ловине 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, т. е. если найдется такая тройка целых чисел a, b, c, что $a^n + b^n = c^n$ ($n \geq 3$), то эллиптическая кривая

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

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 эллиптический кривых, к которым 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 сколько-нибудь 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

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

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

$$N_1 = \frac{N}{\prod\limits_{p:\varepsilon_p=1;\, l|\delta_p} p}. \qquad (12)$$

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

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

Несложные вычисления показывают, что кондуктор этой кривой задается формулой

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

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 доказательством этой гипотезы 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.