УДК 511.2
Черкасов М. Ю.
г. Иркутск, email: cherkasovmy@yandex.ru

КАК ПЬЕР ФЕРМА МОГ БЫ ДОКАЗАТЬ ПОСЛЕДНЮЮ ТЕОРЕМУ

Аннотация. Рассматривается доказательство, основанное на способе *от противного*, которое Пьер Ферма мог бы использовать для доказательства последней теоремы, применяя при этом метод *бесконечного спуска*.
Ключевые слова. Пьер Ферма, последняя теорема, метод бесконечного спуска.

Около 1637 г. на полях книги Диофанта «Арифметика» Пьер Ферма сформулировал свою знаменитую теорему о том, что уравнение $x^n+y^n=z^n$ не имеет решения в целых числах. Там же он оставил замечание: «Я нашел поистине удивительное доказательство этого предложения, но поля здесь слишком узки для того, чтобы вместить его».

Поиски хоть какого-нибудь доказательства этого утверждения длились более 350-ти лет, и закончились лишь в конце XX века. В 1955 году Танияма и Шимура выдвинули гипотезу о связи между эллиптическими кривыми и модулярными кривыми. В 1984 году Герхард Фрэй преобразовал уравнение Ферма в эллиптическую кривую и, тем самым, установил связь между теоремой Ферма и гипотезой ТаниямыШимуры, т.е. если гипотеза верна, то уравнение Ферма не имеет решений в целых числах. В 1993 году Эндрю Уайлс в своем докладе сообщил о найденном им доказательстве гипотезы ТаниямыШимуры. Тем самым доказал последнюю теорему Ферма. В этом доказательстве были обнаружены пробелы и недочеты, после исправления которых, доклад был опубликован в 1995 году. Более подробно историю об этом можно почерпнуть из книги Саймона Сингха «Великая теорема Ферма», МЦНМО, 2000 г.

Пьер Ферма не мог знать ни об эллиптических кривых, ни о модулярных формах. Достаточно часто при доказательстве своих теорем использовал способ доказательства *от противного*, используя метод *бесконечного спуска*. Тогда ход его рассуждений мог быть следующим: допустим, что существует тройка натуральных чисел x, y и z, удовлетворяющих уравнению:

$$x^n+y^n=z^n \qquad (*)$$

Из этой тройки чисел только одно может быть четным. Предположим, что этим числом является x, тогда уравнение (*) можно записать в виде:

$$(2x_1)^n+y^n=z^n$$

или

$$2^n\cdot x_1{}^n=z^n-y^n$$

тогда

$$2^n\cdot x_1{}^n=2^n\cdot M_1$$

в силу допущения существования таких x,y и z, множитель M_1 должен быть представим как разность степеней n двух чисел: $M_1{}^n=z_1{}^n-y_1{}^n$, Таким образом, получили уравнение:

$$x_1{}^n=z_1{}^n-y_1{}^n$$

где $x_1<x$, $y_1<y$,$z_1<z$.

Допустим теперь, что z_1 является четным, тогда, проводя аналогичные рассуждения, получим уравнение:

$$x_2{}^n+y_2{}^n=z_2{}^n$$

где $x_2<x_1$, $y_2<y_1$, $z_2<z_1$.

Подобные рассуждения можно продолжать до бесконечности (в этом и заключается метод *бесконечного спуска*). Т.к. ряд натуральных чисел ограничен снизу, то достаточно рассмотреть случай, когда $x=4$ (или y):

$$(4)^n=z^n-y^n$$

или, при нечетном n

$$2^n\cdot 2^n=(z-y)\cdot(z^{n-1}+z^{n-2}\cdot y+\cdots+z\cdot y^{n-2}+y^{n-1})$$

Выражение $(z^{n-1}+z^{n-2}\cdot y+\cdots+z\cdot y^{n-2}+y^{n-1})$ является суммой нечетного количества нечетных чисел, т.е. является нечетным числом. Следовательно, $(z-y)=2^n$. Таким образом, пришли к противоречию: четное 2^n равно нечетному $(z^{n-1}+z^{n-2}\cdot y+\cdots+z\cdot y^{n-2}+y^{n-1})$, что и доказывает последнюю теорему Ферма.