Liet. matem. rink, **45**, *spec. nr.*, 2006, 24–27

О лемме Эйлера

Юозас Ювенциюс МАЧИС (МII)
e-mail: jmacys@ktl.mii.lt

Хорошо известно (см. [1] или [2], а также [3] или [4]) элементарное доказательство Эйлера теоремы Ферма для случая $n = 3$, данное самим Эйлером и основанное на его же собственной глубокой лемме – более простое доказательство пока не известно. Но вот в единственном опубликованном им доказательстве этой леммы обнаружился пробел, хотя сама лемма и верна.

ЛЕММА ЭЙЛЕРА. *Пусть a и b – такие взаимно простые числа, что $a^2 + 3b^2$ является кубом. Тогда существуют такие целые p и q, что*

$$a = p^3 - 9pq^2, \quad b = 3p^2q - 3q^3.$$

Казалось бы – дело простое: если $a^2 + 3b^2 = k^3$, то k разлагаем на простые множители $k = P_1P_2 \dots P_n$, множители представляем в виде $p_i^2 + 3q_i^2$, перемножаем и получаем равенство:

$$\begin{aligned} k^3 = a^2 + 3b^2 &= (P_1P_2 \dots P_n)^3 \\ &= (p_1^2 + 3q_1^2)^3 (p_2^2 + 3q_2^2)^3 \dots (p_n^2 + 3q_n^2)^3 \\ &= \left[(p_1^2 + 3q_1^2)(p_2^2 + 3q_2^2) \dots (p_n^2 + 3q_n^2)\right]^3 \\ &= (p^2 + 3q^2)^3 = (p^2 - 9pq^2)^2 + 3(3p^2q - 3q^3)^2. \end{aligned}$$

Отсюда делаем вывод: существуют p и q такие, что

$$a = p^2 - 9pq^2, \quad b = 3p^2q - 3q^3. \tag{1}$$

Но сразу возникает множество вопросов: 1) как перемножаются числа $p_i^2 + 3q_i^2$? 2) всегда ли «представимы» простые числа P_i? 3) единственно ли это представление простых чисел? 4) и главное: можно ли отсюда заключить, что верны формулы (1), т.е. каждый ли куб такого вида можно выразить при помощи этих формул?

Следовательно, если опираться на числа, представимые в виде $x^2 + 3y^2$, то нужно строить их арифметику – во всяком случае научиться разлагать их на множители.

Итак – будет ли произведение двух представимых чисел представимым? Начинаем перемножать:

$$(a^2+3b^2)(c^2+3d^2)=a^2c^2+3b^2c^2+3a^2d^2+9b^2d^2. \tag{2}$$

Не сосвсем ясно, что делать дальше. А вот комплексные числа сразу дают ответ (черта сверху означает комплексное сопряжение):

$$\begin{aligned}&(a+ib\sqrt{3})(a-ib\sqrt{3})(c+id\sqrt{3})(c-id\sqrt{3})\\&=\big[(a+ib\sqrt{3})(c+id\sqrt{3})\big]\overline{\big[(a+ib\sqrt{3})(c+id\sqrt{3})\big]}\\&=\big[(ac-3bd)+i\sqrt{3}(ad+bc)\big]\overline{\big[(ac-3bd)+i\sqrt{3}(ad+bc)\big]}\\&=(ac-3bd)^2+3(ad+bc)^2.\end{aligned}$$

Теперь уже ясно, что формулу (2) переписать в нужном виде – это простое школьное упражнение:

$$\begin{aligned}&(a^2c^2-6abcd+9b^2d^2)+3(a^2d^2+2abcd+b^2c^2)\\&\quad=(ac-3bd)^2+3(ad+bc)^2.\end{aligned}$$

Именно из-за этой сиюминутной выгоды все (в том числе и Эйлер) обращались к комплексным числам. А в конце концов никаких выгод это не дало – ведь рассматриваются числа целые.

Итак, произведение двух представимых чисел представимо. Но сразу – первая неожиданность: во всех формулах b можно поменять на $(-b)$. Следовательно,

$$(a^2+3b^2)(c^2+3d^2)=(ac-3bd)^2+3(ad+bc)^2 \tag{3}$$

или

$$(a^2+3b^2)(c^2+3d^2)=(ac+3bd)^2+3(ad-bc)^2. \tag{4}$$

Например,

$$91=13\cdot 7=(1^2+3\cdot 2^2)(2^2+3\cdot 1^2)=(2\mp 6)^2+3(1\pm 4)^2,$$

т.е. $91=4^2+3\cdot 5^2=8^2+3\cdot 3^2$.

Уже этот пример хорошо оттеняет проблемы единственности: число может иметь несколько представлений $a_1^2+3b_1^2=a_2^2+3b_2^2$, и сделать вывод о равенстве их компонент $a_1=a_2$ и $b_1=b_2$ удается далеко не всегда.

На формулы (3) и (4) можно смотреть под разным углом: можно говорить, что умножать можно по закону (3) или по закону (4), а можно говорить, что при соответствующих знаках a, b, c, d всегда умножаем по закону (3). Например, по закону (3)

$$\begin{aligned}91&=13\cdot 7=\big[(1^2+3(-2)^2\big][2^2+3\cdot 1^2]\\&=\big[2-3(-2)\cdot 1\big]^2+3\big[1+(-2)\cdot 2\big]^2=8^2+3\cdot 3^2.\end{aligned}$$

Оказывается, что при умножении всегда лучше пользоваться лишь одним законом – скажем, законом (3) – тогда сразу гарантируется коммутативность и ассоциативность умножения (это проверяется тривиально).

