Последняя теорема Ферма: вызов на столетия

Аннотация

Слайды 1—2. Лекция посвящена более чем 300-летней истории попыток доказательства великой теоремы Ферма, начиная с момента формулирования этого утверждения Пьером Ферма (1642) и заканчивая доказательством теоремы Эндрю Уайлсом (1995). В качестве элементарных примеров рассмотрены уравнение Пифагора и случай $n = 4$, к которому приведено доказательство. Перечислены основные продвижения в области доказательства теоремы для конкретных показателей. Приведены переформулировки теоремы, следствия из неё, а также дан пример ошибочного доказательства. Показано, что метод бесконечного спуска к доказательству великой теоремы Ферма в общем случае неприменим.

1. Краткая история вопроса: от постановки проблемы до наших дней

Слайды 3—4. Все античные знания об уравнениях в целых и рациональных числах изложил Диофант Александрийский (III в. до н.э.) в своем знаменитом трактате «Арифметика», который стал отправной точкой для теоретико-числовых исследований Пьера Ферма (1601 — 1665), Леонарда Эйлера (1707 — 1783), Карла Гаусса (1777 — 1855) и других математиков.

На полях изданного собрания трудов Диофанта Ферма записал:

> «Невозможно разложить куб на два куба, биквадрат — на два биквадрата и, в общем случае, любую степень, большую двух, в сумму таких же степеней; я нашел поистине чудесное доказательство, но эти поля слишком узки, чтобы его вместить».

Слайд 5. На современном языке это значит следующее.

(A) *Пусть n — произвольное натуральное число, большее 2. Тогда уравнение*

$$X^n + Y^n = Z^n$$

не имеет решений в целых числах, каждое из которых отлично от 0 (т. е. оно имеет лишь тривиальные решения, где одно из чисел X, Y, Z равно 0).

Это утверждение было названо *последней теоремой* (*гипотезой* или *проблемой*) *Ферма*. Также широко употребляется термин «великая теорема Ферма».

Слайд 6. На протяжении трех с половиной веков математики — как ученые с мировым именем, так и находчивые любители — пытались доказать знаменитое утверждение Ферма. Изобретались новые подходы, создавались очень сложные теории. Однако несмотря на многочисленные попытки, ни современникам Ферма, ни последующим исследователям найти «чудесное доказательство» не удалось. Утверждение оставалось недоказанным до конца XX века.

Долгожданное доказательство было найдено Эндрю Уайлсом лишь в 90-х годах XX в. В нем были задействованы арифметическая теория эллиптических кривых, теория модулярных форм и т.д.

Начнем с некоторых замечаний.

Слайд 7. Для того чтобы доказать теорему Ферма для всех показателей, больших 2, достаточно доказать ее для показателя 4 и всех нечетных простых показателей p. Действительно, если число n составное, $n > 2$, то оно имеет делитель m, равный или 4, или нечетному простому числу p. Если утверждение теоремы не выполняется для $n = ml$, где $m = 4$ или p, $l > 1$, и x, y, z — такие отличные от нуля целые числа, что $x^n + y^n = z^n$, то $(x^l)^m + (y^l)^m = (z^l)^m$, а значит, теорема не выполнена и для m.

Пусть отличные от нуля целые числа x, y, z таковы, что $x^n+y^n = z^n$, и $x_1 = x/d, y_1 = y/d, z_1 = z/d$, где $d = \text{НОД}(x, y, z)$. Тогда $x_1^n+y_1^n = z_1^n$, где отличные от нуля целые числа x_1, y_1, z_1 попарно взаимно просты. Таким образом, если предположить, что существует нетривиальное решение уравнения Ферма, то это уравнение должно иметь еще одно решение в попарно взаимно простых числах.

В случае нечетных простых показателей p традиционно различают два случая теоремы Ферма.

1) *Первый случай теоремы Ферма* имеет место, если для любых отличных от нуля целых чисел x, y, z, не кратных p, выполнено соотношение $x^p + y^p \neq z^p$.

