Последняя теорема Ферма для любителей

Paulo Ribenboim

Fermat's Last Theorem for Amateurs

Springer

П. Рибенбойм

Последняя теорема Ферма

для любителей

Перевод с английского
А. В. Бегунца, О. В. Попова,
С. Н. Преображенского,
Б. А. Турешбаева

под редакцией
В. Н. Чубарикова

Москва «Мир» 2003

УДК 511
ББК 22.13
Р49

Рибенбойм П.

Р49 Последняя теорема Ферма для любителей: Пер. с англ. — М.: Мир, 2003. — 429 с., ил.

ISBN 5-03-003400-5

Прекрасное введение в алгебраическую и элементарную теорию чисел, отличающееся широтой охвата материала. Автору, известному канадскому математику, удалось органично соединить строгость математических фактов с увлекательностью изложения более чем трехвековой истории изобретения искусных подходов к решению знаменитой последней теоремы Ферма. Приведен исторический очерк с указанием авторов «решений» проблемы и авторов опровержений.

Для всех интересующихся математикой, включая математиков-профессионалов, преподавателей и учащихся старших классов.

ББК 22.13
УДК 511

РФФИ

Издание осуществлено при финансовой поддержке Российского фонда фундаментальных исследований по проекту № 00-01-14117

Редакция литературы по математическим наукам

Translation from the English language edition: *Fermat's Last Theorem for Amateurs* by Paulo Ribenboim

Copyright © 1999 Springer-Verlag New York, Inc. All Rights Reserved

© перевод на русский язык, издательство «Мир», 2003

ISBN 5-03-003400-5 (русск.)
ISBN 0-387-98508-5 (англ.)

От редактора перевода

Книга П. Рибенбойма «Последняя теорема Ферма для любителей» переведена на русский язык в 2001 г. — в год 400-летия со дня рождения знаменитого французского математика П. Ферма. В книге органично сочетаются строгость и доступность доказательств математических фактов с увлекательностью изложения более чем трехвековой истории изобретения искусных методов и создания прекрасных теорий, основная цель которых — доказать последнюю теорему Ферма. Указанное сочетание, безусловно, отражает предназначение книги для любителей. По-видимому, в слово «любитель» не следует вкладывать значение «непрофессиональный математик», а понимать его нужно как «любитель математики». В их круг включаются профессионалы-математики разных уровней квалификации, специалисты из других областей науки, а также школьные учителя и даже учащиеся старших классов. Добавим к этому, что автор книги — известный канадский математик, специалист по алгебраической теории чисел. Ранее в издательстве «Шпрингер» вышла его книга «13 лекций о последней теореме Ферма»[1], которая является более академичной, чем предлагаемая вниманию читателя.

Нам представляется, что с исторической точки зрения, а также для лучшего понимания предмета книги будет уместно процитировать здесь текст письма академика Н. Н. Лузина академику И. М. Виноградову, написанного более полувека назад.

16 апр. 1946 г.

Глубокоуважаемый Иван Матвеевич,
извините за промедление в пересылке Вам обещанных статей Hofmann'a[2]*, касающихся метода Fermat. Причина всегда одна и та*

---

[1] Ribenboim P., *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.

[2] Н. Н. Лузин приложил к письму оттиски двух статей:
Hofmann J. E. *Studien zur Zahlentheorie Fermats* (*Über die Gleichung* $x^2 = py^2 + 1$). Abh. der Preußischen Akademie der Wissenschaften. 1944. № 7. S. 1–19.
Hofmann J. E. *Neues über Fermats zahlentheoretische Herausforderungen von* 1657 (*mit zwei bisher unbekannten Originalstücken Fermats*). Там же. 1943. № 9. S. 1–52.

же: болезнь Надежды Михайловны и необходимость находиться при ней.

Дабы быть вполне ясным, я прошу у Вас позволения сказать несколько слов о самом предмете статей Hofmann'a, которых я совсем не читал, но которые меня интересуют в отношении того пути, по которому направлялась его мысль.

Очарование имени Fermat для меня отнюдь не связано с его "последним предложением", но с его многосторонней деятельностью как предшественника Декарта в изобретении аналитической геометрии, как предшественника Ньютона и Лейбница в изобретении анализа бесконечно малых. То, что Fermat не был профессиональным ученым, как и Эйнштейн, лишь повышает интерес к нему.

Что же касается до его "последнего предложения", то лично у меня к нему интерес всегда был равен нулю. Тяготение к нему отрицательно характеризует человека, сразу помещая его вне круга истинных философов и ученых. Действительно, это в лучшем случае — только спорт, если не говорить о вещах много худших.

Был ли у Fermat особый метод в его творческих актах по Теории Чисел? Метод живой, не исчерпанный личными достижениями самого Fermat, но утраченный уже для его современников, и тем более для потомков? Я не колеблюсь для самого себя отвечать утвердительным "ДА", хотя вполне понимаю формальную позицию тех, кто отвечает отрицательным "НЕТ". Формальная позиция всегда очень сильна и корректна в глазах публики; но она стерильна, особенно сейчас. И, прибавлю, просто скучна.

Те казавшиеся раньше невероятными открытия в истории наук, которые делаются сейчас, достаточно поучительны и совершенно наглядно говорят о том, что научные факты не только приобретаются, но и утрачиваются. Дабы не быть тривиальным, я упомяну только об утраченном методе Frenicle'я распознавания простоты или непростоты числа в 40–50 знаков в течение 2-х суток. Таково свидетельство современников. И метод, который суммарно при этом указывался, был методом НОМОГРАФИИ, говоря современным языком. Великий Fermat им не обладал и должен был в состязании отступить.

Метод Frenicle'я утерян по вине автора, утратившего интерес к "числам" и ушедшего в духовное звание.

Много раз в литературе мелькала тенденция рассматривать Fermat как авантюриста, интриговавшего тогдашний мір своими теоретико-числовыми "фокусами".

Лично для меня такая точка зрения никогда не казалась достойной истинного ученого и философа.

Для доказательства обычно ссылаются на предложение, будто бы доказанное, по словам Fermat, им: о простоте чисел $2^{2^n}+1$.

Я внимательно исследовал в свое время этот пункт и не нашел никаких следов обмана или позы в высказываниях Fermat.

Fermat никогда, нигде, ни одним звуком, ни одним жестом не дает права думать, что он будто бы доказал когда-то и где-то простоту этих чисел.

Всегда он пишет: "считаю за почти достоверное, что ...". Это словечко "почти" упускается из вида.

В другом месте он пишет: "Я исключил громадное число простых делителей в выражении $2^{2^n}+1$, *но окончательный вывод всё еще манкирует."*

Под видом вызова на соревнования он предлагает своим корреспондентам доказать или опровергнуть простоту чисел $2^{2^n}+1$.

Это звучит как нота печали и безнадежности.

И, наконец, видимо теряя голову, он просит: то Pascal'я, то Roberval'я, то Frenicle'я помочь ему в установлении простоты чисел $2^{2^n}+1$.

Обращение к Паскалю я еще понимаю: его великие дарования не ускользнули от Fermat, к которому Pascal относился всегда как к отцу, т. е. с величайшим уважением и пиететом.

Но обращение к завистливому ученому средних сил Roberval'ю, обладавшему неприятным характером, — можно понять лишь как крик отчаяния самого Fermat.

Нет, куда там до позы, до фальшивых заявлений авантюриста: это были жесты утопающего!

Да и потом, в письме к Carcavi, найденном в съестной лавке в корзине для обертки товара, Fermat совершенно ясно указывает природу своего метода: descente infinie. Только он, надеясь на возвращение своего "интереса к числам", его скрыл, на всякий случай, точнее: не самый метод, а его фактическое применение, видимо, достаточно гибкое и глубокое.

Простите, что занял Ваше внимание пустяками: я хотел лишь сказать, что вполне понимаю тех, кто — в анализе исторической научной обстановки времени Fermat, в анализе его перепис-

ки с друзьями и с соперниками, в анализе его мемуаров — ищет следов утраченного метода.

Но Hofmann'a я еще не успел прочесть и поэтому затрудняюсь рекомендовать Вам его как достойного внимания автора.

Глубочайше уважающий Вас Н. Лузин

Что можно добавить к этому письму? Здесь и трепет, и жгучий интерес, и осторожность перед лицом одной из величайших загадок в истории математики. Читая письмо, нельзя не проникнуться всей этой гаммой чувств и переживаний. Подобное впечатление произвела на автора этих строк и книга П. Рибенбойма.

Работа по переводу книги на русский язык была выполнена сотрудниками механико-математического факультета МГУ им. М. В. Ломоносова, участниками руководимого мною семинара «Избранные главы анализа и теории чисел».

Предварительные главы, главы I–III, V, VI, VIII переведены А. В. Бегунцем, глава VII — О. В. Поповым, эпилог и приложения — С. Н. Преображенским, главы IX, X — Б. А. Турешбаевым, глава IV — В. Н. Чубариковым.

Кроме того, А. В. Бегунц и С. Н. Преображенский подготовили также и оригинал-макет русского издания.

П. Рибенбойм включил в книгу обстоятельные списки литературы на английском языке. Редактором перевода составлен список литературы о теореме Ферма на русском языке. Он приведен в конце книги.

Редактор перевода и переводчики считают своим приятным долгом поблагодарить автора, любезно предоставившего электронную версию английского текста книги и приславшего уточнения и исправления, которые были учтены при подготовке русского издания.

Москва, апрель 2002 г. *В. Н. Чубариков*

Предисловие

Хорошо известно, что последняя теорема Ферма доказана. 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. Наконец долгожданное доказательство было найдено. В нем были задействованы арифметическая теория эллиптических кривых, теория модулярных форм и теория представлений Галуа и их деформаций, развитые рядом математиков.

С этим величайшим математическим достижением связаны имена таких ученых, как ТАНИЯМА, ШИМУРА, ФРЕЙ, СЕРР, РИБЕТ, УАЙЛС, ТЕЙЛОР. Их вклад наряду с набросками доказательства обсуждается в эпилоге. Настоящая книга не преследует цель изложить доказательство теоремы Ферма. Напротив, она написана для любителей, учителей и математиков, интересующихся данной проблемой. Всюду, кроме эпилога, используются лишь элементарные методы. Несмотря на то что они не приводят к полному доказательству теоремы, их значимость распространяется далеко за пределы теоремы Ферма. Нельзя не восхищаться результатами, полученными с помощью такого ограниченного набора методов.

Тем не менее, мне хотелось бы предупредить читателей, что, насколько я понимаю — а понимаю я, возможно, не так уж много, — представленные здесь методы не могут привести к доказательству теоремы Ферма для всех показателей.

Изложение является самодостаточным и содержит все детали, так что чтение должно быть достаточно легким.

В большинстве рассуждений используются только рациональные числа и лишь изредка некоторые алгебраические (не рациональные). Поэтому пришлось исключить описание важного вклада Куммера, о котором подробно говорится в моей книге «Классическая теория алгебраических чисел»[1] и в моих «13 лекциях о послед-

---

[1] *Classical Theory of Algebraic Numbers. — Прим. перев.*

ней теореме Ферма»[2] (новое издание этих лекций содержит эпилог, включающий современные результаты).

Уже издано много — а будет еще больше — книг, монографий и статей, в которых объясняются идеи и нить доказательства теоремы Ферма. Читателям, обладающим глубокими знаниями в этой области, лучше обратиться к таким изданиям. Остальным я предлагаю прочесть мою книгу.

В общем, если Вы — любитель или начинающий математик, то Вам должно понравиться то, о чем Вы прочтете, так как я приложил значительные усилия, чтобы обеспечить доступность и подробность изложения.

С другой стороны, если Вы являетесь профессиональным математиком, то Вас может удивить, зачем я предпринял этот шаг сейчас, когда проблема уже решена. Помните, Вавилонская башня не достигла небес, но была одним из чудес античности. Вот и в этой книге собраны замечательные примеры человеческой одаренности, тем более примечательные использованием сугубо элементарных приемов. Было бы непростительной ошибкой позволить этим жемчужинам кануть в небытие. Как сказал Якоби, все они для «l'honneur de l'esprit humain»[3].

Август 1997 г. *Пауло Рибенбойм*

---

[2] *13 Lectures on Fermat's Last Theorem.* — *Прим. перев.*

[3] «Торжества человеческого разума» (*фр.*) — *Прим. перев.*

К читателю

Возможно, у Вас есть соблазн получить Ваше собственное (более простое) доказательство последней теоремы Ферма.

На этот счет у меня есть твердое убеждение. В главе «Права человека» Всеобщей конституции государств и наций должно быть записано:

> *Каждый человек имеет неотъемлемое право на свое доказательство последней теоремы Ферма.*

Однако это торжественное утверждение, касающееся последней теоремы Ферма (далее именуемой Теоремой), должно быть ограничено следующими статьями.

> Статья 1. *Никакое новое доказательство Теоремы не должно быть повторением уже известного.*
>
> Статья 2. *Представление заведомо неверных доказательств Теоремы профессорам, которые еле зарабатывают на жизнь, обучая тому, как правильно строить доказательства, является уголовным преступлением.*

За нарушение последней статьи полагается ссылка в ад. Возвращение в рай возможно только после того, как «преступник» поймет и сможет воспроизвести доказательство Уайлса. (Жестокое наказание.)

Благодарности

Карл Дильхер руководил набором этой книги, внимательно ее прочел и внес ряд ценных предложений. Я очень благодарен ему за существенную помощь.

Также я признателен моим многочисленным коллегам, внесшим необходимые поправки на стадии рукописи этой книги. Особенно хотелось бы выразить благодарность ныне покойному Кустаа Инкери, а также Такаши Аго, Винко Боттери, Хендрику Ленстре, Тауно Метсянкиле и Гаю Тержаняну.

Герхард Фрей, Фернандо Говеа и Эрнст Кани дали мне ценные советы по поводу эпилога, за что я выражаю им глубокую благодарность.

Проблема

На полях изданного Баше собрания трудов Диофанта[1] 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».

На современном языке это значит следующее.

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*[2].

Начнем с некоторых замечаний.

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.

К слову сказать, мы также приведем ряд результатов с доказательствами для четных показателей и показателей, являющихся степенью простого числа.

---

[1] Этот экземпляр книги утерян, но упомянутые заметки вновь появились в 1679 г. в тулузском издании работ Ферма, редактором которого был его сын Самуэль де Ферма.

[2] Также широко употребляется термин «великая теорема Ферма». — *Прим. перев.*

Следующие общие замечания вполне очевидны и будут даны без доказательства.

Если число n нечетно, то уравнение $X^n + Y^n = Z^n$ имеет нетривиальное решение тогда и только тогда, когда уравнение $X^n + Y^n + Z^n = 0$ имеет нетривиальное решение.

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.

Более того, если отличные от нуля попарно взаимно простые числа x, y, z таковы, что $x^n + y^n = z^n$, то числа $x + y, z - x, z - y$ также попарно взаимно просты. В самом деле, если простое число p делит $x + y$ и $z - x$, то $x \equiv z \pmod{p}$, откуда $x^n \equiv z^n \equiv x^n + y^n \pmod{p}$, следовательно, $y^n \equiv 0 \pmod{p}$, так что p делит y, а так как p делит $x + y$, мы получаем, что p делит x, а это противоречит предположению. Таким образом, $\text{НОД}(x+y, z-x) = 1$. Аналогично можно показать, что $\text{НОД}(x+y, z-y) = 1$ и $\text{НОД}(z-x, z-y) = 1$.

Следуя традиции, будем говорить, что *первый случай теоремы Ферма* имеет место для нечетного простого показателя p, если для любых отличных от нуля целых чисел x, y, z, не кратных p, выполнено соотношение $x^p + y^p \neq z^p$.

Второй случай теоремы Ферма имеет место для нечетного простого показателя p, если для любых отличных от нуля попарно взаимно простых целых чисел x, y, z, таких, что p делит xyz, выполняется соотношение $x^p + y^p \neq z^p$. Как говорилось выше, в этом случае p делит ровно одно из чисел x, y, z.

Вообще, будем говорить, 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 $\text{НОД}(m, xyz) = 1$, имеет место соотношение $x^n + y^n \neq z^n$.

Аналогичным образом *второй случай* справедлив для показателя n, если для любых отличных от нуля попарно взаимно простых целых чисел x, y, z, таких, что $\text{НОД}(m, xyz) \neq 1$, выполняется соотношение $x^n + y^n \neq z^n$.

Глава I

Частные случаи

Эта глава посвящена доказательству частных случаев теоремы Ферма — случаев, когда показатели равны 4, 3, 5 и 7 соответственно. Однако мы начнем с рассмотрения исключительного случая, когда показатель равен 2.

I.1. Уравнение Пифагора

Кратко остановимся на уравнении Пифагора

$$X^2 + Y^2 = Z^2. \tag{1.1}$$

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 $d = \text{НОД}(x, y, z)$, то x/d, y/d, z/d удовлетворяют тому же уравнению. Таким образом, достаточно определить *примитивные решения* (x, y, z) уравнения (1.1), а именно такие, что $x > 0$, $y > 0$, $z > 0$, x четно и $\text{НОД}(x, y, z) = 1$, откуда y и z нечетны.

В книге Диксона «История теории чисел» (1920)[1] утверждается, что Пифагор и Платон предложили методы нахождения решений уравнения (1.1). В лемме 1 к предложению 29 десятой книги «Начал» Евклид привел геометрический метод нахождения решений этого уравнения.

Диофант указал метод нахождения всех решений, как это сделано в результате (1A).

---

[1] *History of the Theory of Numbers*, Vol. II, pp. 165–166. — *Прим. перев.*

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

(1A) *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 (1.1). *Эти соотношения устанавливают взаимно однозначное соответствие между множеством пар (a, b), удовлетворяющих указанным условиям, и множеством примитивных решений уравнения* (1.1).

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 (1.1), 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[2], НОД$(z - x, z + x) = 1$. 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

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

---

[2]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, $d = 1$. — *Прим. перев.*

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 (1.1), 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 (1A), найти примитивные решения уравнения (1.1) — 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 (доказательство см. ниже). 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).

Сейчас мы изложим доказательство Ферма, которое имеет большое историческое значение. Начнем с очень простого тождества:

$$\begin{aligned} (a^2 + b^2)(c^2 + d^2) &= (ac + bd)^2 + (ad - bc)^2 \\ &= (ac - bd)^2 + (ad + bc)^2. \end{aligned} \tag{1.2}$$

Теперь докажем такой факт.

(1B) *Простое число p является суммой двух квадратов целых чисел тогда и только тогда, когда $p = 2$ или $p \equiv 1 \pmod 4$.*

Доказательство. Если $p \neq 2$ и $p = a^2 + b^2$, то a и b не могут оба быть четными — в противном случае p делится на 4. Если оба числа

a и b нечетны, то $p \equiv 1+1 = 2 \pmod 4$, поскольку квадрат всякого нечетного числа сравним с 1 по модулю 4. Таким образом, $p = 2$. Если, скажем, a нечетно, а b четно, то $p \equiv 1+0 = 1 \pmod 4$.

Обратно, $2 = 1^2 + 1^2$, поэтому мы можем считать, что $p \equiv 1 \pmod 4$. Из теории квадратичных вычетов известно, что -1 является квадратом по модулю p. Поэтому существует такое число x, $1 \leqslant x \leqslant p-1$, что $x^2 + 1 \equiv 0 \pmod p$, то есть $x^2 + 1 = mp$, где $1 \leqslant m \leqslant p-1$. Следовательно, множество

$$\{m \mid 1 \leqslant m \leqslant p-1 \text{ и } mp = x^2 + y^2 \text{ для некоторых целых чисел } x, y\}$$

непусто. Пусть m_0 — наименьшее целое число в этом множестве, тогда $1 \leqslant m_0 \leqslant p-1$. Мы покажем, что $m_0 = 1$, а значит, p является суммой двух квадратов. Предположим противное, т. е. что $m_0 > 1$. Запишем

$$\begin{cases} x = cm_0 + x_1, \\ y = dm_0 + y_1, \end{cases}$$

где $-m_0/2 < x_1, y_1 \leqslant m_0/2$ и c, d — целые числа. Заметим, что либо x_1, либо y_1 отлично от нуля. В противном случае m_0^2 делит $x^2+y^2 = m_0 p$, а следовательно, m_0 делит p и, таким образом, $m_0 = p$, что невозможно. Но мы имеем $0 < x_1^2 + y_1^2 \leqslant m_0^2/4 + m_0^2/4 = m_0^2/2 < m_0^2$ и $x_1^2 + y_1^2 \equiv x^2 + y^2 \equiv 0 \pmod{m_0}$. Поэтому $x_1^2 + y_1^2 = m_0 m'$, где $1 \leqslant m' < m_0$. Однако $m_0 p = x^2 + y^2$, $m_0 m' = x_1^2 + y_1^2$, а значит, $m_0^2 m' p = (x^2+y^2)(x_1^2+y_1^2) = (xx_1 + yy_1)^2 + (xy_1 - yx_1)^2$. Также имеют место равенства

$$\begin{aligned} xx_1 + yy_1 &= x(x - cm_0) + y(y - dm_0) \\ &= (x^2 + y^2) - m_0(cx + yd) \\ &= m_0 t, \\ xy_1 - yx_1 &= x(y - dm_0) - y(x - cm_0) \\ &= -m_0(xd - yc) \\ &= m_0 u \end{aligned}$$

для некоторых целых чисел t, u. Следовательно, $m'p = t^2 + u^2$, где $1 \leqslant m' < m_0$. Полученное противоречие завершает доказательство. □

(1C) *Натуральное 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.*

Доказательство. Пусть $n = p_1^{k_1} \dots p_r^{k_r}$. Предположим, что k_j четно, если $p_j \equiv 3 \pmod 4$. Тогда $n = n_0^2 n_1$, где $n_0 \geqslant 1$, $n_1 \geqslant 1$ и n_1 есть произведение различных простых чисел, которые либо равны 2, либо сравнимы с 1 по модулю 4. В силу (1B) каждый множитель числа n_1 является суммой двух квадратов. Согласно тождеству (1.2) число n_1, а потому и n является суммой двух квадратов.

Обратно, пусть $n = x^2 + y^2$. Если $x = 0$ или $y = 0$, то утверждение тривиально. Пусть x, y отличны от нуля, $d = \text{НОД}(x, y)$, тогда d^2 делит n. Положим $n = d^2 n'$, $x = dx'$, $y = dy'$, откуда $\text{НОД}(x', y') = 1$ и $n' = x'^2 + y'^2$. Если p делит n', то p не делит x' — в противном случае p также делило бы и y'. Пусть k таково, что $kx' \equiv y' \pmod p$[3]. Тогда $x'^2 + y'^2 \equiv x'^2(1 + k^2) \equiv 0 \pmod p$. Таким образом, p делит $1 + k^2$, то есть -1 является квадратом по модулю p, так что согласно теории квадратичных вычетов $p = 2$ или $p \equiv 1 \pmod 4$. Получается, что если $p_j \equiv 3 \pmod 4$, то p_j не делит n', а следовательно, p_j делит d, так что показатель k_j должен быть четным. □

Обычно говорят, что прямоугольный треугольник является *пифагоровым треугольником*, если его стороны измеряются целыми числами a, b, c. Если c — гипотенуза, то $c^2 = a^2 + b^2$.

По этому вопросу мы рекомендуем книгу Шенкса (1962), которая содержит интересную главу о пифагореизме и его проявлениях, а также книгу Серпинского (1962) и статью Мариани (1962).

В 1908 г. Боттари получил другую параметризацию решений уравнения (1.1). Следующее упрощенное доказательство принадлежит Каттанео (1908).

(1D) *Пусть a, b — взаимно простые нечетные натуральные числа, и s — некоторое натуральное число. Тогда тройка чисел (x, y, z), задаваемая равенствами*

$$\begin{cases} x = 2^{2s-1}a^2 + 2^s ab, \\ y = b^2 + 2^s ab, \\ z = 2^{2s-1}a^2 + b^2 + 2^s ab, \end{cases}$$

является примитивным решением уравнения (1.1). *Эти равенства устанавливают взаимно однозначное соответствие между множеством троек (a, b, s), удовлетворяющих указанным условиям, и множеством примитивных решений уравнения* (1.1).

---

[3] Такое число k существует в силу китайской теоремы об остатках, поскольку $p \nmid x'$. — *Прим. перев.*

Доказательство. Ясно, что если числа x, y, z определены так, как указано выше, то тройка (x, y, z) является примитивным решением уравнения (1.1).

Различные тройки (a, b, s) порождают различные примитивные решения (x, y, z), потому что

$$\begin{cases} b^2 = z - x, \\ 2^{2s-1}a^2 = z - y, \\ 2^s ab = x + y - z. \end{cases}$$

Наконец, если (x, y, z) — примитивное решение, то $0 < x < z$, $0 < y < z$ и $z < x + y$, так как $z^2 = x^2 + y^2 < (x + y)^2$. Отсюда

$$\begin{cases} x = z - u, \\ y = z - v, \\ z = x + y - w, \end{cases}$$

причем $u, v, w > 0$. Тогда

$$\begin{cases} x = v + w, \\ y = u + w, \\ z = u + v + w. \end{cases}$$

Из равенства $x^2 + y^2 = z^2$ следует, что $w^2 = 2uv$, а значит, число w четно. Поскольку НОД$(u, v, w) = 1$ и x четно, а y нечетно, мы заключаем, что v четно, а u нечетно. Пусть $w = 2^s w'$, $v = 2^t v'$, где v', w' нечетны, $s \geqslant 1, t \geqslant 1$. Тогда $2^{2s} w'^2 = 2u \cdot 2^t v'$, так что $t = 2s - 1$, а $w'^2 = uv'$, причем НОД$(u, v') = 1$. Следовательно, числа u, v' обязательно являются квадратами целых чисел: $u = b^2$, $v' = a^2$, и потому $x = 2^{2s-1}a^2 + 2^s ab$, $y = b^2 + 2^s ab$, $z = 2^{2s-1}a^2 + b^2 + 2^s ab$. □

Также представляет интерес описание решений уравнения

$$X^2 + Y^2 = 1. \tag{1.3}$$

Оказывается, решениями в целых числах являются лишь пары $(\pm 1, 0), (0, \pm 1)$.

Мы рассмотрим решения в рациональных числах, а также решения в поле из p элементов для каждого простого числа p.

Пусть, как обычно, $\mathbb{Q}$ — поле рациональных чисел. Для каждого простого числа p обозначим множество $\{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ классов вычетов кольца $\mathbb{Z}$ по модулю p через $\mathbb{F}_p$. Так, если $a, b \in \mathbb{Z}$, то $\overline{a} = \overline{b}$ тогда и только тогда, когда a и b дают один и тот же остаток при делении на p. Операции сложения и умножения в $\mathbb{F}_p$ определяются следующим образом: $\overline{x} + \overline{y} = \overline{x + y}$, $\overline{x}\,\overline{y} = \overline{xy}$. С этими операциями

которые удовлетворяют обычным свойствам, $\mathbb{F}_p$ становится полем: если $\overline{a} \in \mathbb{F}_p$ и $\overline{a} \neq \overline{0}$, то НОД$(a, p) = 1$, а значит, существуют $r, s \in \mathbb{Z}$, такие, что $ar + ps = 1$. Тогда $\overline{a}\,\overline{r} = \overline{1}$ и класс $\overline{r}$ является обратным к $\overline{a}$ элементом поля $\mathbb{F}_p$. Для простоты можно использовать обозначение x вместо $\overline{x}$ для элементов поля $\mathbb{F}_p$. Мы докажем результат, который справедлив для поля $\mathbb{Q}$, а также для каждого поля $\mathbb{F}_p$ при $p > 2$. Таким образом, пусть $F = \mathbb{Q}$ или $\mathbb{F}_p$ (при $p > 2$). (Вообще говоря, в качестве F можно взять любое поле, характеристика которого отлична от 2, то есть такое, для которого $1 + 1 \neq 0$.)

Пусть ∞ — символ, $\infty \notin F$. Положим

$$T = \{\infty\} \cup \{t \in F \mid 1 + t^2 \neq 0\}.$$

Определим множество

$$S = S_F = \{(x, y) \in F \times F \mid x^2 + y^2 = 1\}.$$

Элементы этого множества являются решениями уравнения (1.3) в поле F.

Пусть отображение $\varphi : T \to F \times F$ определяется равенствами

$$\begin{cases} \varphi(\infty) = (0, -1), \\ \text{если } t \in T, \text{ то } \varphi(t) = \left(\dfrac{2t}{1+t^2}, \dfrac{1-t^2}{1+t^2}\right). \end{cases} \tag{1.4}$$

Заметим, что, поскольку $1+t^2 \neq 0$, элемент $1+t^2$ обратим, а значит, отображение φ определено корректно.

(1E) *Во введенных обозначениях φ есть взаимно однозначное отображение из T в S.*

Доказательство. Поскольку

$$\left(\frac{2t}{1+t^2}\right)^2 + \left(\frac{1-t^2}{1+t^2}\right)^2 = 1,$$

$\varphi(t) \in S$ для каждого $t \in F$, такого, что $1 + t^2 \neq 0$. Кроме того, $(0, -1) \in S$, так что $\varphi(T) \subseteq S$.

