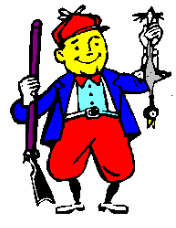


В.С.Ярош

НЕМОДУЛЯРНЫЕ ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ КАК УНИВЕРСАЛЬНЫЙ КЛЮЧ ДЛЯ РЕШЕНИЯ ПРОБЛЕМ P.FERMAT'S, P.GORDAN'S, H.POINCARE'S , A.BEAL'S.

Государственное унитарное предприятие
«Всероссийский научно-исследовательский институт
оптико-физических измерений»
(ГУП «ВНИИ ОФИ»)

103031, Москва, ул. Рождественка, 27
Телефон: 430-42-89
Факс: 437-31 -47

Оглавление

1. Введение

Известно , что доказательство Последней теоремы Пьера Ферма (ПТФ) основано на гипотезе Шимуры-Таниямы, которая утверждает :

Все эллиптические кривые модулярны [2] .

Первые строки основополагающей работы [1] А.Уайлса свидетельствуют об этом. Для убедительности привожу эти первые строки без купюр:

An elliptic curve over **Q** is said to be modular if it has a finite covering by a modular curve of the form $X_0(N)$. Any such elliptic curve has the property that its Hasse-Weil zeta function has an analytic continuation and satisfies a functional equation of the standard type. If an elliptic curve over **Q** with a given j-invariant is modular then it is easy to see that all elliptic curves with the same j-invariant are modular (in which case we say that the j-invariant is modular). A well-known conjecture which grew out of the work of Shimura and Taniyama in the 1950's and 1960's asserts that every elliptic curve over **Q** is modular. However, it only became widely known through its publication in a paper of Weil in 1967 [We] (as an exercise for the interested reader!), in which, moreover, Weil gave conceptual evidence for the conjecture. Although it had been numerically verified in many cases, prior to the results described in this paper it had only been known that finitely many j-invariants were modular.

In 1985 Frey made the remarkable observation that this conjecture should imply Fermat's Last Theorem. The precise mechanism relating the two was formulated by Serre as the ε-conjecture and this was then proved by Ribet in the summer of 1986. Ribet's result only requires one to prove the conjecture for semistable elliptic curves in order to deduce Fermat's Last Theorem.

В предлагаемой статье описано доказательство реального существования бесконечного множества немодулярных эллиптических кривых. Из этого доказательства следует вывод о том, что доказательство ПТФ, предложенное доктором А.Уайлсом, [1], ошибочно. Доказательство этого феномена теории чисел базируется на подстановках , которые автор статьи конструирует из примитивных троек Пифагора , [2],[3]:

$$a_o = v^2 - u^2$$
$$b_o = 2vu \qquad (1)$$
$$c_o = v^2 + u^2$$

Здесь $v > u$ любые натуральные числа различной чётности.

Подстановки имеют следующий ви

$$(X - A) = a_0{}^n$$
$$A = X - a_o{}^n = (b_o{}^n - a_o{}^n)$$
$$X = b_0{}^n \qquad (2)$$
$$(X + B) = c_0{}^n$$
$$B = c_o{}^n - X = c_o{}^n - b_o{}^n = a_o{}^n$$

Эти подстановки внедряются в уравнение Фрея [2] :

$$Y^2 = (X - A) \cdot X \cdot (X + B) \qquad (3)$$

В результате автор получает спектр уравнений собственных эллиптических кривых:

$$Y^2 = (X - a_o{}^n) \cdot X \cdot (X + a_o{}^n) \qquad (4)$$

число которых определяется количеством показателей степени:

$$n = 2, 3, 4, 5, ..., \infty$$

(5)

Эти уравнения могут быть записаны в двух эквивалентных формах:

$$Y^2 = a_o{}^n \cdot b_o{}^n \cdot (b_o{}^n + a_o{}^n) \qquad (6)$$

$$Y^2 = [(2vu)^n \cdot (v^2 - u^2)^n] \cdot (2vu)^n \cdot [(2vu)^n + (v^2 + u^2)^n] \qquad (7)$$

Форма (7) позволяет оценить роль примитивных троек Пифагора в теории чисел. Решить уравнение (7) без использования форм (1) невозможно. Ниже я привожу более точное определение форм (1), позаимствованное из [2]:

Если целые числа v и u таковы, что $v > u > 0$ и НОД $(v, u) = 1$, причём v и u различной чётности, то триада (a_o, b_o, c_o), задаваемая равенствами :

$$a_o = v^2 - u^2$$
$$b_o = 2vu \qquad (8)$$
$$c_o = v^2 + u^2$$

является примитивным решением уравнения:

$$x^2 + y^2 = z^2 \qquad (9)$$

Эти соотношения устанавливают взаимно однозначное соответствие между множеством пар (v, u), удовлетворяющих указанным условиям, и множеством примитивных решений уравнения $x^2 + y^2 = z^2$.

Примечание:

Написание формул (8) принято как у Куранта , [3], что соответствует порядку расстановки примитивных чисел в триаде (a_o, b_o, c_o) ***. У автора [2] вычисление примитивных троек осуществляется по формулам:***

$$a_o = 2vu$$
$$b_o = v^2 - u^2 \qquad (10)$$
$$c_o = v^2 + u^2$$

что соответствует расстановке примитивных чисел в триаде (b_o, a_o, c_o) ***и на результаты дальнейших вычислений не влияет.***

Уравнение Фрея (3), трансформированное в уравнение (6), отображает известное утверждение Пьера Ферма [1] на латинском языке :
Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hans marginis exiguitas non caperet.