2) *Второй случай теоремы Ферма* имеет место, если для любых отличных от нуля попарно взаимно простых целых чисел x, y, z, таких, что p делит xyz, выполняется соотношение $x^p+y^p \neq z^p$. В этом случае p делит ровно одно из чисел x, y, z.

В общем случае говорят, что *первый случай теоремы Ферма* имеет место для произвольного целого показателя $n = 2^u m$, $u \geqslant 0$, m нечетно, если для любых отличных от нуля целых чисел x, y, z, таких, что НОД$(m, xyz) = 1$, имеет место соотношение $x^n + y^n \neq z^n$. Аналогично *второй случай* справедлив для показателя n, если для любых отличных от нуля попарно взаимно простых целых чисел x, y, z, таких, что НОД$(m, xyz) \neq 1$, выполняется соотношение $x^n + y^n \neq z^n$.

2. Уравнение Пифагора

Слайд 8. Кратко остановимся на уравнении Пифагора

$$X^2 + Y^2 = Z^2. \tag{1}$$

Тройка положительных целых чисел (x, y, z), таких, что $x^2 + y^2 = z^2$, называется *пифагоровой тройкой.* Например, $(3, 4, 5)$ — пифагорова тройка, поскольку $3^2 + 4^2 = 5^2$.

Если отличные от нуля целые числа x, y, z таковы, что $x^2 + y^2 = z^2$, то $|x|$, $|y|$, $|z|$ также удовлетворяют этому уравнению. Заметим, что x, y не могут оба быть нечетными, так как в противном случае $z^2 \equiv 1 + 1 \pmod 4$, что невозможно. Более того, если $d =$ НОД(x, y, z), то x/d, y/d, z/d удовлетворяют тому же уравнению. Таким образом, достаточно определить *примитивные решения* (x, y, z) уравнения (1), а именно такие, что $x > 0$, $y > 0$, $z > 0$, x четно и НОД$(x, y, z) = 1$, откуда y и z нечетны.

В книге Диксона «История теории чисел» утверждается, что Пифагор и Платон предложили методы нахождения решений уравнения (1). В лемме 1 к предложению 29 десятой книги «Начал» Евклид привел геометрический метод нахождения решений этого уравнения.

Диофант указал метод нахождения всех решений в форме утверждения (A') (см. далее).

Леонардо Пизанский (Фибоначчи) также привел в 1225 г. интересный метод нахождения решений.

Слайд 9. (A′) *Если целые числа a и b таковы, что $a > b > 0$ и* НОД$(a, b) = 1$, *причем a и b различной четности, то тройка (x, y, z), задаваемая равенствами*

$$\begin{cases} x = 2ab, \\ y = a^2 - b^2, \\ z = a^2 + b^2, \end{cases}$$

является примитивным решением уравнения (1). Эти соотношения устанавливают взаимно однозначное соответствие между множеством пар (a, b), удовлетворяющих указанным условиям, и множеством примитивных решений уравнения (1).

Доказательство. Пусть a и b — целые числа, удовлетворяющие условию утверждения. Определим x, y, z, как указано выше. Тогда

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2.$$

Ясно, что $x > 0$, $y > 0$, $z > 0$, x четно и НОД$(x, y, z) = 1$, потому что если d делит x, y и z, то d делит $2a^2$ и $2b^2$, так что $d = 1$ или $d = = 2$ (поскольку НОД$(a, b) = 1$); но $d \neq 2$, так как y нечетно (поскольку числа a, b имеют разную четность).

Нетрудно видеть, что различным парам (a, b) соответствуют различные тройки (x, y, z).

