

TANIYAMA CONJECTURE  
AND FERMAT LAST  
THEOREM

Yu. P. SOLOV'EV

*The aim of this article is to present an introduction to the circle of ideas which form the background for the recent proof of Fermat Last Theorem: elliptic curves, modular forms, Frey's construction and the Taniyama conjecture.*

*Статья представляет собой введение в круг понятий и идей, на основе которых было получено доказательство последней теоремы Ферма: эллиптические кривые, модулярные формы, конструкция Фрея и гипотеза Таниямы.*

ГИПОТЕЗА ТАНИЯМЫ  
И ПОСЛЕДНЯЯ ТЕОРЕМА ФЕРМА

Ю. П. СОЛОВЬЕВ

Московский государственный университет  
им. М.В. Ломоносова

Нет ни одной математической проблемы, которая была бы столь популярна, как знаменитая последняя теорема Ферма [1]. Ее автор, Пьер Ферма (1601–1665), еще при жизни был признан одним из величайших математиков Европы. Сегодня имя Ферма неотделимо от теории чисел, однако его теоретико-числовые работы были настолько революционны и так опережали свое время, что их значение не было понято современниками и слава Ферма основывалась главным образом на его достижениях в других областях математики: ему принадлежат важные труды по аналитической геометрии (наряду с Декартом Ферма был одним из создателей этой науки), по теории максимумов и минимумов функций, впоследствии развившейся в математический анализ, и по геометрической оптике.

Свои научные результаты Ферма не публиковал. Будучи по профессии юристом, он посвящал математике лишь свободное время и не рассматривал ее как главное дело своей жизни. О сделанных им открытиях известно из его переписки с другими учеными, а также из бумаг, оставшихся после его смерти. В частности, на полях своего экземпляра “Арифметики” Диофанта, великого классического произведения древнегреческой математики, в 1621 году переведенного на латинский язык, Ферма оставил 48 замечаний, содержащих открытые им факты о свойствах чисел.

Доказательства Ферма до нас не дошли, однако в тех случаях, когда он утверждал, что доказал ту или иную теорему, впоследствии эту теорему удавалось доказать. Единственным исключением является следующее утверждение: “Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duas ejusdem nominis fas est dividere; cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet” (“Невозможно разложить куб на два куба, или биквадрат на два биквадрата, или вообще степень, большую двух, на две степени с тем же самым показателем; я нашел этому поистине чудесное доказательство, однако поля слишком узки, чтобы оно здесь вместились.”).

Этот текст, сопровождаемый указанием: “Наблюдение господина Пьера де Ферма”, содержится в издании трудов Диофанта, которое было выпущено Ферма-сыном в 1670 году, через 5 лет после смерти отца. Это подлинное замечание, внесенное Ферма

в его собственный экземпляр трудов Диофанта, в настоящее время утраченный. Каждому, кто держал в руках “Арифметику” Диофанта издания 1621 года, бросаются в глаза необычайно широкие поля – возможно, именно по этой причине Пьер Ферма записывал на них свои замечания.

Таким образом, в переводе на современный математический язык Ферма утверждал, что уравнение

$$a^n + b^n = c^n, \quad n > 2,$$

не имеет целочисленных решений с  $abc \neq 0$ . Это утверждение называется *последней* (или *великой*) *теоремой Ферма*. В настоящее время все специалисты твердо уверены в том, что Ферма не обладал доказательством этой теоремы и, сверх того, что элементарными методами ее нельзя доказать.

Более трехсот лет теорема Ферма привлекала внимание многих поколений математиков и служила беспрецедентным стимулом для развития математики. При попытках ее доказать были разработаны мощные средства, приведшие к созданию обширного раздела математики – теории алгебраических чисел. С помощью сложнейшей теоретико-числовой техники теорема Ферма была проверена для всех  $n \leq 4\,000\,000$ , но до конца 1994 года в общем случае оставалась недоказанной. Получить ее полное доказательство удалось лишь с помощью теории эллиптических кривых. Поэтому мы начнем с краткого экскурса в эту теорию [2].

## ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

Рассмотрим плоскую кривую, заданную уравнением третьей степени

$$f(x, y) = \alpha_3 x^3 + \alpha_2 x^2 y + \dots + \alpha_1 x + \alpha_2 y + \alpha_0 = 0. \quad (1)$$

Все такие кривые естественным образом разбиваются на два класса. К первому классу относятся те кривые, у которых имеются точки заострения (типа точки  $(0; 0)$  у кривой  $y^2 = x^3$ , самопересечения (как точка  $(0; 0)$  у кривой  $y^2 = x^3 + x^2$ ), а также кривые, для которых многочлен  $f(x, y)$  представляется в виде

$$f(x, y) = f_1(x, y) \cdot f_2(x, y),$$

где  $f_1(x, y), f_2(x, y)$  – многочлены меньших степеней. Кривые этого класса называются *вырожденными* кривыми третьей степени. Второй класс кривых образуют невырожденные кривые; мы будем называть их *эллиптическими*. Если коэффициенты многочлена (1) – рациональные числа, то эллиптическая кривая может быть преобразована к так называемой канонической форме

$$y^2 = x^3 + ax + b. \quad (2)$$

С каждой эллиптической кривой можно связать важную числовую характеристику – ее *дискриминант*. Для кривой, заданной в канонической форме (2), дискриминант  $\Delta$  определяется формулой

$$\Delta = -(4a^3 + 27b^2).$$

Пусть  $E$  – некоторая эллиптическая кривая, заданная уравнением

$$y^2 = x^3 + ax + b,$$

в котором  $a$  и  $b$  – целые числа. Для простого числа  $p$  рассмотрим сравнение

$$y^2 \equiv x^3 + \bar{a}x + \bar{b} \pmod{p}, \quad (3)$$

где  $\bar{a}$  и  $\bar{b}$  – остатки от деления целых чисел  $a$  и  $b$  на  $p$ , и обозначим через  $n_p$  число решений этого сравнения. Числа  $n_p$  очень полезны при исследовании вопроса о разрешимости уравнений вида (2) в целых числах: если какое-то  $n_p$  равно нулю, то уравнение (2) не имеет целочисленных решений. Однако вычислить числа  $n_p$  удается лишь в редчайших случаях.

В то же время известно, что  $|p - n_p| \leq 2\sqrt{p}$  (теорема Хассе).

Рассмотрим те простые числа  $p$ , которые делят дискриминант  $\Delta$  эллиптической кривой (2). Можно доказать, что для таких  $p$  многочлен  $x^3 + \bar{a}x + \bar{b}$  можно записать одним из двух способов:

$$x^3 + \bar{a}x + \bar{b} \equiv (x + \bar{\alpha})^2(x + \bar{\beta}) \pmod{p}$$

или

$$x^3 + \bar{a}x + \bar{b} \equiv (x + \bar{\gamma})^3 \pmod{p},$$

где  $\bar{\alpha}, \bar{\beta}, \bar{\gamma}$  – некоторые остатки от деления на  $p$ . Если для всех простых  $p$ , делящих дискриминант кривой, реализуется первая из двух указанных возможностей, то эллиптическая кривая называется *полустабильной*.

Простые числа, делящие дискриминант, можно объединить в так называемый *кондуктор* эллиптической кривой. Если  $E$  – полустабильная кривая, то ее кондуктор  $N$  задается формулой

$$N = \prod_{p|\Delta} p^{\epsilon_p}, \quad (4)$$

где для всех простых чисел  $p \geq 5$ , делящих  $\Delta$ , показатель  $\epsilon_p$  равен 1. Показатели  $\epsilon_2$  и  $\epsilon_3$  вычисляются с помощью специального алгоритма.

## МОДУЛЯРНЫЕ ФОРМЫ И МОДУЛЯРНЫЕ ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

Обозначим через  $H$  верхнюю комплексную полуплоскость. Пусть  $N$  – натуральное и  $k$  – целое числа. *Модулярной параболической формой* веса  $k$  уровня  $N$  называется аналитическая функция  $f(z)$ , заданная в верхней полуплоскости и удовлетворяющая соотношению

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \quad (5)$$

для любых целых чисел  $a, b, c, d$ , таких, что  $ad - bc = 1$  и  $c$  делится на  $N$ . Кроме того, предполагается, что

$$\lim_{t \rightarrow +0} f(r + it) = 0,$$

где  $r$  – рациональное число, и что

$$\lim_{t \rightarrow \infty} f(it) = 0.$$

Пространство модулярных параболических форм веса  $k$  уровня  $N$  обозначается через  $S_k(N)$ . Можно показать, что оно имеет конечную размерность.