На русском это утверждение звучит так:

«Невозможно разложить куб на два куба, биквадрат - на два биквадрата и ,в общем случае, любую степень, большую двух, в сумму таких же степеней».

Уравнение (6), при показателе степени, равном два, приобретает смысл тождественного равенства целых чисел:

$$Y^2 = {a_o}^2 \cdot {b_o}^2 \cdot ({b_o}^2 + {a_o}^2) = = {a_o}^2 \cdot {b_o}^2 \cdot {c_o}^2 \qquad (11)$$

где

$$Y = \sqrt{a_o{}^2 \cdot b_o{}^2 \cdot c_o{}^2} =$$
$$= a_o \cdot b_o \cdot c_o$$

всегда целое число.

Следствием этого утверждения служит уравнение Пьера Ферма , которое выводится из формы (11).

Увеличивая показатель степени в правой части этого уравнения, мы получаем более общую математическую модель для любого показателя степени $n \geq 2$:

$$Y^2 = a_o{}^n \cdot b_o{}^n \cdot (b_o{}^n + a_o{}^n) \qquad (12)$$

Легко видеть, что правый крайний множитель этой математической модели допускает отождествление с уравнением Пьера Ферма, переменными величинами в котором служат примитивные тройки Пифагора:

$$(b_o{}^n + a_o{}^n) = c_o{}^n \qquad (13)$$

Форма (12) доставляет нам третий член этого уравнения :

$$c_o{}^n = (b_o{}^n + a_o{}^n) = \frac{Y^n}{a_o^n \cdot b_o{}^n} \qquad (14)$$

Полагая:

$$x \equiv a_o \ ; \ y \equiv b_o \ ; \ z \equiv c_o \ ;$$

мы приходим к уравнению:

$$x^n + y^n = z^n \qquad (15)$$

Целые числа $x \equiv a_o \ ; \ y \equiv b_o \ ; \ z \equiv c_o \ ;$ содержат в своей основе пары целых чисел $v > u$, см. (1).

Фрей , по-видимому, знал об этом и , в процессе исследования свойств своей эллиптической кривой (3), пришёл к выводу, который адекватен утверждению Ферма, приведенному выше.

2. Демонстрационное частное доказательство

Рассмотрим свойства моих эллиптических кривых (6) и (7).

Вычислим МИНИМАЛЬНЫЙ ДИСКРИМИНАНТ кривой, см. [2], для первой примитивной тройки:

$$\begin{aligned} a_0 &= (2^2 - 1^2) = 3 \\ b_0 &= (2 \cdot 2 \cdot 1) = 4 \\ c_0 &= (2^2 + 1^2) = 5 \end{aligned} \qquad (16)$$

при минимальном n=2 :

$$\Delta = [(a_0 \cdot b_0 \cdot c_0)^{2n}] / 2^8 = 50625 \qquad (17)$$

Для простого n =5 , минимальный дискриминант равен:

$$\Delta = 23.6196 \cdot 10^{14} \qquad (18)$$

Поскольку дискриминанты на равны нулю, кривые НЕСИНГУЛЯРНЫ.
Следовательно - это есть ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ.
На этот факт указывает и то, что простой n=2
НЕ ДЕЛИТ свой дискриминант (17) без остатка.

Специалисты знают, почему число 16 имеет смысл "лакмусной бумажки" для уравнения Фрея, которое он исследовал при n = 5.
Не входя в подробности, продемонстрируем это свойство числа 16 на конкретном примере для примитивной тройки (16).
При n=5 моя кривая получает детерминированное выражение:

$$Y^2 = a_o{}^5 \cdot b_o{}^5 \cdot c_o{}^5 = 3^5 \cdot 4^5 \cdot 5^5 = 243 \cdot 1024 \cdot 3125 = 777600000 \qquad (19)$$

При этом:

$$a_0{}^{n-1} = 3^4 = 81$$

удовлетворяет сравнению:

$$a_o{}^{n-1} \equiv 1 \pmod{16}$$

ибо число

$$(a_o{}^4 = 81) - 1 = 80$$

делится на 16 без остатка:

$$80/16 = 5$$

но

$$b_o{}^{n-1} = 4^4 = 256$$

не удовлетворяет сравнению:

$$b_o{}^{n-1} \equiv 1 \pmod{16}$$

ибо число

$$(b_o{}^4 = 256) - 1 = 255$$

делится на 16 с остатком:

$$255/16 = 15.9375$$

Следовательно, числа, формирующие рассматриваемую эллиптическую кривую, не могут СРАВНИВАТЬСЯ по модулю $d = 2^{5-1} = 16$ без остатка, равного единице.
При этом, само число 16 удовлетворяет сравнению, отображающему свойства ПТФ при всех простых показателях степени n :

$$a^{n-1} \equiv 1 \pmod{n} \qquad (20)$$

Если a = 2 и n = 5, то сравнение (20) соблюдается:

$$2^{5-1} \equiv 1 \pmod{5} \qquad (21)$$

ибо:

$$(2^4 = 16) - 1 = 15$$

делится на модуль 5 без остатка.