Обратно, пусть (x, y, z) — примитивное решение уравнения (1), так что $x^2 + y^2 = z^2$. Из равенства НОД$(x, y, z) = 1$ получаем НОД$(x, z) = 1$. Число x четно, значит, z нечетно, а следовательно, НОД$(z - x, z + x) = 1$. (Если $d \mid (z - x)$ и $d \mid (z + x)$, то $d \mid 2z$ и $d \mid 2x$. Но $d \neq 2$, а числа x и z взаимно просты. Значит, $d = 1$.) Поскольку $y^2 = (z - x)(z + x)$, из разложения на простые множители следует, что $z - x$ и $z + x$ являются квадратами целых чисел, скажем, $z + x = t^2$, $z - x = u^2$, причем t, u должны быть нечетными целыми числами, удовлетворяющими условию $t > u > 0$. Пусть a и b — целые числа, такие, что $2a = t + u$, $2b = t - u$, откуда

$t = a + b$, $u = a - b$ и $a > b > 0$. Тогда

$$\begin{cases} x = ((a+b)^2 - (a-b)^2)/2 = 2ab, \\ y^2 = u^2t^2 = (a-b)^2(a+b)^2 = (a^2-b^2)^2, \quad \text{так что } y = a^2 - b^2, \\ z = ((a+b)^2 + (a-b)^2)/2 = a^2 + b^2. \end{cases}$$

Заметим, что НОД$(a, b) = 1$, потому что НОД$(z - x, z + x) = 1$, и, наконец, поскольку t нечетно и $a + b = t$, мы заключаем, что числа a, b не являются нечетными одновременно. □

Например, наименьшие примитивные решения уравнения (1), упорядоченные по возрастанию значений z, таковы:

$$\begin{array}{llll} (4,3,5), & (12,5,13), & (8,15,17), & (24,7,25), \\ (20,21,29), & (12,35,37), & (40,9,41), & (28,45,53), \\ (60,11,61), & (56,33,65), & (16,63,65), & (48,55,73). \end{array}$$

Принимая во внимание утверждение (A′), найти примитивные решения уравнения (1) — значит определить, какие нечетные положительные числа являются суммами двух квадратов целых чисел, и в каждом случае выписать все такие представления. Ферма доказал, что положительное число n является суммой двух квадратов целых чисел тогда и только тогда, когда каждый простой делитель p числа n, такой, что $p \equiv 3 \pmod 4$, входит в разложение числа n на простые множители в четной степени. Пусть для каждого целого числа n, которое является суммой двух квадратов целых чисел, $r(n)$ обозначает число таких упорядоченных пар (a, b), что $a^2 + b^2 = n$, причем целые числа a, b *не* обязательно положительны. Например, $r(1) = 4$, $r(5) = 8$. Якоби и независимо от него Гаусс доказали, что

$$r(n) = 4\left(d_1(n) - d_3(n)\right),$$

где $d_1(n)$ (соответственно $d_3(n)$) есть количество делителей числа n, которые сравнимы с 1 по модулю 4 (соответственно сравнимы с 3 по модулю 4) (см. Харди и Райт (1938, с. 241)).

С учетом этого можно в явном виде выписать все примитивные пифагоровы тройки (x, y, z).

3. Биквадратное уравнение: метод бесконечного спуска, площадь пифагорова треугольника, вывод неразрешимости

Слайд 10. Перейдем теперь к случаю $n = 4$. Ферма рассматривал вопрос, может ли площадь пифагорова треугольника быть квадратом целого числа (наблюдение к Вопросу 20 Книги VI «Арифметики» Диофанта). Это привело его к уравнению

$$X^4 - Y^4 = Z^2, \tag{2}$$

и он доказал (дата неизвестна) следующее утверждение.

(B) *Уравнение (2) не имеет решений в целых числах, каждое из которых отлично от нуля.*

Доказательство. Пусть утверждение неверно и (x, y, z) — тройка натуральных чисел, такая, что $x^4 - y^4 = z^2$, причем x — наименьшее возможное число. Тогда НОД$(x, y) = 1$, так как если простое число p является общим делителем чисел x и y, то p^4 делит z^2, следовательно, p^2 делит z. Полагая $x = px'$, $y = py'$, $z = p^2z'$, получим $x'^4 - y'^4 = z'^2$, где $0 < x' < x$, что противоречит выбору тройки (x, y, z).