Если $t \in F$, $1+t^2 \neq 0$, то $(1-t^2)/(1+t^2) \neq -1$, так как $1+1 \neq 0$. Далее, если $t_1, t_2 \in F$, $1 + t_1^2 \neq 0$, $1 + t_2^2 \neq 0$, то, как легко видеть, $\varphi(t_1) \neq \varphi(t_2)$. Таким образом, отображение φ взаимно однозначно (так как $1 + 1 \neq 0$).

Теперь покажем, что $\varphi(T) = S$. Ясно, что $(0, -1) = \varphi(\infty)$. Пусть $(x, y) \in S$, $(x, y) \neq (0, -1)$. Если $x = 0$, то $y = 1$ и $(0, 1) = \varphi(0)$. Если

же $x \neq 0$, то положим $t = (1-y)/x$, откуда получим

$$1 + t^2 = \frac{2(1-y)}{x^2}, \qquad 1 - t^2 = \frac{2y(y-1)}{x^2}$$

и

$$\frac{2t}{1+t^2} = x, \qquad \frac{1-t^2}{1+t^2} = y,$$

а следовательно, $(x, y) = \varphi(t)$, что и завершает доказательство. □

Если $F = \mathbb{Q}$, то $1 + t^2 \neq 0$ для всех $t \in \mathbb{Q}$, так что $T = \mathbb{Q} \cup \{\infty\}$. Если $F = \mathbb{F}_p$, где $p > 2$, то $1 + t^2 = 0$ тогда и только тогда, когда $-\overline{1}$ является квадратом по модулю p. Согласно уже упоминавшемуся результату Ферма число -1 является квадратом по модулю $p > 2$ тогда и только тогда, когда $p \equiv 1 \pmod 4$.

Пусть N_p обозначает число элементов множества $S_{\mathbf{F}_p}$.

(1F) *Справедливо равенство $N_2 = 2$, и если $p > 2$, то*

$$N_p = \begin{cases} p-1 & \text{при} \quad p \equiv 1 \pmod 4, \\ p+1 & \text{при} \quad p \equiv -1 \pmod 4. \end{cases}$$

Доказательство. Так как $S_{\mathbf{F}_2} = \{(0,1),(1,0)\}$, мы получаем, что $N_2 = 2$. Пусть $p > 2$. Если $p \equiv 1 \pmod 4$, то существуют 2 элемента t_1, t_2, такие, что $t_1^2 + 1 = t_2^2 + 1 = 0$. Таким образом, выполняется равенство $\#(T) = (p-2) + 1 = p - 1$, а следовательно, в силу (1E) и равенство $\#(S) = p - 1$.

Аналогично, если $p \equiv -1 \pmod 4$, то $\#(T) = p+1$ и $\#(S) = p+1$. □

Список литературы[4]

Euclid, *The Elements*, Book X (editor T.L. Heath, 3 volumes), Cambridge University Press, Cambridge, 1908; reprinted by Dover, New York, 1956.

1621 Bachet, C.G., *Diophanti Alexandrini Arithmeticorum libri sex et de numeris multangulis liber unus*, S.H. Drovart, Paris, 1621; reprinted by S. de Fermat, with notes by P. de Fermat, 1670.

1676 Frénicle de Bessy, *Traité des Triangles Rectangles en Nombres*, Paris, 1676; reprinted in Mém. Acad. Roy. Sci. Paris, **5** (1729), 83–166.

[4] Полужирным шрифтом отмечены работы, имеющиеся на русском языке, список которых приведен на с. 413. — *Прим. ред.*

1863 Gauss, C. F., *Zur Theorie der Complexen Zahlen* (I), Neue Theorie der Zerlegung der Cuben, *Collected Works*, Vol. II, pp. 387–391, Königliche Ges. Wiss., Göttingen, 1876.

1908 Bottari, A., *Soluzione intere dell'equazione pitagorica e applicazione alle dimostrazione di alcune teoremi della teoria dei numeri*, Period. Mat., (3), **23** (1908), 218–220.

1908 Cattaneo, P., *Osservazioni sopra due articoli del Signor Amerigo Bottari*, Period. Mat., (3), **23** (1908), 218–220.

1915 Carmichael, R. D., *Diophantine Analysis*, Wiley, New York, 1915.

1920 Dickson, L. E., *History of the Theory of Numbers*, Vol. II, Carnegie Institution, Washington, DC, 1920; reprinted by Chelsea, New York, 1971.

1938 Hardy, G. H. and Wright, E. M., *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford, 1938.

1962 Mariani, J., *The group of Pythagorean numbers*, Amer. Math. Monthly, **69** (1962), 125–128; reprinted in *Selected Papers in Algebra*, Math. Assoc. of America, 1977, pp. 25–28.

1962 Shanks, D., *Solved and Unsolved Problems in Number Theory*, Vol. I, Spartan, Washington, DC, 1962; reprinted by Chelsea, New York, 1978.

1962 Sierpiński, W., *Pythagorean Triangles*, Yeshiva University, New York, 1962.

1972 Ribenboim, P., *L'Arithmétique des Corps*, Hermann, Paris, 1972.

I.2. Биквадратное уравнение

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

$$X^4 - Y^4 = Z^2, \tag{2.1}$$

и он доказал (дата неизвестна) следующее утверждение.

(2A) *Уравнение* (2.1) *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

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

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

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

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 (1A) 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. □

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 (2.1) 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

$$x_0 > x_1 > x_2 > \ldots,$$

что невозможно.

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.).

(2B) ***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 (2A). □

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.).

(2C) *Уравнение*

$$X^4 + Y^4 = Z^4 \tag{2.2}$$

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 (2A). □

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

Сопряженным к (2A) является следующий результат (см. явное доказательство Эйлера, 1770).

(2D) *Уравнение*

$$X^4 + Y^4 = Z^2 \tag{2.3}$$

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

Доказательство. Пусть утверждение неверно и тройка натуральных чисел (x, y, z) такова, что $x^4 + y^4 = z^2$, причем число z – наименьшее из возможных. Как и при доказательстве утверждения (2A), можно считать, что НОД$(x, y) = 1$. Заметим также, что x и y не могут быть одновременно нечетными, иначе $z^2 = x^4 + y^4 \equiv 2 \pmod 4$, а это невозможно. Итак, можно, например, считать число x четным.

Из равенства $(x^2)^2 + (y^2)^2 = z^2$ следует, что тройка (x^2, y^2, z) является примитивным решением уравнения (1.1). Согласно (1A)

существуют целые числа a и b, такие, что $a > b > 0$, НОД$(a, b) = 1$, хотя бы одно из чисел a и b четно и

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

Более того, число b должно быть четным. Действительно, если b нечетно, то a четно и $y^2 = a^2 - b^2 \equiv -1 \pmod 4$, что невозможно.

Теперь рассмотрим соотношение $b^2 + y^2 = a^2$, где y, b, a — натуральные числа, b четно и НОД$(b, y, a) = 1$. Согласно (1A) существуют целые числа c, d, такие, что $c > d > 0$, НОД$(c, d) = 1$, числа c и d имеют различную четность и

$$\begin{cases} b = 2cd, \\ y = c^2 - d^2, \\ a = c^2 + d^2. \end{cases}$$

Следовательно, $x^2 = 2ab = 4cd(c^2 + d^2)$. Но числа $c, d, c^2 + d^2$ попарно взаимно просты. Разлагая x^2 в произведение простых множителей, заключаем, что $c, d, c^2 + d^2$ суть квадраты натуральных чисел, скажем,

$$\begin{cases} c = p^2, \\ d = q^2, \\ c^2 + d^2 = r^2. \end{cases}$$

Следовательно,

$$p^4 + q^4 = r^2, \tag{2.4}$$

то есть тройка (p, q, r) является решением уравнения (2.3). Но $z = a^2 + b^2 = (c^2 + d^2)^2 + 4c^2d^2 > r^4 > r$ (так как $r > 1$). Это противоречит выбору числа z как наименьшего из возможных и завершает доказательство. □

Другие доказательства теоремы Ферма для показателя 4 даны авторами, указанными в табл. 1. Теперь приведем утверждение, равносильное теореме Ферма для показателя 4 (см. Врэнчеану, 1979).

(2E) *Следующие утверждения равносильны.*

(1) *Последняя теорема Ферма имеет место для показателя* 4.

(2) *Для любого отличного от нуля целого числа* m *уравнение* $2X^4 = mY(m^2 + Y^2)$ *имеет в отличных от нуля целых числах лишь решения* (m, m) *и* $(-m, m)$.

Таблица 1. ПТФ для показателя 4

Автор	Год
Френикль де Бесси	1676
Эйлер	1738 (опубл. в 1747), 1771
Кауслер	1795/6 (опубл. в 1802)
Барлоу	1811
Лежандр	1823, 1830
Шопи	1825
Теркем	1846
Бертран	1851
Лебег	1853, 1859, 1862
Пепен	1883
Тафельмахер	1893
Бендц	1901
Гамбиоли	1901
Кронекер	1901
Банг	1905
Боттари	1908
Рыхлик	1910
Нутцхорн	1912
Кармайкл	1913
Врэнчеану	1966

Доказательство. (1) $\Rightarrow$ (2) Пусть $m \neq 0$. Предположим, что существуют отличные от нуля целые числа u, t, такие, что $2u^4 = mt(m^2 + t^2)$. Положим $x = 2u$, $y = t - m$, $z = t + m$. Тогда $z^4 - y^4 = (z-y)(z+y)(z^2+y^2) = 2m \cdot 2t(2t^2+2m^2) = 8mt(t^2+m^2) = 16u^4 = x^4$.

По условию $xyz = 0$. Если $x = 0$, то $y = \pm z$, откуда $m = 0$ или $t = 0$, что противоречит предположению. Если $y = 0$, то $t = m$, $x = \pm z$, откуда $u = \pm m$. Если же $z = 0$, то $x = 0$, что снова противоречит предположению.

(2) $\Rightarrow$ (1) Если $x^4 + y^4 = z^4$, то $2x^4 = 2(z^4 - y^4) = 2(z-y) \times (z+y)(z^2+y^2) = (z-y)(z+y)\left[(z-y)^2 + (z+y)^2\right]$. Тогда, положив $m = z - y$, получим, что $t = z + y$, $u = x$ удовлетворяют соотношению $2u^4 = mt(m^2 + t^2)$. Если одно из чисел m, u или t равно 0, то $x = 0$. Если же $mtu \neq 0$, то по предположению $t = m$, откуда $y = 0$, что невозможно. □

В завершение настоящего раздела продемонстрируем, как применяется приведенный выше метод для решения некоторых подобных диофантовых уравнений.

(2F) *Уравнение*

$$X^4 - 4Y^4 = \pm Z^2$$

не имеет решений в отличных от нуля целых числах.

Доказательство. Достаточно рассмотреть уравнение $X^4 - 4Y^4 = Z^2$. Действительно, если x, y, z — отличные от нуля целые числа, такие, что $x^4 - 4y^4 = -z^2$, то $4x^4 - (2y)^4 = -(2z)^2$, откуда $(2y)^4 - 4x^4 = (2z)^2$ и тройка $(2y, x, 2z)$ есть решение первого уравнения.

Далее, если натуральные числа x, y, z таковы, что $x^4 - 4y^4 = z^2$ и НОД$(x, y, z) = 1$ (как можно считать без ограничения общности), то существуют такие целые числа a, b, $a > b > 0$, что

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

Из условия НОД$(a, b) = 1$ следует, что a и b являются квадратами целых чисел, скажем, $a = c^2$, $b = d^2$. Следовательно, $x^2 = c^4 + d^4$, что невозможно согласно (2D). □

Следующее утверждение принадлежит Лежандру.

(2G) *Пусть целые числа x, y, z отличны от нуля и*

$$x^4 + y^4 = 2z^2.$$

Тогда $x^2 = y^2$ и $z^2 = x^4$.

Доказательство. Из соотношений

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

следует, что

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

(в частности, $x^4 - y^4$ четно). Поскольку x, y, z отличны от нуля, согласно (2A) мы имеем $x^4 = y^4$, а значит, $x^2 = y^2$. Следовательно, $z^2 = x^4$. □

(2H) *Пусть x, y, z — такие отличные от нуля целые числа, что $2x^4 + 2y^4 = z^2$. Тогда $x^2 = y^2$, $z^2 = 4x^4$.*

Доказательство. Умножив имеющееся равенство на 8, получим $(2x)^4 + (2y)^4 = 2(2z)^2$. Согласно (2G) справедливы соотношения $(2x)^2 = (2y)^2$ и $(2z)^2 = (2x)^4$, следовательно, $x^2 = y^2$, $z^2 = 4x^4$. □

Следующий результат принадлежит Люка (1877). Мы представим более простое доказательство Облафа (1952).

(2I) *Уравнение*

$$4X^4 - 1 = 3Y^4$$

имеет в целых числах лишь тривиальные решения $(\pm 1, \pm 1)$.

Доказательство. Пусть целые числа x, y таковы, что $3y^4 = 4x^4 - 1 = (2x^2 + 1)(2x^2 - 1)$. Так как $2x^2 - 1 \not\equiv 0 \pmod 3$, существуют целые числа a и b, такие, что $2x^2 + 1 = 3a^4$, $2x^2 - 1 = b^4$. Согласно (2G) последнее уравнение имеет лишь решения $x = \pm 1$, $b = \pm 1$, откуда $y = \pm 1$. □

Список литературы

Fermat, P., Ad problema XX commentarii in ultimam questionem Arithmeticorum Diophanti. Area trianguli rectanguli in numeris non potest esse quadratus. *Oeuvres*, Vol. I, p. 340 (in Latin), Vol. III, pp. 271–272 (in French). Publiées par les soins de MM. Paul Tannery et Charles Henry. Gauthier-Villars, Paris, 1891, 1896.

Fermat, P., Commentaire sur la question 24 du Livre VI de Diophante. *Oeuvres*, Vol. I, pp. 336–338 (in Latin), Vol. III, pp. 270–271 (in French). Publiées par les soins de MM. Paul Tannery et Charles Henry. Gauthier-Villars, Paris, 1891, 1896.

1636 Fermat, P., Lettre à Mersenne [pour Sainte-Croix] (Sept. 1636). *Oeuvres*, Vol. III, pp. 286–292. Publiées par les soins de MM. Paul Tannery et Charles Henry. Gauthier-Villars, Paris, 1896.

1638 Fermat, P., Lettre de Fermat à Mersenne (début Juin, 1638). *Correspondance du Père Marin Mersenne*, Vol. 7, pp. 272–283. Commencée par Mme. Paul Tannery, publiée et annotée par Cornelis de Waard. Ed. du C.N.R.S, Paris, 1962.

1640 Fermat, P., Lettre à Mersenne (Mai ?, 1640). *Oeuvres*, Vol. II, pp. 194–195. Publiées par les soins de MM. Paul Tannery et Charles Henry. Gauthier-Villars, Paris, 1894.

1643 Fermat, P., Lettre à Saint-Martin (31 Mai, 1643). *Oeuvres*, Vol. II, pp. 258–260. Publiées par les soins de MM. Paul Tannery et Charles Henry. Gauthier-Villars, Paris, 1894.

1643 Fermat, P., Lettre à Mersenne (Août, 1643). *Oeuvres*, Vol. II, pp. 260–262. Publiées par les soins de MM. Paul Tannery et Charles Henry. Gauthier-Villars, Paris, 1894.

1654 Fermat, P., Lettre à Pascal (25 Septembre, 1654). *Oeuvres*, Vol. II, pp. 310–314. Publiées par les soins de MM. Paul Tannery et Charles Henry. Gauthier-Villars, Paris, 1894.

1658 Fermat, P., Lettre à Digby [for Wallis] (7 Avril, 1658). *Oeuvres*, Vol. II, pp. 374–378. Publiées par les soins de MM. Paul Tannery et Charles Henry. Gauthier-Villars, Paris, 1894.

1659 Fermat, P., Lettre à Carcavi (Août, 1659). Relation des nouvelles découvertes en la science des nombres. *Oeuvres*, Vol. II, pp. 431–436. Publiées par les soins de MM. Paul Tannery et Charles Henry. Gauthier-Villars, Paris, 1894.

1676 Frénicle de Bessy, *Traité des Triangles Rectangles en Nombres*, Vol. I, Paris, 1676; reprinted in Mém. Acad. Roy. Sci. Paris, **5** (1729), 1666–1699.

1738 Euler, L., *Theorematum quorundam arithmeticorum demonstrationes*, Comm. Acad. Sci. Petrop., **10** (1738) 1747, 125–146; also in *Opera Omnia*, Ser. I, *Commentationes Arithmeticae*, Vol. I, pp. 38–58. Teubner, Leipzig, 1915.

1770/1 Euler, L., *Vollständige Anleitung zur Algebra*, 2 volumes. Royal Acad. Sci., St. Petersburg. French translation with notes of M. Bernoulli and additions of M. de LaGrange, Kais. Acad. Wiss., St. Petersburg, 1770; English translation by Rev. J. Hewlitt, Longman, Hurst, Rees, Orme, London, 1822. Also in *Opera Omnia*, Ser. I, Vol. I, pp. 437ff. Teubner, Leipzig, 1911.

1777 Lagrange, J.L., *Sur quelques problèmes de l'analyse de Diophante*. Nouveaux Mém. Acad. Sci. Belles Lettres, Berlin, 1777; reprinted in *Oeuvres*, Vol. IV (publiées par les soins de M. J.-A. Serret), pp. 377–398, Gauthier-Villars, Paris, 1869.

1802 Kausler, C.F., *Nova demonstratio theorematis nec summam, nec differentiam duorum biquadratorum biquadratum esse posse*, Novi Acta Acad. Petrop., **13** (1795/6), 1802, 237–244.

1808 Legendre, A.M., *Essai sur la Théorie des Nombres* (2^e édition), p. 343, Courcier, Paris, 1808.

1811 Barlow, P., *An Elementary Investigation of Theory of Numbers*, pp. 144–145, J. Johnson, St. Paul's Church-Yard, London, 1811.

1825 Schopis, *Einige Sätze aus der unbestimmten Analytik*, Programm, Gummbinnen, 1825.

1830 Legendre, A.M., *Théorie des Nombres* (3^e édition), Vol. II, p. 5, Firmin Didot Frères, Paris, 1830; reprinted by A. Blanchard, Paris, 1955.

1846 Terquem, O., *Théorèmes sur les puissances des nombres*, Nouv. Ann. Math., **5** (1846), 70–87.

1851 Bertrand, J., *Traité Élémentaire d'Algèbre*, pp. 217–230 and 395, Hachette, Paris, 1851.

1853 Lebesgue, V.A., *Résolution des équations biquadratiques* $z^2 = x^4 \pm 2^m y^4$, $z^2 = 2^m x^4 - y^4$, $2^m z^2 = x^4 \pm y^4$, J. Math. Pures Appl., **18** (1853), 73–86.

1859 Lebesgue, V.A., *Exercices d'Analyse Numérique*, pp. 83–84 and 89, Leiber et Faraguet, Paris, 1859.

1862 Lebesgue, V.A., *Introduction à la Théorie des Nombres*, pp. 71–73, Mallet-Bachelier, Paris, 1862.

1877 Lucas, E., *Sur la résolution du système des équations* $2v^2 - u^2 = w^2$ *et* $2v^2 + u^2 = 3z^2$, Nouv. Ann. Math., 2e série, **36** (1877), 409–416.

1883 Pepin, T., *Étude sur l'équation indéterminée* $ax^4 + by^4 = cz^2$, Atti Accad. Naz. Lincei, **36** (1883), 34–70.

1893 Tafelmacher, W.L.A., *Sobre la ecuación* $x^4 + y^4 = z^4$, Ann. Univ. Chile, **84** (1893), 307–320.

1901 Bendz, T.R., *Öfver diophantiska ekvationen* $x^n + y^n = z^n$, Almqvist & Wiksells Boktrycken, Uppsala, 1901.

1901 Gambioli, D., *Memoria bibliografica sull'ultimo teorema di Fermat*, Period. Mat., **16** (1901), 145–192.

1901 Kronecker, L., *Vorlesungen über Zahlentheorie*, Vol. I, pp. 35–38, Teubner, Leipzig, 1901; reprinted by Springer-Verlag, Berlin, 1978.

1905 Bang, A., *Nyt Bevis for at Ligningen* $x^4 - y^4 = z^4$, *ikke kan have rationale Løsinger*, Nyt Tidsskrift Mat., **16B** (1905), 35–36.

1908 Bottari, A., *Soluzione intere dell'equazione pitagorica e applicazione alla dimostrazione di alcune teoremi della teoria dei numeri*, Period. Mat., **23** (1908), 104–110.

1910 Bachmann, P., *Niedere Zahlentheorie*, Vol. II, Teubner, Leipzig, 1910; reprinted by Chelsea, New York, 1968.

1910 Rychlik, K., *On Fermat's last theorem for* $n = 4$ *and* $n = 3$ (in Bohemian), Časopis Pěst. Mat., **39** (1910), 65–86.

1912 Nutzhorn, F., *Den ubestemte Ligning* $x^4 + y^4 = z^4$, Nyt Tidsskrift Mat., **23B** (1912), 33–38.

1913 Carmichael, R.D., *On the impossibility of certain Diophantine equations and systems of equations*, Amer. Math. Monthly, **20** (1913), 213–221.

1915 Carmichael, R.D., *Diophantine Analysis*, Wiley, New York, 1915.

1952 Obláth, R., *Über einige unmögliche diophantische Gleichungen*, Matem. Tidsskrift Ser. A (1952), 53–62.

1966 Vrănceanu, G., *Asupra teorema lui Fermat pentru* $n = 4$, Gaz. Mat. Ser. A, **71** (1966), 334–335; reprinted in *Opera Matematica*, Vol. 4, pp. 202–205, Edit. Acad. Rep. Soc. Romana, Bucureşti, 1977.

1977 Edwards, H.M., *Fermat's Last Theorem, A Genetic Introduction to Algebraic Number Theory*, Springer-Verlag, New York, 1977.

1979 Vrănceanu, G., *Une interprétation géométrique du théorème de Fermat*, Rev. Roumaine Math. Pures Appl., **24** (1979), 1137–1140.

I.3. Гауссовы числа

В этом разделе мы докажем, что уравнение $X^4 + Y^4 = Z^2$ не имеет решений в отличных от нуля целых числах из гауссова поля. В явном виде этот результат содержится в работе Гильберта «Zahlbericht» (1897, теорема 169) (см. также Зоммер (1907) и Хенкок (1931)).

Множество комплексных чисел вида $\alpha = a + bi$, где $i = \sqrt{-1}$ и $a, b \in \mathbb{Q}$, составляет гауссово поле $K = \mathbb{Q}(i)$. Числа $\alpha = a + bi$, где $a, b \in \mathbb{Z}$, называются *целыми гауссовыми числами*. Они образуют кольцо, обозначаемое через $A = \mathbb{Z}[i]$.

Пусть $\alpha, \beta \in K$. Будем говорить, что β делит α, если найдется такое целое гауссово число γ, что $\alpha = \beta\gamma$. В этом случае будем писать $\beta \mid \alpha$. Два отличных от нуля целых гауссовых числа α, β называются *ассоциированными*, если α делит β и β делит α; в таком случае будем писать $\alpha \sim \beta$. Целые гауссовы числа, ассоциированные с 1, называются (гауссовыми) *единицами*. Легко видеть, что они равны ± 1, $\pm i$.

Отличное от нуля целое гауссово число α называется *простым*, если оно не является единицей и все целые гауссовы числа, делящие α, суть единицы или ассоциированные с α. В поле гауссовых чисел каждое отличное от нуля целое гауссово число α является произведением простых целых гауссовых чисел: $\alpha = \gamma_1\gamma_2 \dots \gamma_s$. Это разложение единственно в следующем смысле: если также суще-

ствует разложение $\alpha = \delta_1\delta_2\ldots\delta_t$, где каждое δ_i — простое целое гауссово число, то $s = t$ и можно так изменить порядок в произведении (если требуется), чтобы γ_i и δ_i были ассоциированными для всех $i = 1, \ldots, s$.

Следовательно, можно очевидным способом определить наибольший общий делитель отличных от нуля целых гауссовых чисел, который будет единственным с точностью до умножения на единицу.

Пусть α, β, γ — гауссовы числа, причем $\gamma \neq 0$. Будем писать $\alpha \equiv \beta \pmod{\gamma}$, если γ делит $\alpha - \beta$. Отношение сравнения $\equiv$ удовлетворяет тем же свойствам, что и для обычных целых чисел. Целое гауссово число $\lambda = 1 - i$ простое, причем $2 = i\lambda^2$, откуда $\lambda^2 \mid 2$, но $\lambda^3 \nmid 2$. Легко видеть, что $1 + i = i(1 - i) = i\lambda$.

Существует в точности четыре различных класса чисел, сравнимых между собой по модулю 2, а именно классы, содержащие 0, 1, i и λ. В самом деле, эти числа попарно несравнимы по модулю 2. С другой стороны, так как числа a и b четны, число $a+bi$ сравнимо с 0, 1, i или λ по модулю 2. В частности, если $\lambda \nmid \alpha = a+bi$, то $\alpha \equiv 1 \pmod{2}$ или $\alpha \equiv i \pmod{2}$. Тогда $\alpha^2 \equiv \pm 1 \pmod{4}$ и $\alpha^4 \equiv 1 \pmod{8}$, то есть $\alpha^4 \equiv 1 \pmod{\lambda^6}$, так как $8 = -i\lambda^6$.

Теперь мы готовы доказать следующий результат.

(3A) *Уравнение*

$$X^4 + Y^4 = Z^2$$

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

Доказательство. Пусть $\xi, \eta, \theta \in \mathbb{Z}[i]$ отличны от нуля и таковы, что $\xi^4 + \eta^4 = \theta^2$. Без ограничения общности можно полагать, что $\text{НОД}(\xi, \eta) = 1$. Действительно, если $\delta = \text{НОД}(\xi, \eta)$, то $\xi = \delta\xi'$, $\eta = \delta\eta'$, где $\xi', \eta' \in \mathbb{Z}[i]$, $\text{НОД}(\xi', \eta') = 1$. Значит, δ^4 делит θ^2 и, таким образом, δ^2 делит θ, то есть $\theta = \delta^2\theta'$, где $\theta' \in \mathbb{Z}[i]$. Следовательно, $\xi'^4 + \eta'^4 = \theta'^2$, где $\text{НОД}(\xi', \eta') = 1$.

Поскольку $\text{НОД}(\xi, \eta) = 1$, числа ξ, η, θ попарно взаимно просты. Рассмотрим два случая.

Случай 1: λ не делит $\xi\eta$.

Согласно сделанному замечанию $\xi^4 \equiv 1 \pmod{\lambda^6}$ и $\eta^4 \equiv 1 \pmod{\lambda^6}$, поэтому $\theta^2 = \xi^4 + \eta^4 \equiv 2 \pmod{\lambda^6}$. Из соотношения $2 = i\lambda^2$ следует, что $\lambda^2 \mid \theta^2$, а значит, $\lambda \mid \theta$. Однако $\lambda^2 \nmid \theta$, потому что $\lambda^4 \nmid 2$. Таким образом, $\theta = \lambda\theta_1$, где $\lambda \nmid \theta_1$. Из этого представле-

ния следует, что $\lambda^2\theta_1^2 \equiv 2 = i\lambda^2 \pmod{\lambda^6}$, поэтому $\theta_1^2 \equiv i \pmod{\lambda^4}$ и, следовательно, $\theta_1^4 \equiv -1 \pmod{\lambda^6}$, так как $\lambda^4 \sim 4$, $\lambda^6 \sim 8$. Однако $\lambda \nmid \theta_1$, поэтому $\theta_1^4 \equiv 1 \pmod{\lambda^6}$. Вычитая полученные сравнения, приходим к выводу, что $2 \equiv 0 \pmod{\lambda^6}$, а это невозможно.

Случай 2: λ делит ξ.

В этом случае $\lambda \nmid \eta\theta$. Представим ξ в виде $\xi = \lambda^m\xi'$, где $m \geqslant 1$, $\xi' \in \mathbb{Z}[i]$ и $\lambda \nmid \xi'$. Нам достаточно доказать следующее утверждение.

Пусть $n \geqslant 1$ и ε — единица в $\mathbb{Z}[i]$ (то есть $\varepsilon = \pm 1$ или $\pm i$). Пусть, далее, существуют попарно взаимно простые числа $\alpha, \beta, \gamma \in \mathbb{Z}[i]$, не кратные λ, такие, что $\varepsilon\lambda^{4n}\alpha^4 + \beta^4 = \gamma^2$. Тогда

(a) $n \geqslant 2$;

(b) существуют единица ε_1 и такие попарно взаимно простые числа $\alpha_1, \beta_1, \gamma_1 \in \mathbb{Z}[i]$, не кратные λ, что

$$\varepsilon_1\lambda^{4(n-1)}\alpha_1^4 + \beta_1^4 = \gamma_1^2.$$

Предположение имеет место для $n = m$, $\varepsilon = 1$, $\alpha = \xi'$, $\beta = \eta$, $\gamma = \theta$. Несколько раз применив приведенное утверждение, найдем единицу ε' и попарно взаимно простые числа $\alpha', \beta', \gamma' \in \mathbb{Z}[i]$, не кратные λ, такие, что

$$\varepsilon'\lambda^4\alpha'^4 + \beta'^4 = \gamma'^2.$$

Это противоречит п. (a) нашего утверждения.

