Math-Net.Ru

Общероссийский математический портал

Ю. Ю. Мачис, О предполагаемом доказательстве Эйле-
ра, *Матем. заметки*, 2007, том 82, выпуск 3, 395–400

DOI: <https://doi.org/10.4213/mzm3992>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.198.55.26

26 апреля 2023 г., 15:13:15

О предполагаемом доказательстве Эйлера

Ю. Ю. Мачис

Предполагают, что Эйлер владел элементарным доказательством теоремы Ферма для случая $n = 3$. Наша заметка показывает, что это весьма правдоподобно: пользуясь результатами Эйлера, можно элементарно доказать, что уравнение $x^3 + y^3 = z^3$ не имеет решений в ненулевых целых числах.

Библиография: 5 названий.

Приведем несколько цитат из книги Г. Эдвардса “Последняя теорема Ферма” о случае $n = 3$ этой теоремы [1; с. 39–40]; удобно также пользоваться адекватным русским текстом перевода с первого издания книги – см. [2; с. 56–57].

“Обычно считается, что Эйлер привел доказательство для случая $n = 3$, но оно было “неполным”, поскольку содержало фундаментальный пробел. Предложить другое доказательство того утверждения, при доказательстве которого Эйлер допустил ошибку, далеко не просто. Залатать первоначальное доказательство Эйлера очень желательно ввиду элегантности и общности этого доказательства”. И далее ([1; с. 45–46] или [2; с. 63]):

“В 1753 г. Эйлер заявил, что он умеет доказывать последнюю теорему Ферма при $n = 3$ (письмо 1753 г. к Гольдбаху), однако единственным опубликованным им доказательством является доказательство из “Алгебры” (1770). Размышляя об этом ошибочном доказательстве, разумно предположить, что в своем первоначальном методе он использовал менее оригинальное рассуждение, показывающее, что $a^2 + 3b^2$ – куб только тогда, когда $a = p^3 - 9pq^2$, $b = 3p^2q - 3q^3$, и что лишь позже ему пришла в голову элегантная, но неверная, идея доказать эту лемму, используя тот “факт”, что произведение двух взаимно простых сомножителей $a + b\sqrt{-3}$ и $a - b\sqrt{-3}$ является кубом, только если кубами являются оба сомножителя. Тех идей, которые Эйлер использовал в более ранней работе, достаточно для доказательства необходимой леммы о кубах вида $a^2 + 3b^2$.”

Итак, Эдвардс предполагает, что Эйлер владел правильным элементарным доказательством леммы, но восстановить его “далеко не просто”, хотя и очень желательно.

На ту же лемму опирается изложение в остальном вполне элементарного доказательства Эйлера, приведенное в книге Постникова [3; с. 34–38] (или [4; с. 31–34]).

Вот это злосчастное утверждение.

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

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

Простым раскрытием скобок убеждаемся, что $a^2 + 3b^2 = (p^2 + 3q^2)^3$. Вышеупомянутый “пробел” состоит в том, что необходимо убедиться в возможности представить при помощи формул леммы каждый куб такого вида.

Основываясь на более ранней работе Эйлера, Эдвардс излагает весьма правдоподобную версию того, как Эйлер элементарным путем, изучая числа вида $a^2 + 3b^2$, мог добыть вспомогательные утверждения, необходимые для доказательства леммы. Эдвардс также показал, что методы Эйлера достаточны и для правильного доказательства леммы, но приведенное Эдвардсом доказательство требует перехода к комплексным числам (см. [1; с. 52–54] или [2; с. 70–73]).

Оказывается, что это излишне – для доказательства леммы вполне достаточно самой арифметики чисел вида $a^2 + 3b^2$. Приведем вспомогательные утверждения, необходимые нам для элементарного доказательства леммы. В основном мы будем следовать изложению в [1] и [2], однако ради краткости некоторые утверждения будем формулировать не в самом общем виде, а лишь в виде, достаточном для наших целей.

УТВЕРЖДЕНИЕ 1. Произведение двух чисел, каждое из которых представимо в виде $a^2 + 3b^2$ (или кратко здесь и далее: представимо), тоже представимо.