В Ы В О Д

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ (4) – (6) – (7) - НЕМОДУЛЯРНЫ
ГИПОТЕЗА ШИМУРЫ - ТАНИЯМЫ ОШИБОЧНА
ДОКАЗАТЕЛЬСТВО УАЙЛСА – НЕДОСТОВЕРНО

Это - локальная математическая катастрофа. Однако, в этом событии есть и положительная сторона. Автор [2] пишет:
«Изучение теоремы Ферма привело к созданию теории алгебраических чисел, подобно тому, как изучение квадратичных полей было вызвано гауссовой теорией квадратичных форм. Ветвь математики, лежащая на стыке теории чисел и алгебраической геометрии и называемая *арифметической алгебраической геометрией* , развивалась не только исходя из своих внутренних потребностей, но также имея в виду доказательство последней теоремы Ферма. Неужели этот стимул исчезнет теперь, когда ПТФ доказана ? Отнюдь нет. Варианты задачи , обобщения на высшие размерности, будут продолжать терзать математиков.»
Эффективность перехода от бесконечного ряда натуральных чисел к бесконечному ряду примитивных троек Пифагора теория чисел будет ещё долго и тщательно изучать.

3. Проблема Пьера Ферма и проблема инвариантов Пауля Гордана.

В формулировке алгоритма решения проблемы инвариантов Пауля Гордана (1837-1912) , предложенной Давидом Гильбертом (1861-1944),[4]-[7], содержится алгоритм решения проблемы Пьера Ферма (1601-1665). Согласно [8] этот алгоритм описывается следующим образом. Гильберт полагает:
«Пусть задана бесконечная система форм от конечного числа переменных».
В нашем случае мы имеем бесконечное количество уравнений:

$$\begin{aligned} &x^2 + y^2 = z^2 \\ &x^3 + y^3 = z^3 \\ &x^4 + y^4 = z^4 \\ &x^5 + y^5 = z^5 \\ &\dots\dots\dots\dots\dots \\ &x^n + y^n = z^n \end{aligned} \tag{22}$$

с конечным числом переменных x, y, z, n

Гильберт задаёт вопрос:
«При каких условиях существует конечная система форм, через которую все другие выражаются в виде линейных комбинаций, коэффициенты суть целые рациональные функции от тех же переменных ?»
В книгах [4], [5], опубликованных в 1993 году на русском и английском в Москве, издательством «Инженер», использована следующая линейная комбинация из примитивных троек Пифагора :

$$L_o = (a_o{}^{n-2} + b_o{}^{n-2} + c_o{}^{n-2}) \tag{23}$$

в которой, применительно к уравнениям (17) , принято :

$$x \equiv a_o \ ; \ y \equiv b_o \ ; \ z \equiv c_o \ ; \tag{24}$$

В результате были получены три формулы для вычисления корней уравнений (22) :

$$\begin{aligned} x_n &= \sqrt[n]{a_o{}^2 \cdot D_n} \\ y_n &= \sqrt[n]{b_o{}^2 \cdot D_n} \\ z_n &= \sqrt[n]{c_o{}^2 \cdot D_n} \end{aligned} \tag{25}$$

Здесь используется общий множитель, основанный на комбинации (23):

$$D_n = L_o / 3 = (a_o{}^{n-2} + b_o{}^{n-2} + c_o{}^{n-2}) / 3 \tag{26}$$

С выводом и анализом формул (25) можно познакомиться в книгах [4], [5].

4. Проблема П.Ферма и вторичные приведенные формы теории чисел А.Пуанкаре

В первой публикации [9] , во Ведении, А.Пуанкаре выделяет следующее: "Арифметическое исследование гомогенных форм является одним из наиболее интересных вопросов теории чисел и вопросов , которые - больше всего интересны для геометров." Следовательно, А,Пуанкаре исходил из фундаментального свойства всех законов природы . Такое фундаментальное свойство законов природы было окончательно осмыслено и нашло своё отображение в Принципе всеобщей ковариантности , [11] :
«Каждая физическая величина должна описываться геометрическим объектом (независимо от наличия координат), а все законы физики должны выражаться в виде геометрических соотношений между этими геометрическими объектами».
Этот Принцип прекрасно иллюстрируется приведенным выше утверждением П.Ферма:

«Невозможно разложить куб на два куба, биквадрат - на два биквадрата и ,в общем случае, любую степень, большую двух, в сумму таких же степеней».

Ниже мы рассмотрим наглядную иллюстрацию Принципа всеобщей ковариантности .
Цель этого раздела статьи в том, чтобы подтвердить геометрическую сущность одного специального раздела Теории чисел Пуанкаре, который содержит информацию о точном геометрическом доказательстве Последней теоремы Ферма.
С этой целью, обратимся к публикации [12] Пуанкаре, переведенной на русский язык, смотри. [10] . Привожу цитату из [10], стр.888:

"Всё, о чём мы говорили до сих пор, применимо только к главным приведенным формам, к которым применимы следующие результаты. Существуют классы приведенных форм. При этом:

1.В каждом классе, вообще говоря, есть только одна главная приведенная форма.
2. Существует бесконечно много классов.

3.Главные приведенные формы делятся на три вида.
4.Форм первого и второго вида конечное число.
5.Формы третьего вида разделяются на бесконечное множество родов, а каждый род содержит бесконечное множество приведенных форм.

Займёмся вторичными приведенными формами»

Вторичные приведенные формы имеют смысл инвариантов

Из анализа этих форм, давайте выберем фрагмент исследования, который имеет связь с геометрическим доказательством Последней теоремы Ферма, [9] , [10] стр.819.