Мы можем записать $z^2 = x^4 - y^4 = (x^2 + y^2)(x^2 - y^2)$, причем, как легко видеть, НОД$(x^2 + y^2, x^2 - y^2)$ равен 1 или 2, поскольку НОД$(x, y) = 1$. Рассмотрим два случая.

Случай 1: НОД$(x^2 + y^2, x^2 - y^2) = 1$.

Так как произведение $(x^2 + y^2)(x^2 - y^2)$ является квадратом целого числа, каждое из чисел $x^2 + y^2$ и $x^2 - y^2$ есть квадрат целого числа. Говоря более точно, существуют натуральные числа s и t, удовлетворяющие условию НОД$(s, t) = 1$, такие, что

$$\begin{cases} x^2 + y^2 = s^2, \\ x^2 - y^2 = t^2. \end{cases}$$

Отсюда следует, что s и t должны быть нечетны (так как $2x^2 = s^2 + t^2$, числа s и t имеют одну и ту же четность, но они не могут быть оба четными).

Итак, существуют натуральные числа u и v, такие, что

$$\begin{cases} u = (s+t)/2, \\ v = (s-t)/2 \end{cases}$$

и непременно НОД$(u, v) = 1$, потому что s и t нечетны.

Ясно, что $uv = (s^2 - t^2)/4 = y^2/2$, откуда $y^2 = 2uv$. Поскольку НОД$(u, v) = 1$, существуют натуральные числа l и m, такие, что

$$\begin{cases} u = 2l^2, \\ v = m^2 \end{cases} \qquad \text{или} \qquad \begin{cases} u = l^2, \\ v = 2m^2. \end{cases}$$

Рассмотрим лишь первую возможность, так как вторая совершенно аналогична. Итак, u четно, НОД$(u, v, x) = 1$ и

$$u^2 + v^2 = \frac{(s+t)^2 + (s-t)^2}{4} = \frac{s^2 + t^2}{2} = x^2.$$

Из (A$'$) следует, что существуют натуральные числа a и b, $0 < b < a$, такие, что НОД$(a, b) = 1$ и

$$\begin{cases} 2l^2 = u = 2ab, \\ m^2 = v = a^2 - b^2, \\ \quad x = a^2 + b^2, \end{cases}$$

откуда $l^2 = ab$. Таким образом, существуют натуральные числа c и d, такие, что НОД$(c, d) = 1$ и

$$\begin{cases} a = c^2, \\ b = d^2, \end{cases}$$

а значит, $m^2 = c^4 - d^4$. Заметим, что $0 < c < a < x$ и тройка натуральных чисел (c, d, m) является решением рассматриваемого уравнения, что противоречит выбору числа x как наименьшего из возможных.

Случай 2: НОД$(x^2 + y^2,\ x^2 - y^2) = 2$.

Теперь x и y нечетны, а z четно. Согласно результату (A$'$) существуют такие натуральные числа a, b, $b < a$, что НОД$(a, b) = 1$ и

$$\begin{cases} x^2 = a^2 + b^2, \\ y^2 = a^2 - b^2, \\ z \ = 2ab. \end{cases}$$

Следовательно, $x^2y^2 = a^4 - b^4$, где $0 < a < x$, а это противоречит выбору числа x как наименьшего из возможных. □

Слайд 11. Изложенное рассуждение принадлежит Ферма и называется *методом бесконечного спуска*. Этот метод можно сформулировать так: если бы тройка (x_0, y_0, z_0) являлась решением уравнения (2) в натуральных числах, то нашлось бы еще одно решение этого уравнения в натуральных числах (x_1, y_1, z_1), где $x_1 < x_0$. Повторяя этот процесс, мы получили бы бесконечную убывающую последовательность натуральных чисел

$$x_0 > x_1 > x_2 > \cdots,$$

что невозможно.