ДОКАЗАТЕЛЬСТВО. Утверждение следует из тождества

$$(a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd)^2 + 3(ad + bc)^2 \quad (1)$$

или из тождества

$$(a^2 + 3b^2)(c^2 + 3d^2) = (ac + 3bd)^2 + 3(ad - bc)^2. \quad (2)$$

Правилом (2) представления произведения мы пользоваться не будем: достаточно в правиле (1) множитель $a^2 + 3b^2$ переписать как $a^2 + 3(-b)^2$ и получим представление (2). В соответствии с этим мы будем считать, что компонентами a и b представлений $a^2 + 3b^2$ могут быть произвольные целые числа, при этом будем различать, скажем, представления $a^2 + 3b^2$ и $(-a)^2 + 3b^2$ (ср. [1; с. 49] или [2; с. 67, конец доказательства утверждения 2']).

УТВЕРЖДЕНИЕ 2. При представлении по правилу (1) произведения произвольно-го числа представимых множителей порядок перемножения на результат представления не влияет.

ДОКАЗАТЕЛЬСТВО. Очевидно, умножение представимых чисел по правилу (1) коммутативно. Оно также ассоциативно, поскольку результаты умножения

$$\begin{aligned} & [(a^2 + 3b^2)(c^2 + 3d^2)](e^2 + 3f^2) \\ &= [(ac - 3bd)^2 + 3(ad + bc)^2][e^2 + 3f^2] \\ &= [(ac - 3bd)e - 3(ad + bc)f]^2 + 3[(ac - 3bd)f + (ad + bc)e]^2 \end{aligned}$$

и

$$\begin{aligned}
& (a^2 + 3b^2)[(c^2 + 3d^2)(e^2 + 3f^2)] \\
&= [(ce - 3df)^2 + 3(cf + de)^2][a^2 + 3b^2] \\
&= [(ce - 3df)a - 3(cf + de)b]^2 + 3[(ce - 3df)b + (cf + de)a]^2
\end{aligned}$$

совпадают. Поэтому при перемножении по правилу (1) произвольного числа множителей в любом порядке представление всегда получится то же.

Из формулы (1) следует, что зачастую не приходится надеяться на единственность представления (например, если $a = d = 1$, $\pm b = c = 2$, то $13 \cdot 7 = 91 = 8^2 + 3 \cdot 3^2 = 4^2 + 3 \cdot 5^2$). Кроме того, если компоненты хотя бы одного из сомножителей (например, a и b) не являются взаимно простыми, то и в представлении произведения по правилу (1) компоненты не взаимно просты. Отметим здесь также, что и утверждение леммы не верно, если a и b не взаимно просты: достаточно рассмотреть число $13^3 = 13^2 + 3 \cdot 26^2$ и уравнение $26 = 3p^2q - 3q^3$ целых решений не имеет.

УТВЕРЖДЕНИЕ 3. Число $(a^2 + 3b^2)^3$ можно представить по формуле

$$(a^2 + 3b^2)^3 = (a^3 - 9ab^2)^2 + 3(3a^2b - 3b^3)^2. \quad (3)$$

ДОКАЗАТЕЛЬСТВО. По формуле (1)

$$(a^2 + 3b^2)^2 = (a^2 - 3b^2)^2 + 3(2ab)^2.$$

Умножив это тождество на $a^2 + 3b^2$ по правилу (1), получаем представление (3).

УТВЕРЖДЕНИЕ 4. Если a и b взаимно просты, то каждый нечетный делитель числа $a^2 + 3b^2$ можно представить в виде $c^2 + 3d^2$.

ДОКАЗАТЕЛЬСТВО см. в [1; с. 50] или [2; с. 68].

УТВЕРЖДЕНИЕ 5. Если целые числа a и b взаимно просты и $a^2 + 3b^2$ делится на нечетное простое число P , то P можно представить в виде $P = p^2 + 3q^2$, причем p можно брать неотрицательным, а знак q выбрать таким образом, что $a^2 + 3b^2 = (p^2 + 3q^2)(u^2 + 3v^2)$ в смысле умножения по правилу (1) при некоторых взаимно простых целых u и v .