Этот фрагмент у Пуанкаре описан так (смотри страницу 889 в [10]):
"Так как три целых числа $(a_1;a_2;a_3)$ взаимно просты, то всегда есть Девять Целых Чисел, удовлетворяющих следующим условиям:

$$\begin{aligned} &a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3 = 1 \\ &a_1 = \beta_2\gamma_3 - \beta_3\gamma_2 \\ &a_2 = \beta_3\gamma_1 - \beta_1\gamma_3 \\ &a_3 = \beta_1\gamma_2 - \beta_2\gamma_1 \end{aligned} \tag{27}$$

Мы построим систему Девяти Целых Чисел в виде Трёх инвариантов:

$$F'_a = a'_1 \cdot \alpha'_1 = a'_2 \cdot \alpha'_2 = a'_3 \cdot \alpha'_3 \tag{28}$$

$$F'_b = b'_1 \cdot \beta'_1 = b'_2 \cdot \beta'_2 = b'_3 \cdot \beta'_3 \tag{29}$$

$$F'_c = c'_1 \cdot \gamma'_1 = c'_2 \cdot \gamma'_2 = c'_3 \cdot \gamma'_3 \tag{30}$$

левые части которых формируются из примитивных троек Пифагора:

$$\begin{aligned} &F'_a = {a_0}^2 \cdot D_n \\ &F'_b = {b_0}^2 \cdot D_n \\ &F'_c = {c_0}^2 \cdot D_n \end{aligned} \tag{31}$$

Общий множитель D_n будем вычислять по формуле (26). Элементы правых частей инвариантов (28), (29) и (30) будем вычислять по формулам, приведенным ниже. Вывод этих формул описан в книгах [4], [5] :

$$\begin{aligned} &\alpha'_1 = (a_0 \cdot D_n) / \sqrt{{a_0}^{n-2}} \\ &\alpha'_2 \ = (a_0 \cdot D_n) / \sqrt{{b_o}^{n-2}} \\ &\alpha'_3 = (a_0 \cdot D_n) / \sqrt{{c_0}^{n-2}} \end{aligned} \tag{32}$$

$$\beta_1' = (b_0 \cdot D_n) / \sqrt{a_0^{\,n-2}}$$
$$\beta_2' = (b_0 \cdot D_n) / \sqrt{b_0^{\,n-2}} \qquad (33)$$
$$\beta_3' = (b_o \cdot D_n) / \sqrt{c_0^{\,n-2}}$$

$$\gamma_1' = (c_0 \cdot D_n) / \sqrt{a_o^{\,n-2}}$$
$$\gamma_2' = (c_0 \cdot D_n) / \sqrt{b_0^{\,n-2}} \qquad (34)$$
$$\gamma_3' = (c_0 \cdot D_n) / \sqrt{c_0^{\,n-2}}$$

$$a_1' = a_0 \cdot \sqrt{a_0^{\,n-2}}$$
$$a_2' = a_0 \cdot \sqrt{b_0^{\,n-2}} \qquad (35)$$
$$a_3' = a_0 \cdot \sqrt{c_0^{\,n-2}}$$

$$b_1' = b_0 \cdot \sqrt{a_0^{\,n-2}}$$
$$b_2' = b_0 \cdot \sqrt{b_0^{\,n-2}} \qquad (36)$$
$$b_3' = b_0 \cdot \sqrt{c_0^{\,n-2}}$$

$$c_1' = c_0 \cdot \sqrt{a_0^{\,n-2}}$$
$$c_2' = c_0 \cdot \sqrt{b_0^{\,n-2}} \qquad (37)$$
$$c_3' = c_0 \cdot \sqrt{c_o^{\,n-2}}$$

Первую инвариантную форму Пуанкаре, см.(2):

$$a_1'\alpha_1' + a_2'\alpha_2' + a_3'\alpha_3' = 1 \qquad (38)$$

представим в виде трёх инвариантных форм

$$(a_1'\alpha_1' + a_2'\ \alpha_2' + a_3'\alpha_3') / 3F'_a = 1$$
$$(b_1'\beta_1' + b_2'\beta_2' + b_3'\beta_3') / 3F'_b = 1 \qquad (39)$$
$$(c_1'\gamma_1' + c_2'\gamma_2' + c_3'\gamma_3') / 3F'_c = 1$$

Вернёмся ещё раз к утверждению Пуанкаре :
Так как три целых числа $(a_1; a_2; a_3)$ взаимно просты, то всегда есть Девять Целых Чисел, удовлетворяющих следующим условиям:

$$\begin{aligned} &a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3 = 1 \\ &a_1 = \beta_2\gamma_3 - \beta_3\gamma_2 \\ &a_2 = \beta_3\gamma_1 - \beta_1\gamma_3 \\ &a_3 = \beta_1\gamma_2 - \beta_2\gamma_1 \end{aligned} \tag{40}$$

Следуя этому утверждению, конструируем математические модели триады взаимно простых целых чисел $(a_1; a_2; a_3)$ из взаимно простых триад примитивных троек Пифагора (a_o, b_o, c_o).