Сначала покажем, что $n \geqslant 2$. Действительно, $\varepsilon\lambda^{4n}\alpha^4 + \beta^4 - 1 = \gamma^2 - 1$, и, так как $\lambda \nmid \beta$, мы получаем $\beta^4 \equiv 1 \pmod{\lambda^6}$, а поэтому $\gamma^2 \equiv 1 \pmod{\lambda^4}$. Но $\lambda \nmid \gamma$, следовательно, $\gamma \equiv i \pmod{\lambda^2}$ или $\gamma \equiv 1 \pmod{\lambda^2}$. В первом случае $\gamma^2 \equiv -1 \pmod{\lambda^4}$, откуда следует, что λ^4 делит 2, что противоречит предположению. Итак, $\gamma - 1 = \lambda^2\mu$, где $\mu \in \mathbb{Z}[i]$, и, следовательно, $\gamma + 1 = \lambda^2\mu + 2 = \lambda^2(\mu + i)$. Но $\mu \equiv i \pmod{\lambda}$ вне зависимости от того, является ли λ делителем числа μ, потому что $1 \equiv i \pmod{\lambda}$; значит, $\mu \equiv -i \pmod{\lambda}$. Мы показали, что в любом случае $\lambda \mid \mu(\mu+i)$, поэтому λ^5 делит $\gamma^2 - 1 = \lambda^4\mu(\mu + i)$, откуда следует, что λ^5 делит $\varepsilon\lambda^{4n}\alpha^4 + (\beta^4 - 1)$. Но λ^6 делит $\beta^4 - 1$, $\lambda \nmid \alpha$, а поэтому $\lambda^5 \mid \lambda^{4n}$, следовательно, $n \geqslant 2$.

Теперь докажем утверждение п. (b). Нетрудно видеть, что $\varepsilon\lambda^{4n}\alpha^4 = \gamma^2 - \beta^4 = (\gamma - \beta^2)(\gamma + \beta^2)$. Заметим, что НОД$(\gamma - \beta^2, \gamma + \beta^2) = \lambda^2$. Действительно, λ должно делить хотя бы один из множителей в правой части, а значит, оно делит оба сомножителя, потому что $(\gamma + \beta^2) - (\gamma - \beta^2) = 2\beta^2$ кратно λ^2. Так как λ^4 делит

правую часть, λ^2 непременно делит оба сомножителя:

$$\begin{cases} \gamma \mp \beta^2 = \lambda^2 \nu, \\ \gamma \pm \beta^2 = \lambda^{4n-2} \nu', \end{cases}$$

где $\nu, \nu' \in \mathbb{Z}[i]$ и $\text{НОД}(\nu, \nu') = 1$. Следовательно, $\varepsilon \lambda^{4n} \alpha^4 = \lambda^{4n} \nu \nu'$ и, так как разложение на множители единственно с точностью до умножения на единицу, ν, ν' должны быть четвертыми степенями с точностью до умножения на единицу: $\nu = \omega \kappa^4$, $\nu' = \omega' \kappa'^4$, где $\kappa, \kappa' \in \mathbb{Z}[i]$, $\text{НОД}(\kappa, \kappa') = 1$, ω, ω' — единицы. Таким образом,

$$\begin{cases} \gamma \mp \beta^2 = \omega \lambda^2 \kappa^4, \\ \gamma \pm \beta^2 = \omega' \lambda^{4n-2} \kappa'^4. \end{cases}$$

Вычитая из второй пары равенств первую, получим

$$\pm 2\beta^2 = \omega' \lambda^{4n-2} \kappa'^4 - \omega \lambda^2 \kappa^4.$$

Следовательно,

$$\pm \beta^2 = -i\omega' \lambda^{4n-4} \kappa'^4 + i\omega \kappa^4,$$

откуда

$$\omega_1' \lambda^{4(n-1)} \kappa'^4 + \omega_1 \kappa^4 = \beta^2,$$

где единицы имеют вид $\omega_1' = -i\omega'$, $\omega_1 = i\omega$. Покажем, что $\omega_1 = 1$, из чего будет следовать утверждение п. (b). Из условия $n \geqslant 2$ следует, что $\lambda^4 \mid (\beta^2 - \omega_1 \kappa^4)$. Однако $\lambda \nmid \beta$, поэтому $\lambda \nmid \kappa$, а следовательно, $\kappa^4 \equiv 1 \pmod{\lambda^6}$, так что $\lambda^4 \mid (\beta^2 - \omega_1)$. Но λ^6 делит $\beta^4 - 1 = (\beta^2 - 1)(\beta^2 + 1)$, поэтому $\beta^2 \equiv 1$ или $-1 \pmod{\lambda^4}$. Это значит, что $\omega_1 = \pm 1$. Если $\omega_1 = -1$, то, умножив на -1, получим соотношение

$$-\omega_1' \lambda^{4(n-1)} \kappa'^4 + \kappa^4 = (i\beta)^2.$$

Итак, рассмотрев все случаи, мы установили справедливость утверждения п. (b), что и завершает доказательство. □

Список литературы

1897 Hilbert, D., *Die Theorie der algebraischen Zahlkörper*, Jahresber. Deutsch. Math.-Verein., **4** (1897), 175–546; reprinted in *Gesammelte Abhandlungen*, Vol. I, Chelsea, New York, 1965.

1907 Sommer, J., *Vorlesungen über Zahlentheorie*, Teubner, Leipzig, 1907.

1931 Hancock, H., *Foundations of the Theory of Algebraic Numbers*, Vol. I., Macmillan, New York, 1931.

I.4. Кубическое уравнение

Ферма поставил задачу показать, что куб не может быть равен сумме двух отличных от нуля кубов. См. письма Мерсенну [для Сен-Круа] (сентябрь 1636 г.), Мерсенну (май 1640 г.), Дигби [для Валлиса] (7 апреля 1658 г.), Каркави (август 1659 г.), приведенные в списке литературы к разд. I.2; см. также письмо к Дигби [для Броункера] (15 августа 1657 г.).

Эйлер нашел доказательство этого утверждения. 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 $a^2 + 3b^2$. Заметим, что еще в своей статье от 1760 г. Эйлер строго доказал, что если нечетное простое число p делит $a^2 + 3b^2$ (где a и b — отличные от нуля взаимно простые целые числа), то существуют целые числа u, v, такие, что $p = u^2 + 3v^2$. Тем не менее, Эйлер не доказал полностью лемму 4.7, необходимую для доказательства главного утверждения. На страницах своей книги (1808, 1830) Лежандр приводит доказательство Эйлера без доведения деталей рассуждения до конца.

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 $c = 1, 2, 3, 4, 7$. Шумахер (1894) в явном виде отметил недостающее звено в рассуждениях. В 1901 г. Ландау предложил строгое доказательство; ту же цель преследовала и статья Холдена (1906), а в 1915 г. подробное доказательство вновь было представлено в книге Кармайкла[5]. В 1966 г. Бергман опубликовал статью, в которой подверг доказательство Эйлера историческому рассмотрению и тщательному анализу. Далее, в 1972 г. Р. Лежандр указал, что рассуждения Эйлера были несовершенными. Это доказательство также обсуждается в книге Эдвардса (1977).

(4A) *Уравнение*

$$X^3 + Y^3 + Z^3 = 0 \tag{4.1}$$

имеет лишь тривиальные решения в целых числах.

---

[5]Предложенное Пизой (1955) упрощение доказательства Эйлера содержит ошибку, как указал Иф (1956).

Доказательство. Предположим, что x, y и z — отличные от нуля попарно взаимно простые целые числа, такие, что $x^3 + y^3 + z^3 = 0$. Тогда они должны быть различными (потому что 2 не является кубом) и ровно одно из них четно, скажем, x, y нечетны, а z четно. Из всех решений с такими свойствами выберем то, для которого значение $|z|$ минимально.

Наша цель — указать такие отличные от нуля попарно взаимно простые целые числа l, m, n, что $l^3 + m^3 + n^3 = 0$, n четно и $|n| < |z|$. Тогда мы получим противоречие. Так как числа $x + y$, $x - y$ четны, существуют целые числа a и b, такие, что $2a = x + y$, $2b = x - y$. Отсюда $x = a + b$, $y = a - b$ и, следовательно, $a, b \neq 0$, $\text{НОД}(a, b) = 1$, причем a и b имеют различную четность.

Легко видеть, что справедлива цепочка равенств

$$-z^3 = x^3 + y^3 = (a + b)^3 + (a - b)^3 = 2a(a^2 + 3b^2).$$

Но $a^2 + 3b^2$ нечетно, а z четно, откуда следует, что z^3 кратно 8, а значит, $2a$ кратно 8 и, следовательно, b нечетно. Нетрудно проверить, что $\text{НОД}(2a, a^2 + 3b^2)$ равен 1 или 3. В самом деле, если p — такое простое число, что p^k $(k \geqslant 1)$ делит $2a$ и $a^2 + 3b^2$, то $p \neq 2$, откуда следует, что p^k делит a, а значит, и $3b^2$; но b не кратно p, поэтому $k = 1$ и $p = 3$.

Теперь рассмотрим два случая.

Случай 1: $\text{НОД}(2a, a^2 + 3b^2) = 1$.

Тогда a не делится на 3. Из равенства $-z^3 = 2a(a^2 + 3b^2)$, учитывая единственность разложения целых чисел на простые множители, получим, что $2a$ и $a^2 + 3b^2$ являются кубами:

$$\begin{cases} 2a = r^3, \\ a^2 + 3b^2 = s^3, \end{cases}$$

где s нечетно и не кратно 3. Здесь мы воспользуемся утверждением, которое обоснуем позже: если s нечетно и $s^3 = a^2 + 3b^2$, где $\text{НОД}(a, b) = 1$, то s также должно иметь вид $s = u^2 + 3v^2$, где $u, v \in \mathbb{Z}$ и

$$\begin{cases} a = u(u^2 - 9v^2), \\ b = 3v(u^2 - v^2). \end{cases}$$

Тогда v нечетно, u четно (потому что b нечетно), $u \neq 0$, u не кратно 3 (так как a не кратно 3) и $\text{НОД}(u, v) = 1$. Следовательно, числа $2u$, $u + 3v, u - 3v$ попарно взаимно просты и, поскольку $r^3 = 2a =$

$= 2u(u-3v)(u+3v)$, мы можем заключить, что $2u$, $u-3v$, $u+3v$ являются кубами:

$$\begin{cases} 2u &= -n^3, \\ u-3v &= l^3, \\ u+3v &= m^3, \end{cases}$$

причем l, m, n отличны от 0 (так как u не кратно 3) и попарно взаимно просты. Отсюда заключаем, что

$$l^3 + m^3 + n^3 = 0,$$

где n четно. Теперь покажем, что $|z| > |n|$. В самом деле,

$$|z|^3 = |2a(a^2+3b^2)| = |n^3(u^2-9v^2)(a^2+3b^2)| \geqslant 3|n^3| > |n^3|,$$

потому что $u^2 - 9v^2 = l^3m^3 \neq 0$ и $b \neq 0$, так как b нечетно. Это противоречит минимальности $|z|$.

Случай 2: $\text{НОД}(2a,\, a^2+3b^2) = 3$.

Представим a в виде $a = 3c$. Таким образом, c четно и, более того, c кратно 4, в то время как b не кратно 3 (так как a и b взаимно просты). Итак, $-z^3 = 6c(9c^2+3b^2) = 18c(3c^2+b^2)$, причем $\text{НОД}(18c, 3c^2+b^2) = 1$. В самом деле, c четно, b нечетно, а следовательно, $3c^2+b^2$ нечетно, $3c^2+b^2$ не кратно 3 и $\text{НОД}(b,c) = 1$. Принимая во внимание единственность разложения целых чисел на простые множители, получим, что $18c$ и $3c^2+b^2$ являются кубами:

$$\begin{cases} 18c &= r^3, \\ 3c^2+b^2 &= s^3, \end{cases}$$

где s нечетно и r не кратно 3. Согласно тому же указанному результату $s = u^2+3v^2$, где $u, v \in \mathbb{Z}$ и

$$\begin{cases} b = u(u^2-9v^2), \\ c = 3v(u^2-v^2). \end{cases}$$

Таким образом, u нечетно, v четно (так как b нечетно), $v \neq 0$, $\text{НОД}(u,v) = 1$. Кроме того, числа $2v$, $u+v$, $u-v$ попарно взаимно просты. Поскольку $r^3 = 18c = 54v(u+v)(u-v)$, мы можем заключить, что $(r/3)^3 = 2v(u+v)(u-v)$ и $2v$, $u+v$, $u-v$ являются кубами:

$$\begin{cases} 2v &= -n^3, \\ u+v &= l^3, \\ u-v &= -m^3. \end{cases}$$

Таким образом, $l^3 + m^3 + n^3 = 0$, где l, m, n отличны от 0 и n четно. Теперь покажем, что $|z| > |n|$. В самом деле,

$$\begin{aligned} |z|^3 &= 18|c|(3c^2 + b^2) \\ &= 54|v(u^2 - v^2)|(3c^2 + b^2) \\ &= 27|n|^3|u^2 - v^2|(3c^2 + b^2) \\ &> |n|^3. \end{aligned}$$

Так как $u^2 - v^2 = -l^3m^3 \neq 0$, мы получаем $|3c^2 + b^2| \geqslant 1$. Это снова противоречит выбору значения $|z|$ как наименьшего из возможных. □

Нам осталось обосновать возможность представления s в виде $s = u^2 + 3v^2$. Для этой цели воспользуемся приемом, который был известен еще Ферма, когда он изучал целые числа вида $u^2 + 3v^2$.

Пусть S — множество целых чисел вида $a^2 + 3b^2$ $(a, b \in \mathbb{Z})$. Множество S замкнуто относительно умножения, так как

$$(a^2 + 3b^2)(c^2 + 3d^2) = (ac \pm 3bd)^2 + 3(ad \mp bc)^2 \qquad (4.2)$$

(равенство имеет место для согласованных знаков).

Лемма 4.1. *Пусть простое число p отлично от 2 и 3. Тогда следующие условия равносильны:*

(1) $p \equiv 1 \pmod 6$;
(2) -3 *есть квадрат по модулю* p;
(3) *многочлен* $X^2 + X + 1$ *имеет корень в* $\mathbb{F}_p$.

Доказательство. Чтобы доказать эквивалентность высказываний (1) и (2), вычислим символ Лежандра, используя квадратичный закон взаимности Гаусса:

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p-1)/2}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Итак, $(-3/p) = +1$ тогда и только тогда, когда $p \equiv 1 \pmod 3$, то есть $p \equiv 1 \pmod 6$.

Чтобы доказать равносильность высказываний (2) и (3), преобразуем наш многочлен:

$$X^2 + X + 1 = \left(X + \frac{1}{2}\right)^2 + \frac{3}{4}.$$

Если существует $\alpha \in \mathbb{F}_p$, такое, что $\alpha^2 + \alpha + 1 = 0$, то $-3 = 4\left(\alpha + \frac{1}{2}\right)^2$. Обратно, если $-3 = \beta^2$, где $\beta \in \mathbb{F}_p$, положим $\alpha = -\frac{1}{2} + \beta/2$, откуда получим $\alpha^2 + \alpha + 1 = 0$. □

Лемма 4.2. *Пусть целое число k отлично от нуля, а число p простое, причем $p = c^2 + 3d^2 \in S$, $pk = a^2 + 3b^2 \in S$. Тогда p делит $ac \pm 3bd$ и $ad \mp bc$ (где знаки согласованы) и*

$$k = \left(\frac{ac \pm 3bd}{p}\right)^2 + 3\left(\frac{ad \mp bc}{p}\right)^2 \in S.$$

Доказательство. Согласно тождеству (4.2) мы имеем

$$k = \frac{(a^2 + 3b^2)(c^2 + 3d^2)}{(c^2 + 3d^2)^2} = \left(\frac{ac \pm 3bd}{c^2 + 3d^2}\right)^2 + 3\left(\frac{ad \mp bc}{c^2 + 3d^2}\right)^2.$$

Но $(ac+3bd)(ac-3bd) = a^2c^2 - 9b^2d^2 = a^2(c^2+3d^2) - 3(a^2+3b^2)d^2 = (a^2-3kd^2)(c^2+3d^2)$. Так как число $c^2+3d^2 = p$ простое, мы можем считать, что, скажем, p делит $ac + 3bd$, то есть $(ac+3bd)/p \in \mathbb{Z}$. Значит, и $3\left((ad-bc)/p\right)^2 \in \mathbb{Z}$, а следовательно, $(ad-bc)/p \in \mathbb{Z}$, так что $k \in S$. □

Лемма 4.3. *Простое число p принадлежит множеству S тогда и только тогда, когда $p = 3$ или $p \equiv 1 \pmod 3$.*

Доказательство. Если $p = a^2 + 3b^2$, $p \neq 3$, то $b \neq 0$; таким образом, $p \equiv a^2 \pmod 3$ и $3 \nmid a$. Значит, $p \equiv a^2 \equiv 1 \pmod 3$.

Ясно, что $3 \in S$. Пусть $p \equiv 1 \pmod 3$. Так как $(-3/p) = 1$, существует число t, такое, что $0 < t < p/2$ и $-3 \equiv t^2 \pmod p$. Тогда $mp = t^2 + 3 < (p/2)^2 + 3 < p^2$, следовательно, $0 < m < p$. Теперь заметим, что для любого $t \geqslant 1$ существует не более одного простого числа $p \neq 2, 3$, такого, что $p \mid (t^2 + 3)$, но $p \nmid (u^2 + 3)$ для всякого u, $1 \leqslant u < t$.

Действительно, предположим, что существуют два различных таких простых числа p, p', $p < p'$. Согласно предшествующему замечанию должны выполняться условия $0 < t < p/2$ и $t^2 + 3 = pm$, где $0 < m < p$. Так как $p' \mid (t^2 + 3)$, мы заключаем, что $p' \mid m$, следовательно, $p' \leqslant m < p$, а это невозможно.

Теперь мы готовы доказать наше утверждение. Предположим, что существует такое простое число p, $p \equiv 1 \pmod 3$, что $p \notin S$. Выберем наименьшее p, удовлетворяющее этому условию. Пусть t — наименьшее натуральное число, такое, что $p \mid (t^2+3)$. Тогда $0 < t < p/2, t^2 + 3 = mp$, где $0 < m < p$. Пусть p' — произвольное простое число, делящее m, $m = p'm'$. Тогда $p' \leqslant m < p$, а значит, $p' \in S$. Из соотношения $p'(pm') = pm = t^2 + 3 \in S$ и леммы 4.2 следует, что $pm' \in S$. Если $m' = 1$, то $p \in S$, что и требовалось доказать. Если простое число p'' делит m', причем $m' = p''m''$, то $p'' \leqslant m' < p$,

следовательно, $p'' \in S$, так что $p''(pm'') = pm' \in S$ и согласно лемме 4.2 мы получаем $pm'' \in S$, где $m'' < m'$. Повторяя это рассуждение, заключаем, что $p \in S$. □

Будет полезно привести еще одно доказательство того факта, что если $p \equiv 1 \pmod 3$, то $p \in S$, в котором используется «метод ящиков» Дирихле.

Если $p \equiv 1 \pmod 3$, то существует число t, $1 \leqslant t \leqslant p-1$, такое, что $-3 \equiv t^2 \pmod p$. Рассмотрим множество всех пар (m, n), таких, что $0 \leqslant m, n \leqslant [\sqrt{p}]$. Так как количество этих пар превосходит p, существуют две различные пары (m, n), (m', n'), такие, что $m + nt \equiv m' + n't \pmod p$. Итак, $m \neq m'$ и $n \neq n'$, скажем, $n > n'$, следовательно, $t \equiv (m'-m)/(n-n') \pmod p$. Поскольку $0 < n - n' < \sqrt{p}$ и $0 < |m'-m| < \sqrt{p}$, мы заключаем, что $t \equiv \pm a/b \pmod p$, где $0 < a < \sqrt{p}$, $0 < b < \sqrt{p}$. Таким образом, $a^2 + 3b^2 \equiv 0 \pmod p$ и мы можем записать $a^2 + 3b^2 = kp$, где $0 < k < 4$. Отсюда следует, что $a^2 \equiv k \pmod 3$, а значит, $k \equiv 0$ или $1 \pmod 3$, то есть $k = 1$ или 3. Если $k = 1$, то $p \in S$. Если же $k = 3$, то $3 \mid a$, т. е. $a = 3a'$, и, разделив на 3, мы получим $p = b^2 + 3a'^2 \in S$.

Лемма 4.4. *Пусть $m = u^2 + 3v^2$, где $u, v \neq 0$, НОД $(u, v) = 1$, u нечетное простое число p делит m. Тогда $p \in S$.*

Доказательство. Так как $3 \in S$, можно считать, что $p \neq 3$. Поскольку p делит m, мы можем заключить, что p не делит v, иначе оно также делило бы и u, что противоречит предположению. Пусть число v' таково, что $vv' \equiv 1 \pmod p$. Тогда $(uv')^2 \equiv -3 \pmod p$ и $(-3/p) = 1$, т. е. $p \equiv 1 \pmod 3$. Применив лемму 4.3, заключаем, что $p \in S$. □

Следующая лемма дополняет предыдущие.

Лемма 4.5. *Пусть p — простое число, $p \in S$. Тогда его представление в виде $p = a^2 + 3b^2$ (где $a \geqslant 0$, $b \geqslant 0$) единственно.*

Доказательство. Воспользовавшись леммой 4.2 при $k = 1$, т. е. полагая, что $p = a^2 + 3b^2 = c^2 + 3d^2$ (где $a, c \geqslant 0$, $b > 0$, $d > 0$), мы получаем

$$1 = \left(\frac{ac \pm 3bd}{p}\right)^2 + 3\left(\frac{ad \mp bc}{p}\right)^2,$$

следовательно, $p = ac \pm 3bd$, $ad = \pm bc$. Таким образом, $pd = acd \pm \pm 3bd^2 = \pm bc^2 \pm 3bd^2 = \pm b(c^2 + 3d^2) = \pm bp$. Итак, $d = \pm b$, а значит, $b = d$, откуда следует, что $a = c$. □

ЛЕММА 4.6. *Пусть* $m = 3$ *или* $m = u^2 + 3v^2$, *где* $u, v \neq 0$ *и* НОД$(u, v) = 1$. *Если* m *нечетно и* $m = \prod_{i=1}^{n} p_i^{e_i}$ (*где* $p_1, \ldots, p_n$ — *простые числа и* $e_i \geqslant 1$), *то существуют целые числа* a_i, b_i ($i = 1, \ldots, n$), *такие, что* $p_i = a_i^2 + 3b_i^2$ *и*

$$u + v\sqrt{-3} = \prod_{i=1}^{n} (a_i + b_i\sqrt{-3})^{e_i}.$$

ДОКАЗАТЕЛЬСТВО. Доказательство проведем с помощью индукции по m. При $m = 3$ утверждение очевидно. Пусть $m > 3$. Тогда $m = u^2 + 3v^2$, где $u, v \neq 0$, НОД$(u, v) = 1$. Пусть простое число p делит m, т. е. $m = pk$. Согласно лемме 4.4 мы можем записать $p = a^2 + 3b^2$ и по лемме 4.2 получаем $k = c^2 + 3d^2$, где

$$c = (ua \pm 3vb)/p, \quad d = (ub \mp va)/p$$

(знаки согласованы). Также мы видим, что

$$(a \pm b\sqrt{-3})(c \mp d\sqrt{-3}) = (ac + 3bd) \pm (bc - ad)\sqrt{-3},$$

причем

$$ac + 3bd = \frac{1}{p}(ua^2 \pm 3vab + 3ub^2 \mp 3vab) = u,$$

$$\pm(bc - ad) = \pm\frac{1}{p}(uab \pm 3vb^2 - uab \pm va^2) = v,$$

то есть

$$(a \pm b\sqrt{-3})(c \mp d\sqrt{-3}) = u + v\sqrt{-3}.$$

Если $k = 1$, то утверждение очевидно. Пусть $k \neq 1$. Тогда или $k = 3$, или $k \neq 3$. В последнем случае $c \neq 0$ (если $c = 0$, то d делит u, v, следовательно, $d = 1$ и $k = 3$, что противоречит предположению); аналогично $d \neq 0$ (если $d = 0$, то c делит u, v, следовательно, $c = 1$ и $k = 1$, что снова противоречит предположению). Более того, НОД$(c, d) = 1$, так как НОД$(u, v) = 1$. По предположению индукции утверждение выполнено для k, а значит, число $c \mp d\sqrt{-3}$ представимо в указанном виде. Так как $(a \pm b\sqrt{-3})(c \mp d\sqrt{-3}) = u + v\sqrt{-3}$, утверждение справедливо и для m. □

ЛЕММА 4.7. *Пусть* E — *множество всех троек* (u, v, s), *таких, что* s *нечетно,* НОД$(u, v) = 1$ *и* $s^3 = u^2 + 3v^2$, *и пусть* F — *множество всех пар* (t, w), *для которых* НОД$(t, w) = 1$, $3 \nmid u$, $t \not\equiv w$

(mod 2). *Тогда отображение* Φ: $F \longrightarrow E$, *определяемое соотношением* $\Phi(t, w) = (u, v, s)$, *где*

$$\begin{cases} u = t(t^2 - 9w^2), \\ v = 3w(t^2 - w^2), \\ s = t^2 + 3w^2, \end{cases}$$

является накрытием множества E.

Доказательство. Ясно, что $u^2 + 3v^2 = s^3$. Так как t и w имеют различную четность, s нечетно. Теперь покажем, что НОД$(u, v) = 1$. Действительно, заметим сначала, что НОД$(t^2 - 9w^2, t^2 - w^2) = 1$, потому что если простое число p делит $t^2 - 9w^2$ и $t^2 - w^2$, то оно делит $9t^2 - 9w^2$, а также $8t^2$, следовательно, $p = 2$ (p не может делить t, поскольку НОД$(t, w) = 1$). Но так как t и w имеют различную четность, это невозможно. Предположим теперь, что p — простое число, $e \geqslant 1$ и p^e делит u и v. Тогда $p \nmid (t^2 - w^2)$, а значит, $p \mid 3w$, так что $p \mid t$ в обоих случаях. Так как $p \mid v$ и $p \nmid w$, мы заключаем, что $p = 3$, а это невозможно. Таким образом, $\Phi(t, w) = (u, v, s) \in E$.

Проведем обратные рассуждения. Зададим тройку $(u, v, s) \in E$. Пусть $s^3 = \prod_{i=1}^{n} p_i^{e_i}$ есть разложение s^3 в произведение простых чисел ($p_1, \ldots, p_n$ различны, $e_i \geqslant 1$). Тогда $e_i = 3e_i'$ для всех i. Согласно лемме 4.6 существуют целые числа a_i, b_i $(i = 1, \ldots, n)$, такие, что $p_i = a_i^2 + 3b_i^2$ и

$$u + v\sqrt{-3} = \prod_{i=1}^{n} (a_i + b_i\sqrt{-3})^{e_i}.$$

Пусть $t, w \in \mathbb{Z}$ определяются из соотношения

$$\prod_{i=1}^{n} (a_i + b_i\sqrt{-3})^{e_i'} = t + w\sqrt{-3},$$

так что $u + v\sqrt{-3} = (t + w\sqrt{-3})^3$. Раскрыв скобки в правой части, получим $u = t(t^2 - 9w^2)$, $v = 3w(t^2 - w^2)$, следовательно, $3 \nmid t$. Наконец, домножив на сопряженное $u - v\sqrt{-3} = (t - w\sqrt{-3})^3$, получим, что $s^3 = u^2 + 3v^2 = (t^2 + 3w^2)^3$, поэтому $s = t^2 + 3w^2$. Отсюда следует, что числа t и w имеют различную четность, причем НОД$(t, w) = 1$, $\Phi(t, w) = (u, v, s)$. □

Итак, мы провели исчерпывающее доказательство утверждения (4A).

Теперь докажем результат, принадлежащий Кронекеру (1859) (см. также Врэнчеану (1956, 1960)).

(4B)

(1) *Следующие утверждения равносильны.*

(a) *Уравнение* $x^3+y^3+z^3=0$ *имеет лишь тривиальные решения в целых числах.*

(b) *Для любого отличного от нуля целого числа* m *уравнение* $4X^3-3mY^2=m^3$ *имеет в целых числах лишь решения* (m,m) *и* $(m,-m)$.

(2) *Все решения уравнения* $4U^3+27T^2=-1$ *в рациональных числах суть* $\left(-1,\frac{1}{3}\right)$ *и* $\left(-1,-\frac{1}{3}\right)$.

(3) *Единственные многочлены третьей степени с рациональными коэффициентами, сумма корней которых равна* 0, *а дискриминант равен* $+1$, *— это многочлены* $X^3-X\pm\frac{1}{3}$.