Слайд 12. Получим в качестве следствия исходное утверждение Ферма, предложенное в качестве задачи или упомянутое в письмах Мерсенну [для Сен-Круа] (сентябрь 1636 г.), Мерсенну (май 1640 г.), Сен-Мартену (31 мая 1643 г.), Мерсенну (август 1643 г.), Паскалю (25 сентября 1654 г.), Дигби [для Валлиса] (7 апреля 1658 г.), Каркави (август 1659 г.).

(C) *Площадь пифагорова треугольника не является квадратом целого числа.*

Доказательство. Пусть a, b, c — стороны пифагорова треугольника, причем c — его гипотенуза. Тогда $c^2 = a^2 + b^2$. Предположим, что площадь является квадратом целого числа s: $ab/2 = s^2$. Тогда

$$\begin{cases} (a+b)^2 = c^2 + 4s^2, \\ (a-b)^2 = c^2 - 4s^2. \end{cases}$$

Следовательно, $(a^2 - b^2)^2 = c^4 - (2s)^4$, а значит, уравнение $X^4 - Y^4 = Z^2$ имеет нетривиальное решение в целых числах, что противоречит утверждению (B). □

Приведем еще одно утверждение, предложенное в качестве задачи или упомянутое в письмах Мерсенну [для Сен-Круа] (сентябрь 1636 г.), Мерсенну (1638 г.), Мерсенну (май 1640 г.).

(D) *Уравнение*

$$X^4 + Y^4 = Z^4$$

не имеет решений в целых числах, каждое из которых отлично от 0.

Доказательство. Если x, y и z — отличные от нуля целые числа, такие, что $x^4 + y^4 = z^4$, то $z^4 - y^4 = (x^2)^2$, что противоречит утверждению (B). □

Изложенные результаты были заново получены Эйлером (1770) и Лежандром (1808, 1830).

4. Основные продвижения в поисках доказательства

Слайд 13. Сам Пьер Ферма дал строгое доказательство своей знаменитой теоремы только для случая $n = 4$. Следующим шагом были попытки доказательства для первых простых нечетных показателей.

Случай $n = 3$. П. Ферма писал о случае $n = 3$ в нескольких письмах к Мерсенну, Дигби, Каркави и другим современникам, однако полного доказательства представлено не было. Впервые доказательство этого утверждения нашел Эйлер. Оно основывалось на методе бесконечного спуска и было представлено в его книге по алгебре, опубликованной в 1770 г. в Санкт-Петербурге и переведенной в 1802 г. на немецкий, а в 1822 г. на английский язык. Однако в результате критического изучения доказательства Эйлера был обнаружен важный пробел, связанный со свойствами делимости целых чисел вида $a^2 + 3b^2$.

В 1875 г. вышла объемная статья Пепена, посвященная числам вида $a + b\sqrt{-c}$. Автор указал на моменты, которые не были достаточно обоснованы Эйлером, когда тот рассматривал числа вида $a^2 + cb^2$, в частности при $c = 1, 2, 3, 4, 7$.

Строгое доказательство предложил в 1901 г. Э. Ландау; ту же цель преследовала и статья Холдена (1906), а в 1915 г. подробное доказательство вновь было представлено в книге Кармайкла.

Слайд 14. Случай $n = 5$. Этот случай был впервые рассмотрен П. Дирихле. В 1825 г. его статья была представлена в Парижской академии наук, но доказательство, опубликованное в 1828 г., не охватывало все возможные случаи. К тому времени как А. Лежандр опубликовал полное независимое доказательство, Дирихле уже обосновал последний остававшийся не разобранным случай. В дальнейшем новые варианты доказательства опубликовали и другие авторы: К. Гаусс (1863, посмертное издание), В. А. Лебег (1843), Г. Ламе (1847) и др.

Слайд 15. Случай $n = 7$. В 1839 г. Г. Ламе впервые доказал теорему Ферма для показателя 7. Более простое доказательство в 1840 г. нашел В. А. Лебег. Более простое рассуждение, основанное на идее Лежандра, предложил Дженокки (1874 г. и 1876 г.).