В результате получаем девять легко вычисляемых формул для трёх триад $(a_1; a_2; a_3)$:

$$\begin{aligned} a_1 &= a_1'^2 = a_0{}^2(a_0{}^{n-2}) \\ a_2 &= a_2'^2 = a_0{}^2(b_0{}^{n-2}) \\ a_3 &= a_3'^2 = a_0{}^2(c_0{}^{n-2}) \end{aligned} \tag{41}$$

$$\begin{aligned} b_1 &= b_1'^2 = b_0{}^2(a_0{}^{n-2}) \\ b_2 &= b_2'^2 = b_0{}^2(b_0{}^{n-2}) \\ b_3 &= b_3'^2 = b_0{}^2(c_0{}^{n-2}) \end{aligned} \tag{42}$$

$$\begin{aligned} c_1 &= c_1'^2 = c_0{}^2(a_0{}^{n-2}) \\ c_2 &= c_2'^2 = c_0{}^2(b_0{}^{n-2}) \\ c_3 &= c_3'^2 = c_0{}^2(c_0{}^{n-2}) \end{aligned} \tag{43}$$

а также три формулы обнуления правых частей трёх последних условий Пуанкаре, см. (27) и (40) :

$$\begin{aligned} &\beta_2'\gamma_3' - \beta_3'\gamma_2' = 0 \\ &\beta_3'\gamma_1' - \beta_1'\gamma_3' = 0 \\ &\beta_1'\gamma_2' - \beta_2'\gamma_1' = 0 \end{aligned} \tag{44}$$

Кажущееся противоречие с условиями Пуанкаре (27) и (40) можно устранить, используя результаты доказательства теоремы Жордана, полученные самим Пуанкаре, см. [10] на стр.867.

Пуанкаре констатирует:
«Для того, чтобы формы, алгебраически эквивалентные данной форме, распадались на *бесконечное число классов*, необходимо и достаточно, чтобы не только дискриминант, но ещё и другие образованные нами инварианты *одновременно обращались в нуль*».

В результате, используя инварианты (31) , мы приходит к формулам :

$$\begin{aligned} a &= \sqrt[n]{F'_a} = \sqrt[n]{a_o{}^2 \cdot D_n} \\ b &= \sqrt[n]{F'_b} = \sqrt[n]{b_o{}^2 \cdot D_n} \\ c &= \sqrt[n]{F'_c} = \sqrt[n]{c_o{}^2 \cdot D_n} \end{aligned} \tag{45}$$

которые эквивалентны формулам (25) :

$$\begin{aligned} x_n &= \sqrt[n]{a_o{}^2 \cdot D_n} \\ y_n &= \sqrt[n]{b_o{}^2 \cdot D_n} \\ z_n &= \sqrt[n]{c_o{}^2 \cdot D_n} \end{aligned} \tag{46}$$

для вычисления *бесконечного число классов* (терминология Пуанкаре) корней уравнений Пьера Ферма, см. (22):

$$\begin{aligned} &x^2 + y^2 = z^2 \\ &x^3 + y^3 = z^3 \\ &x^4 + y^4 = z^4 \\ &x^5 + y^5 = z^5 \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &x^n + y^n = z^n \end{aligned} \tag{47}$$

5. Алгоритм решения Conjecture A.Beal

Широко известна проблема решения уравнения , которое сложнее, чем уравнение Пьера Ферма. Существование такого уравнения предположил банкир из Техаса (США) Андрей Бил. Гипотеза Била известна в литературе и в Интернете, как Conjecture Beal.

Известна также формулировка этой гипотезы :

Пусть существуют положительные целые числа A, B, C, x, y, z . При условии x, y, z > 2 существуют решения уравнения

$A^x + B^y = C^z$

в которых числа

A, B, C

имеют общий множитель

Автор этой статьи описывает алгоритм решения уравнения Била и алгоритм решения ещё более сложного уравнения. Эти два более сложных уравнения и уравнение Ферма образуют систему уравнений:

$$\begin{aligned} &a^n + b^n = c^n \\ &A^x + B^y = C^z \\ &A^p \cdot x + B^q \cdot y = C^r \cdot z \end{aligned} \tag{48}$$

6.Теорема

Система уравнений (48) имеет решения, основу которых образуют два натуральных числа : 2 и 9 .

7. Доказательство Теоремы

Изучение свойств моей эллиптической кривой мы начинали с определения первой примитивной тройки Пифагора:

$$\begin{aligned} a_0 &= (2^2 - 1^2) = 3 \\ b_0 &= (2 \cdot 2 \cdot 1) = 4 \\ c_0 &= (2^2 + 1^2) = 5 \end{aligned} \tag{49}$$

и, в конечном счёте , получили уравнение моей эллиптической кривой при показателе степени n=2, см. (11):

$$\begin{aligned} Y^2 &= a_o{}^2 \cdot b_o{}^2 \cdot (b_o{}^2 + a_o{}^2) = \\ &= a_o{}^2 \cdot b_o{}^2 \cdot c_o{}^2 \end{aligned} \tag{50}$$

Увеличивая показатель степени в правой части этого уравнения, мы получили более общую математическую модель при любом показателе степени $n \geq 2$:

$$Y^2 = a_o{}^n \cdot b_o{}^n \cdot (b_o{}^n + a_o{}^n) \tag{51}$$

Легко видеть, что правый крайний множитель этой математической модели допускает отождествление с уравнением Пьера Ферма, переменными величинами в котором служат примитивные тройки Пифагора:

$$(b_o{}^n + a_o{}^n) = c_o{}^n \tag{52}$$

Форма (51) доставляет нам третий легко вычисляемый член этого уравнения :

$$c_o{}^n = (b_o{}^n + a_o{}^n) = \frac{Y^n}{a_o^n \cdot b_o{}^n} \tag{53}$$

Числа 2 и 9 можно представить в виде разложения на простые числа:

$$[2=(1+1)]=(3-1)$$
$$9=(3+3+3)=[(1+2^3)=3^2] \qquad (54)$$

Из простых чисел этих разложений можно интуитивно сконструировать , согласно [3] , два общих множителя :

$$S_2=2^n \qquad (55)$$

$$S_3=(3^3)^n \qquad (56)$$

Здесь n показатель степени :

$$n=2,3,4,5,....,\infty \qquad (57)$$

Любые решения уравнения Била

$$A^x+B^y=C^z \qquad (58)$$

доставляют следующие формулы:

$$[(1+1)=2]\cdot S_2 \qquad (59)$$

$$[(1+2^3)=3^2]\cdot S_3 \qquad (60)$$

8.Комментарий

Автор [3] , Р.Курант пишет :