(4) *Если дискриминант кубического многочлена с рациональными коэффициентами является шестой степенью отличного от нуля рационального числа, то его корни имеют вид* $r+s\sqrt{3}\sin(\pi/9)$, $r+s\sqrt{3}\sin(2\pi/9)$, $r-s\sqrt{3}\sin(4\pi/9)$.

Доказательство. (1) (a)⇒(b) Пусть x,y — целые числа и пара (x,y) удовлетворяет уравнению $4x^3-3my^2=m^3$. Положив $u=-2x$, $v=y+m$, получим, что $u^3+v^3=-8x^3+y^3+3y^2m+3ym^2+m^3=-2m^3-6my^2+y^3+3y^2m+3ym^2+y^3=(y-m)^3$. Таким образом, или $x=0$ (откуда $-3y^2=m^2$, что невозможно), или $y=\pm m$; в последнем случае $x=m$.

(b)⇒(a) Пусть x,y,z — произвольные целые числа. Положим $n=z-y$, $m=-(z+y)$. Тогда

$$x^3+y^3+z^3=x^3-\left(\frac{m+n}{2}\right)^3-\left(\frac{m-n}{2}\right)^3=\frac{1}{4}(4x^3-m^3-3mn^2).$$

Если $x^3+y^3+z^3=0$, то $4x^3-3mn^2=m^3$. Ясно, что при $m=0$ мы получим $x=0$. Если же $m\neq 0$, то по предположению пара (x,n) должна совпасть с (m,m) или с $(m,-m)$. В случае когда $x=m=n$, имеем $z=0$, а если $x=m=-n$, то $y=0$.

(2) Пусть рациональные числа u,t таковы, что $4u^3+27t^2=-1$. Положив $u=-x/m$, $t=y/(3m)$, получим $-4x^3+3my^2=-m^3$. Согласно (1) имеем $x=m$, $y=\pm m$, следовательно, $u=-1$, $t=\pm\frac{1}{3}$.

(3) Пусть многочлен X^3+aX+b имеет рациональные коэффициенты и его дискриминант $\delta=1$. Так как $\delta=-(4a^3+27b^2)$, согласно (2) получаем $a=-1$, $b=\pm\frac{1}{3}$.

(4) Пусть многочлен $f(X)=X^3+a_1X^2+a_2X+a_3$ имеет рациональные коэффициенты. Если $g(X)=f(X-a_1/3)$, то $g(X)$ и

$f(X)$ имеют один и тот же дискриминант, причем $g(X)$ имеет вид $g(X) = X^3 + uX + t$ и его коэффициенты рациональны.

Если дискриминант является шестой степенью отличного от нуля рационального числа, скажем, $-(4u^3+27t^2) = r^6$, то $4\,(u/2)^3 + 27\,(t/r^3)^2 = -1$. Следовательно, $u = -r^2$, $t = \pm r^3/3$, откуда получаем

$$g(X) = X^3 - r^2X \pm \frac{r^3}{3} = r^3\left[\left(\frac{X}{r}\right)^3 - \left(\frac{X}{r}\right) \pm \frac{1}{3}\right].$$

Корнями многочленов

$$X^3 - X \pm \frac{1}{3}$$

являются числа

$$\pm(2\sqrt{3}/3)\sin(\pi/9),\ \pm(2\sqrt{3}/3)\sin(2\pi/9),\ \mp(2\sqrt{3}/3)\sin(4\pi/9),$$

откуда следует, что корни многочлена $f(X)$ имеют указанный вид. □

В 1944 г. Шмид провел обратные рассуждения, установив эквивалентность следующих высказываний и получив теорему Ферма для показателя 3 как следствие утверждения (2); см. также Врэнчеану (1956, 1960, 1979), где этот результат содержится в явном виде.

(4C) *Следующие утверждения равносильны.*

(1) *Последняя теорема Ферма справедлива для показателя* 3.

(2) *Для любого целого числа* $m \neq 0$ *уравнение* $4X^3 - 3mY^2 = m^3$ *имеет в целых числах лишь решения* (m, m) *и* $(m, -m)$.

(3) *Все решения уравнения* $4U^3 + 27T^2 = -1$ *в рациональных числах суть* $\left(-1, \frac{1}{3}\right)$ *и* $\left(-1, -\frac{1}{3}\right)$.

Доказательство. При доказательстве утверждения (4B) мы показали, что из (1) следует (2) и из (2) следует (3). Теперь предположим, что выполнено утверждение (3), и покажем, что теорема Ферма справедлива для показателя 3.

Допустим противное. Пусть существуют отличные от нуля попарно взаимно простые целые числа x, y, z, такие, что $x^3 + y^3 = z^3$, откуда $y \neq z$. Положим $u = x/(y - z)$, $t = (y + z)/(3(y - z))$. Тогда, как легко видеть, $4u^3 + 27t^2 = -1$. Значит, по предположению $u = -1$, $t = \pm 1/3$, откуда следует, что $y - z = \pm(y + z)$. Но тогда $y = 0$ или $z = 0$, что противоречит выбору тройки x, y, z. □

Таблица 2. ПТФ для показателя 3

Автор	Год
Кауслер	1795/6, опубл. в 1802 г.
Лежандр	1823, 1830
Кальцолари	1855
Ламе	1865
Тейт	1872
Гюнтер	1878
Гамбиоли	1901
Крей	1909
Рыхлик	1910
Штокхаус	1910
Кармайкл	1915
ван дер Корпут	1915
Туэ	1917
Дуарте	1944

В 1885 г. Перрен доказал, что если уравнение $X^3 + Y^3 + Z^3 = 0$ имеет хотя бы одно нетривиальное решение в отличных от нуля взаимно простых целых числах, то найдется бесконечно много таких решений, получаемых из предполагаемого с помощью рациональных операций. Разумеется, сейчас это утверждение не представляет никакого интереса, поскольку мы доказали, что такого нетривиального решения не существует.

В табл. 2 приведен список авторов, опубликовавших доказательство теоремы Ферма для показателя 3.

В заключение этого раздела применим метод бесконечного спуска для изучения уравнения, схожего с (4.1) (см. Лежандр, 1808, 1830).

(4D) *Если m — натуральное число, то уравнение*

$$X^3 + Y^3 = 2^m Z^3 \tag{4.3}$$

имеет нетривиальные примитивные решения в целых числах, для которых z нечетно, тогда и только тогда, когда $m = 3s + 1$, причем решениями являются тройки $(\pm 2^s, \pm 2^s, \pm 1)$.

Доказательство. Предположим, что отличные от нуля целые числа x, y, z таковы, что НОД$(x, y, z) = 1$, z нечетно и $x^3 + y^3 = 2^m z^3$. Заметим сначала, что $3 \nmid m$, иначе мы могли бы записать

$m = 3m'$ и тройка $(x, y, 2^{m'}z)$ являлась бы нетривиальным решением уравнения $X^3+Y^3 = Z^3$, что противоречит (4A). Далее отметим, что числа x и y имеют одну и ту же четность, поскольку $m \geqslant 1$. Для начала будем полагать, что оба они нечетны, следовательно, НОД$(x, y) = 1$. Итак, мы имеем

$$2^m z^3 = x^3 + y^3 = (x + y)(x^2 - xy + y^2),$$

где НОД$(x + y,\ x^2 - xy + y^2) = 1$ или 3. Действительно, если число p простое, $e \geqslant 1$ и p^e делит $x+y$ и $x^2 - xy + y^2$, то $x \equiv -y \pmod{p^e}$, а значит, $x^2 - xy + y^2 \equiv 3x^2 \pmod{p^e}$. Таким образом, $p^e \mid 3x^2$, а так как НОД$(x, y) = 1$, мы получаем, что $p \nmid x$, следовательно, $p^e \mid 3$, то есть $p^e = 3$, что и доказывает наше утверждение.

Более того, поскольку $x^2 - xy + y^2 = (x + y)^2 - 3xy$, условие $3 \mid (x + y)$ равносильно тому, что $3 \mid (x^2 - xy + yz)$, что, в свою очередь, эквивалентно условию $3 \mid z$, а это равносильно равенству НОД$(x + y,\ x^2 - xy + y^2) = 3$.

Рассмотрим два случая.

Случай 1: $3 \nmid z$.

Так как НОД$(x + y,\ x^2 - xy + y^2) = 1$ и число $x^2 - xy + y^2$ нечетно, существуют нечетные взаимно простые целые числа a и b, такие, что

$$\begin{cases} x + y = 2^m a^3, \\ x^2 - xy + y^2 = b^3, \end{cases}$$

причем $z = ab$. Поскольку $x+y$, $x-y$ четны, справедливо равенство

$$b^3 = \left(\frac{x+y}{2}\right)^2 + 3\left(\frac{x-y}{2}\right)^2.$$

Из леммы 4.6 следует, что существуют целые числа t, w, такие, что

$$\frac{x+y}{2} + \frac{x-y}{2}\sqrt{-3} = (t + w\sqrt{-3})^3$$

и

$$\begin{cases} (x + y)/2 = t(t^2 - 9w^2), \\ (x - y)/2 = 3w(t^2 - w^2), \end{cases}$$

$$b = t^2 + 3w^2.$$

Если $t = 0$ или $t^2 - 9w^2 = 0$, то $x = -y$, следовательно, $z = 0$, что противоречит предположению. Если $w = 0$ или $t^2 - w^2 = 0$, то $x = y$ и $2x^3 = 2^m z^3$, так что $m = 1$, $x = y = z = \pm 1$. Заметим, что $|t^2 - 9w^2| \neq 1$, иначе выполнялись бы равенства $t+3w = \pm 1$, $t-3w = \pm 1$, что, как легко видеть, невозможно.

Далее, $3 \not| t$, поскольку в противном случае $3 \mid b$, следовательно, $3 \mid z$, что противоречит предположению. Так как b нечетно, числа $t+3w$ и $t-3w$ также нечетны. Следовательно, t, $t+3w$, $t-3w$ — отличные от нуля попарно взаимно простые целые числа. Поскольку $2^{m-1}a^3 = t(t+3w)(t-3w)$, существуют отличные от нуля целые числа c, d, e, такие, что

$$\begin{cases} t &= 2^{m-1}c^3, \\ t+3w &= d^3, \\ t-3w &= e^3, \end{cases}$$

причем c, d, e нечетны, попарно взаимно просты и $a = cde$. Следовательно, $d^3 + e^3 = 2^m c^3$, а значит, тройка (d, e, c) является решением уравнения того же вида, что и рассматриваемое. Но $2^{m-1}|c|^3 = |t| < |t| \times |t^2 - 9w^2| = 2^{m-1}|a|^3$, а следовательно, $|c| < |a|$. Далее, $2^m|a|^3 = |x+y| \leqslant |x+y||x^2-xy+y^2| = |x^3+y^3| = 2^m|z|^3$, так что $|c| < |z|$. Так как $3 \not| c$, повторяя это рассуждение для решения (d, e, c), получим последовательность решений (d_1, e_1, c_1), (d_2, e_2, c_2), ..., где $|z| > |c_1| > |c_2| > \ldots$, причем все c_i — отличные от нуля целые числа, что невозможно.

Случай 2: $3 \mid z$.

Теперь НОД$(x+y,\, x^2-xy+y^2) = 3$. Заметим, что $3^2 \not| \left(x^2 - xy + y^2 = (x+y)^2 - 3xy\right)$ (иначе выполнялось бы условие $3 \mid xy$, значит, x и y были бы кратны 3, что противоречит предположению).

Таким образом, существуют нечетные взаимно простые целые числа a и b, такие, что

$$\begin{cases} x+y &= 2^m \times 3^2 a^3, \\ x^2 - xy + y^2 &= 3b^3, \end{cases}$$

причем $3 \not| b$ и $z = 3ab$. Так как $x+y$, $x-y$ четны и $3 \mid (x+y)$, мы получаем $3b^3 = \left((x+y)/2\right)^2 + 3\left((x-y)/2\right)^2$, поэтому $b^3 = \left((x-y)/2\right)^2 + 3\left((x+y)/6\right)^2$. Из леммы 4.6 следует, что существуют целые числа t, w, такие, что

$$\frac{x-y}{2} + \frac{x+y}{6}\sqrt{-3} = (t + w\sqrt{-3})^3$$

и

$$\begin{cases} (x-y)/2 &= t(t^2 - 9w^2), \\ (x+y)/6 &= 3w(t^2 - w^2), \\ b &= t^2 + 3w^2. \end{cases}$$

Если $t = 0$ или $t^2 - 9w^2 = 0$, то $x = y = z = \pm 1$, причем $m = 1$. Если $w = 0$ или $t^2 - w^2 = 0$, то $x = -y$, так что $z = 0$. Это противоречит предположению. Отсюда следует, что $|t^2 - w^2| \neq 1$, так как в противном случае выполнялись бы равенства $t + w = \pm 1$. $t - w = \pm 1$, что, как легко видеть, невозможно.

Так как b нечетно, числа $t+3w$, $t-3w$, а значит, и $t+w$, $t-w$ также нечетны. Следовательно, w, $t-w$, $t+w$ — отличные от нуля попарно взаимно простые целые числа. Поскольку $2^{m-1}a^3 = (x+y)/18 = w(t-w)(t+w)$, существуют такие отличные от нуля целые числа c, d, e, что

$$\begin{cases} w = 2^{m-1}, \\ t + w = d^3, \\ t - w = e^3, \end{cases}$$

причем c, d, e нечетны и попарно взаимно просты и $a = cde$. Таким образом, $d^3 - e^3 = 2^m c^3$, а значит, тройка $(d, -e, c)$ является решением уравнения того же вида, что и данное.

Но $2^{m-1}|c|^3 = |w| < |w||t^2 - w^2| = |x+y|/18 = 2^{m-1}|a|^3$, а значит, $|c| < |a|$. Далее,

$$\begin{aligned} 2^m 3^2 |a|^3 &= |x+y| \\ &\leqslant \frac{|x+y||x^2 - xy + y^2|}{3} \\ &= \frac{|x^3 + y^3|}{3} \\ &= \frac{2^m |z|^3}{3}, \end{aligned}$$

следовательно, $|c| < |a| \leqslant |z|/3$.

В зависимости от того, делится c на 3 или нет, мы повторяем эти рассуждения, следуя первому или второму случаю, и получаем последовательность решений (d_1, e_1, c_1), (d_2, e_2, c_2), ..., где $|z| > |c_1| > |c_2| > \ldots$, причем все c_i — отличные от нуля целые числа, что невозможно.

Пусть теперь числа x, y четны, причем натуральное число s таково, что 2^s есть наибольшая степень числа 2, делящая оба эти числа. Число z нечетно, значит, $3s \leqslant m$, а следовательно, $3s < m$. Положив $x = 2^s x', y = 2^s y'$, получим $x'^3 + y'^3 = 2^{m-3s} z^3$. Хотя бы одно из чисел x', y' нечетно, а так как они имеют одинаковую четность, они оба нечетны. Значит, согласно первой части доказательства $x' = y' = z' = \pm 1$, причем $m - 3s = 1$. Таким образом.

решениями исходного уравнения являются тройки $(\pm 2^s, \pm 2^s, \pm 1)$, а $m = 3s + 1$. □

В дальнейшем теория уравнений вида $X^3 + Y^3 = AZ^3$ получила свое развитие в работах Лежандра (1808, 1830), Пепена (1870, 1875, 1881), Люка (1878, 1880), Сильвестра (1856, 1879) и Гурвица (1917), доказавшего неразрешимость этого уравнения в целых числах для многих значений величины A, но это выходит за рамки нашей книги. Еще одна интересная статья о тернарных кубических диофантовых уравнениях принадлежит Морделлу (1956) (см. также Морделл (1969)).

Список литературы

1657 Fermat, P., Lettre à Digby (15 Août, 1657). *Oeuvres*, Vol. II, pp. 342–346. Publiées par les soins de MM. Paul Tannery et Charles Henry. Gauthier-Villars, Paris, 1894.

1760 Euler, L., *Supplementum quorundam theorematum arithmeticorum quae in non nullis demonstrationibus supponuntur.* Novi Comm. Acad. Sci. Petrop., **8** (1760/1), 1763, 105–128. Also in *Opera Omnia*, Ser. I, Vol. II, pp. 556–575. Teubner, Leipzig, 1915.

1770 Euler, L., *Vollständige Anleitung zur Algebra*, 2 volumes. Royal Acad. Sci., St. Petersburg, 1770. English translation by Rev. J. Hewlitt, Longman, Hurst, Rees, Orme, London, 1822. Also in *Opera Omnia*, Ser. I, Vol. I, pp. 486–490. Teubner, Leipzig, 1911.

1802 Kausler, C.F., *Nova demonstratio theorematis nec summam, nec differentiam duorum cuborum cubum esse posse*, Novi Acta Acad. Petrop., **13** (1795/6), 1802, 245–253.

1808 Legendre, A.M., *Essai sur la Théorie des Nombres* (2^e édition), Courcier, Paris, 1808.

1823 Legendre, A.M., *Recherches sur quelques objets d'analyse indéterminée, et particulièrement sur le théorème de Fermat.* Mém. Acad. Roy. Sci. Institut France, **6** (1823), 1–60. Reprinted as the "Second Supplément" in 1825, to a printing of *Essai sur la Théorie des Nombres* (2^e édition), Courcier, Paris; reprinted in Sphinx-Oedipe, **4** (1909), 97–128.

1830 Legendre, A.M., *Théorie des Nombres* (3^e édition), Vol. II, pp. 357–360, Firmin Didot Frères, Paris, 1830; reprinted by A. Blanchard, Paris, 1955.

1855 Calzolari, L., *Tentativo per dimostrare il teorema di Fermat sull'-equazione indeterminata* $x^n + y^n = z^n$, Ferrara, 1855.

1856 Sylvester, J.J., *Recherches sur les solutions en nombres entiers positifs ou négatifs de l'équation cubique homogène à trois variables*, Ann. Sci. Mat. Fis., B. Tortolini, **7** (1856), 398–400; reprinted in *Collected Math. Papers*, Vol. II, pp. 63–64, Cambridge University Press, Cambridge, 1908; reprinted by Chelsea, New York, 1976.

1859 Kronecker, L., *Über cubische Gleichungen mit rationalen Coefficienten*, J. Reine Angew. Math., **56** (1859), 188–189; also in *Werke*, Vol. I, pp. 121–122, Teubner, Leipzig, 1895.

1865 Lamé, G., *Étude des binômes cubiques* $x^3 \mp y^3$, C. R. Acad. Sci. Paris, **61** (1865), 921–924 and 961–965.

1870 Pepin, T., *Sur la décomposition d'un nombre entier en une somme de deux cubes rationnels*, J. Math. Pures Appl., (2), **15** (1870), 217–236.

1870 Tait, P.G., *Mathematical Notes*, Proc. Roy. Soc. Edinburgh, **7** (1872), 144.

1875 Pepin, T., *Sur certains nombres complexes compris dans la formule* $a + b\sqrt{-c}$, J. Math. Pures Appl. (3), **1** (1875), 317–372.

1878 Günther, S., *Über die unbestimmte Gleichung* $x^3 + y^3 = z^3$, Sitzungsber. Böhm Ges. Wiss., 1878, pp. 112–120.

1879 Lucas, E., *Sur l'équation indéterminée* $X^3 + Y^3 = AZ^3$, Nouv. Ann. Math., (2), **17** (1879), 425–426.

1879 Sylvester, J.J., *On certain ternary cubic form equations*, Amer. J. Math., **2** (1879), 280–285 and 357–393; also in *Collected Math. Papers*, Vol. III, 1909, Art. 39, pp. 312–391, Cambridge University Press, Cambridge, 1909; reprinted by Chelsea, New York, 1976.

1880 Lucas, E., *Théorèmes généraux sur l'impossibilité des équations cubiques indéterminées*, Bull. Soc. Math. France, **8** (1880), 173–182.

1880 Sylvester, J.J., *Sur les diviseurs des fonctions cyclotomiques*, C. R. Acad. Sci. Paris, **90** (1880), 287–289 and 345–347; also in *Collected Math. Papers*, Vol. III, 1909, Art. 44, pp. 428–432 and also p. 437; reprinted by Chelsea, New York, 1976.

1881 Pepin, T., *Mémoire sur l'équation indéterminée* $x^3 + y^3 = Az^3$, Atti Accad. Naz. Lincei, **34** (1881), 78–130.

1885 Perrin, R., *Sur l'équation indéterminée* $x^3 + y^3 = z^3$, Bull. Soc. Math. France, **13** (1885), 194–197.

1894 Schumacher, J., *Nachtrag zu Nr. 1077, XXIII, 269*, Z. Math. Naturwiss. Unterricht, **25** (1894), 350–351.

1898 Palmström, A., *Équation* $x^3+y^3=z^3$, L'Interm. Math., **5** (1898), 95.

1901 Gambioli, D., *Memoria bibliografica sull'ultimo teorema di Fermat*, Period. Mat., (2), **16** (1901), 145–192.

1901 Landau, E., *Sur une démonstration d'Euler d'un théorème de Fermat*, L'Interm. Mat., **8** (1901), 145–147.

1906 Holden, H., *On the complete solution in integers for certain values of* p, *of* $a(a^2+pb^2)=c(c^2+pd^2)$, Messenger Math., **36** (1906), 189–192.

1907 Sommer, J., *Vorlesungen über Zahlentheorie*, Teubner, Leipzig, 1907.

1909 Krey, H., *Neuer Beweis eines arithmetischen Satzes*, Math. Naturwiss. Blätter, **6** (1909), 179–180.

1910 Rychlik, K., *On Fermat's last theorem for* $n=4$ *and* $n=3$ (in Bohemian), Časopis Pěst. Mat., **39** (1910), 65–86.

1910 Stockhaus, H., *Beitrag zum Beweis des Fermatschen Satzes*, Brandstetter, Leipzig, 1910, 90 pp.

1910 Welsch, *Réponse à une question de E. Dubouis*, L'Interm. Math., **17** (1910), 179–180.

1915 Carmichael, R.D., *Diophantine Analysis*, Wiley, New York, 1915.

1915 van der Corput, J.G., *Quelques formes quadratiques et quelques équations indéterminées*, Nieuw Archief Wisk., **11** (1915), 45–47.

1917 Hurwitz, A., *Über ternäre diophantische Gleichungen dritten Grades*, Vierteljahrschrift Natur. Gesells. Zürich, **62** (1917), 207–209; reprinted in *Math. Werke*, Vol. II, pp. 446–468, Birkhäuser, Basel, 1933.

1917 Thue, A., *Et bevis for at ligningen* $A^3+B^3=C^3$ *er umulig i hele fra nul forskjellige tal* A, B *og* C, Arch. Mat. Naturv., **34** (1917), no. 15, 5 pp.; reprinted in *Selected Mathematical Papers*, pp. 555–559, Universitetsforlaget, Oslo, 1977.

1929 Nagell, T., *L'Analyse Indéterminée de Degré Supérieur*, Mémoires des Sciences Math., Vol. 39, Gauthier-Villars, Paris, 1929.

1931 Hancock, H., *Foundations of the Theory of Algebraic Numbers*, Vol. I, Macmillan, New York, 1931.

1936 Nagell, T., *Bemerkungen über die Diophantische Gleichung* $x^3+y^3=Az^3$, Arkiv Mat. Astr. Fysik, **25B** (1936), no. 5, 6 pp.

1944 Duarte, F.J., *Sobre la ecuación* $x^3+y^3+z^3=0$, Bol. Acad. Ciencias Fis. Mat. Naturales. Caracas. **8** (1944), 971–979.

1944 Schmid, F., *Über die Gleichung* $x^3 + y^3 + z^3 = 0$, Sitzungsber. Akad. Wiss., Wien, IIa, **152** (1944), 7–14.

1955 Pizá, P.A., *On the case* $n = 3$ *of Fermat's last theorem*, Math. Mag., **28** (1955), 157–158.

1956 Mordell, L.J., *The diophantine equation* $x^3 + y^3 + z^3 + kxyz = 0$, Colloque sur la Théorie des Nombres, Bruxelles, 1955, Centre Belge Rech. Math., 1956, pp. 67–76.

1956 Vrănceanu, G., *Asupra unei teoreme echivalenti cu teorema lui Fermat* (On a theorem equivalent to Fermat's theorem), Gaz. Mat. Fiz. Bucuresti Ser. **A**, **8** (61) (1956), 23–24; reprinted in *Opera Matematică*, Vol. III, pp. 97–98, Edit. Acad. Rep. Soc. Romania, Bucureşti, 1973.

1956 Yf, P., *Comment on Pedro Pizá's "On the case* $n = 3$ *of Fermat's last theorem,"* Math. Mag., **29** (1956), 205–206.

1960 Vrănceanu, G., *Observatii asupra unei note precedente* (Remarks on a preceding note), Gaz. Mat. Fiz. (Bucureşti), Ser. **A**, **12** (1960), 1–2; reprinted in *Opera Matmatică*, Vol. III, pp. 463–464, Edit. Acad. Rep. Soc. Romania, Bucureşti, 1973.

1964 Sierpiński, W., *Elementary Theory of Numbers.*, Monografie Matematyczne, no. 42, 1964, Polska Akad. Nauk, Warszawa, 1964.

1966 Bergmann, G., *Über Eulers Beweis des großen Fermatschen Satzes für den Exponenten* 3, Math. Ann., **164** (1966), 159–175.

1966 Grosswald, E., *Topics from the Theory of Numbers*, Macmillan, New York, 1966.

1969 Mordell, L.J., *Diophantine Equations.* Academic Press, New York, 1969.

1972 Legendre, R., *Sur la résolution par Euler de l'équation de Fermat pour l'exposant* 3, C. R. Acad. Sci. Paris, **275** (1972), 413–414.

1977 Edwards, H.M., *"Fermat's Last Theorem". A Genetic Introduction to Algebraic Number Theory*, Springer-Verlag, New York, 1977.

1979 Vrănceanu, G., *Une interprétation géométrique du théorème de Fermat*, Rev. Roumaine Math. Pures Appl., **24** (1979), 1137–1140.

I.5. Поле Эйзенштейна

В этом разделе мы введем понятие поля Эйзенштейна и приведем доказательство Манна и Вебба последней теоремы Ферма для показателя 3, в котором используются лишь очень простые свойства

поля Эйзенштейна. Затем будет приведено доказательство Гаусса того факта, что кубическое уравнение Ферма имеет лишь тривиальные решения в поле Эйзенштейна.

Множество комплексных чисел вида $a + b\sqrt{-3}$, где a и b — рациональные числа, образует поле, называемое *полем Эйзенштейна* и обозначаемое через $K = \mathbb{Q}(\sqrt{-3})$. Числа $\alpha = (a + b\sqrt{-3})/2$, где a и b — обычные целые числа одинаковой четности, называются *целыми* в K. Они составляют кольцо, обозначаемое через A. Пусть $\alpha, \beta \in K$. Будем говорить, что β *делит* α, если найдется такое целое число $\gamma \in A$, что $\alpha = \beta\gamma$. В таком случае будем писать $\beta \mid \alpha$. Два отличных от нуля целых числа α, β называются *ассоциированными*, если α делит β и β делит α. В этом случае будем писать $\alpha \sim \beta$. Целые числа, ассоциированные с 1, называются *единицами* в K. Нетрудно показать, что они равны ± 1, $\pm\zeta$, $\pm\zeta^2$, где $\zeta = (-1 + \sqrt{-3})/2$, $\zeta^2 = (-1 - \sqrt{-3})/2$. Заметим, что $\zeta^3 = 1$, то есть ζ является примитивным корнем третьей степени из 1, причем $1 + \zeta + \zeta^2 = 0$. Отличное от нуля целое число $\alpha \in A$ называется *простым*, если оно не является единицей и все целые числа, делящие α, суть единицы или ассоциированные с α.

В рассматриваемом поле $\mathbb{Q}(\sqrt{-3})$ каждое отличное от нуля целое число α можно представить в виде произведения простых целых чисел: $\alpha = \gamma_1\gamma_2 \ldots \gamma_s$. Это разложение единственно в следующем смысле: если существует еще одно представление $\alpha = \delta_1\delta_2 \ldots \delta_t$, где все δ_i — простые числа поля K, то $s = t$ и можно так переставить сомножители (если требуется), чтобы γ_i и δ_i были ассоциированными для всех $i = 1, \ldots, s$. Следовательно, можно очевидным образом определить понятие наибольшего общего делителя отличных от нуля целых чисел из A, который будет единственным с точностью до умножения на единицу из A.

Доказательство следующих свойств можно найти в любом стандартном курсе, посвященном алгебраическим числам, например в книге Рибенбойма (1999).

Сопряженным с числом $\alpha = (a + b\sqrt{-3})/2$ называется число $\alpha' = (a - b\sqrt{-3})/2$. *Норма* числа α есть $N(\alpha) = \alpha\alpha' = (a^2 + 3b^2)/4$.