Другие случаи. Большое число статей посвящено доказательству теоремы Ферма для конкретных показателей, отличных от 3, 4, 5, 7. Используемые методы в большинстве случаев зависели от частных свойств показателя и не могли быть обобщены.

Из результатов для других показателей следует отметить замечательную теорему Софи Жермен, которая устанавливала «росчерком пера» (по выражению Лежандра) первый случай теоремы Ферма для всех простых показателей, меньших 100. Лежандр развил идеи С. Жермен в своей работе 1823 г.

5. Как, кем и когда проблема решена

Слайды 16—17. Долгожданное доказательство теоремы Ферма было получено только в конце XX века, спустя более трех столетий после того, как Ферма её сформулировал. 23 июня 1993 г. на своей третьей лекции в Институте Ньютона в Кембридже английский математик Эндрю Уайлс (род. 1953) объявил о доказательстве последней теоремы Ферма. В рукописи Уайлса, тщательно изученной различными экспертами, обнаружились пробелы, которые Уайлс устранил с помощью своего ученика Тейлора и в октябре 1994 г. опубликовал в журнале *Annals of Mathematics* две рукописи, занимающие более ста страниц (одна из них в соавторстве с Тейлором). Они содержали доказательство *гипотезы Шимуры—Таниямы* для случая полуустойчивых эллиптических кривых. Ранее Рибетом было показано, что эта гипотеза влечет за собой справедливость последней теоремы Ферма.

Доказательство Уайлса весьма сложно и является глубоким исследованием в теории эллиптических кривых и модулярных форм. Использованные в нём понятия далеко выходят за рамки знаний, обычно ожидаемых от любителей и даже от профессиональных математиков, работающих в других областях. При этом метод Уайлса в дальнейшем был применен и к другим диофантовым уравнениям.

6. Комбинаторная переформулировка

Слайд 18. Существует множество переформулировок великой теоремы Ферма — утверждений, которые ей эквивалентны.

Приведем одну неожиданную эквивалентную комбинаторную формулировку последней теоремы Ферма, предложенную в 1989 г. В. Квайном.

Рассмотрим множество, состоящее из $n \geqslant 3$ шаров, которые требуется распределить по z корзинам, окрашенным в белый, синий или красный цвет. Пусть W, B и R — число белых, синих и красных корзин соответственно. Тогда $z = W + B + R$. Введем следующие обозначения:

$(r'b)$ — число таких размещений n шаров по корзинам, что красные корзины остаются пустыми, но не все синие корзины пусты;

(rb') — число таких размещений n шаров по корзинам, что синие корзины пусты, а хотя бы в одной красной что-то есть;

(rb) — число таких размещений n шаров по корзинам, что не все синие и красные корзины пусты;

(w) — число таких размещений n шаров по корзинам, что все шары сосредоточены в белых корзинах.

(E) *Последняя теорема Ферма справедлива для показателя n тогда и только тогда, когда $(w) \neq (rb)$ для всех множеств из z корзин.*

Доказательство. Число всех размещений из n шаров по z корзинам равно z^n, поэтому

$$z^n = (w) + (r'b) + (rb') + (rb).$$

Пусть $x = R + W$ и $y = B + W$. Тогда число всех размещений из n шаров по корзинам, окрашенным в красный или белый цвет, равно

$$x^n = (w) + (rb'),$$

а число размещений из n шаров по синим и белым корзинам равно

$$y^n = (w) + (r'b).$$

Если последняя теорема Ферма справедлива для показателя $n \geqslant 3$, то $z^n \neq x^n + y^n$, а значит, $(rb) \neq (w)$.