«Конечно, начало конструктивного творчества, интуитивное начало, являющееся источником наших идей и доводов в их пользу, с трудом укладываются в простые философские формулировки; и тем не менее именно это начало есть подлинная суть любого математического открытия, даже если оно относится к самым абстрактным областям. Если целью является чёткая дедуктивная форма, то движущая сила математики – это интуиция и конструкция. В допущении, что математика есть не более чем система следствий, извлекаемых из определений и постулатов, которые должны быть только совместимы между собой, а в остальном являются продуктом свободной фантазии математиков, таится серьёзная угроза для самого существования науки».

9.Демонстрационные примеры.

Пример 1.

Имеем уравнение Била (58) .

$$A^x+B^y=C^z$$

Полагая n=1, согласно (56) и (60) , запишем:

$$S_3=(3^3)^1$$

$$[(1+2^3)=3^2]\cdot 3^3$$

что эквивалентно уравнению:

$$3^3+6^3=3^5, \qquad (61)$$

в котором:

A=3, B=6, C=3, x=3, y=3, z=5

Роль общих множителей здесь выполняют числа :

$\mathbf{3}$ и $\mathbf{3^3}$

Пример 2.

Имеем уравнение Била (58) .

$$A^x + B^y = C^z$$

Полагая n=2, согласно (56) и (60) ,запишем:

$$S_3 = (3^3)^2$$

$$[(1+2^3) = 3^2]\cdot 3^6$$

что эквивалентно уравнению:

$$3^6 + 18^3 = 3^8, \qquad (62)$$

в котором:

A=3 , B=18 , C=3, x=6, y=3, z=8 .

Роль общих множителей здесь выполняют числа :

3 и 3^6

Следующий пример сопровождается геометрической интерпретацией.

Пример 3.

Имеем уравнение Била (58) .

$$A^x + B^y = C^z$$

Полагая n=3, согласно (56) и (60) ,запишем:

$$S_3 = (3^3)^3$$

$$[(1+2^3) = 3^2]\cdot 3^9$$

что эквивалентно уравнению:

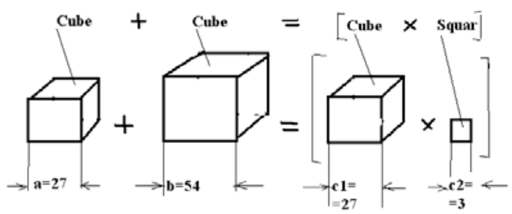
$$3^9 + 54^3 = 3^{11}, \qquad (63)$$

в котором:

A=3, B=54, C=3, x=9, y=3, z=11 .

Роль общих множителей здесь выполняют числа :

3 и 3^9



Три куба и один квадрат иллюстрируют полученное выше уравнение:

$$27^3 + 54^3 = [27^3 \cdot 3^2]$$

Пример 4.

Имеем уравнение Била (58) .

$$A^x + B^y = C^z$$

Полагая n=8, согласно (55) и (59) ,запишем:

$$S_2 = 2^8$$

$$[(1+1) = 2]\times 2^8$$

что эквивалентно уравнению:

$$2^8 + 4^4 = 2^9, \tag{64}$$

в котором:

A=2, B=4, C=2, x=8, y=4, z=9 .

Роль общих множителей здесь выполняют числа :

$$2 \quad \text{и} \quad 2^8$$

Примечание

В публикации известных математиков:
H.Darmon and A.Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. Bull. London. Math. Soc.27(1995), 513-543, [13], описана неудачная попытка решения проблемы Conjecture Beal. Авторы демонстрируют десять уравнений, которые очень близки к решению поставленной задачи:

$$1 + 2^3 = 3^2 : 2^5 + 7^2 = 3^4 : \ 7^3 + 13^2 = 2^9 : \ 2^7 + 17^3 = 71^2$$

$$3^5 + 11^4 = 122^2 : 17^7 + 76271^3 = 21063928^2 : 1414^3 + 2213459^2 = 65^7 :$$

$$43^8 + 96222^3 = 30042907^2 : 9262^3 + 15312283^2 = 113^7 : 33^8 + 1549034^2 = 15613^3$$

Но в этих примерах нет общих множителей для чисел A, B и C. Следовательно, эти примеры не имеют ничего общего с общей проблемой A. Beal и P. Fermat.

10.Следствие

Чтобы окончательно решить систему уравнений :

$$\begin{aligned} &a^n + b^n = c^n \\ &A^x + B^y = C^z \\ &A^p \cdot x + B^q \cdot y = C^r \cdot z \end{aligned} \tag{65}$$

необходимо построить алгоритм решения уравнения :

$$A^p \cdot x + B^q \cdot y = C^r \cdot z \tag{66}$$

Полагая в уравнении (66) $x = y = z = 1$, мы получаем аналог уравнения Била:

$$A^p + B^q = C^r \tag{67}$$

Как было показано выше, такое уравнение мы умеем решать, вычленяя из него общие множители. Здесь задача состоит в том, чтобы найти алгоритм вычисления новых чисел чисел (x , y , z). Поступаем следующим образом. Если произвольно назначить новые $x = K_x$ и $y = K_y$ целые положительные числа , то уравнение (66) можно записать в следующем виде:

$$A^p \cdot K_x + B^q \cdot K_y = C^r \cdot z \tag{68}$$

Из этого уравнения следует формула для вычисления неизвестного целого числа

$$z = (A^P \cdot K_x + B^q \cdot K_Y) / C^r = K_z \tag{69}$$

Из уравнения :

$$A^p \cdot x + B^q \cdot K_y = C^r \cdot z \tag{70}$$

Находим математическую модель целого числа x :

$$x = (C^r \cdot K_z - B^q \cdot K_y) / A^P \tag{71}$$

В этой модели принятое нами целое число x выражается через известные члены решённого уравнения Била (67).