Пусть $\alpha \in A$. Тогда $A\alpha = \{\beta\alpha \mid \beta \in A\}$ является идеалом, состоящим из чисел, кратных α. Пусть $\alpha, \beta, \gamma \in A$, $\alpha \neq 0$. Если α делит $\beta - \gamma$, то будем писать

$$\beta \equiv \gamma \pmod{\alpha}$$

и говорить, что β и γ *сравнимы по модулю* α. Это отношение экви-

валентности на кольце A. Множество классов эквивалентности обозначается через $A/A\alpha$; класс эквивалентности, содержащий β, обозначается через $\overline{\beta}$ и называется *классом вычетов для* β. Определим сложение и умножение классов вычетов: $\overline{\beta}+\overline{\gamma}=\overline{\beta+\gamma}$, $\overline{\beta}\cdot\overline{\gamma}=\overline{\beta\gamma}$. Тогда $A/A\alpha$ будет кольцом, называемым *кольцом вычетов кольца* A *по модулю* α. Кольцо вычетов $A/A\alpha$ конечно, и число его элементов равно $|N(\alpha)|$.

Опишем теперь разложение простых чисел p в произведение простых элементов кольца A.

(1) Элемент $p=3$ разветвлен, то есть $3=(-\zeta^2)\lambda^2$, откуда $3\sim$ $\sim\lambda^2$, где $\lambda=1-\zeta=(3-\sqrt{-3})/2$ — простой элемент в A. В кольце A существует три класса вычетов по модулю λ; множество $\{0,1,-1\}$ является системой представителей поля $A/A\lambda$. Норма числа λ равна $N(\lambda)=\lambda\lambda'=(1-\zeta)(1-\zeta^2)=1-\zeta-\zeta^2+1=3$, так как $1+\zeta+\zeta^2=0$.

(2) Элемент $p=2$ инертен, то есть число 2 простое в A. В кольце A существует четыре класса вычетов по модулю 2, то есть поле $A/A2$ состоит из четырех элементов. Норма числа 2 равна $N(2)=4$.

(3) Если $p\equiv 1 \pmod 3$, то $p\sim\lambda_1\lambda_2$, где λ_1,λ_2 — простые элементы кольца A, не являющиеся ассоциированными ($\lambda_1\not\sim\lambda_2$). В таком случае говорят, что p разлагается (или расщепляется). В этом случае A/Ap состоит из p^2 элементов и является прямым произведением двух экземпляров поля $\mathbb{F}_p$, состоящего из p элементов, причем

$$N(\lambda_1)=N(\lambda_2)=p.$$

(4) Если $p\equiv -1 \pmod 3$, то p — простой элемент, то есть p инертен. Тогда поле A/Ap состоит из p^2 элементов и $N(p)=p^2$.

Теперь мы готовы представить доказательство последней теоремы Ферма для показателя 3, принадлежащее Манну и Веббу (1978). В нем используются такие факты, как единственность разложения на простые множители, ассоциированность и простота элементов $1-\zeta$ и $1-\zeta^2$, равенство $(1-\zeta)(1-\zeta^2)=3$ и тот факт, что единицами в K являются лишь ±1, $\pm\zeta$, $\pm\zeta^2$.

Предположим, что существует такая тройка ненулевых целых чисел (x,y,z), что $x^3+y^3+z^3=0$. Из всех таких троек выберем ту, для которой выражение $|xyz|$ минимально. Если $d=\text{НОД}\,(x,y,z)$, то тройка чисел $(x/d,y/d,z/d)$ также удовлетворяет рассматриваемому уравнению. Но поскольку значение $|xyz|$ является наимень-

шим из возможных, $d = 1$. Таким образом, числа x, y, z попарно взаимно просты.

Рассмотрим два случая.

Случай 1: $3 \nmid xyz$.

Заметим, что если $3 \nmid a$, то $a^3 \equiv \pm 1 \pmod 9$, так что $x^3+y^3+z^3 \not\equiv \not\equiv 0 \pmod 9$ и выражение $x^3 + y^3 + z^3$ не может быть равно нулю. Значит, этот случай невозможен.

Случай 2: $3 \mid xyz$.

Пусть, скажем, $3 \mid z$. Тогда $3 \nmid xy$. Если $x \equiv y \pmod 3$, то $x^3 \equiv y^3 \pmod 3$ и $x^3 + y^3 + z^3 \equiv \pm 1 \pmod 3$, что невозможно, поскольку $x^3+y^3+z^3 = 0$. Итак, $x \not\equiv y \pmod 3$ и, скажем, $x \equiv 1 \pmod 3$, $y \equiv 2 \pmod 3$. Следовательно, $x^2-xy+y^2 \equiv 0 \pmod 3$, но $x^2-xy+y^2 \not\equiv 0 \pmod 9$. В силу сказанного выше $\text{НОД}(x + y, x^2 - xy + y^2) = 3$, а поскольку $-z^3 = x^3 + y^3 = (x+y)(x^2 - xy + y^2)$, мы заключаем, что z^3 делится на 27, так что $x + y$ кратно 9. Разделив на 27, получим

$$\left(-\frac{z}{3}\right)^3 = \frac{x+y}{9} \cdot \frac{x^2 - xy + y^2}{3}.$$

Положим $x + y = 9t^2$, $(x + \zeta y)(x + \zeta^2 y) = x^2 - xy + y^2 = 3u^3$. Тогда число u не кратно 3. Покажем, что $\text{НОД}(x + \zeta y, x + \zeta^2 y) = 1 - \zeta$. В самом деле, если простой элемент θ делит $x + \zeta y$ и $x + \zeta^2 y$, то он делит также и $(1 - \zeta)x = -\zeta(x + \zeta y) + (x + \zeta^2 y)$ и аналогично делит $(1 - \zeta)y$. А так как $\text{НОД}(x, y) = 1$, мы заключаем, что θ делит $1 - \zeta$. Таким образом, элементы

$$\frac{x + \zeta y}{1 - \zeta} \quad \text{и} \quad \frac{x + \zeta^2 y}{1 - \zeta^2}$$

взаимно просты, потому что $1 - \zeta \sim 1 - \zeta^2$.

Итак, из равенства

$$u^3 = \frac{x + \zeta y}{1 - \zeta} \cdot \frac{x + \zeta^2 y}{1 - \zeta^2}$$

следует, что $x+\zeta y = (1-\zeta)(a+b\zeta)^3\eta$, где η — единица в K. Покажем, что $\eta = 1$. Мы можем записать

$$\eta(a+b\zeta)^3 = \frac{x + \zeta y}{1 - \zeta} = \frac{(x + \zeta y)(1 - \zeta^2)}{3} = \frac{2x - y}{3} + \frac{x + y}{3}\zeta = d + 3t^3\zeta.$$

Справедливо сравнение $\eta(a^3 + b^3) \equiv d \pmod 3$. Число 3 не делит $a + b\zeta$, значит, d не кратно 3. Если $\eta \neq \pm 1$, то $\eta = \pm\zeta$ или $\pm\zeta^2 = \pm(1 + \zeta)$, так что $d - \eta(a^3 + b^3) = d \mp (a^3 + b^3)\zeta$ и соответственно $d \pm (a^3 + b^3)(1 + \zeta) = [d \pm (a^3 + b^3)] \pm (a^3 + b^3)\zeta$. Так

как $3 \mid d \mp \eta(a^3 + b^3)$, во всех случаях $3 \mid d$, что невозможно. Значит, $\eta = \pm 1$, следовательно, $x + \zeta y = \pm(1-\zeta)(a+b\zeta)^3$. Раскрывая скобки и учитывая равенство $1 + \zeta + \zeta^2 = 0$, получим

$$x + \zeta y = \pm(a^3 + 3a^2b - 6ab^2 + b^3) \pm \zeta(-a^3 + 6a^2b - 3ab^2 - b^3).$$

Отсюда $9t^3 = x + y = \pm(9a^2b - 9ab^2)$, так что $t^3 = \pm ab(a-b)$. Но НОД$(a, b) = 1$, поскольку НОД$(x, y) = 1$. Значит, и НОД$(a-b, a) =$ $=$ НОД$(a - b, b) = 1$. Таким образом, положив $a = -x_1^3$, $b = y_1^3$ и $a - b = z_1^3$, получим, что $x_1^3 + y_1^3 + z_1^3 = 0$.

Но, как установлено ранее, $|x_1 y_1 z_1| < |xyz|$. Это противоречит выбору тройки (x, y, z) и завершает доказательство.

Теперь докажем теорему Гаусса. В доказательстве мы не будем использовать факты (2), (3) и (4).

Нам потребуется следующее точное сравнение.

Лемма 5.1. *Пусть $\alpha \in A$ и λ не делит α. Тогда $\alpha^3 \equiv \pm 1 \pmod{\lambda^4}$.*

Доказательство. Так как $\alpha \not\equiv 0 \pmod{\lambda}$, можно сделать вывод, что $\alpha \equiv \pm 1 \pmod{\lambda}$. Сначала предположим, что $\alpha \equiv 1 \pmod{\lambda}$, т. е. $\alpha - 1 = \beta\lambda$, где $\beta \in A$. Тогда $\alpha - \zeta = (\alpha - 1) + (1 - \zeta) = \beta\lambda + \lambda =$ $= \lambda(\beta + 1)$, $\alpha - \zeta^2 = (\alpha - \zeta) + (\zeta - \zeta^2) = \lambda(\beta + 1) + \zeta\lambda = \lambda(\beta - \zeta^2)$. Следовательно, $\alpha^3 - 1 = (\alpha - 1)(\alpha - \zeta)(\alpha - \zeta^2) = \lambda^3\beta(\beta + 1)(\beta - \zeta^2)$. Но $1 - \zeta^2 = (1 + \zeta)\lambda$, или $\zeta^2 \equiv 1 \pmod{\lambda}$. Отсюда заключаем, что элементы β, $\beta + 1$, $\beta - \zeta^2$ принадлежат трем различным классам по модулю λ, а значит, один из них кратен λ. Таким образом, $\alpha^3 \equiv 1 \pmod{\lambda^4}$. Если $\alpha \equiv -1 \pmod{\lambda}$, то $-\alpha^3 = (-\alpha)^3 \equiv 1 \pmod{\lambda^4}$, значит, $\alpha^3 \equiv -1 \pmod{\lambda^4}$. □

Следующий результат Гаусса позволяет получить утверждение (4A).

(5A) *Уравнение*

$$X^3 + Y^3 + Z^3 = 0 \tag{5.1}$$

не имеет решений в алгебраических целых числах, принадлежащих полю $\mathbb{Q}(\sqrt{-3})$, каждое из которых отлично от 0.

Доказательство. Предположим, что элементы $\xi, \eta, \theta \in A$ отличны от нуля и удовлетворяют уравнению $\xi^3 + \eta^3 + \theta^3 = 0$. Если НОД$(\xi, \eta, \theta) = \delta$, то ξ/δ, η/δ, θ/δ удовлетворяют тому же уравнению, причем НОД $(\xi/\delta, \eta/\delta, \theta/\delta) = 1$. Таким образом, можно полагать, что НОД$(\xi, \eta, \theta) = 1$, а следовательно, ξ, η, θ попарно взаимно

просты. Значит, λ не может делить какие-либо два из элементов ξ, η, θ. Можно считать, например, что $\lambda \nmid \xi$, $\lambda \nmid \eta$.

Случай 1: Предположим, что $\lambda \nmid \theta$.

Тогда

$$\begin{cases} \xi^3 \equiv \pm 1 \pmod{\lambda^3}, \\ \eta^3 \equiv \pm 1 \pmod{\lambda^3}, \\ \theta^3 \equiv \pm 1 \pmod{\lambda^3}, \end{cases}$$

следовательно, $0 = \xi^3 + \eta^3 + \theta^3 \equiv \pm 1 \pm 1 \pm 1 \pmod{\lambda^3}$. Восемь вариантов расстановки знаков в правой части сравнения приводят к ± 1 или ± 3. Эти числа не сравнимы с 0 по модулю λ^3, так как ± 1 — единицы, а ± 3 ассоциированы с λ^2, поэтому не кратны λ^3.

Случай 2: Предположим, что $\lambda \mid \theta$.

Пусть $\theta = \lambda^m \psi$, $\psi \in A$, $m \geqslant 1$, причем λ не делит ψ. В сущности, нам требуется доказать следующее утверждение.

Пусть $n \geqslant 1$ и ε — единица в A. Тогда если существуют такие попарно взаимно простые элементы $\alpha, \beta, \gamma \in A$, не кратные λ, что $\alpha^3 + \beta^3 + \varepsilon\lambda^{3n}\gamma^3 = 0$, то

(a) $n \geqslant 2$;

(b) существуют единица ε_1 и такие попарно взаимно простые элементы $\alpha_1, \beta_1, \gamma_1 \in A$, не кратные λ, что $\alpha_1^3 + \beta_1^3 + \varepsilon_1\lambda^{3(n-1)}\gamma_1^3 = 0$.

Действительно, предположение выполняется при $n = m$, $\varepsilon = 1$, $\alpha = \xi$, $\beta = \eta$, $\gamma = \psi$. Применяя приведенное выше утверждение повторно, найдем единицу ε' и элементы $\alpha', \beta', \gamma' \in A$, не кратные λ, такие, что $\alpha'^3 + \beta'^3 + \varepsilon'\lambda^3\gamma'^3 = 0$, а это противоречит пункту (a).

Сначала покажем, что $n \geqslant 2$. В самом деле, $\lambda \nmid \alpha$ и $\lambda \nmid \beta$. Тогда согласно лемме 5.1 мы имеем $\alpha^3 \equiv \pm 1 \pmod{\lambda^4}$, $\beta^3 \equiv \pm 1 \pmod{\lambda^4}$ и $\pm 1 \pm 1 \equiv -\varepsilon\lambda^{3n}\gamma^3 \pmod{\lambda^4}$, $\lambda \nmid \gamma$. Так как $\lambda \nmid \pm 2$, левая часть равенства должна быть равна 0. Поскольку $\lambda \nmid \gamma$, мы заключаем, что $3n \geqslant 4$, так что $n \geqslant 2$.

Теперь докажем (b). Справедливо соотношение

$$-\varepsilon\lambda^{3n}\gamma^3 = \alpha^3 + \beta^3 = (\alpha + \beta)(\alpha + \zeta\beta)(\alpha + \zeta^2\beta). \qquad (5.2)$$

Так как простой элемент λ делит правую часть, он должен делить хотя бы один из сомножителей в левой части. Но $\alpha + \beta \equiv \alpha + \zeta\beta \equiv \alpha + \zeta^2\beta \pmod{\lambda}$, потому что $\lambda = 1 - \zeta$, $1 - \zeta^2 = -\zeta^2\lambda$, а значит, λ делит все три множителя. Следовательно, $(\alpha + \beta)/\lambda$, $(\alpha + \zeta\beta)/\lambda$, $(\alpha + \zeta^2\beta)/\lambda \in A$ и

$$-\varepsilon\lambda^{3(n-1)}\gamma^3 = \left(\frac{\alpha + \beta}{\lambda}\right)\left(\frac{\alpha + \zeta\beta}{\lambda}\right)\left(\frac{\alpha + \zeta^2\beta}{\lambda}\right).$$

Так как $n \geqslant 2$, элемент λ делит правую часть, а значит, и хотя бы один из сомножителей в левой части. Но λ не может делить два множителя, иначе среди чисел $\alpha+\beta$, $\alpha+\zeta\beta$, $\alpha+\zeta^2\beta$ найдутся два элемента, сравнимые по модулю λ^2, а это невозможно. Действительно, если $(\alpha+\beta)-(\alpha+\zeta\beta)=\beta(1-\zeta)=\beta\lambda\equiv 0 \pmod{\lambda^2}$, то $\lambda \mid \beta$, что противоречит предположению; если $(\alpha+\beta)-(\alpha+\zeta^2\beta)=$ $=\beta(1-\zeta^2)=-\beta\zeta^2\lambda\equiv 0 \pmod{\lambda^2}$, то мы снова получаем $\lambda \mid \beta$: наконец, из соотношений $(\alpha+\zeta\beta)-(\alpha+\zeta^2\beta)=\zeta\beta(1-\zeta)=\zeta\beta\lambda\equiv 0 \pmod{\lambda^2}$ также следует, что $\lambda \mid \beta$.

Предположим, что λ делит $(\alpha+\beta)/\lambda$ (остальные случаи сводятся к этому заменой β на $\zeta\beta$ или $\zeta^2\beta$). Тогда $\lambda^{3(n-1)}$ делит $(\alpha+\beta)/\lambda$. Следовательно,

$$\begin{cases} \alpha+\beta &= \lambda^{3n-2}\kappa_1, \\ \alpha+\zeta\beta &= \lambda\kappa_2, \\ \alpha+\zeta^2\beta &= \lambda\kappa_3, \end{cases} \tag{5.3}$$

где $\kappa_1, \kappa_2, \kappa_3 \in A$ и λ не делит κ_1, κ_2, κ_3. Перемножив равенства, получим

$$-\varepsilon\gamma^3 = \kappa_1\kappa_2\kappa_3. \tag{5.4}$$

Заметим, что элементы κ_1, κ_2, κ_3 попарно взаимно просты. В самом деле, если, например, $\delta \in A$ делит κ_1, κ_2, то δ делит и $(\alpha+\beta)-(\alpha+\zeta\beta)=\beta(1-\zeta)=\beta\lambda$ (если δ делит κ_1, κ_3 или κ_2, κ_3, то рассуждения аналогичны). Но λ не делит $\kappa_1, \kappa_2, \kappa_3$, а значит, элемент δ не является ассоциированным с λ. Следовательно, δ делит β, а значит, также и α, что невозможно.

Из единственности разложения на множители в кольце A и соотношения (5.4) следует, что элементы κ_1, κ_2, κ_3 являются ассоциированными с кубами, т. е. существуют единицы $\omega_i \in A$ и элементы $\mu_i \in A$, такие, что $\kappa_i = \omega_i\mu_i^3$ $(i=1,2,3)$. Тогда

$$\begin{cases} \alpha+\beta &= \lambda^{3n-2}\mu_1^3\omega_1, \\ \alpha+\zeta\beta &= \lambda\mu_2^3\omega_2, \\ \alpha+\zeta^2\beta &= \lambda\mu_3^3\omega_3. \end{cases} \tag{5.5}$$

Снова заметим, что μ_1, μ_2, μ_3 попарно взаимно просты, причем λ не делит μ_1, μ_2, μ_3. Таким образом,

$$\begin{aligned} 0 &= (\alpha+\beta)+\zeta(\alpha+\zeta\beta)+\zeta^2(\alpha+\zeta^2\beta) \\ &= \lambda^{3n-2}\mu_1^3\omega_1+\zeta\lambda\mu_2^3\omega_2+\zeta^2\lambda\mu_3^3\omega_3. \end{aligned}$$

следовательно,

$$\mu_2^3 + \tau\mu_3^3 + \tau'\lambda^{3(n-1)}\mu_1^3 = 0,$$

где τ, τ' — единицы, элементы μ_1, μ_2, $\mu_3 \in A$ отличны от нуля и НОД$(\mu_2, \mu_3) = 1$. Если $\tau = 1$, то утверждение (b) доказано. Если $\tau = -1$, то, заменив μ_3 на $-\mu_3$, снова получим (b). Нам осталось доказать, что единица τ не может быть равна $\pm\zeta$ или $\pm\zeta^2$. В самом деле, $\mu_2^3 + \tau\mu_3^3 \equiv 0 \pmod{\lambda^2}$ и, так как $\mu_2^3 \equiv \pm 1 \pmod{\lambda^4}$, $\mu_3^3 \equiv \pm 1 \pmod{\lambda^4}$, мы получаем $\mu_2^3 + \tau\mu_3^3 \equiv \pm 1 \pm \tau \equiv 0 \pmod{\lambda^2}$. Однако $\pm 1 \pm \zeta \not\equiv 0 \pmod{\lambda^2}$ и $\pm 1 \pm \zeta^2 \not\equiv 0 \pmod{\lambda^2}$, следовательно, $\tau \neq \neq \pm\zeta, \pm\zeta^2$, что и завершает доказательство утверждения (b) и, как уже отмечалось, всей теоремы. □

Приведем несколько результатов, схожих с (5A), которые можно доказать теми же методами. Эти утверждения можно приписать Эйлеру и Лежандру.

(5B) *Пусть p — простое число, $p \equiv 2$ или $5 \pmod 9$. Пусть, далее, ε — единица в K и существует элемент $x \in A$, такой, что $x^3 \equiv \varepsilon \pmod p$. Тогда $\varepsilon = \pm 1$.*

Доказательство. Предположим, что $\varepsilon = \pm\zeta$ или $\pm\zeta^2$ и существует элемент $x \in A$, такой, что $x^3 \equiv \varepsilon \pmod p$. Так как $p \equiv 2 \pmod 3$, мы заключаем, что p есть простой элемент в A, поле A/Ap состоит из p^2 элементов и $x^{p^2-1} \equiv 1 \pmod p$. Но $p^2 - 1 = (p+1)(p-1) = 3(r+1)(3r+1)$, причем $p = 3r + 2$. Следовательно,

$$\varepsilon^{r+1} \equiv \varepsilon^{(r+1)(3r+1)} \equiv x^{p^2-1} \equiv 1 \pmod p.$$

Если $r \equiv 0$ или $1 \pmod 3$, то p делит $1 \mp \zeta$ или $1 \mp \zeta^2$. Так как $1 - \zeta^2 = (1+\zeta)(1-\zeta)$ и $1 + \zeta = -\zeta^2$, $1 + \zeta^2 = -\zeta$ — единицы, p делит $1 - \zeta$. Отсюда следует, что $p = 3$, а это противоречит предположению. Следовательно, $r \equiv 2 \pmod 3$ и $p \equiv 8 \pmod 9$, что снова невозможно. □

Следуя Морделлу, докажем еще один классический результат.

(5C) *Пусть p — простое число, $p \equiv 2$ или $5 \pmod 9$ и ε — единица в $\mathbb{Q}(\zeta)$. Тогда уравнение*

$$X^3 + Y^3 + \varepsilon a Z^3 = 0, \tag{5.6}$$

где $a = p$ или p^2, $a \neq 2$, имеет лишь тривиальные решения (x, y, z) в $\mathbb{Q}(\zeta)$, а именно $z = 0$, $x \in \{-y, -\zeta y, -\zeta^2 y\}$. При $a = 2$ и $\varepsilon = 1$ существуют также решения $x^3 = y^3 = -z^3 = 1$, а при $\varepsilon = -1$ — решения $x^3 = y^3 = z^3 = \pm 1$.

Доказательство. Для начала заметим, что если тройка (x, y, z) является решением, причем $x = 0$ или $y = 0$, то непременно $z = 0$. Действительно, если каждый из элементов x, y равен 0, то и $z = 0$. Пусть, например, $x = 0$, а $y \neq 0$. Можно считать, что НОД$(y, z) = 1$. Тогда p делит y, следовательно, $p^3 \mid az^3$, а значит, $p \mid z$, что противоречит предположению.

Пусть теперь элементы $x, y, z \in A$ таковы, что $x^3 + y^3 + \varepsilon az^3 = 0$, причем $xyz \neq 0$. Можно также считать, что НОД$(x, y, z) = 1$. откуда следует, что x, y, z попарно взаимно просты.

Из всех возможных решений выберем то, для которого модуль нормы $|N(xyz)|$ наименьший. Заметим, что $x^3 + y^3 \neq 0$, так как $z \neq 0$. Отсюда следует, что x не совпадает ни с одним из элементов $-y, -\zeta y, -\zeta^2 y$.

Рассмотрим резольвенты Лагранжа:

$$\begin{cases} \alpha = x + y, \\ \beta = \zeta x + \zeta^2 y, \\ \gamma = \zeta^2 x + \zeta y. \end{cases}$$

Нетрудно видеть, что $\alpha, \beta, \gamma \in A$, $\alpha, \beta, \gamma = 0$ и

$$\begin{aligned} \alpha\beta\gamma &= \zeta^2(x^2 + \zeta y^2 + (1 + \zeta)xy)(\zeta x + y) \\ &= \zeta^2(\zeta x^3 + \zeta y^3 + (1 + \zeta + \zeta^2)x^2 y + (1 + \zeta + \zeta^2)xy^2) \\ &= x^3 + y^3 = -\varepsilon az^3. \end{aligned}$$

Пусть $\delta =$ НОД$(\alpha, \beta, \gamma) \in A$. Тогда НОД$(\alpha/\delta, \beta/\delta, \gamma/\delta) = 1$ и

$$\frac{\alpha}{\delta} \cdot \frac{\beta}{\delta} \cdot \frac{\gamma}{\delta} = -\varepsilon a \left(\frac{z}{\delta}\right)^3.$$

Следовательно, a делит в точности один из множителей в левой части, скажем, γ/δ (остальные случаи аналогичны). Согласно теореме единственности разложения на множители, справедливой для кольца A,

$$\begin{cases} \alpha/\delta = \varepsilon_1 \alpha_1^3, \\ \beta/\delta = \varepsilon_2 \beta_1^3, \\ \gamma/\delta = \varepsilon_3 a \gamma_1^3, \end{cases}$$

где $\varepsilon_1, \varepsilon_2, \varepsilon_3$ — единицы в A, причем $\alpha_1, \beta_1, \gamma_1 \in A$, $\alpha_1\beta_1\gamma_1 \neq 0$, НОД$(\alpha_1, \beta_1, \gamma_1) = 1$. Следовательно,

$$\varepsilon_1 \alpha_1^3 + \varepsilon_2 \beta_1^3 + \varepsilon_3 a \gamma_1^3 = 0.$$

Положим $\varepsilon' = \varepsilon_2/\varepsilon_1, \varepsilon'' = \varepsilon_3/\varepsilon_1$. Тогда

$$\alpha_1^3 + \varepsilon' \beta_1^3 + \varepsilon'' a \gamma_1^3 = 0. \tag{5.7}$$

Отметим, что $p \not| \beta_1$. В самом деле, если $p \mid \beta_1$, то $p \mid \alpha_1$, следовательно, $p^3 \mid a{\gamma_1}^3$, а значит, $p \mid \gamma_1$, что невозможно, так как НОД$(\alpha_1, \beta_1, \gamma_1) = 1$. Переходя в соотношении (5.7) к классам эквивалентности по модулю p, получим $\alpha_1^3 + \varepsilon'\beta_1^3 \equiv 0 \pmod{p}$, так что ε' есть куб по модулю p. Из утверждения (5B) следует, что $\varepsilon' = \pm 1$, поэтому

$$\alpha_1^3 + (\pm\beta_1)^3 + \varepsilon'' a\gamma_1^3 = 0,$$

а значит, $(\alpha_1, \pm\beta_1, \gamma_1)$ — еще одно нетривиальное решение уравнения (5.6), причем НОД$(\alpha_1, \pm\beta_1, \gamma_1) = 1$. По предположению

$$|N(xyz)|^3 \leqslant |N(\alpha_1\beta_1\gamma_1)|^3 = \left|N\left(\frac{\alpha\beta\gamma}{\delta^3 a}\right)\right| = \left|N\left(\frac{z}{\delta}\right)\right|^3,$$

так что $|N(\delta xy)| \leqslant 1$. Это значит, что x, y, δ являются единицами. Следовательно, $x^3 = \pm 1$, $y^3 = \pm 1$ и $\pm 1 \pm 1 + \varepsilon a z^3 = 0$.

Если $a \neq 2$, то $z = 0$, что противоречит предположению.

Если $a = 2$, то или $z = 0$, или $x^3 = y^3 \neq 0$, $x^3 + \varepsilon z^3 = 0$. Значит, ε есть куб по модулю p, а следовательно, согласно (5B) мы получаем, что $\varepsilon = \pm 1$. При $\varepsilon = +1$ решением является тройка $x^3 = y^3 = -z^3 = 1$, а при $\varepsilon = -1$ — тройка $x^3 = y^3 = z^3 = \pm 1$. □

В качестве прямого следствия имеем следующий результат.

(5D) *Уравнение*

$$X^3 + 4Y^3 = 1 \tag{5.8}$$

не имеет решений в отличных от нуля целых числах.

Доказательство. Рассмотрим уравнение

$$X^3 + T^3 + 4Y^3 = 0. \tag{5.9}$$

Если (x, y) — нетривиальное решение уравнения (5.8), то $(x, -1, y)$ — нетривиальное решение уравнения (5.9), что невозможно согласно результату (5C). □

Отметим еще несколько следствий.

(5E) *Уравнения*

$$X^6 - 27Y^6 = 2Z^3, \tag{5.10}$$

$$X^6 - 16 \times 27Y^6 = Z^3, \tag{5.11}$$

$$16X^6 - 27Y^6 = Z^3 \tag{5.12}$$

не имеют решений в отличных от нуля целых числах.

Доказательство. Предположим, что $x^6 - 27y^6 = 2z^3$, где x, y, z - отличные от нуля целые числа. Тогда $(x^2)^3 + (-3y^2)^3 - 2z^3 = 0$. В силу утверждения (5C) мы получаем $x^6 = y^6 = z^6 = \pm 1$ и, следовательно, $|x| = |y| = |z| = 1$, что невозможно.