Обратно, пусть утверждение теоремы Ферма не выполняется для показателя $n \geqslant 3$, т. е. существуют натуральные числа x, y, z такие, что $x^n + y^n = z^n$. Определим числа W, B, R из равенств

$$\begin{cases} B = z - x, \\ R = z - y, \\ W = x + y - z. \end{cases}$$

Согласно изложенному рассуждению $(w) = (rb)$. $\square$

7. Ошибочные доказательства

Слайд 19. За долгие столетия были предложены буквально тысячи ошибочных доказательств последней теоремы Ферма. Это можно объяснить тем, что формулировку данной задачи легко поймет даже любитель. Кроме того, академии и фонды предлагали значительные премии, которые стимулировали попытки как дилетантов, так и профессиональных математиков.

Статьи с ошибочными доказательствами публиковались даже в солидных математических журналах (ошибки в них указывались позднее, уже после публикации). Среди авторов ошибочных доказательств можно отметить известного математика Ф. Линдемана, который впервые доказал трансцендентность числа π. Некоторые авторы предлагали по нескольку десятков неверных доказательств, одно за другим.

Слайд 20. Попытки найти элементарное доказательство не прекращаются и по сей день.

Так, в августе 2005 года многие СМИ объявили о том, что омский ученый Александр Ильин нашел простое доказательство великой теоремы Ферма. Новость об этом даже попала на телевидение. Вот это «доказательство», опубликованное в «Новой газете»:

> Итак, требуется доказать, что если X и Y — целые числа в уравнении $X^n + Y^n = Z^n$, то Z (при $n > 2$) всегда не целое. Прежде чем браться за теорему Ферма, повторим теорему Пифагора: «Квадрат гипотенузы равен сумме квадратов катетов». Мы вправе для ее написания использовать любые переменные. Запишем ее таким образом: $X^2 + Y^2 = R^2$, где X, Y, R — целые числа, а Z, утверждает Ферма, — не целое. Попробуем доказать. Понятно, Z не равно R при одних и тех же X, Y. Легко доказуемо алгебраически, да и просто логически, что Z всегда меньше, чем R. Когда мы возводим X и Y в более высокую степень, то умножаем их на самих себя. Потом их складываем и получаем Z в той же степени n. А при возведении в нее R каждое из слагаемых надо умножить на R, которое больше, чем X и Y. К примеру, $R^3 = (X^2 + Y^2)R = X^2R + Y^2R$.
>
> Записываем длины сторон треугольника XYR в тригонометрическом виде: $X = R\sin A$, $Y = R\cos A$. А значит, $Z^n = X^n + Y^n = R^n(\sin A + \cos A)$. Тогда $Z = R(\sin A + \cos A)$. Ранее мы доказали, что Z всегда меньше R, стало быть, $\sin A + \cos A < 1$. Такую тригонометрическую функцию можно найти в любом учебнике математики старших классов и убедиться по графику или таблице, что если значение функции меньше 1, то угол A больше $60°$ и меньше $90°$. А что произойдет в этом случае с прямым углом , находящимся между катетами? Он больше уже не будет прямым и окажется в тех же пределах: $60° < B < 90°$.
>
> Любой десятиклассник, у которого по математике выше тройки, с ходу воспроизведет вам формулу соотношения сторон треугольника $Z^2 = X^2 + Y^2 - 2XY\cos B$. При $60° < B < 90°$ $\cos B$ — число не целое. А значит, и Z неминуемо является таковым при целых значениях X и Y. Что и требовалось доказать.

Слайд 21. Это «доказательство», разумеется, ошибочно. Например, в последнем абзаце содержится заведомо неверное утверждение: из того, что число $\cos B$ не целое, не следует, что $2XY\cos B$ (а значит и Z) не целое. В тексте доказательства есть много и других ошибок (попробуйте в качестве упражнения найти их как можно больше).

Еще более сложны для рассмотрения другие замысловатые и более объёмные «доказательства». Большое их количество можно найти в различных источниках (брошюрах, изданных на средства авторов, сети Интернет и т.п.).

Еще больше попыток доказательства присылались энтузиастами профессиональным математикам на проверку и не публиковались после указания на ошибки, найти которые — часто непростой труд.