Тем не менее главное – научиться разлагать представимые числа на простые множители, т.е. научиться делить. Г. Эдвардс (см. [1] или [2]) поставил перед собой задачу убедить всех, что Эйлер знал корректное докзательство своей леммы, и его будто бы подвело лишь стремление к краткости в изложении. Г. Эдвардс построил целую арифметику чисел $a^2 + 3b^2$ (опираясь на аналоги результатов Эйлера по арифметике чисел вида $a^2 + b^2$ и чисел вида $a^2 + 2b^2$) и показал, что из нее следует лемма Эйлера, но не сумел избежать столь нежелательного перехода к комплексным числам. И причина этой неудачи кроется, скорее всего, в том, что, не отказавшись от закона умножения (4), он не смог добиться однозначности деления двух представимых чисел одно на другое.

В докладе [5] и в статье [6] автор показывает, как не переходя к комплексным числам можно осуществить идею Г. Эдвардса и тем самым построить абсолютно элементарное доказательство теоремы Ферма в случае $n = 3$.

Интересно, что удалось построить и другое элементарное доказательство. Дело в том, что вот уже сто лет, как известно доказательство леммы Эйлера, не опирающееся на комплексные числа, но, к сожалению, опирающееся на закон квадратичной взаимности, символы Лежандра и другие глубокие результаты теории чисел (см. [5], стр. 88–93, или [6], стр. 384–387). Ключевой момент в нашем построении состоит в элементарном доказательстве следующего факта.

ТЕОРЕМА. Каждое простое число вида $3n+1$ представимо в виде a^2+3b^2.

Доказательство. Заметим, что разности

$$2^{p-1} - 1, 3^{p-1} - 2^{p-1}, \ldots, (p-1)^{p-1} - (p-2)^{p-1}$$

делятся на p. Действительно,

$$2^p - 2 = 1 + C_p^1 + C_p^2 + \cdots + C_p^{p-2} + C_p^{p-1} + C_p^p - 2 = C_p^1 + C_p^2 + \cdots + C_p^{p-1}$$

делится на p, поскольку каждое слагаемое $C_p^k = \dfrac{p(p-1)\cdots(p-k+1)}{1\cdot 2\cdots k}$ делится на p ввиду взаимной простоты p с меньшими числами. Далее, $m^p - m$ делится на m по индукции, поскольку

$$(m+1)^p - (m+1) - (m^p - m) = C_p^1 m^{p-1} + \cdots + C_p^{p-1}$$

делится на p. Но поскольку $m^p - m = m(m^{p-1} - 1)$ делится на p, то из-за простоты p $m^{p-1} - 1$ для $m < p$ делится на p (фактически мы доказали Малую теорему Ферма). Поэтому и разности $m^{p-1} - (m-1)^{p-1}$ делятся на p.

Итак, разности $(p-1)^{3n}-(p-2)^{3n}, (p-2)^{3n}-(p-3)^{3n}, \ldots, 2^{3n}-1^{3n}$ делятся на p. Разложим каждую из этих разностей на множители: $a^{3n}-b^{3n}=(a^n-b^n)(a^{2n}+a^nb^n+b^{2n})$. Поскольку a и b различаются на единицу, то они взаимно просты и одно из них четно. Поэтому второй множитель можно записать в виде $A^2+A(2B)+(2B)^2=(A+B)^2+3B^2$ со взаимно простыми A и B. Если p не делит хотя бы одну из разностей чисел $1^n, 2^n, 3^n, \ldots, (p-1)^n$, то оно делит число вида c^2+3d^2, а тем самым является таковым (см. [1], стр. 50, или [2], стр. 68). Следовательно, в этом случае лемма доказана.

Осталось лишь показать, что второй случай на самом деле невозможен – p не может делить все разности чисел $1^n, 2^n, \ldots, (p-1)^n$.

Допустим противное, и пусть p делит все разности этих чисел. Следовательно, p делит и вторые разности, и третьи, ..., и n-ые разности. Но хорошо известно, что n-ые разности последовательности $1^n, 2^n, 3^n, \ldots$ равны $n!$ (см., например, [1], стр. 48, или [2], стр. 66), и $p=3n+1$ делить $n!$ не может. Противоречие. Теорема доказана.

Литература

1. H. Edwards, *Fermat's Last Theorem*, Springer, New York (2000).
2. Г. Эдвардс, *Последняя теорема Ферма*, Мир, Москва (1980).
3. М.М. Постников, *Введение в теорию алгебраических чисел*, Наука, Москва (1982).
4. М.М. Постников, *Теорема Ферма*, Наука, Москва (1978).
5. Ю. Мачис, Об одном диофантовом уравнении, в кн.: *KTU konferencijos „Matematika ir matematinis modeliavimas" darbai* (2006), с. 101–105.
6. Ю.Ю. Мачис, О предполагаемом доказательстве Эйлера, *Математические заметки*, **79**, в печати (2007).
7. T. Andreescu, D. Andrica, *An Introduction to Diophantine Equations*, GIL Publishing House, Zalau (2002).
8. W. Sierpinski, *Elementary Theory of Numbers*, PWN, Warsaw (1964).

REZIUMĖ

J. Mačys. Eulerio lemos klausimu

Nagrinėjami nauji Eulerio lemos įrodymo variantai, kurie suteikia galimybę konstruoti elementarius Fermat teoremos įrodymus atveju $n=3$.

SUMMARY

J. Mačys. On Euler's lemma

Some new versions of the proof of Euler's lemma are considered. These allow to construct elementary proofs of Fermat's theorem in the case $n=3$.

Keywords: Fermat's theorem, Euler's lemma, diophantine equations, elemntary proof.