Пусть $x^6 - 16 \times 27y^6 = z^3$. Тогда, умножив на 2^3, получим $(2x^2)^3 + (-2z)^3 - 2(2^2 \times 3y^2)^3 = 0$. Согласно (5C) мы имеем $(2x^2)^3 = (-2z)^3 = (2^2 \times 3y^2)^3 = \pm 1$, следовательно, $2x^2 = \pm 1$, что противоречит предположению.

Наконец, если $16x^6 - 27y^6 = z^3$, то $(3y^2)^3 + z^3 - 2(2x^2)^3 = 0$, откуда в силу утверждения (5C) мы заключаем, что $(3y^2)^3 = z^3 = (2x^2)^3 = \pm 1$, а значит, $2x^2 = \pm 1$, т. е. мы вновь приходим к противоречию. □

Далее, Лежандр доказал следующий результат.

(5F) *Уравнение*

$$X^3 + Y^3 = 3Z^3$$

не имеет решений в целых числах, отличных от нуля.

Доказательство. Доказательство повторяет предыдущие рассуждения с соответствующими изменениями. □

В 1856 г. Сильвестр также объявил, что справедливо следующее утверждение.

(5G) *Уравнение*

$$X^3 + Y^3 + Z^3 + 6XYZ = 0$$

не имеет решений в целых числах, отличных от нуля.

Список литературы

1856 Sylvester, J.J., *Recherches sur les solutions en nombres entiers positifs ou négatifs de l'équation cubique homogène à trois variables*, Ann. Sci. Matem. Fis. (Tortolini), **7** (1856), 398–400. Reprinted in *Mathematical Papers*, Vol. II, pp. 14–15; Cambridge University Press, Cambridge, 1908.

1876 Gauss, C.F., *Zur Theorie der complexen Zahlen.* (I) Neue Theorie der Zerlegung der Cuben; *Werke*, Vol. II, pp. 387–391, Königl. Ges. Wiss., Göttingen, 1876.

1978 Mann, H.B. and Webb, W.A., *A short proof of Fermat's theorem for* $n = 3$, Math. Student, **46** (1978), 103–104.

1999 Ribenboim, P., *Classical Theory of Algebraic Numbers*, Springer-Verlag, New York, 1999.

I.6. Уравнение пятого порядка

Случай $n = 5$ был впервые рассмотрен 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 Лежандр опубликовал полное независимое доказательство, Дирихле уже обосновал последний остававшийся не разобранным случай. Мы изложим доказательство Дирихле на современном языке, используя ряд фактов, касающихся арифметики квадратичного поля $K = \mathbb{Q}(\sqrt{5})$, доказательства которых можно найти, например, в книге Рибенбойма (1999).

Пусть A — кольцо целых чисел из $\mathbb{Q}(\sqrt{5})$. Элементы кольца A имеют вид $(a+b\sqrt{5})/2$, где a и b — целые числа одинаковой четности. Обратимые элементы из A, т. е. единицы поля K, образуют группу по умножению. Элемент $(a + b\sqrt{5})/2$ является единицей тогда и только тогда, когда его норма

$$\left(\frac{a+b\sqrt{5}}{2}\right)\left(\frac{a-b\sqrt{5}}{2}\right) = \frac{a^2-5b^2}{4}$$

равна ± 1 (т. е. $a^2 - 5b^2 = \pm 4$). Можно показать, что единицы кольца A — это в точности элементы $\pm((1+\sqrt{5})/2)^e$, где целое число e произвольно.

При доказательстве нам потребуется следующий важный факт: каждый элемент из A можно представить в виде произведения степеней простых элементов единственным способом (с точностью до единицы), или, что то же самое, каждый идеал в A — главный. Заметим, что в кольце A элементы 2, $\sqrt{5}$ являются простыми.

Начнем с рассмотрения одного свойства, касающегося определенных главных идеалов кольца A, являющихся пятыми степенями.

(6A)

(1) *Пусть отличные от нуля целые числа a и b таковы, что* $\text{НОД}(a,b) = 1$, $a \not\equiv b \pmod 2$, $5 \nmid a$, $5 \mid b$. *Пусть, далее, $a^2 - 5b^2$ является пятой степенью элемента из A. Тогда существуют отличные от нуля целые числа c, d, такие, что*

$$\begin{cases} a = c(c^4 + 50c^2d^2 + 125d^4), \\ b = 5d(c^4 + 10c^2d^2 + 5d^4), \end{cases} \tag{6.1}$$

причем $\text{НОД}(c,d) = 1$, $c \not\equiv d \pmod 2$, $5 \nmid c$.

(2) *Пусть нечетные числа* a *и* b *таковы, что* $\text{НОД}(a,b) = 1$, $5 \nmid a$, $5 \mid b$. *Пусть, далее,* $(a^2 - 5b^2)/4$ *является пятой степенью элемента из* A. *Тогда существуют (отличные от нуля) нечетные числа* c, d, *такие, что*

$$\begin{cases} a = c(c^4 + 50c^2d^2 + 125d^4)/16, \\ b = 5d(c^4 + 10c^2d^2 + 5d^4)/16, \end{cases} \tag{6.2}$$

причем $\text{НОД}(c,d) = 1$ *и* $5 \nmid c$.

Доказательство. Пусть отличные от нуля целые числа c и d удовлетворяют условиям (6.1) (соответственно условиям (6.2)). Тогда $\text{НОД}(c,d) = 1$, $5 \nmid c$, причем числа c и d не могут иметь одинаковую четность, иначе a и b были бы четны (соответственно c и d не могут иметь различную четность, иначе они оба были бы кратны 16, следовательно, c и d должны быть нечетными).

Теперь докажем существование чисел c и d в каждом случае.

(1) Сначала заметим, что если $a+b\sqrt{5} = ((h+k\sqrt{5})/2)^5$, где $h \equiv k \pmod 2$, то h и k четны. Действительно, $2^5 b = 5k(h^4 + 10h^2k^2 + 5k^4)$, значит, 2^5 делит $h^4 + 10h^2k^2 + 5k^4$. Если h и k нечетны, то $h \equiv \pm 1, \pm 3 \pmod 8$, следовательно, $h^2 \equiv 1, 9 \pmod{16}$, $h^4 \equiv 1, 17 \pmod{32}$ и такие же сравнения справедливы для k, k^2, k^4. Таким образом, $h^4 + 10h^2k^2 + 5k^4$ сравнимо по модулю 32 или с

$$1 + 10k^2 + 5k^4 \equiv \begin{cases} 1 + 10 + 5 \equiv 16, \\ 1 + 90 + 85 \equiv 16, \end{cases}$$

или с

$$17 + 26k^2 + 5k^4 \equiv \begin{cases} 17 + 26 + 5 \equiv 16, \\ 17 + 234 + 85 \equiv 16, \end{cases}$$

что невозможно.

Теперь покажем, что $\text{НОД}(a + b\sqrt{5}, a - b\sqrt{5}) = 1$. В самом деле, если простой элемент $\alpha \in A$ делит $a + b\sqrt{5}$ и $a - b\sqrt{5}$, то α делит $2a$ и $2b\sqrt{5}$. Если $\alpha \mid \sqrt{5}$, то $\alpha = \sqrt{5}\omega$ (ω — единица в A). Тогда $\sqrt{5}$ делит $2a$, 5 делит $4a^2$ (в $\mathbb{Z}$), а значит, $5 \mid a$, что противоречит предположению. Таким образом, α делит $2b$. Так как существуют целые числа s и t, такие, что $2 + 2bt = 2$, элемент α делит 2. Но элемент 2 прост в A, а потому $\alpha = 2\omega$ (ω — единица в A). Итак, 2 делит числа $a+b\sqrt{5}$ и $a-b\sqrt{5}$, следовательно, их произведение $(a+b\sqrt{5}) \times (a - b\sqrt{5}) = a^2 - 5b^2$ кратно 4. Но числа a и b имеют различную четность, а значит, $a^2 - 5b^2$ нечетно. Таким образом, мы пришли к противоречию.

Так как НОД $(a+b\sqrt{5},\ a-b\sqrt{5}) = 1$ и a^2-5b^2 является пятой степенью элемента из A, учитывая единственность разложения на множители в A, заключаем, что $a+b\sqrt{5}$ также является, с точностью до умножения на единицу, пятой степенью некоторого элемента, скажем, $a+b\sqrt{5} = ((m+n\sqrt{5})/2)^5$, где $m \equiv n \pmod 2$. Следовательно,

$$a+b\sqrt{5} = \left(\frac{m+n\sqrt{5}}{2}\right)^5 \left(\frac{t+u\sqrt{5}}{2}\right),$$

где $t \equiv u \pmod 2$, $(t+u\sqrt{5})/2$ — единица в A, так что $t^2-5u^2 = \pm 4$.

Положим $((m+n\sqrt{5})/2)^5 = (m'+n'\sqrt{5})/2$. Тогда $16m' \equiv m^5 \pmod 5$, $16n' \equiv 0 \pmod 5$, а значит, $5 \mid n'$. Далее, $4a = m't + 5n'u$, $4b = m'u + n't$, поэтому $5 \nmid m'$ (иначе выполнялось бы условие $5 \mid a$, что противоречит предположению), а следовательно, $5 \nmid m$. Из условий $5 \mid n'$, $5 \mid b$ следует, что $5 \mid m'u$, а значит, $5 \mid u$. Если $u = 0$, то $t = \pm 2$ и $a+b\sqrt{5} = \pm((m+n\sqrt{5})/2)^5$. Согласно сделанному в начале доказательства замечанию числа m и n четны. Положим $c = \pm m/2$, $d = \pm n/2$. Ясно, что числа c и d удовлетворяют соотношениям (6.1).

Если же $u \neq 0$, то $(t+u\sqrt{5})/2 \neq \pm 1$, следовательно, $(t+u\sqrt{5})/2 = \pm((1+\sqrt{5})/2)^e$ для некоторого показателя $e \neq 0$. Заменив при необходимости число $(1+\sqrt{5})/2$ на обратное число $-(1-\sqrt{5})/2$, можно считать, что $e > 0$ и даже что $e > 1$ (иначе мы получили бы, что $u = \pm 1$, а это противоречит условию $5 \mid u$). Тогда $\pm 2^{e-1} \times \times (t+u\sqrt{5}) = (1 \pm \sqrt{5})^e$. Следовательно,

$$\pm 2^{e-1}u = e + 5\binom{e}{3} + 5^2\binom{e}{5} + \ldots,$$

поэтому $2^{e-1}u \equiv \pm e \pmod 5$ и, так как $5 \mid u$, должно выполняться условие $5 \mid e$. Таким образом, $e = 5f$. Пусть

$$\frac{m+n\sqrt{5}}{2}\left(\frac{1\pm\sqrt{5}}{2}\right)^f = \frac{c'+d'\sqrt{5}}{2},$$

где $c' \equiv d' \pmod 2$. Тогда $a+b\sqrt{5} = \pm((c'+d'\sqrt{5})/2)^5$. Согласно сделанному в начале доказательства замечанию числа c' и d' четны. Положим $c = \pm c'/2$, $d = \pm d'/2$. Тогда c и d удовлетворяют соотношениям (6.1).

(2) Доказательство в этом случае очень похоже на приведенное выше, поэтому мы лишь укажем основные этапы. Сначала докажем, что НОД $((a+b\sqrt{5})/2,\ (a-b\sqrt{5})/2) = 1$, откуда сделаем вывод, что

$(a+b\sqrt{5})/2 = ((m+n\sqrt{5})/2)^5((t+u\sqrt{5})/2)$, где $m \equiv n \pmod 2$, $t \equiv u \pmod 2$, $t^2 - 5u^2 = \pm 4$. Тогда $5 \mid u$. Если $u = 0$, то положим $c = \pm m$, $d = \pm n$. Для чисел c и d справедливы соотношения (6.2). Если же $u \neq 0$, то $(t + u\sqrt{5})/2 = \pm((1 \pm \sqrt{5})/2)^e$, где $e > 0$ (и даже $e > 1$). Поэтому $e = 5f$, и, положив

$$\pm\left(\frac{m+n\sqrt{5}}{2}\right)\left(\frac{1\pm\sqrt{5}}{2}\right)^f = \frac{c+d\sqrt{5}}{2},$$

получим, что $(a + b\sqrt{5})/2 = ((c + d\sqrt{5})/2)^5$, причем снова имеют место соотношения (6.2). □

(6B) *Уравнение*

$$X^5 + Y^5 + Z^5 = 0 \tag{6.3}$$

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

Доказательство. Предположим, что существуют отличные от нуля целые числа x, y, z, такие, что $x^5 + y^5 + z^5 = 0$. Можно считать, что НОД$(x, y, z) = 1$, а значит, x, y, z попарно взаимно просты.

Случай 1: xyz не кратно 5.

Тогда x, y, z сравнимы с ± 1 или с ± 2 по модулю 5. Поскольку $x^5 \equiv x \pmod 5$, $y^5 \equiv y \pmod 5$, $z^5 \equiv z \pmod 5$, мы заключаем, что $x + y + z \equiv x^5 + y^5 + z^5 = 0 \pmod 5$.

Если числа x, y, z попарно несравнимы по модулю 5, то $x + y + z \not\equiv 0 \pmod 5$. Значит, например, $x \equiv y \pmod 5$. Тогда $-z \equiv x + y \equiv 2x \pmod 5$. Возводя сравнения в пятую степень:

$$x^5 \equiv y^5 \pmod{5^2}, \quad -z^5 \equiv 2^5 x^5 \pmod{5^2},$$

мы получим $-z^5 = x^5 + y^5 \equiv 2x^5 \pmod{5^2}$, следовательно, $2^5 x^5 \equiv 2x^5 \pmod{5^2}$, так что $2^5 \equiv 2 \pmod{5^2}$, а это неверно. Тем самым утверждение в первом случае доказано.

Случай 2: $5 \mid z$ (например).

Тогда $5 \nmid xy$. Из равенства НОД$(x, y) = 1$ следует, что числа x и y или оба нечетны, или имеют различную четность.

Пусть сначала x, y нечетны. Тогда $-z^5 = x^5 + y^5$ четно, следовательно, z кратно 2 и 5. Значит, $z = 2^m 5^n z'$, где $m \geqslant 1$, $n \geqslant 1$, z' не кратно ни 2, ни 5. Переобозначив z' через z, получим отличные от нуля попарно взаимно простые целые числа x, y, z, такие, что

$$-2^{5m}5^{5n}z^5 = x^5 + y^5, \tag{6.4}$$

где x, y, z нечетны и не кратны 5, $m \geqslant 1$, $n \geqslant 1$. Положим $2p = x + y$, $2q = x - y$ (p и q — целые числа, не равные 0). Тогда $x = p + q$, $y = p - q$, причем НОД$(p, q) = 1$ и p, q не являются одновременно нечетными. Следовательно,

$$-2^{5m}5^{5n}z^5 = (p+q)^5 + (p-q)^5 = 2p(p^4 + 10p^2q^2 + 5q^4).$$

Так как $5 \mid p$ или $5 \mid (p^4 + 10p^2q^2 + 5q^4)$, в любом случае $5 \mid p$. Положим $p = 5r$. Итак, $5 \nmid q$, НОД$(r, q) = 1$ и числа q, r имеют различную четность. Таким образом,

$$-2^{5m}5^{5n}z^5 = 2 \times 5^2 r(q^4 + 50q^2r^2 + 125r^4).$$

Пусть $t = q^4 + 50q^2r^2 + 125r^4 = (q^2 + 25r^2)^2 - 5(10r^2)^2$. Положим $u = q^2 + 25r^2$, $v = 10r^2$. Тогда u, v не равны 0, u нечетно, $10 \mid v$, НОД$(u, v) = 1$. Следовательно, число t нечетно, $5 \nmid t$, НОД$(t, r) = 1$, а значит, $5 \mid r$ (так как $5n > 2$).

Так как НОД$(2 \times 5^2 r, t) = 1$, элементы $2 \times 5^2 r$ и t являются пятыми степенями целых чисел. Но $t = u^2 - 5v^2$, где $u \not\equiv v \pmod 2$, НОД$(u, v) = 1$, $5 \nmid u$, $5 \mid v$. Согласно (6A) существуют отличные от нуля целые числа c и d, такие, что

$$\begin{cases} u = c(c^4 + 50c^2d^2 + 125d^4), \\ v = 5d(c^4 + 10c^2d^2 + 5d^4), \end{cases}$$

причем НОД$(c, d) = 1$, $c \not\equiv d \pmod 2$, $5 \nmid c$. Отсюда следует, что $5 \mid d$, так как $5 \mid r$, а значит, $5^3 \mid v$. Заметим также, что $d > 0$. Умножив второе соотношение на 2×5^3, получим, что $(2 \times 5^2 r)^2 = 2 \times 5^3 \times 10r^2 = 2 \times 5^4 d(c^4 + 10c^2d^2 + 5d^4)$ и это число является пятой степенью целого числа (так как $2 \times 5^2 r$ является пятой степенью целого числа).

Но НОД$(2 \times 5^4 d, c^4 + 10c^2d^2 + 5d^4) = 1$, потому что число $c^4 + 10c^2d^2 + 5d^4$ нечетно, $5 \nmid c$ и НОД$(c, d) = 1$. Следовательно, $2 \cdot 5^4 d$ и $c^4 + 10c^2d^2 + 5d^4 = (c^2 + 5d^2)^2 - 5(2d^2)^2$ — пятые степени целых чисел. Так как числа $c^2 + 5d^2$ и $2d^2$ не являются одновременно нечетными, НОД$(c^2 + 5d^2, 2d^2) = 1$, $5 \nmid (c^2 + 5d^2)$ и $5 \mid 2d^2$, согласно (6A) мы вновь можем сделать вывод, что существуют отличные от нуля целые числа c' и d', такие, что

$$\begin{cases} c^2 + 5d^2 = c'(c'^4 + 50c'^2d'^2 + 125d'^4), \\ 2d^2 = 5d'(c'^4 + 10c'^2d'^2 + 5d'^4) \end{cases}$$

и НОД$(c', d') = 1$, $c' \not\equiv d' \pmod 2$, $5 \nmid c'$. Отсюда следует, что $5 \mid d'$, потому что $5^2 \mid d^2$. Заметим также, что $d' > 0$. Умножив второе

соотношение на 2×5^8, получим

$$2^2 \times 5^8 d^2 = (2 \times 5^4 d)^2 = 2 \times 5^9 d'(c'^4 + 10c'^2 d'^2 + 5d'^4),$$

причем это число является пятой степенью целого числа. Поскольку элементы $2 \times 5^9 d'$, $c'^4 + 10c'^2 d'^2 + 5d'^4$ взаимно просты, они также являются пятыми степенями целых чисел. Это аналогично доказанному выше утверждению о том, что $2 \times 5^4 d$, $c^4 + 10c^2 d^2 + 5d^4$ — пятые степени целых чисел. Более того, $0 < d' < d$, потому что $25d'^5 \leqslant 5d'(c'^4 + 10c'^2 d'^2 + 5d'^4) = 2d^2$, следовательно,

$$0 < d' \leqslant \sqrt[5]{(2d^2)/25} < d.$$

Продолжая этот процесс, получим целое число d'', такое, что $0 < d'' < 1$, а это невозможно.

Остается рассмотреть случай, когда x и y имеют различную четность. Мы опустим часть вычислений.

Пусть $x + y = p$, $x - y = q$, следовательно, p и q нечетны, НОД$(p, q) = 1$, $2x = p+q$, $2y = p-q$. Справедлива цепочка равенств $-2^5 \times 5^{5n} z^5 = (2x)^5 + (2y)^5 = (p+q)^5 + (p-q)^5 = 2p(p^4 + 10p^2 q^2 + 5q^4)$. Так как $5 \mid p$, положив $p = 5r$, получим, что $5 \nmid q$, НОД$(q, r) = 1$, числа q и r оба нечетны и

$$-2^5 \times 5^{5n} z^5 = 2 \times 5^2 rt,$$

причем $t = q^4 + 50q^2 r^2 + 125r^4 = u^2 - 5v^2$, где $u = q^2 + 25r^2$, $v = 10r^2$. Тогда числа u и v не равны 0, четны, $u \equiv 2 \pmod 4$, $5 \nmid t$ и НОД$(t, r) = 1$, а значит, $5 \mid r$ (так как $5n > 2$). Положим $u = 2u'$, $v = 2v'$. Тогда числа u' и v' нечетны, НОД$(u', v') = 1$, $5 \nmid u'$, $5 \mid v'$. Если $t' = t/4 = u'^2 - 5v'^2$, то $t' \equiv 0 \pmod 4$, причем $-5^{5n} z^5 = 5^2 rt'/4$, где НОД$\left(5^2 r, t'/4\right) = 1$. Таким образом, $5^2 r$ и $t'/4 = (u'^2 - 5v'^2)/4$ являются пятыми степенями целых чисел. Согласно (6A) существуют отличные от нуля целые числа c и d, такие, что

$$\begin{cases} u' = c(c^4 + 50c^2 d^2 + 125d^4)/16, \\ v' = 5d(c^4 + 10c^2 d^2 + 5d^4)/16, \end{cases}$$

причем НОД$(c, d) = 1$, оба числа c и d нечетны и $5 \nmid c$. Более того, $5 \mid r$, так что $5^2 \mid v'$, а следовательно, $5 \mid d$. Заметим также, что $d > 0$.

Умножив второе соотношение на 5^3, получим

$$(5^2 r)^2 = 5^3 v' = \frac{5^4 d}{4}\left[\left(\frac{c^2 + 5d^2}{2}\right)^2 - 5d^4\right],$$

где $\left((c^2+5d^2)/2\right)^2 - 5d^4 \equiv 0 \pmod 4$. Так как оба множителя в правой части взаимно просты и $(5^2r)^2$ является пятой степенью целого числа, 5^4d и $\frac{1}{4}[((c^2+5d^2)/2)^2 - 5(d^2)^2]$ также являются пятыми степенями целых чисел. В силу (6A) существуют отличные от нуля целые числа c' и d', такие, что

$$\begin{aligned}(c^2+5d^2)/2 &= c'(c'^4+50c'^2d'^2+125d'^4)/16,\\ d^2 &= 5d'(c'^4+10c'^2d'^2+5d'^4)/16,\end{aligned}$$

причем $\text{НОД}(c',d') = 1$, оба числа c' и d' нечетны и $5 \nmid c'$. Более того, $5 \mid d'$ и $d' > 0$. Умножив второе соотношение на 5^8, получим

$$\begin{aligned}5^8d^2 = (5^4d)^2 &= \frac{5^9d'}{16}(c'^4+10c'^2d'^2+5d'^4)\\ &= \frac{5^9d'}{4}\left[\left(\frac{c'^2+5d'^2}{2}\right)^2 - 5(d'^2)^2\right].\end{aligned}$$

Мы вновь заключаем, что $5^9d'$ и $\frac{1}{4}[((c'^2+5d'^2)/2)^2 - 5(d'^2)^2]$ являются пятыми степенями целых чисел. Это аналогично предыдущему утверждению. Более того, $0 < d' < d$, так как $25d'^5 \leqslant 16d^2$. Продолжение этой процедуры приводит к противоречию. □

В 1912 г. Племель доказал усиленный вариант предыдущей теоремы (см. также Нагель (1958)).

(6C) *Уравнение*

$$X^5 + Y^5 + Z^5 = 0$$

имеет лишь тривиальные решения в целых числах из поля $\mathbb{Q}(\sqrt{5})$.

Другие доказательства теоремы Ферма для показателя 5 были найдены авторами, указанными в табл. 3.

Список литературы

1825 Schopis, *Einige Sätze aus der unbestimmten Analytik*, Progr. Gummbinnen, 1825, pp. 12–15.

1828 Dirichlet, P.G.L., *Mémoire sur l'impossibilité de quelques équations indéterminées du* 5^e *degré*, J. Reine Angew. Math., **3** (1828), 354–375; reprinted in *Werke*, Vol. I, pp. 1–20 and 21–46, G. Reimer Verlag, Berlin, 1889, and also by Chelsea, New York, 1969.

Таблица 3. ПТФ для показателя 5

Автор	Случай	Год
Гаусс	оба	1863 (посмертное издание)
Шопи	первый	1825
Лебег	оба	1843
Ламе	оба	1847
Гамбиоли	оба	1901 и 1903/4
Веребрюсов	оба	1905
Мириманов	первый	1909
Рыхлик	оба	1910
Гайяши[6]	оба	1911
ван дер Корпут	оба	1915
Тержанян	оба	1987

1830 Legendre, A.M., *Théorie des Nombres* (3^e édition), Vol. II, p. 5, Firmin Didot Fréres, Paris, 1830; reprinted by A. Blanchard, Paris, 1955.

1843 Lebesgue, V.A., *Théorèmes nouveaux sur l'équation indéterminée* $x^5 + y^5 = az^5$, J. Math. Pures Appl., (1), **8** (1843), 49–70.

1847 Lamé, G., *Mémoire sur la résolution en nombres complexes de l'équation* $A^5 + B^5 + C^5 = 0$, J. Math. Pures Appl., (1), **12** (1847), 137–171.

1875 Gauss, C.F., *Zur Theorie der complexen Zahlen.* (I) Neue Theorie der Zerlegung der Cuben, *Werke*, Vol. II, pp. 387–391, Königl. Ges. Wiss. Göttingen, 2nd ed., 1875.

1901 Gambioli, D., *Memoria bibliografica sull'ultimo teorema di Fermat*, Period. Mat., **16** (1901), 145–192.

1903/4 Gambioli, D., *Intorno all' ultimo teorema di Fermat*, Il Pitagora, **10** (1903/4), 11–13 and 41–42.

1905 Werebrusow, A.S., *On the equation* $x^5 + y^5 = Az^5$ (in Russian), Moskov. Math. Samml., **25** (1905), 466–473.

1909 Mirimanoff, D., *Sur le dernier théorème de Fermat*, Enseign. Math., **11** (1909), 49–51.

1910 Rychlik, K., *On Fermat's last theorem for* $n = 5$ (in Bohemian), Časopis Pěst. Mat., **39** (1910), 185–195, 305–317.

[6]Это доказательство может быть неверным, согласно информации из частной беседы.

1911 Hayashi, T., *On Fermat's last theorem*, Indian Math. Club, Madras, **3** (1911), 111–114; reprinted in Science Reports, Tôhoku Imp. Univ., (1), **1** (1911/12), 51–54.

1912 Plemelj, J., *Die Unlösbarkeit von* $x^5 + y^5 + z^5 = 0$ *im Körper* $k(\sqrt{5})$, Monatsh. Math., **23** (1912), 305–308.

1915 van der Corput, J.G., *Quelques formes quadratiques et quelques équations indéterminées*, Nieuw Archief Wisk., **11** (1915), 45–75.

1958 Nagell, T., *Sur l'équation* $x^5 + y^5 = z^5$, Arkiv. Mat., **3** (1958), 511–514.

1973/4 Terjanian, G., *L'équation* $x^n + y^n = z^n$ *pour* $n = 5$ *et* $n = 14$, Sém. Th. des Nombres, Bordeaux, 1973/4, exp. no. 5, 6 pp.

1987 Terjanian, G., *Sur une question de V.A. Lebesgue*, Ann. Inst. Fourier, **37** (1987), 19–37.

1999 Ribenboim, P., *Classical Theory of Algebraic Numbers*, Springer-Verlag, New York, 1999.

I.7. Уравнение седьмого порядка

В 1839 г. Ламе доказал теорему Ферма для показателя 7. Более простое доказательство в 1840 г. нашел Лебег. Рассуждение Дженокки (1874 г. и 1876 г.), основанное на идее Лежандра (1830), было еще проще. Мы воспроизводим его по книге Нагеля (1951).

(7A)

(1) *Пусть корни кубического уравнения с рациональными коэффициентами* x, y, z *удовлетворяют уравнению* $x^7+y^7+z^7 = 0$. *Тогда или* $xyz = 0$, *или числа* x, y, z *пропорциональны (в определенном порядке) корням третьей степени из* 1, *а именно* $1, \zeta = (-1+\sqrt{-3})/2, \zeta^2 = (-1-\sqrt{-3})/2$.

(2) *Уравнение* $x^7+y^7+z^7 = 0$ *имеет лишь тривиальные решения в целых числах.*

Доказательство. (1) Предположим, что x, y, z — корни многочлена $f(X) = X^3 - pX^2 + qX - r$, где $p, q, r \in \mathbb{Q}$. Тогда

$$\begin{cases} p = x + y + z, \\ q = xy + xz + yz, \\ r = xyz. \end{cases}$$

Случай 1: $p = 0$.

Воспользуемся тождеством (см. разд. II.5)

$$(X+Y)^7 - X^7 - Y^7 = 7XY(X+Y)(X^2+XY+Y^2)^2.$$

Если $x+y+z=0$ и $x^7+y^7+z^7=0$, то $7xy(x+y)(x^2+xy+y^2)^2=0$. Следовательно, или $x=0$, или $y=0$, или $z=-(x+y)=0$, или $xyz\neq 0$, но $x^2+xy+y^2=0$. Таким образом, $(y/x)^2+y/x+1=0$, а значит, y/x является корнем третьей степени из 1, причем $y/x\neq 1$. Тогда $y=x\zeta$ (или $y=x\zeta^2$) и $z=-(x+y)=-x(1+\zeta)=x\zeta^2$, так что x,y,z пропорциональны числам $1,\zeta,\zeta^2$ (или $1,\zeta^2,\zeta$).