В дальнейшем нас будут особо интересовать модулярные параболические формы веса 2. Для малых  $N$  размерность пространства  $S_2(N)$  представлена в табл. 1. В частности,

$$\dim S_2(2) = 0. \quad (6)$$

Отметим, что эта нехитрая формула сыграет важную роль в доказательстве теоремы Ферма.

**Таблица 1.** Размерности пространства  $S_2(N)$

dim $S_2(N)$												
$N \leq 10$	11	12	13	14	15	16	17	18	19	20	21	22
0	1	0	0	1	1	0	1	0	1	1	1	2

Из условия (5) следует, что  $f(z + 1) = f(z)$  для каждой формы  $f \in S_2(N)$ . Стало быть,  $f$  является периодической функцией. Такую функцию можно представить в виде

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \quad q = e^{2\pi iz}. \quad (7)$$

Назовем модулярную параболическую форму  $f(z) \in S_2(N)$  *собственной*, если ее коэффициенты – целые числа, удовлетворяющие соотношениям

$$a_1 = 1;$$

$$a_p^r a_p = a_{p^{r+1}} p c_{p^{r-1}} \quad \text{для простого } p, \\ \text{не делящего число } N; \quad (8)$$

$$a_{p^r} = (a_p)^r \quad \text{для простого } p, \text{ делящего число } N;$$

$$a_{mn} = a_m a_n, \quad \text{если } (m, n) = 1.$$

Сформулируем теперь определение, играющее ключевую роль в доказательстве теоремы Ферма. Эллиптическая кривая с рациональными коэффициентами и кондуктором  $N$  называется *модулярной*, если найдется такая собственная форма

$$f(z) = \sum_{n=1}^{\infty} a_n q^n \in S_2(N), \quad (9)$$

что  $a_p = p - n_p$  для почти всех простых чисел  $p$ . Здесь  $n_p$  – число решений сравнения (3).

## ГИПОТЕЗА ТАНИЯМЫ

Определение модулярной эллиптической кривой является настолько жестким, что на первый взгляд кажется невероятным существование хотя бы одной такой кривой. Трудно представить, что функция  $f(z)$ , удовлетворяющая перечисленным выше весьма ограничительным условиям (5) и (8), разлагается в ряд (7), коэффициенты которого связаны с практически невычислимыми числами  $n_p$ . Однако эмпирический материал, полученный в первой половине нашего века, позволил японскому математику Ю. Танияме (1927–1958) сформулировать в 1955 году удивительную гипотезу.

**Гипотеза Таниямы.** *Всякая эллиптическая кривая с рациональными коэффициентами является модулярной.*

В течение почти двадцати лет эта гипотеза не привлекала к себе внимания и стала популярной лишь в середине 70-х годов благодаря работам Г. Шимуры и А. Вейля.

В 1985 году немецкий математик Герхард Фрей предположил, что если теорема Ферма неверна, то есть если найдется такая тройка целых чисел  $a, b, c$ , что  $a^n + b^n = c^n$  ( $n \geq 3$ ), то эллиптическая кривая

$$y^2 = x(x - a^n)(x - c^n) \quad (10)$$

не может быть модулярной, что противоречит гипотезе Таниямы. Самому Фрею не удалось доказать это утверждение, однако вскоре доказательство было получено американским математиком Кеннетом Рибетом. Другими словами, Рибет показал, что *последняя теорема Ферма является следствием гипотезы Таниямы.*

23 июня 1993 года математик из Принстона Эндрю Уайлс, выступая на конференции по теории чисел в Кембридже (Великобритания), анонсировал доказательство гипотезы Таниямы для полустабильных эллиптических кривых, к которому относятся кривые вида (10). Тем самым он заявил, что доказал последнюю теорему Ферма. Дальнейшие события развивались довольно драматически. В начале декабря 1993 года, за несколько дней до того, как рукопись работы Уайлса должна была пойти в печать, в его доказательстве были обнаружены пробелы. Исправление их заняло свыше года. Текст с доказательством гипотезы Таниямы, написанный Уайлсом в сотрудничестве с Тейлором, вышел в свет летом 1995 года (см. [3, 4]).