ДОКАЗАТЕЛЬСТВО. Согласно утверждению 4 P можно представить в виде $P = p^2 + 3q^2$. Далее, поскольку

$$(pb - aq)(pb + aq) = p^2b^2 + 3q^2b^2 - 3q^2b^2 - a^2q^2 = b^2(p^2 + 3q^2) - q^2(a^2 + 3b^2)$$

делится на простое $p^2 + 3q^2$, то на него делится либо $pb - aq$, либо $pb + aq$. Выберем p неотрицательным, а знак q таким, чтобы на $P = p^2 + 3q^2$ делилось $pb - aq$. Тогда

$$P(a^2 + 3b^2) = (p^2 + 3(-q)^2)(a^2 + 3b^2) = (pa + 3qb)^2 + 3(pb - aq)^2$$

и это равенство можно разделить на P^2 :

$$\frac{a^2 + 3b^2}{P} = \left(\frac{pa + 3qb}{P}\right)^2 + 3\left(\frac{pb - aq}{P}\right)^2.$$

Если обозначить

$$\frac{pa + 3qb}{P} = u, \quad \frac{pb - aq}{P} = v,$$

то

$$\begin{aligned} (p^2 + 3q^2)(u^2 + 3v^2) &= (pu - 3qv)^2 + 3(pv + qu)^2 \\ &= \left(p \frac{pa + 3qb}{P} - 3q \frac{pb - aq}{P} \right)^2 + 3 \left(p \frac{pb - aq}{P} + q \frac{pa + 3qb}{P} \right)^2 \\ &= \left(\frac{a(p^2 + 3q^2)}{P} \right)^2 + 3 \left(\frac{b(p^2 + 3q^2)}{P} \right)^2 = a^2 + 3b^2, \end{aligned}$$

как и требовалось. Кроме того, u и v взаимно просты, поскольку иначе $a = pu - 3qv$ и $b = pv + qu$ имели бы общий делитель.

УТВЕРЖДЕНИЕ 6. Если простое число P представимо, то это представление единственно с точностью до знаков компонент.

ДОКАЗАТЕЛЬСТВО. Ясно, что $P = 2$ непредставимо: если $2 = p^2 + 3q^2$, то $q = 0$, а тогда $p^2 = 2$; противоречие. Итак, пусть нечетное простое $P = a^2 + 3b^2 = p^2 + 3q^2$. Ясно, что a и b взаимно просты. Согласно утверждению 5 имеем

$$a^2 + 3b^2 = (p^2 + 3q^2)(u^2 + 3v^2)$$

при соответствующем выборе знаков. Тогда

$$\begin{aligned} P &= P(u^2 + 3v^2), \quad u^2 + 3v^2 = 1, \quad v = 0, \quad u = \pm 1, \\ a &= pu - 3qv = \pm p, \quad b = pv + qu = \pm q. \end{aligned}$$

Следовательно, представления $a^2 + 3b^2$ и $p^2 + 3q^2$ совпадают с точностью до знаков компонент.

УТВЕРЖДЕНИЕ 7. Пусть целые числа a, b взаимно просты и $a^2 + 3b^2$ нечетно. Тогда имеет место равенство

$$a^2 + 3b^2 = (p_1^2 + 3q_1^2)(p_2^2 + 3q_2^2) \cdots (p_m^2 + 3q_m^2)[(\pm 1)^2 + 3 \cdot 0^2] \quad (4)$$

в смысле умножения по правилу (1), где множители $p_i^2 + 3q_i^2$ однозначно определены с точностью до знаков компонент тем обстоятельством, что произведение в правой части является разложением $a^2 + 3b^2$ на (нечетные) простые множители. Кроме того, в это разложение может входить только один из множителей $p^2 + 3q^2$ и $p^2 + 3(-q)^2$.

ДОКАЗАТЕЛЬСТВО. Если $a^2 + 3b^2 \neq 1$, то это число имеет делитель P , равный нечетному простому, и из утверждения 5 следует, что $a^2 + 3b^2 = (p^2 + 3q^2)(u^2 + 3v^2)$, где $p^2 + 3q^2 = P$, а u и v взаимно просты. Множитель $u^2 + 3v^2$ меньше числа $a^2 + 3b^2$, из него опять выделяем простой нечетный множитель. Повторение этого процесса приведет в конце концов к выражению вида

$$a^2 + 3b^2 = (p_1^2 + 3q_1^2)(p_2^2 + 3q_2^2) \cdots (p_m^2 + 3q_m^2)(u^2 + 3v^2),$$

где $u^2 + 3v^2 = 1$. Тогда $v = 0$, $u = \pm 1$, и разложение завершено. Кроме того, если бы в разложение входило $p^2 + 3q^2$ и $p^2 + 3(-q)^2$, то их произведение давало бы множитель $(p^2 + 3q^2)^2$, а это при взаимно простых a и b невозможно.