Случай 2: $p\neq 0$.

Пусть $k\geqslant 1$ и $s_k=x^k+y^k+z^k$ — сумма k-х степеней корней уравнения $f(X)=0$. По формулам Ньютона

$$\begin{aligned}
s_1 &= p,\\
s_2 &= s_1p-2q,\\
s_3 &= s_2p-s_1q+3r,\\
s_4 &= s_3p-s_2q+s_1r,\\
s_5 &= s_4p-s_3q+s_2r,\\
s_6 &= s_5p-s_4q+s_3r,\\
s_7 &= s_6p-s_5q+s_4r.
\end{aligned}$$

Сделав подстановку, получим

$$x^7+y^7+z^7=p^7-7p^5q+7p^4r+14p^3q^2-21p^2qr-7pq^3+7pr^2+7q^2r.$$

Положим $m=pq-r\in\mathbb{Q}$. Тогда

$$x^7+y^7+z^7=p^7-7(pq-r)(p^4-p^2q+q^2)+7(pq-r)^2p,$$

то есть

$$x^7+y^7+z^7=p^7-7m(p^4-p^2q+q^2)+7m^2p.$$

Так как $x^7+y^7+z^7=0$, мы получаем

$$p^7-7m(p^4-p^2q+q^2)+7m^2p=0.$$

Обозначим $q/p^2=Q$, $m/p^3=M$. Тогда

$$p^7-7p^3M(p^4-p^4Q-p^4Q^2)+7p^7M^2=0,$$

следовательно,

$$M^2-M(1-Q+Q^2)+\frac{1}{7}=0.$$

Поскольку число M рационально, деленный на 4 дискриминант $((1-Q+Q^2)/2)^2-\frac{1}{7}$ является квадратом отличного от нуля рационального числа. Пусть $2Q-1=s/t$, где целые числа s и t взаимно просты, причем $t>0$. Тогда $Q=(t+s)/2t$, а следовательно.

$64t^4[((3t^2+s^2)/8t^2)^2-\frac{1}{7}]=s^4+6t^2s^2-t^4/7=u^2$, где рациональное число u отлично от нуля.

Так как число $7u^2$ целое, u также должно быть целым, а значит, t кратно 7, и, следовательно, $7\nmid s$. Пусть $t=7^ev$, где $e\geqslant 1$, $7\nmid v$. Тогда

$$s^4+6\times 7^{2e}v^2s^2-7^{4e-1}v^4=u^2. \tag{7.1}$$

Из (7.1) получим, что

$$(s^2+3\times 7^{2e}v^2)^2-u^2=64\times 7^{4e-1}v^4, \tag{7.2}$$

следовательно,

$$(s^2+3\times 7^{2e}v^2+u)(s^2+3\times 7^{2e}v^2-u)=64\times 7^{4e-1}v^4. \tag{7.3}$$

Теперь покажем, что НОД$(s^2+3\times 7^{2e}v^2+u, s^2+3\times 7^{2e}v^2-u)$ есть степень числа 2. Действительно, пусть простое число $p\neq 2$ таково, что $p\mid(s^2+3\times 7^{2e}v^2+u)$ и $p\mid(s^2+3\times 7^{2e}v^2-u)$. Тогда $p\mid 2u$, а значит, $p\mid u$. Кроме того, $p\mid 2(s^2+3\times 7^{2e}v^2)$, следовательно, $p\mid(s^2+3\times 7^{2e}v^2)$. Если $p=7$, то, так как $e\geqslant 1$, мы заключаем, что $7=p\mid s$, а это невозможно. Если же $p\neq 7$, то в силу (7.3) мы делаем вывод, что $p\mid 64\times 7^{4e-1}v^4$, следовательно, $p\mid v$, а значит, $p\mid s$, и это снова противоречие. Таким образом, наибольший общий делитель двух сомножителей из (7.3) есть степень числа 2.

Подслучай (а): v нечетно.

Из соотношения (7.3) следует, что

$$\begin{cases} s^2+3\times 7^{2e}v^2\pm u=7^{4e-1}Aa^4, \\ s^2+3\times 7^{2e}v^2\mp u=Bb^4, \end{cases} \tag{7.4}$$

где целые числа a и b взаимно просты, $ab=v$ (а значит, a и b нечетны), A и B четны и $AB=64$.

Из системы (7.4) получим, что

$$2s^2+6\times 7^{2e}v^2=7^{4e-1}Aa^4+Bb^4. \tag{7.5}$$

Заметим, что если x нечетно, то $x^2\equiv 1 \pmod 8$, а так как $7\equiv -1 \pmod 8$, мы получаем

$$s^2\equiv -3\times 7^{2e}a^2b^2+7^{4e-1}\frac{A}{2}a^4+\frac{B}{2}b^4\equiv -3-\frac{A}{2}+\frac{B}{2} \pmod 8.$$

Рассмотрим все возможные значения A, B:

$$\begin{array}{llll} A=32, & B=2 & \Rightarrow & s^2 \equiv -2 \pmod 8, \text{ что невозможно,} \\ A=16, & B=4 & \Rightarrow & s^2 \equiv -1 \pmod 8, \text{ что невозможно,} \\ A=8, & B=8 & \Rightarrow & s^2 \equiv -3 \pmod 8, \text{ что невозможно,} \\ A=4, & B=16 & \Rightarrow & s^2 \equiv 3 \pmod 8, \text{ что невозможно,} \\ A=2, & B=32 & \Rightarrow & s^2 \equiv 4 \pmod 8. \end{array}$$

В последнем случае соотношение (7.5) можно переписать так:

$$s^2 + 3 \times 7^{2e} a^2 b^2 = 7^{4e-1} a^4 + 16 b^4.$$

Умножив это равенство на 64, получим

$$64s^2 + 6 \times 7^{2e} \times 32 a^2 b^2 - 64 \times 16 b^4 = 7^{4e-1} \times 64 a^4,$$

откуда

$$64s^2 - (32b^2 - 3 \times 7^{2e} a^2)^2 = 7^{4e-1} \times 64 a^4 - 7^{4e} \times 3^2 a^4 = 7^{4e-1} a^4,$$

а следовательно,

$$(8s + 32b^2 - 3 \times 7^{2e} a^2)(8s - 32b^2 + 3 \times 7^{2e} a^2) = 7^{4e-1} a^4. \qquad (7.6)$$

Заметим, что НОД $(8s + 32b^2 - 3 \times 7^{2e} a^2, 8s - 32b^2 + 3 \times 7^{2e} a^2) = 1$. Действительно, так как a нечетно, рассматриваемые числа также нечетны. Пусть $p \mid (8s + 32b^2 - 3 \times 7^{2e} a^2)$ и $p \mid (8s - 32b^2 + 3 \times 7^{2e} a^2)$. Тогда $p \mid 16s$, следовательно, $p \mid s$, и аналогично $p \mid (32b^2 - 3 \times \times 7^{2e} a^2)$. Но $p \mid 7^{4e-1} a^4$ (согласно (7.6)). Если $p = 7$, то $p = 7 \mid s$, что невозможно. Если же $p \neq 7$, то $p \mid a$, следовательно, $p \mid b$, т. е. мы снова получаем противоречие. Это доказывает утверждение, и, таким образом,

$$\begin{cases} 8s \pm 32b^2 \mp 3 \times 7^{2e} a^2 = c^4, \\ 8s \mp 32b^2 \pm 3 \times 7^{2e} a^2 = 7^{4e-1} d^4, \end{cases} \qquad (7.7)$$

где целые числа c и d взаимно просты, причем $cd = a$. Следовательно, c и d нечетны. Из системы (7.7) можно сделать вывод, что

$$\mp 3 \equiv c^4 \pmod 8,$$

а этого быть не может. Итак, доказано, что подслучай (a) невозможен.

Подслучай (b): v четно.

Тогда s нечетно (потому что t четно), а значит, u тоже нечетно. Перепишем соотношение (7.2) в виде

$$(s^2 + 3 \times 7^{2e} v^2)^2 - u^2 = 4 \times 7^{4e-1} (2v)^4$$

и, заметив, что оба множителя в левой части равенства (7.3) четны и их наибольший общий делитель равен 2, получим, что

$$\begin{cases} s^2 + 3 \times 7^{2e} v^2 \pm u = 2 \times 7^{4e-1} A^4, \\ s^2 + 3 \times 7^{2e} v^2 \mp u = 2 \times B^4, \end{cases} \tag{7.8}$$

где целые числа A, B взаимно просты и $AB = 2v$, следовательно, одно из чисел A или B четно. Таким образом,

$$s^2 = -3 \times 7^{2e} v^2 + 7^{4e-1} A^4 + B^4 = -\frac{3}{4} \times 7^{2e} A^2 B^2 + 7^{4e-1} A^4 + B^4. \tag{7.9}$$

Если B четно, то A нечетно и $s^2 \equiv -3v^2 - 1 \pmod 8$, а значит, $s^2 \equiv -1 \pmod 4$, что невозможно.

Если A четно, то B нечетно. Положив $A = 2A_1$, из (7.9) получим

$$s^2 = -3 \times 7^{2e} A_1^2 B^2 + 7^{4e-1} \times 2^4 A_1^4 + B^4,$$

а следовательно, $1 \equiv s^2 \equiv -3A_1^2 + 1 \pmod 8$. Отсюда $3A_1^2 \equiv 0 \pmod 8$, так что $4 \mid A_1$. Положим $A_1 = 4A_2$. Тогда $A = 8A_2$ и равенство (7.9) перепишется в виде

$$s^2 = -3 \times 16 \times 7^{2e} A_2^2 B^2 + 7^{4e-1} \times 8^4 \times A_2^4 + B^4,$$

а следовательно,

$$\begin{aligned} s^2 - (B^2 - 3 \times 8 \times 7^{2e} A_2^2)^2 &= 7^{4e-1} \times 8^4 \times A_2^4 - 3^2 \times 8^2 \times 7^{4e} A_2^4 \\ &= 7^{4e-1} \times 8^2 \times A_2^4. \end{aligned} \tag{7.10}$$

Отсюда получаем

$$\begin{aligned} (s - B^2 + 3 \times 8 \times 7^{2e} A_2^2)(s + B^2 - 3 \times 8 \times 7^{2e} A_2^2) \\ = 7^{4e-1} \times 4 \times (2A_2)^4. \end{aligned} \tag{7.11}$$

Оба множителя в левой части равенства (7.11) четны, и, как и раньше, легко видеть, что их наибольший общий делитель равен 2. Таким образом,

$$\begin{cases} s \mp B^2 \pm 3 \times 8 \times 7^{2e} A_2^2 = 2c_2^4, \\ s \pm B^2 \mp 3 \times 8 \times 7^{2e} A_2^2 = 7^{4e-1} \times 2d_2^4, \end{cases} \tag{7.12}$$

где взаимно простые целые числа c_2 и d_2 таковы, что $c_2 d_2 = 2A_2$.

Вычитая из первого соотношения системы (7.12) второе, после деления на 2 получим $\mp B^2 \pm 3 \times 8 \times 7^{2e} A_2^2 = c_2^4 - 7^{4e-1} d_2^4$, следовательно,

$$\pm B^2 = \pm 6 \times 7^{2e} c_2^2 d_2^2 - c_2^4 + 7^{4e-1} d_2^4. \tag{7.13}$$

Так как всякий отличный от нуля квадрат по модулю 7 равен 1, 2 или 4, мы получаем $B^2 + c_2^4 \not\equiv 0 \pmod 7$. Значит, в (7.13) нужно

Таблица 4. ПТФ для показателя 7

Автор	Случай	Год
Лежандр (Софи Жермен)	первый	1823 (см. разд. II.3)
Дженокки	оба	1864
Пепен	оба	1876
Мейе	оба	1897

взять отрицательные знаки:

$$B^2 = c_2^4 + 6 \times 7^{2e} c_2^2 d_2^2 - 7^{4e-1} d_2^4. \tag{7.14}$$

Это уравнение имеет тот же вид, что и (7.1). Более того,

$$v = \frac{AB}{2} = 4A_2 B \geqslant 2c_2 d_2 > d_2.$$

Продолжая рассуждения, основанные на методе бесконечного спуска, заключаем, что подслучай (b) также не реализуется. Таким образом, и второй случай невозможен, что и доказывает часть (1) нашего утверждения.

(2) Пусть целые числа x, y, z таковы, что $x^7 + y^7 + z^7 = 0$. Рассмотрим многочлен $f(X) = X^3 - pX^2 + qX - r$ с корнями x, y, z. Поскольку числа x, y, z не могут быть пропорциональны $1, \zeta, \zeta^2$, в силу доказанного утверждения (1) заключаем, что $xyz = 0$. □

Другие доказательства теоремы Ферма для показателя 7 были найдены авторами, указанными в табл. 4.

Список литературы

1823 Legendre, A.M., *Recherches sur quelques objets d'analyse indéterminée, et particulièrement sur le théorème de Fermat*, Mém. Acad. Roy. Sci. Institut France, **6** (1823), 1–60; reprinted as the "Second Supplément" in 1825, to a printing of *Essai sur la Théorie des Nombres* (2^e édition), Courcier, Paris; reprinted in Sphinx Oedipe, **4** (1909), 97–128.

1839 Lamé, G., *Mémoire sur le dernier théorème de Fermat*, C. R. Acad. Sci. Paris, **9** (1839), 45–46.

1839 Cauchy, A. and Liouville, J., *Rapport sur un mémoire de M. Lamé relatif au dernier théorème de Fermat*, C. R. Acad. Sci. Paris. **9** (1839), 359–363; also appeared in J. Math. Pures Appl., 5

(1840), 211–215 and *Oeuvres Complètes*, Sér. 1, Vol. 4, pp. 494–504, Gauthier-Villars, Paris, 1884.

1840 Lamé, G., *Mémoire d'analyse indéterminée démontrant que l'équation* $x^7 + y^7 = z^7$ *est impossible en nombres entiers*, J. Math. Pures Appl., **5** (1840), 195–211.

1840 Lebesgue, V.A., *Démonstration de l'impossibilité de résoudre l'équation* $x^7 + y^7 + z^7 = 0$ *en nombres entiers*, J. Math. Pures Appl., **5** (1840), 276–279.

1840 Lebesgue, V.A., *Addition à la note sur l'équation* $x^7 + y^7 + z^7 = 0$, J. Math. Pures Appl., **5** (1840), 348–349.

1864 Genocchi, A., *Intorno all'equazioni* $x^7 + y^7 + z^7 = 0$, Annali Mat., **6** (1864), 287–288.

1874 Genocchi, A., *Sur l'impossiblilité de quelques égalités doubles*, C. R. Acad. Sci. Paris, **78** (1874), 433–436.

1876 Genocchi, A., *Généralisation du théorème de Lamé sur l'impossibilité de l'équation* $x^7 + y^7 + z^7 = 0$, C. R. Acad. Sci. Paris, **82** (1876), 910–913.

1876 Pepin, T., *Impossibilité de l'équation* $x^7 + y^7 + z^7 = 0$, C. R. Acad. Sci. Paris, **82** (1876), 676–679 and 743–747.

1897 Maillet, E., *Sur l'équation indéterminée* $ax^{\lambda^t} + by^{\lambda^t} = cz^{\lambda^t}$, Assoc. Française Avanc. Sci., St. Etienne, Sér. II, **26** (1897), 156–168.

1951 Nagell, T., *Introduction to Number Theory*, Wiley, New York, 1951; reprinted by Chelsea, New York, 1962.

I.8. Другие частные 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, а значит, обобщены быть не могут.

Отметим, что согласно устному сообщению Тержаняна доказательство Гайяши (1911) второго случая для показателя 13 содержит ошибку.

Брчич-Костич изучал уравнение $x^4 + y^2 = z^6$ и в 1956 г. показал, что оно не имеет решений во взаимно простых целых числах. Однако у этого уравнения есть нетривиальные решения в целых числах, не являющихся попарно взаимно простыми.

Мы приведем элементарные доказательства Бройша (1960) для показателей 6 и 10. Разумеется, справедливость утверждения теоре-

мы для этих показателей следует из соответствующих утверждений для показателей 3 и 5. Но мы представим доказательства, совершенно независимые от этих результатов. Следующие вспомогательные утверждения, полученные методом бесконечного спуска, также принадлежат Бройшу.

(8A) *Не существует натуральных чисел x, y, u, v, таких, что*

$$x^2 + y^2 = u^2 + v^2, \tag{8.1}$$

$$xy = 2uv. \tag{8.2}$$

Доказательство. Предположим противное и из всех возможных решений выберем то, для которого положительное произведение xy минимально. Тогда никакие три из четырех целых чисел x, y, u, v не могут иметь общего делителя, превосходящего единицу. Более того, $\text{НОД}(x, y) = 1$, поскольку если простое число p делит x и y, то p делит u или v, что противоречит предположению. Аналогично доказывается, что $\text{НОД}(u, v) = 1$. Следовательно, одно из чисел x, y четно, а другое нечетно. Пусть, например, $2 \mid y$. Тогда $x^2 + y^2$ нечетно, а значит, одно из чисел u или v четно. Пусть, скажем, u четно. Тогда с учетом (8.2) получим, что $4 \mid y$; из сравнения $x^2 \equiv 1 \pmod 8$ следует, что $x^2 + y^2 \equiv 1 \pmod 8$. Далее, согласно (8.1) мы получаем $u^2 \equiv 0 \pmod 8$, а значит, $u \equiv 0 \pmod 4$ и $8 \mid y$.

Пусть $y = 2^{r+1}y'$ (где $r \geqslant 2$ и y' нечетно). Тогда $u = 2^r u'$, причем число u' нечетно. Таким образом,

$$\begin{aligned} &xy' = u'v, \quad \text{числа } x, y', u', v \text{ нечетны,} \\ &\text{НОД}(x, y') = \text{НОД}(u', v) = 1. \end{aligned} \tag{8.3}$$

Более того, если

$$\begin{aligned} a &= \text{НОД}(x, u'), \qquad b = \text{НОД}(x, v), \\ c &= \text{НОД}(y', u'), \qquad d = \text{НОД}(y', v), \end{aligned}$$

то числа a, b, c, d попарно взаимно просты, причем b и d нечетны, а значит, $b^2 \equiv d^2 \equiv 1 \pmod 8$. Итак, $x = ab$, $y' = cd$, $u' = ac$, $v = bd$. Следовательно, исходное уравнение принимает вид

$$a^2b^2 + 2^{2r+2}c^2d^2 = 2^{2r}a^2c^2 + b^2d^2.$$

Положив $t = 2^r c$, получим

$$3t^2d^2 = (a^2 - d^2)(t^2 - b^2), \tag{8.4}$$

где числа t, a, b, d попарно взаимно просты и $4 \mid t$. Отсюда следует, что d^2 делит $t^2 - b^2$, а $t^2 - b^2$ делит $3d^2$.

Это возможно тогда и только тогда, когда выполнено одно из следующих условий:

(I) $t^2 - b^2 = 3d^2$;
(II) $t^2 - b^2 = d^2$;
(III) $t^2 - b^2 = -3d^2$;
(IV) $t^2 - b^2 = -d^2$.

Но $t^2 \equiv 0 \pmod 8$ и $b^2 \equiv d^2 \equiv 1 \pmod 8$. Следовательно, случаи I, II, III не реализуются. Если $t^2 - b^2 = -d^2$, то $3t^2 = d^2 - a^2$, а значит,

$$b^2 = d^2 + t^2 = a^2 + 4t^2. \tag{8.5}$$

В силу утверждения (1A) существуют такие целые числа m, n, $r, s > 0$, что

$$\begin{cases} b = m^2 + n^2, \\ t = 2mn \end{cases} \tag{8.6}$$

и

$$\begin{cases} b = r^2 + s^2, \\ 2t = 2rs. \end{cases} \tag{8.7}$$

Отсюда получим соотношения

$$r^2 + s^2 = m^2 + n^2 \tag{8.8}$$

и

$$rs = 2mn. \tag{8.9}$$

Итак, мы нашли новое решение исходной системы, для которого $rs = t = 2^r c \leqslant 2^r y' < y \leqslant xy$, что противоречит выбору четверки (x, y, u, v). □

(8B) *Не существует натуральных чисел x, y, u, v, таких, что*

$$x^2 - y^2 = u^2 + v^2, \tag{8.10}$$

$$xy = 2uv. \tag{8.11}$$

Доказательство. Снова предположим противное и рассмотрим такие натуральные числа, удовлетворяющие соотношениям (8.10) и (8.11), что произведение xy минимально.

Рассуждая, как и раньше, заметим, что одно из чисел x, y четно, а другое нечетно. Таким образом, $x^2 - y^2 \equiv u^2 + v^2 \equiv 1 \pmod 4$, а значит, x непременно нечетно, а y четно. Как и в предыдущем доказательстве, получим уравнения (8.3), (8.4), (8.5) и (8.6), где

Таблица 5. ПТФ для различных показателей

Автор	Показатель	Случай	Год
Кауслер	6	оба	1806
Софи Жермен (Лежандр)	все простые, меньшие 100	первый	1823 (см. гл. III)
Дирихле	14	оба	1832
Ламе[7]	11, 17, 23, 29, 41	первый	1847
Мэтьюс	11, 17	первый	1885/6
Тафельмахер[8]	11, 17, 23, 29	первый	1892
Туэ	6	оба	1896
Тафельмахер	6	оба	1897
Линд	6	оба	1909
Мириманов	11, 17	первый	1909
Капферер	6, 10	оба	1913
Свифт	6	оба	1914
Кокотт	11	первый	1915
Фелл	11, 17, 23	первый	1943
Бройш	6, 10	оба	1960
Тержанян	14	оба	1974

$t = 2^r c, r \geqslant 2$, и соотношение $a^2b^2 - 2^{2r+2}c^2d^2 = 2^{2r}a^2c^2 + b^2d^2$. Следовательно,

$$5t^2d^2 = (a^2 - d^2)(b^2 - t^2), \tag{8.12}$$

поэтому d^2 делит $b^2 - t^2$, а $b^2 - t^2$ делит $5d^2$. С помощью того же рассуждения, что и раньше, рассмотрев сравнения по модулю 8, мы заключаем, что $b^2 - t^2 = d^2$. Отсюда следует, что $5t^2 = a^2 - d^2$, а значит,

$$b^2 = d^2 + t^2 \qquad \text{и} \qquad b^2 + 4t^2 = a^2. \tag{8.13}$$

Согласно утверждению (1A) существуют такие целые числа $m, n, r, s > 0$, что

$$\begin{cases} b = m^2 + n^2, \\ t = 2mn \end{cases} \tag{8.14}$$

и

$$\begin{cases} b = r^2 - s^2, \\ 2t = 2rs. \end{cases} \tag{8.15}$$

---

[7] Статья Ламе (1847) не содержит доказательств.

[8] Доказательство Тафельмахера (1892) справедливо лишь для первого случая; см. также Dickson, *History of the Theory of Numbers*, Vol. II, p. 755.

Итак, справедливы соотношения

$$r^2 - s^2 = m^2 + n^2 \tag{8.16}$$

и

$$rs = 2mn. \tag{8.17}$$

Так как $rs < xy$, полученные результаты опять противоречат выбору решения (x, y, u, v). □

С помощью этих фактов Бройш доказал следующий результат.

(8C) *Уравнение*

$$x^6 + y^6 = z^6$$

неразрешимо в натуральных числах.

Доказательство. Предположим противное. Пусть попарно взаимно простые натуральные числа x, y, z таковы, что $x^6 + y^6 = z^6$. Тогда x и y не могут одновременно быть кратными 3, а значит, можно считать, что $3 \nmid x$. Воспользуемся разложением на множители

$$x^6 = z^6 - y^6 = (z + y)(z - y)(z^2 + zy + y^2)(z^2 - zy + y^2).$$

Последние два множителя в этом произведении должны быть нечетными, так как числа y и z не являются одновременно четными. Более того, легко видеть, что каждый из множителей $z^2 + zy + y^2$ и $z^2 - zy + y^2$ взаимно прост с остальными множителями правой части (так как $3 \nmid x$). Следовательно, в силу единственности разложения целых чисел на простые множители

$$\begin{cases} z^2 + zy + y^2 = b^6, \\ z^2 - zy + y^2 = c^6, \end{cases}$$

где b, c — натуральные числа. Складывая и вычитая эти соотношения, получим $2(z^2 + y^2) = b^6 + c^6$ и $2zy = b^6 - c^6$. Но числа b и c нечетны, следовательно, $b^3 + c^3 = 2m$, $b^3 - c^3 = 2n$ (где $m > 0, n > 0$). Возводя эти равенства в квадрат и складывая, получим $b^6 + c^6 = 2(m^2 + n^2)$, а умножая, получим $b^6 - c^6 = 4mn$. Таким образом, $z^2 + y^2 = m^2 + n^2$, $zy = 2mn$. Согласно утверждению (8A) это невозможно. □

(8D) *Уравнение*

$$x^{10} + y^{10} = z^{10}$$

неразрешимо в натуральных числах.

Доказательство. Пусть x, y, z — попарно взаимно простые натуральные числа, такие, что $x^{10} + y^{10} = z^{10}$. Тогда x и y одновременно

не кратны 5, поэтому можно считать, что $5 \nmid x$. Разложим x^{10} на множители:

$$\begin{aligned} x^{10} &= z^{10} - y^{10} \\ &= (z+y)(z-y)(z^4 + z^3y + z^2y^2 + zy^3 + y^4) \\ &\quad \times (z^4 - z^3y + z^2y^2 - zy^3 + y^4). \end{aligned}$$

Последние два множителя в этом произведении должны быть нечетными, так как числа y и z не являются одновременно четными. Более того, легко видеть, что каждый из этих множителей взаимно прост с остальными множителями правой части (так как $5 \nmid x$). Следовательно, в силу единственности разложения целых чисел на простые множители

$$\begin{cases} z^4 + z^3y + z^2y^2 + zy^3 + y^4 = b^{10}, \\ z^4 - z^3y + z^2y^2 - zy^3 + y^4 = c^{10}, \end{cases}$$

где b и c — целые числа, $b > c > 0$. Складывая и вычитая эти соотношения, получим

$$2(z^4 + z^2y^2 + y^4) = b^{10} + c^{10}, \quad 2(z^3y + zy^3) = b^{10} - c^{10}.$$

Но числа b и c нечетны, поэтому $b^5 + c^5 = 2m$, $b^5 - c^5 = 2n$ (где $m > 0$, $n > 0$). Возводя эти равенства в квадрат и складывая, получим $b^{10} + c^{10} = 2(m^2 + n^2)$, а умножая, получим $b^{10} - c^{10} = 4mn$. Таким образом,

$$\begin{cases} z^4 + z^2y^2 + y^4 = m^2 + n^2, \\ zy(z^2 + y^2) = 2mn. \end{cases}$$

Теперь положим $z^2 + y^2 = r$, $zy = s$. Тогда $r^2 - s^2 = m^2 + n^2$, $rs = 2mn$, что невозможно согласно утверждению (8B). □

Дирихле (1832) доказал теорему Ферма для показателя 14 еще до того, как Ламе нашел доказательство для показателя 7. Также Дирихле доказал такой результат.

(8E) *Уравнение*

$$X^{14} - Y^{14} = 2^m 7^{1+n} Z^{14}$$

(*где* $m \geqslant 0, n \geqslant 0$) ***не имеет решений в отличных от нуля целых числах*** x, y, z, *где* x, y ***взаимно просты.***

Тержанян в 1974 г. доказал следующее утверждение.

(8F) *Пусть натуральное число a кратно 7 и не имеет простых делителей $p \equiv 1 \pmod 7$. Пусть, далее, взаимно простые натуральные числа x, y и целое неотрицательное число z таковы, что*

$$x^{14} - y^{14} = az^{14}.$$

Тогда $x = y = 1$ и $z = 0$.

Отсюда он вывел простое доказательство теоремы Ферма для показателя 14.

В 1885 г. Мэтьюс получил доказательство первого случая теоремы Ферма для показателей 11 и 17. В 1943 г. Фелл указал другое доказательство для показателя 11 и заявил, что его методом можно также разрешить первый случай для показателей 17 и 23.

Список литературы

1806 Kausler, C.F., *Nova demonstratio theorematis nec summam, nec differentiam duorum cubo-cuborum cubu-cubum esse posse*, Novi Acta Acad. Petrop., **15** (1806), 146–155.

1823 Legendre, A.M., *Recherches sur quelques objets d'analyse indéterminée, et particulièrement sur le théorème de Fermat*, Mém. Acad. Roy. Sci. Institut France, **6** (1823), 1–60; reprinted as the "Second Supplément" in 1825, to a printing of *Essai sur la Théorie des Nombres* (2^e édition), Courcier, Paris; reprinted in Sphinx-Oedipe, **4** (1909), 97–128.

1832 Dirichlet, G.L., *Démonstration du théorème de Fermat pour le cas des 14^e puissances*, J. Reine Angew. Math., **9** (1832), 390–393; reprinted in *Werke*, Vol. I, pp. 189–194, G. Reimer, Berlin, 1889; reprinted by Chelsea, New York, 1969.