Из уравнения :

$$A^p \cdot K_x + B^q \cdot y = C^r \cdot z \tag{72}$$

Выводим формулу для вычисления неизвестной величины y с помощью известных членов уравнения Била (67) :

$$y = (C^r \cdot K_z - A^p \cdot K_x) / B^q \tag{73}$$

11. Заключение

Около двух с половиною столетий длился поиск решения проблемы Пьера Ферма различными математическими способами прямого назначения. И вот, в 1986 году появился новый, косвенный метод доказательства справедливости Последней теоремы Ферма. Этот метод предложил Frey G. Идея Фрея состояла в том, чтобы целые числа $A = a^q$ и $B = b^q$ задавали такие свойства эллиптической кривой:

$$Y^2 = (X - A) \cdot X \cdot (X + B)$$

которые одновременно задавали бы свойства уравнения Ферма:

$$a^q + b^q = c^q$$

Здесь a, b, c натуральные попарно взаимно простые числа и $q \geq 2$ простой показатель степени. Фрей пришёл к выводу, что такая ситуация невозможна и наметил идею метода, позволяющего получить противоречие с гипотезой Шимуры-Таниямы, которая утверждает :

Все эллиптические кривые модулярны.

Реализация этой идеи потребовала многих лет работы и завершилась известным доказательством ПТФ, которое предложил в 1995 году доктор Wiles A , [1]. Гипотеза Шимуры-Таниямы и основанное на ней доказательство ПТФ доктора Уайлса оказались ложными. Ложность гипотезы и доказательства невозможно обнаружить с помощью любых натуральных и идеальных чисел . Эту ложность можно обнаружить только с помощью примитивных троек Пифагора.

Если целые числа v и u таковы, что $v > u > 0$ и НОД $(v, u) = 1$, причём v и u различной чётности, то триада (a_o, b_o, c_o), задаваемая равенствами :

$$a_o = v^2 - u^2$$

$$b_o = 2vu$$

$$c_o = v^2 + u^2$$

является примитивным решением уравнения:

$$x^2 + y^2 = z^2$$

Эти соотношения устанавливают взаимно однозначное соответствие между множеством пар (v, u), удовлетворяющих указанным условиям, и множеством примитивных решений уравнения $x^2 + y^2 = z^2$.

Примитивные тройки Пифагора помогли автору этой статьи не только обнаружить упомянутую математическую ложность, но и создали основу для объединения проблемы Ферма, проблемы инвариантов Георга Гордана, проблемы приведенных вторичных форм теории чисел А.Пуанкаре в единую проблему теории чисел . Вместо недостоверного доказательства, описанного в работе [1] , размером 10 Мбайт на 40 страницах ,получено достоверное доказательство ПТФ на 10 страницах (1.3 Мбайт).

Это - локальная математическая катастрофа. Однако, в этом событии есть и положительная сторона. Автор [2] пишет:

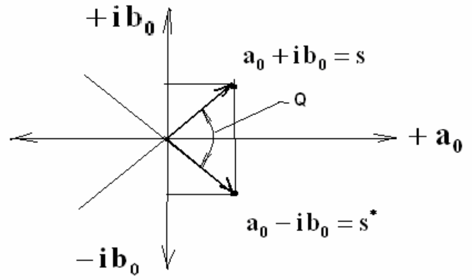
«Изучение теоремы Ферма привело к созданию теории алгебраических чисел, подобно тому, как изучение квадратичных полей было вызвано гауссовой теорией квадратичных форм. Ветвь математики, лежащая на стыке теории чисел и алгебраической геометрии и называемая *арифметической алгебраической геометрией* , развивалась не только исходя из своих внутренних потребностей, но также имея в виду доказательство последней теоремы Ферма. Неужели этот стимул исчезнет теперь, когда ПТФ доказана ? Отнюдь нет. Варианты задачи , обобщения на высшие размерности, будут продолжать терзать математиков.»

Эффективность перехода от бесконечного ряда натуральных чисел к бесконечному ряду примитивных троек Пифагора убедительно подтверждает факт открытия бесконечного ряда немодулярных эллиптических кривых. Теория чисел будет ещё долго и тщательно изучать этот феномен рациональных и комплексных чисел чисел ,ибо существует инвариант

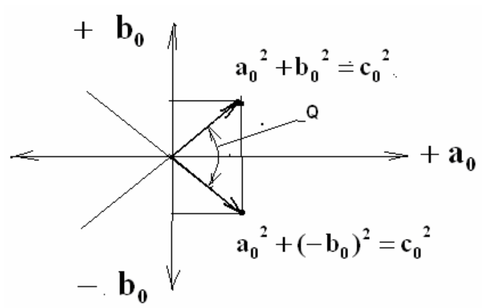
:

$$\mathbf{S = s \cdot s^* = (a_0 + i \cdot b_0) \cdot (a_0 - i \cdot b_0) = }$$
$$\mathbf{= a_0{}^2 + b_0{}^2 = c^2} \quad ,$$