ДОКАЗАТЕЛЬСТВО ЛЕММЫ. Итак, $k^3 = a^2 + 3b^2$, причем a и b взаимно просты. Далее, a и b – различной четности: оба четными быть не могут, а если бы оба были нечетными, то

$$k^3 = 4 \frac{a-b}{2} \left(\frac{a-b}{2} + b \right) + 4b^2$$

делилось бы на 4, но не делилось на 8. (Этот невозможный случай одинаковой четности в доказательстве леммы в [1; с. 53] или [2; с. 71] почему-то не исключен – может быть, это обстоятельство тоже отчасти помешало обнаружить элементарное доказательство?)

Итак, k^3 , а тем самым и k , нечетны.

Впрочем, $k^3 = a^2 + 3b^2$ не делится не только на 2, но также и на 3. Действительно, в противном случае k^3 , делясь на 3, делилось бы и на 27, a^2 делилось бы на 3, следовательно, и на 9. Тогда $3b^2$ делилось бы на 9, b^2 делилось на 3, и как a , так и b , делились бы на 3, что противоречит их взаимной простоте. За счет этого обстоятельства формулировки вспомогательных утверждений можно было еще несколько ослабить.

Пользуясь утверждением 7, разложим $a^2 + 3b^2$ в произведение (4). Поскольку в разложение может входить лишь один из множителей $p_i^2 + 3q_i^2$ и $p_i^2 + 3(-q_i)^2$, а p_i выбраны положительными, то все множители $p_i^2 + 3q_i^2$ однозначно определены. Поскольку $a^2 + 3b^2$ является кубом, то в разложении (4) все простые нечетные множители распадаются на группы по три совпадающих. Если взять из каждой такой группы по одному множителю и перемножить их по правилу (1), то получим такое число $p^2 + 3q^2$, что

$$a^2 + 3b^2 = (p^2 + 3q^2)^3 [(\pm 1)^2 + 3 \cdot 0^2].$$

Если в последней скобке оказывается +1, то на основании (3)

$$a^2 + 3b^2 = (p^3 - 9pq^2)^2 + 3(3p^2q - 3q^3)^2,$$

а поскольку согласно утверждению (2) представления совпадают, то

$$a = p^3 - 9pq^2, \quad b = 3p^2q - 3q^3. \quad (5)$$

Если же в последней скобке оказывается -1, то

$$\begin{aligned} a^2 + 3b^2 &= [-(p^3 - 9pq^2)]^2 + 3[-(3p^2q - 3q^3)]^2, \\ a &= (-p)^3 - 9(-p)(-q)^2, \quad b = 3(-p)^2(-q) - 3(-q)^3, \end{aligned}$$

т.е. a и b опять вычисляются по формулам (5), что и требовалось.

Лемма доказана.

Поскольку и в остальном доказательство элементарно, то тем самым, возможно, восстановлено предполагаемое доказательство Эйлера теоремы Ферма для $n = 3$. Очевидным также становится ответ на вопрос, почему здесь столь удобны комплексные числа.

Доказательство леммы, основанное на теории квадратичных вычетов, можно найти в [5; с. 384–388]. Оно весьма сложно, и обычно считалось, что элементарного доказательства теоремы Ферма для $n = 3$ не существует (ср. [3; с. 12] или [4; с. 10]). Впрочем, и в [5] в условиях леммы тоже безо всякой надобности требуется, чтобы число $x^2 + 3y^2$ было нечетным.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] H. Edwards, *Fermat's Last Theorem*, Springer, New York, 2000.
- [2] Г. Эдвардс, *Последняя теорема Ферма*, Генетическое введение в алгебраическую теорию чисел, Мир, М., 1980.
- [3] М. М. Постников, *Введение в теорию алгебраических чисел*, Наука, М., 1982.
- [4] М. М. Постников, *Теорема Ферма*, Введение в теорию алгебраических чисел, Наука, М., 1978.
- [5] W. Sierpinski, *Elementary Theory of Numbers*, PWN, Warsaw, 1964.

Ю. Ю. Мачис

Институт математики и информатики, г. Вильнюс, Литва

E-mail: jmacys@ktl.mii.lt

Поступило

03.02.2006