8. В поисках элементарного доказательства: что мог иметь в виду сам Ферма?

Слайд 22. Многие считают, что Ферма не мог знать доказательства своей теоремы для всех n, а доказательство, о котором он писал, применимо лишь для некоторых значений n и представляет собой вариант метода бесконечного спуска.

В работе Эйлера *Opera Posthuma Mathematica et Physica*, Petropoli, 1862, Vol. 1, pp. 231–232, “Fragmenta arithmetica ex adversariis mathematicis deprompta”, содержится следующее рассуждение, принадлежащее Лекселю (Lexell A.J.). Оно представляет собой попытку применить метод бесконечного спуска к уравнению Ферма, что и мог иметь в виду сам Ферма. Однако эта попытка не удалась.

Предположим, что последняя теорема Ферма не имеет места для некоторого показателя $n > 2$. Можно считать, что n — нечетное простое число (мы воспользуемся лишь нечетностью n) и что существуют отличные от нуля целые числа a, b, c (не обязательно положительные), такие, что $a^n + b^n = c^n$, причем c четно, a и b нечетны, $a \neq b$ и НОД$(a, b, c) = 1$. Положим

$$\begin{cases} x = c^n/2, \\ y = (a^n - b^n)/2, \\ z = abc^{n-2}/2. \end{cases}$$

Тогда x, y, z — целые числа, причем x четно. Справедливы равенства

$$\begin{cases} x + y = a^n, \\ x - y = b^n, \end{cases}$$

следовательно,

$$\frac{x^2 - y^2}{4x^2} = \left(\frac{ab}{c^2}\right)^n = \left(\frac{z}{x}\right)^n.$$

Отсюда получим, что

$$\begin{aligned} x(x^n - 4z^n) &= x^{n-1}\left[x^2 - 4x^2\left(\frac{z}{x}\right)^n\right] \\ &= x^{n-1}y^2 = (x^{(n-1)/2}y)^2. \end{aligned}$$

Пусть $d = \text{НОД}(x, z)$. Тогда $d = c^{n-2}/2$, потому что $\text{НОД}(ab, c) = 1$. Положим $x = dx'$, $z = dz'$. Тогда x' кратно 4, $\text{НОД}(x', z') = 1$ и $d^{n+1}x'(x'^n - 4z'^n)$ есть квадрат целого числа, а значит, и $x'(x'^n - -4z'^n)$ тоже квадрат целого числа, причем $\text{НОД}(x', x'^n - 4z'^n) = 4$. Следовательно, существуют целые числа r, s, такие, что

$$\begin{cases} x' = r^2, \\ x'^n - 4z'^n = s^2. \end{cases}$$

Таким образом,

$$r^{2n} - s^2 = (r^n + s)(r^n - s) = 4z'^n.$$

Так как $r \equiv s \pmod 2$, мы заключаем, что $\text{НОД}(r^n + s, r^n - s) = 2$, а значит,

$$\begin{cases} r^n + s = 2t^n, \\ r^n - s = 2u^n. \end{cases}$$

Складывая эти равенства, получим $r^n = t^n + u^n$. Итак, мы получили нетривиальное решение уравнения Ферма, причем число r четно. Если бы выполнялось неравенство $r < c$, то, применяя метод спуска, мы пришли бы к противоречию. Однако

$$r^2 = x' = \frac{x}{d} = c^2,$$

поэтому $r = c$, так что метод спуска не применим.

Заключение

Слайд 23. Итак, многовековые поиски «чудесного доказательства», о котором писал Ферма на полях «Арифметики» Диофанта, так и не привели к успеху. Однако попытки многих учёных доказать теорему Ферма привнесли множество интересных идей в самые разные направления не только теории чисел, но и других областей математики. Один из ярких примеров — создание теории алгебраических чисел, к которому привело именно изучение теоремы Ферма. В процессе поиска решения знаменитой проблемы было получено множество замечательных результатов, которые существенно обогатили мир математики.