который имеет геометрическое отображение как в системе координат :



так и в системе координат:



При этом имеет место быть векторное произведение :

$$\mathbf{[\,s, s^*\,]}$$

длина вектора которого

$$\left| S \right| = \left| s, s^* \right| = \left| s \right| \cdot \left| s^* \right| \cdot \sin Q$$

служит аргументом в модели универсальной дзета функции

$$\zeta(S) = 2^S \pi^{S-1} \sin \frac{\pi S}{2} \ \Gamma \ (1 - S) \ \zeta (1 - S) = 0$$

Согласно [2] для модулярных кривых Фрея:

$$Y^2 \equiv X \cdot (X - a^q) \cdot (X + b^q) \pmod{p}$$

в которых используются подстановки Фрея:

$$A = a^q \ , \ B = b^q$$

и простые числа (q, p)

«Ключевой момент состоит в том, чтобы связать локальные данные с *некоторым объектом* (аналитической функцией комплексного переменного) при помощи *некоторого глобального инварианта* (бесконечного произведения по простым числам)», см.[2], стр.389.

Для немодулярных эллиптических кривых с моими подстановками, см.(2) :

$$(X - A) = {a_0}^n$$

$$A = X - {a_o}^n = ({b_o}^n - {a_o}^n)$$

$$X = {b_0}^n$$

$$(X + B) = {c_0}^n$$

$$B = {c_o}^n - X = {c_o}^n - {b_o}^n = {a_o}^n$$

ключевой момент состоит в том, чтобы связать эти локальные данные с некоторым объектом (аналитической функцией комплексного переменного) при помощи некоторого «глобального» инварианта.

Роль такого некоторого объекта и «глобального» инварианта выполняет функция :

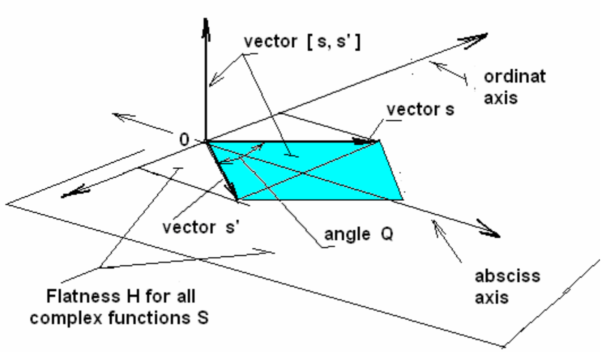
$$S = s \cdot s^* = (a_0 + i \cdot b_0) \cdot (a_0 - i \cdot b_0) =$$
$$= {a_0}^2 + {b_0}^2 = c^2$$

и дзета функция :

$$\zeta(S) = 2^S \pi^{S-1} \sin \frac{\pi S}{2} \ \Gamma \ (1 - S) \ \zeta (1 - S) = 0$$

где используются бесконечные произведения не простых чисел, а бесконечные произведения комплексных переменных , составленных из примитивных троек Пифагора.

Геометрическая интерпретация «глобального» инварианта S в трёхмерном пространстве представлена ниже:



Complex function S is general mathematical invariant for flatness H and at the same time it is complex function over field N of all natural numbers v > u ..

Более подробное исследование этого феномена теории чисел читатель найдёт в Интернете , на последней ссылке сайта http://yvsevolod-28.narod.ru/index.html

.

Литература

1. «Wiles A. 1995. Modular elliptic curves and Fermat's Last Theorem. Annals of Mathematics 141:443.»

2.Рибенбойм П., Последняя теорема Ферма, пер. с англ, М., Мир, (2003), с.13,16,264,384-386, 389.

3.Курант Р. и Роббинс Г., Что такое математика ? , пер. с англ., М., Просвещение, (1967),с.21,47.

4.Ярош В.С., Финал многовековой загадки Диофанта и Ферма (Великая теорема Ферма доказана окончательно для всех n >2), М., Инженер, (1993), на 50 стр.

5.Yarosh V.S. , Denouement of the multicentury enigma of Diophant and Fermat (The Great Fermat theorem is finally proved for all n > 2), M., Engineer (1993) , 50 s.

6.Ярош В.С. , ,Окончательное решение Великой или Последней Теоремы Ферма, в сборнике научных трудов Алгоритмы и структуры систем обработки информации Тульского Государственного технического университета (1993),с.68-79.

7.Ярош В.С. , О некотором ошибочном утверждении в теории чисел и о полноте окончательного решения теоремы Ферма, в сборнике научных трудов Алгоритмы и структуры систем обработки информации Тульского Государственного Университета (1995), с.130-137.

8.Рид К. , Гильберт, пер.с англ.,М., «Наука», 1977, с.47.

9. H.Pouincare, Journal de l*Ecole politechnique,1881, Cahier 50, 150 – 253

10.А.Пуанкаре, Избранные труды, т.2, М., «Наука», 1972, с.819,867,888-889

11.Ч.Мизнер, К.Торн, Дж.Уилер, Гравитация, т.1, пер. с англ.,М., «Мир», 1977, с.370

**12.H.Poincare, Journal de l*Ecole politechnique, 1882,
Cachier 51, 45-91.**
13.H.Darmon and A.Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. Bull. London. Math. Soc.27(1995), 513-543.

Всеволод Сергеевич Ярош
18 декабря 2008 года

121354, Москва, Можайское шоссе, 39, кв.306
Тел.(495) 444-00-94
E-mail: yvsevolod-26@yandex.ru