Интеграл выражения, стоящего в числителе, представится теперь в виде суммы интегралов

$$\int_0^\infty \zeta^p e^{-\zeta} d\zeta, \quad \int_0^\infty \zeta^{p+1} e^{-\zeta} d\zeta, \quad \ldots, \quad \int_0^\infty \zeta^{(n+1)p-1} e^{-\zeta} d\zeta$$

с целыми коэффициентами, а так как эти последние интегралы имеют, согласно равенствам (5), соответственно значения $p!, (p+1)!, \cdots$, то эту сумму можно представить в виде числа $p!$ умноженного на некоторое целое число A_ν, таким образом, для каждого из рассматриваемых интегралов мы имеем

$$M_\nu = \frac{p!A_\nu}{(p-1)} = p \cdot A_\nu \qquad (\nu = 1, 2, \ldots, n),$$

т. е. все они являются целыми числами, кратными p.

Если мы сопоставим это с доказанным в п. 2, то мы увидим, что можно применить указанное выше предложение и сказать: целое число $a_0M + a_1M_1 + \cdots + a_nM_n$ заведомо не делится на p и, следовательно, отлично от нуля.

4. Вторая часть доказательства относится к сумме $a_1\varepsilon_1 + \cdots + a_n\varepsilon_n$, где, согласно равенству (4а),

$$\varepsilon_\nu = \int_0^\nu \frac{z^{p-1}\{(z-1)(z-2)\ \ldots\ (z-n)\}^p e^{-z+\nu}}{(p-1)!}\,dz,$$

и нам нужно доказать, что, придавая числу p надлежащие значения, можно сделать эти ε_ν сколь угодно малыми; при этом мы воспользуемся тем, что мы можем считать p сколь угодно большим, так как те условия, которым мы пока подчинили простое число p ($p > n$, $p > a_0$) могут быть удовлетворены произвольно большими простыми числами.

Изобразим, прежде всего, геометрически ход изменения подынтегральной функции (рис. 2).

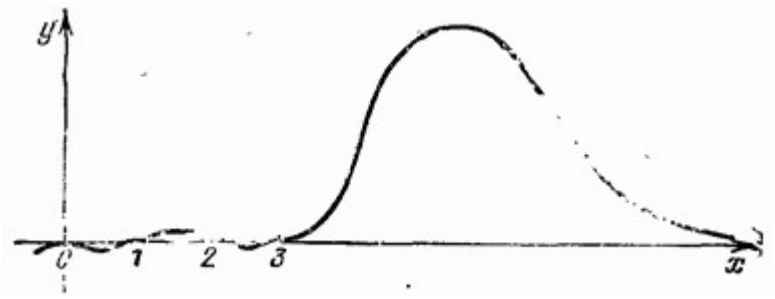

Рис. 2

При $z = 0$ кривая касается оси z, при $z = 1, 2, \cdots, n$ она касается оси z и в то же время пересекает ее (так как p — число нечетное). Мы сейчас увидим, что под влиянием знаменателя $(p-1)!$ кривая во всем промежутке $(0,n)$ не поднимается высоко над осью z, если только взять p достаточно большим; таким образом, очевидно, что интеграл ε_ν будет очень мал, Заметим, что вне этого промежутка (при $z > n$) подынтегральная функция быстро возрастает и затем асимптотически приближается к оси z, как и рассмотренная выше функция $z^{\rho-1}e^{-z}$ [для $\rho = (n+1)p$]; это объясняет, как получаются эти быстро возрастающие с возрастанием p значения интеграла M, взятого по всему промежутку от 0 до ∞.

Для того чтобы действительно оценить величины интегралов ε_ν оказывается достаточным применить следующий грубый прием. Обозначим через G и g_ν наибольшие значения модуля функции $z, (z-1), \cdots, (z-n)$ и функции $z, (z-1), \cdots, (z-n)e^{-z+\nu}$ в промежутке $(0,n)$, так что

$$\left.\begin{aligned} &|z(z-1)\dots(z-n)|\leqslant G,\\ &|(z-1)(z-2)\dots(z-n)e^{-z+\nu}|\leqslant g_\nu \end{aligned}\right\} \text{ при } 0\leqslant z\leqslant n.$$

Так как модуль интеграла не превышает интеграла от модуля подынтегральной функции, то для каждого ν мы имеем

$$|\varepsilon_\nu|\leqslant\int_0^\nu \frac{G^{p-1}g_\nu}{(p-1)!}\,dz=\frac{G^{p-1}g_\nu\nu}{(p-1)!}. \quad (6)$$

Числа G, g_ν, ν не зависят от p, а стоящий в знаменателе факториал $(p-1)!$ возрастает, как известно, $\frac{G^{p-1}}{(p-1)}$ быстрее, чем степень G^{p-1} или, точнее, при достаточно большом p дробь делается меньше какого угодно наперед

!

заданного числа, как бы мало оно ни было. Равенство (6) показывает, таким образом, что, принимая за p достаточно большое число, мы можем сделать сколь угодно малым каждое из чисел ε_ν.

Отсюда непосредственно следует, что мы можем сделать сколь угодно малой сумму $a_1\varepsilon_1+\dots+a_n\varepsilon_n$ состоящую из n членов; в самом деле,

$$\begin{aligned}|a_1\varepsilon_1+a_2\varepsilon_2+\dots+a_n\varepsilon_n|\leqslant\\ \leqslant|a_1|\cdot|\varepsilon_1|+|a_2|\cdot|\varepsilon_2|+\dots+|a_n|\cdot|\varepsilon_n|;\end{aligned}$$

согласно равенству (6) это выражение не превосходит

$$(|a_1|\cdot 1g_1+|a_2|\cdot 2g_2+\dots+|a_n|\cdot ng_n)\cdot\frac{G^{p-1}}{(p-1)!};$$

а так как множитель, заключенный в скобки, имеет постоянное не зависящее от p значение, то благодаря $\frac{G^{p-1}}{(p-1)}$ множителю мы можем всю правую часть, а

!

следовательно, и левую, т. е. $|a_1\varepsilon_1+\dots+a_n\varepsilon_n|$ сделать как угодно малой в частности меньше единицы.

Но это приводит нас к тому противоречию с равенством (3):

$$(a_0M+a_1M_1+\dots+a_nM_n)+(a_1\varepsilon_1+\dots+a_n\varepsilon_n)=0,$$

которое мы выше имели в виду; оно состоит в том, что целое число, отличное от нуля, после прибавления к нему правильной дроби должно обратиться в нуль. Поэтому последнее равенство не может иметь места, и таким образом доказана трансцендентность числа e.

Список литературы.

1.Клейн Ф. ”Элементарная математика с точки зрения высшей”, Наука, 1987.

2. https://en.wikipedia.org/wiki/Transcendental_number