В рамках этой статьи нет возможности сколь угодно подробно обсудить гипотезу Таниямы и привести ее доказательство (занимающее в оригинале около 150 страниц). Поэтому ограничимся тем, что покажем, как из этой гипотезы вытекает последняя теорема Ферма.

## ВЫВОД ТЕОРЕМЫ ФЕРМА ИЗ ГИПОТЕЗЫ ТАНИЯМЫ

Доказательство теоремы Ферма начнем со следующего замечания. Ясно, что если эта теорема доказана для некоторого показателя  $n$ , то тем самым она доказана и для всех показателей, кратных  $n$ . Так как всякое целое число  $n > 2$  делится или на 4, или на нечетное простое число, то можно поэтому ограничиться случаем, когда показатель равен либо четырем, либо нечетному простому числу. Для  $n = 4$  элементарное доказательство теоремы Ферма было получено Эйлером. Таким образом, достаточно изучить уравнение

$$a^l + b^l = c^l, \quad (11)$$

в котором показатель  $l$  есть нечетное простое число.

Воспользуемся теперь следующей теоремой.

**Теорема 1** (Рибет). Пусть  $E$  — эллиптическая кривая с рациональными коэффициентами, имеющая дискриминант

$$\Delta = \prod_{p|\Delta} p^{\delta_p}$$

и кондуктор

$$N = \prod_{p|\Delta} p^{\varepsilon_p}.$$

Предположим, что  $E$  является модулярной, и пусть

$$f(z) = q + \sum_{n=2}^{\infty} a_n q^n \in S_2(N)$$

есть соответствующая собственная форма уровня  $N$ . Фиксируем простое число  $l$ , и пусть

$$N_1 = \frac{N}{\prod_{p: \varepsilon_p = 1; l|\delta_p} p}. \quad (12)$$

Тогда существует такая параболическая форма

$$f_1(z) = \sum_{n=1}^{\infty} d_n q^n \in S_2(N_1)$$

с целыми коэффициентами, что разности  $a_n - d_n$  делятся на  $l$  для всех  $1 \leq n < \infty$ .

Теперь теорему Ферма можно получить простыми вычислениями.

**Теорема 2.** Из гипотезы Таниямы для полустабильных эллиптических кривых следует последняя теорема Ферма.

**Доказательство.** Предположим, что теорема Ферма неверна, и пусть

$$a^l + b^l = c^l$$

есть соответствующий контрпример (как и выше, здесь  $l$  — нечетное простое число). Применим теорему 1 к эллиптической кривой

$$y^2 = x(x - a^l)(x - c^l).$$

Несложные вычисления показывают, что кондуктор этой кривой задается формулой

$$N = \prod_{p|abc} p. \quad (13)$$

Сравнивая формулы (12) и (13), мы видим, что  $N_1 = 2$ . Следовательно, по теореме 1 найдется параболическая форма

$$f_1(z) = \sum_{n=1}^{\infty} d_n q^n,$$

лежащая в пространстве  $S_2(2)$ . Но в силу соотношения (6) это пространство нулевое. Поэтому  $d_n = 0$  для всех  $n$ . В то же время  $a_1 = 1$ . Стало быть, разность  $a_1 - d_1 = 1$  не делится на  $l$  и мы приходим к противоречию. Таким образом, теорема доказана.

Заметим в заключение, что значение гипотезы Таниямы не ограничивается связью с теоремой Ферма. С ее доказательством открываются новые горизонты в алгебраической геометрии и теории чисел.

## ЛИТЕРАТУРА

1. Постников М.М. Теорема Ферма. М.: Наука, 1972.
2. Прасолов В.В., Соловьев Ю.П. Эллиптические кривые и алгебраические уравнения. М.: Факториал, 1997.
3. Wiles A. Modular Elliptic Curves and Fermat's Last Theorem // Ann. Math. 1995. Vol. 141. P. 443.
4. Taylor R.L., Wiles A. Ring-Theoretic Properties of Certain Hecke Algebras // Ibid. P. 553.

\* \* \*

Юрий Петрович Соловьев, доктор физико-математических наук, профессор Московского государственного университета им. М.В. Ломоносова. Специалист в области дифференциальной геометрии, алгебраической и дифференциальной топологии, математической физики. Автор 60 научных статей, десяти монографий и учебников.