1847 Lamé, G., *Troisième mémoire sur le dernier théorème de Fermat*, C. R. Acad. Sci. Paris, **24** (1847), 888.

1885 Matthews, G.B., *Note in connection with Fermat's last theorem*, Messenger Math., **15** (1886), 68–74.

1892 Tafelmacher, W.L.A., *Sobre el teorema de Fermat de que la ecuación $x^n + y^n = z^n$ no tiene solución en numeros enteros x, y, z, i siendo $n > 2$*, Ann. Univ. Chile, Santiago, **82** (1892), 271–300 and 415–437.

1896 Thue, A., *Über die Auflösbarkeit einiger unbestimmter Gleichungen*, Det Kongel. Norske Videnskabers Selskabs Skrifter, 1896, no. 7, 14 pp.; reprinted in *Selected Mathematical Papers*, pp. 19–30, Universitetsforlaget, Oslo, 1977.

1897 Tafelmacher, W.L.A., *La ecuación $x^3 + y^3 = z^2$: Una demonstración nueva del teorema de Fermat para el caso de las sestas potencias*, Ann. Univ. Chile, Santiago, **97** (1897), 63–80.
1909 Lind, B., *Einige zahlentheoretische Sätze*, Arch. Math. Phys., (3), **15** (1909), 368–369.
1909 Mirimanoff, D., *Sur le dernier théorème de Fermat*, L'Enseign. Math., **11** (1909), 49–51.
1911 Hayashi, T., *On Fermat's last theorem*, Indian Math. Club, Madras, **3** (1911), 111–114. Reprinted in Sci. Rep., Tôhoku Imp. Univ., (1), **1** (1911/2), 51–54.
1913 Kapferer, H., *Beweis des Fermatschen Satzes für die Exponenten* 6 *und* 10, Archiv Math. Phys., (3), **21** (1913), 143–146.
1914 Swift, E., *Solution to Problem 206*, Amer. Math. Monthly, **21** (1914), 238–239.
1915 Kokott, P., *Über einen Spezialfall des Fermatschen Satzes*, Arch. Math. Phys., (3), **24** (1915), 90–91.
1916 Swift, E., *Solution to Problem 209*, Amer. Math. Monthly, **23** (1916), 261.
1943 Fell, J., *Elementare Beweise des großen Fermatschen Satzes für einige besondere Fälle*, Deutsche Math., **7** (1943), 184–186.
1956 Brčić-Kostić, M., *Solution of the diophantine equation $x^4 + y^2 = z^6$* (in Serbo-Croatian, Esperanto summary), Bull. Soc. Math. Phys. Serbie, **8** (1956), 125–136.
1960 Breusch, R., *A simple proof of Fermat's last theorem for $n = 6$, $n = 10$*, Math. Mag., **33** (1960), 279–281.
1974 Terjanian, G., *L'équation $x^n + y^n = z^n$ pour $n = 5$ et $n = 14$*, Sém. Th. des Nombres, Bordeaux, 1973/4, exp. no. 5, 6 pp.
1974 Terjanian, G., *L'équation $x^{14} + y^{14} = z^{14}$ en nombres entiers*, Bull. Sci. Math., Sér. 2, **98** (1974), 91–95.

I.9. Приложение

Что скрывалось за «чудесным доказательством» Ферма?[9]

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. Оно представляет собой попытку применить

[9] Автор выражает признательность Э. Бомбьери, обратившему его внимание на эту проблему.

метод бесконечного спуска к уравнению Ферма, что и мог иметь в виду сам Ферма.

Но 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 $d =$ НОД(x, z). Тогда $d = c^{n-2}/2$, потому что НОД$(ab, c) = 1$. Положим $x = dx'$, $z = dz'$. Тогда x' кратно 4, 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 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 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.

Глава II

4 эпизода

В этой главе мы обсудим ряд вопросов, которые нам потребуются в дальнейшем. Разумеется, они представляют значительный интерес не только в связи с последней теоремой Ферма.

II.1. p-адическое нормирование

Пусть p — простое число, целое число a отлично от нуля и $v_p(a)$ — показатель степени числа p в разложении числа a в произведение степеней простых чисел:

$$a = p^{v_p(a)} b, \quad \text{где } p \nmid b.$$

Величина $v_p(a)$ называется *p-адическим значением* числа a. Будем считать, что $v_p(0) = \infty$.

Легко видеть, что

$$\begin{cases} v_p(ab) = v_p(a) + v_p(b); \\ v_p(a+b) \geqslant \min\{v_p(a), v_p(b)\}; \\ \text{если } v_p(a) < v_p(b_1), v_p(b_2), \ldots, v_p(b_k), \\ \qquad \text{то } v_p(a + b_1 + b_2 + \ldots + b_k) = v_p(a). \end{cases} \tag{1.1}$$

Если $v_p(a) = e \geqslant 1$, то будем говорить, что p^e есть точная степень числа p, делящая a, и писать $p^e \parallel a$.

Вообще, если НОД$(a, a') = 1$, $a' > 0$, положим $v_p(a/a') = v_p(a) - v_p(a')$. Тогда для всех рациональных чисел r, s также выполнены свойства (1.1). Отображение $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ называют *p-адическим нормированием* поля $\mathbb{Q}$.

Будем говорить, что число $r = a/a'$ является *p-целым*, если $v_p(r) \geqslant 0$. Ясно, что каждое целое число суть p-целое (для всякого простого числа p). Множество $\mathbb{Z}_p$ всех p-целых рациональных чисел есть подкольцо в поле рациональных чисел $\mathbb{Q}$. Опишем это подкольцо в явном виде: $r \in \mathbb{Z}_p$ тогда и только тогда, когда $r = 0$ или $r = p^k a/b$, где $k \geqslant 0$, $b > 0$, НОД$(a, b) = 1$, $p \nmid a$ и $p \nmid b$.

Если $r, s \in \mathbb{Q}$, $e \geqslant 1$ и $v_p(r-s) \geqslant e$, то будем писать $r \equiv s \pmod{p^e}$ и говорить, что p^e делит $r-s$ (в $\mathbb{Z}_p$). Это отношение сравнения удовлетворяет обычным свойствам сравнений целых чисел по модулю натурального числа.

Ясно также, что рациональное число r принадлежит $\mathbb{Z}$ тогда и только тогда, когда r является p-целым для всякого простого числа p.

Мы приведем два результата, которые имеют множество приложений. Для каждого действительного числа x обозначим через $[x]$ единственное целое число, такое, что $[x] \leqslant x < [x]+1$. Величина $[x]$ называется *целой частью* от x.

В 1808 г. Лежандр нашел формулу для точной степени p^m простого числа p, которая делит $a!$ (тогда p^{m+1} не делит $a!$). Существует замечательное выражение для m в терминах p-адического разложения числа a:

$$a = a_k p^k + a_{k-1} p^{k-1} + \ldots + a_1 p + a_0,$$

где $p^k \leqslant a < p^{k+1}$ и $0 \leqslant a_i \leqslant p-1$ (при $i = 0, 1, \ldots, k$). Целые числа $a_0, a_1, \ldots, a_k$ являются цифрами числа a по основанию p.

Рассмотрим, например, основание 5. Мы можем записать $328 = 2 \times 5^3 + 3 \times 5^2 + 3$, а значит, цифры числа 328 по основанию 5 суть 2, 3, 0, 3. Используя введенные обозначения, запишем следующий результат.

(1A) *Если $a \geqslant 1$, то $v_p(a!) = m$, где*

$$m = \sum_{i=1}^{\infty} \left[\frac{a}{p^i}\right] = \frac{a - (a_0 + a_1 + \ldots + a_k)}{p-1}.$$

Доказательство. По определению $a! = p^m b$, причем $p \nmid b$. Разделим a на p с остатком: $a = q_1 p + r_1$, где $0 \leqslant q_1$, $0 \leqslant r_1 < p$. Это означает, что $q_1 = [a/p]$. Целые числа, кратные p и не превосходящие a, имеют вид $p, 2p, \ldots, q_1 p \leqslant a$. Следовательно, $p^{q_1}(q_1!) = p^m b'$, где $p \nmid b'$. Таким образом, $q_1 + m_1 = m$, где p^{m_1} есть точная степень числа p, делящая $q_1!$. Так как $q_1 < a$, по индукции получаем

$$m_1 = \left[\frac{q_1}{p}\right] + \left[\frac{q_1}{p^2}\right] + \left[\frac{q_1}{p^3}\right] + \ldots$$

Но несложно проверить, что

$$\left[\frac{q_1}{p^i}\right] = \left[\frac{[a/p]}{p^i}\right] = \left[\frac{a}{p^{i+1}}\right].$$

Поэтому

$$m = \left[\frac{a}{p}\right] + \left[\frac{a}{p^2}\right] + \left[\frac{a}{p^3}\right] + \dots$$

Теперь выведем еще одно равенство, связанное с p-адическими цифрами числа $a = a_k p^k + \dots + a_1 p + a_0$. Из соотношений

$$\begin{aligned}
\left[\frac{a}{p}\right] &= a_k p^{k-1} + \dots + a_1, \\
\left[\frac{a}{p^2}\right] &= a_k p^{k-2} + \dots + a_2, \\
&\vdots \\
\left[\frac{a}{p^k}\right] &= a_k
\end{aligned}$$

следует, что

$$\begin{aligned}
\sum_{i=0}^{\infty} \left[\frac{a}{p^i}\right] &= a_1 + a_2(p+1) + a_3(p^2+p+1) + \dots \\
&\quad + a_k(p^{k-1} + p^{k-2} + \dots + p + 1) \\
&= \frac{1}{p-1}\{a_1(p-1) + a_2(p^2-1) + \dots + a_k(p^k-1)\} \\
&= \frac{1}{p-1}\{a - (a_0 + a_1 + \dots + a_k)\}. \quad \square
\end{aligned}$$

В 1852 г. Куммер воспользовался результатом Лежандра и определил точную степень p^m числа p, делящую биномиальный коэффициент

$$\binom{a+b}{a} = \frac{(a+b)!}{a!\,b!},$$

где $a \geqslant 1$, $b \geqslant 1$.

(1B) *Точная степень числа p, делящая $\binom{a+b}{a}$, равна $\varepsilon_0+\varepsilon_1+\dots+\varepsilon_t$, то есть числу «переносов» при сложении чисел a и b, записанных по основанию p.*

Доказательство. Пусть

$$\begin{aligned}
a &= a_0 + a_1 p + \dots + a_t p^t, \\
b &= b_0 + b_1 p + \dots + b_t p^t,
\end{aligned}$$

где $0 \leqslant a_i \leqslant p-1$, $0 \leqslant b_i \leqslant p-1$, причем или $a_t \neq 0$, или $b_t \neq 0$. Пусть $S_a = \sum_{i=0}^{t} a_i$, $S_b = \sum_{i=0}^{t} b_i$ — суммы p-адических цифр чисел

a и b. Определим последовательно числа c_i, $0 \leqslant c_i \leqslant p-1$, и $\varepsilon_i = 0$ или 1 из следующих соотношений:

$$\begin{aligned} a_0 + b_0 &= \varepsilon_0 p + c_0, \\ \varepsilon_0 + a_1 + b_1 &= \varepsilon_1 p + c_1, \\ \varepsilon_1 + a_2 + b_2 &= \varepsilon_2 p + c_2, \\ &\vdots \\ \varepsilon_{t-1} + a_t + b_t &= \varepsilon_t p + c_t. \end{aligned}$$

Последовательно умножив эти уравнения на $1, p, p^2, \ldots$ и сложив, получим

$$\begin{aligned} a + b + \varepsilon_0 p + \varepsilon_1 p^2 + \ldots + \varepsilon_{t-1} p^t &= \varepsilon_0 p + \varepsilon_1 p^2 + \ldots + \varepsilon_t p^{t+1} \\ &\quad + c_0 + c_1 p + \ldots + c_t p^t. \end{aligned}$$

Таким образом, $a + b = c_0 + c_1 p + \ldots + c_t p^t + \varepsilon_t p^{t-1}$, а это и есть запись числа $a+b$ по основанию p. Аналогично, складывая эти уравнения, получим

$$S_a + S_b + (\varepsilon_0 + \varepsilon_1 + \ldots + \varepsilon_{t-1}) = (\varepsilon_0 + \varepsilon_1 + \ldots + \varepsilon_t)p + S_{a+b} - \varepsilon_t.$$

Согласно результату Лежандра

$$\begin{aligned} (p-1)m &= (a+b) - S_{a+b} - a + S_a - b + S_b \\ &= (p-1)(\varepsilon_0 + \varepsilon_1 + \ldots + \varepsilon_t). \end{aligned}$$

Отсюда следует результат Куммера. □

Эта теорема Куммера была заново доказана Люка в 1878 г. В 1991 г. Фресней обобщил результат, заменив целые числа на p-адические целые числа[1].

Приведенные теоремы Лежандра и Куммера нашли множество приложений в так называемом *p-адическом анализе*.

Список литературы

1808 Legendre, A.M., *Essai sur la Théorie des Nombres* (2^e édition), Courcier, Paris, 1808.

1852 Kummer, E.E., *Über die Ergänzungssätze zu den allgemeinen Reziprozitätsgesetzen*, J. Reine Angew. Math., **44** (1852), 93–146; reprinted in *Collected Papers*, Vol. I (editor A. Weil), pp. 485–538, Springer-Verlag, New York, 1975.

[1] Вероятно, этот результат до сих пор не опубликован; автор использовал препринт.

1878 Lucas, E., *Sur les congruences des nombres eulériens et des coefficients différentiels*, Bull. Soc. Math. France, **6** (1878), 49–54.

II.2. Многочлены деления круга

Пусть $n \geqslant 1$ и $\zeta_n = \cos(2\pi/n) + i\sin(2\pi/n)$. Тогда $\zeta_1 = 1$, $\zeta_2 = -1$, $\zeta_3 = (-1 + i\sqrt{3})/2$, $\zeta_4 = i$, $\zeta_5 = \cos 72° + i \sin 72°$, $\zeta_6 = (1 + i\sqrt{3})/2$ и т. д.

Все степени числа ζ_n также являются корнями n-й степени из 1, а это значит, что они являются корнями многочлена $X^n - 1$. Пусть ω — произвольный корень n-й степени из 1. Наименьшее натуральное число d, такое, что $\omega^d = 1$, называется порядком корня ω из единицы. Тогда непременно d делит n. Будем говорить, что число ω является примитивным корнем степени d из 1.

Все степени ζ_n^j при $j = 1, 2, \ldots, n$ различны, причем $\zeta_n^n = 1$, а значит, ζ_n есть примитивный корень из единицы порядка n. Так как существует в точности n корней степени n из 1, каждый из них является степенью ζ_n^j. Более того, как легко видеть, ζ_n^j есть примитивный корень степени n из 1 тогда и только тогда, когда НОД $(j, n) = 1$. Таким образом, число примитивных корней степени n из 1 равно $\varphi(n)$, где φ обозначает функцию Эйлера.

Многочленом деления круга степени n называют выражение вида

$$\Phi_n(X) = \prod_{\text{НОД}\,(j,n)=1} (X - \zeta_n^j) \tag{2.1}$$

(произведение берется по всем j, $1 \leqslant j \leqslant n$, НОД $(j, n) = 1$). Это многочлен степени $\varphi(n)$ со старшим коэффициентом единица (в дальнейшем такие многочлены будут называться *приведенными*). Так как этот многочлен инвариантен относительно перестановок его корней, согласно теории Галуа его коэффициенты являются целыми числами.

Сгруппировав корни степени n из 1 согласно их порядку, получим

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{2.2}$$

Отсюда следует (это можно доказать и непосредственно), что

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \ldots + X + 1, \tag{2.3}$$

$$\Phi_{p^e}(X) = \frac{X^{p^e}-1}{X^{p^{e-1}}-1} \tag{2.4}$$
$$= X^{p^{e-1}(p-1)} + X^{p^{e-1}(p-2)} + \ldots + X^{p^{e-1}} + 1$$

для всех простых чисел p и $e \geqslant 1$. Следовательно, для $m \mid n$ и $m \neq n$ справедливо равенство

$$X^n - 1 = (X^m - 1)\Phi_n(X) \prod_d \Phi_d(X) \tag{2.5}$$

(произведение берется по всем d, $1 \leqslant d < n$, $d \mid n$, $d \nmid m$).

Обозначим через *μ функцию Мёбиуса*

$$\mu(p_1 \ldots p_r) = \begin{cases} (-1)^r, & \text{если все простые числа } p_i \text{ различны,} \\ 0 & \text{в противном случае.} \end{cases} \tag{2.6}$$

Тогда

$$\Phi_n(X) = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)}. \tag{2.7}$$

Отметим следующее свойство: если простое число p делит m, то

$$\Phi_{pm}(X) = \Phi_m(X^p) \quad (\text{при } p \mid m). \tag{2.8}$$

Если же p не делит m и $s \geqslant 1$, то

$$\Phi_{p^s m}(X) = \frac{\Phi_m(X^{p^s})}{\Phi_m\left(X^{p^{s-1}}\right)} \quad (\text{при } p \nmid m,\ s \geqslant 1). \tag{2.9}$$

Теперь рассмотрим соответствующие однородные многочлены двух переменных. Пусть

$$\Phi_n(X, Y) = Y^{\varphi(n)} \Phi_n\left(\frac{X}{Y}\right). \tag{2.10}$$

Тогда

$$X^n - Y^n = \prod_{d|n} \Phi_d(X, Y). \tag{2.11}$$

Если $m \mid n$ и $m \neq n$, то

$$X^n - Y^n = (X^m - Y^m)\Phi_n(X, Y) \prod_d \Phi_d(X, Y) \tag{2.12}$$

(произведение берется по всем d, $1 \leqslant d < n$, $d \mid n$, $d \nmid m$). Также справедливо равенство

$$\Phi_n(X, Y) = \prod_{d|n} \left(X^{n/d} - Y^{n/d}\right)^{\mu(d)}, \tag{2.13}$$

и, как и выше,

$$\Phi_{pm}(X,Y) = \Phi_m(X^p, Y^p) \qquad (\text{при } p \mid m), \tag{2.14}$$

$$\Phi_{p^s m}(X,Y) = \frac{\Phi_m\left(X^{p^s}, Y^{p^s}\right)}{\Phi_m\left(X^{p^{s-1}}, Y^{p^{s-1}}\right)} \qquad (\text{при } p \nmid m,\ s \geqslant 1). \tag{2.15}$$

II.3. Делители биномов

Пусть a и b — отличные от нуля различные целые числа. В этом разделе мы рассмотрим биномы $a^n \pm b^n$, а также целые числа вида $(a^n - b^n)/(a-b)$ и обсудим вопрос об их делителях.

(ЗА) *Пусть a, b — отличные от нуля различные целые числа. Тогда*

(1) *если $p \neq 2$, $p \nmid ab$ и $v_p(a-b) = e \geqslant 1$, то $v_p\left(a^{p^r} - b^{p^r}\right) = e + r$ для каждого натурального числа r;*

(2) *если $2 \nmid ab$ и $v_2(a-b) = e \geqslant 2$, то $v_2\left(a^{2^r} - b^{2^r}\right) = e + r$ для каждого натурального числа r;*

(3) *если простое число p делит $a^p - b^p$, то и $p^2 \mid (a^p - b^p)$.*

Доказательство. (1) Достаточно показать, что $v_p(a^p - b^p) = e+1$, а затем повторить это рассуждение. Согласно предположению $a = b + kp^e$, где $p \nmid k$, следовательно,

$$a^p = b^p + \binom{p}{1} b^{p-1} k p^e + \binom{p}{2} b^{p-2} k^2 p^{2e} + \ldots + k^p p^{pe}.$$

Так как p делит $\binom{p}{j}$ при $j = 1, \ldots, p-1$, мы получаем

$$v_p\left[\binom{p}{j} b^{p-j} k^j p^{je}\right] \geqslant 1 + je.$$

Поскольку $v_p(k^p p^{pe}) = pe$, мы заключаем, что $v_p(a^p - b^p) = e + 1$.

(2) Как и в случае (1), достаточно показать, что $v_2(a^2 - b^2) = e + 1$. Согласно предположению $a = b + 2^e k$, где $e \geqslant 2$ и числа a, b, k нечетны. Тогда $a^2 = b^2 + 2^{e+1} kb + 2^{2e} k^2$ и, так как $e + 1 < 2e$, мы получаем $v_2(a^2 - b^2) = e + 1$.

(3) Согласно предположению $a \equiv a^p \equiv b^p \equiv b \pmod p$. Возводя это сравнение в p-ю степень, получим $a^p \equiv b^p \pmod{p^2}$, а значит, $p^2 \mid (a^p - b^p)$. □

Если $n \geqslant 1$ и отличные от нуля целые числа a, b различны, положим

$$Q_n(a,b) = \frac{a^n - b^n}{a-b} = \sum_{k=0}^{n-1} a^k b^{n-1-k} \tag{3.1}$$

и будем также считать, что $Q_0(a,b) = 0$. Представим $Q_n(a,b)$ $(n \geqslant 1)$ в следующем виде:

$$\begin{aligned} Q_n(a,b) &= \frac{[(a-b)+b]^n - b^n}{a-b} \qquad (3.2)\\ &= (a-b)^{n-1} + \binom{n}{1}(a-b)^{n-2}b + \ldots \\ &\quad + \binom{n}{n-2}(a-b)b^{n-2} + nb^{n-1} \\ &= (a-b)e + nb^{n-1}, \end{aligned}$$

где $e \in \mathbb{Z}$. Далее, если $n = p$ — простое число, то

$$Q_p(a,b) = (a-b)^{p-1} + pf, \tag{3.3}$$

где $f \in \mathbb{Z}$.

Укажем теперь ряд свойств целых чисел $Q_n(a,b)$. До 1729 г. Жакме установил нижеследующее свойство (5) в случае, когда n равно нечетному простому числу p. Эйлер в 1738 г. показал, что если p — нечетное простое число и $a > 1$, то НОД $(Q_p(a,\pm 1), a \pm 1) = = 1$ или p; если p делит $a \pm 1$, то $v_p(Q_p(a,\pm 1)) = 1$; более того, если $p \neq 3$, $a \neq 2$, то $Q_p(a,\pm 1)$ нечетно и больше чем 1.

В 1769 г. Лагранж установил нижеследующее свойство (4), а также (6) в случае, когда n равно простому числу p. В 1837 г. Куммер доказал (4) в случае, если $n = p$ — простое число. В 1888 г. Сильвестр доказал частный случай утверждения (3). В 1897 г. Ф. Люка доказал частные случаи утверждений (5) и (6). Позднее свойства (4), (5), (6) и (7) были установлены Инкери (1946) и Виванти (1947). Большинство утверждений в той же самой форме, в которой они приводятся ниже, можно найти в статье Мёллера (1955).

(3В) *Пусть $n > m \geqslant 1$, целые числа a, b отличны от нуля и различны. Тогда*

(1) *если $n = mq + r$, где $r \geqslant 0$, то*

$$Q_n(a,b) = a^r Q_q(a^m, b^m) Q_m(a,b) + b^{mq} Q_r(a,b);$$

если $n = mq - r$, *где* $r \geqslant 0$, *то*

$$Q_n(a,b) = \left[a^{m-r}Q_{q-1}(a^m,b^m) + b^{n-m}\right]Q_m(a,b) - a^{m-r}b^{n-m}Q_r(a,b).$$

***Пусть**, далее,* a, b — *взаимно простые числа. Тогда*

(2) *если* $d = \text{НОД}(n,m)$, *то* $Q_d(a,b) = \text{НОД}\,(Q_n(a,b),\, Q_m(a,b))$;

(3) $\prod_{p|n} Q_p(a,b)$ *делит* $Q_n(a,b)$;

(4) $\text{НОД}\,(Q_n(a,b), a-b) = \text{НОД}\,(n,\, a-b)$;

(5) *если* $p \mid (a-b)$, $p \nmid n$, *то* $p \nmid Q_n(a,b)$;

(6) *если нечетное простое число* p *делит* $a-b$, *то* $v_p\,(Q_n(a,b)) = v_p(n)$;

(7) *если* $4 \mid (a-b)$, *то* $v_2\,(Q_n(a,b)) = v_2(n)$;
если $2 \parallel (a-b)$, *но* $4 \nmid (a-b)$, *то* $v_2\,(Q_n(a,b)) \geqslant v_2(n)$;

(8) *если* n *нечетно, то* $Q_n(a,b)$ *нечетно*;

(9) *если* n *нечетно и* $e > 0$, *то* $\text{НОД}\,(Q_n(a,b),\, a^{2^e n} + b^{2^e n}) = 1$;

(10) *если каждый простой делитель числа* n *делит* $a-b$, *то произведение* $n(a-b)$ *делит* $a^n - b^n$.

Доказательство. (1) Пусть $n = mq + r$. Тогда

$$Q_n(a,b) = \frac{a^{mq+r} - b^{mq+r}}{a-b}$$

$$= \frac{a^{mq+r} - a^r b^{mq} + a^r b^{mq} - b^{mq+r}}{a-b}$$

$$= a^r \times \frac{a^{mq} - b^{mq}}{a-b} + \frac{a^r - b^r}{a-b} \times b^{mq}$$

$$= a^r \times \frac{a^{mq} - b^{mq}}{a^m - b^m} \times \frac{a^m - b^m}{a-b} + \frac{a^r - b^r}{a-b} \times b^{mq}$$

$$= a^r Q_q(a^m,\, b^m) Q_m(a,b) + Q_r(a,b) b^{mq}.$$

Пусть теперь $n = mq - r$. Тогда

$$\left[a^{m-r}Q_{q-1}(a^m, b^m) + b^{n-m}\right] Q_m(a,b) - a^{m-r}b^{n-m}Q_r(a,b)$$

$$= a^{m-r}\frac{a^{(q-1)m} - b^{(q-1)m}}{a^m - b^m} \times \frac{a^m - b^m}{a-b} + b^{n-m} \times \frac{a^m - b^m}{a-b}$$

$$-a^{m-r}b^{n-m}\frac{a^r - b^r}{a-b}$$

$$= \frac{a^n - a^{m-r}b^{(q-1)m} + a^m b^{n-m} - b^n - a^m b^{n-m} + a^{m-r}b^{n-m+r}}{a-b}$$

$$= \frac{a^n - b^n}{a-b} = Q_n(a,b).$$

(2) Так как числа a и b взаимно просты, a и b также взаимно просты и с числами $Q_k(a,b) = a^{k-1} + a^{k-2}b + \ldots + ab^{k-2} + b^{k-1}$ для каждого $k \geqslant 1$. Из утверждения (1) следует, что $Q_d(a,b)$ делит $Q_n(a,b)$ и $Q_m(a,b)$. Пусть натуральные числа r и s таковы, что $d = sm - rn$ (или $d = rn - sm$). Тогда $sm = rn + d$ и в силу утверждения (1) мы получаем

$$Q_s(a^m, b^m)Q_m(a,b) = Q_{sm}(a,b) = a^d Q_r(a^n, b^n)Q_n(a,b) + b^{rn}Q_d(a,b).$$

Если t делит $Q_m(a,b)$ и $Q_n(a,b)$, то t делит $b^{rn}Q_d(a,b)$; но $Q_m(a,b)$ и b взаимно просты, следовательно, $t \mid Q_d(a,b)$, что и требовалось доказать.

(3) Согласно утверждению (2) целые числа $Q_p(a,b)$ (для всех простых чисел p, делящих n) попарно взаимно просты. Из утверждения (1) следует, что если $p \mid n$, то $Q_p(a,b)$ делит $Q_n(a,b)$. Таким образом, $\prod_{p|n} Q_p(a,b)$ делит $Q_n(a,b)$.

(4) Так как НОД$(a,b) = 1$, из соотношений (3.2) следует, что НОД$(Q_n(a,b),\, a-b) =$ НОД$(n,\, a-b)$.

(5) Это очевидное следствие свойства (4).

(6) Пусть $n = p^r m$, $p \nmid m$, $r \geqslant 0$, так что $v_p(n) = r$. Пусть $a_1 = a^m$, $b_1 = b^m$. Так как $p \mid (a-b)$, из утверждения (5) следует, что p не делит $Q_m(a,b) = (a^m - b^m)/(a-b) = (a_1 - b_1)/(a-b)$, а значит, $v_p(a_1 - b_1) = v_p(a-b) \geqslant 1$. Следовательно, $v_p\left(a_1^{p^r} - b_1^{p^r}\right) = v_p(a_1 - b_1) + r$. Таким образом,

$$v_p\left(Q_n(a,b)\right) = v_p\left(\frac{a_1^{p^r} - b_1^{p^r}}{a_1 - b_1}\right) + v_p\left(\frac{a_1 - b_1}{a-b}\right) = r = v_p(n).$$

(7) Пусть $n = 2^r m$, $2 \nmid m$, $r \geqslant 0$, так что $v_2(n) = r$. Пусть $a_1 = a^m$, $b_1 = b^m$. Как и при доказательстве утверждения (6), мы получаем $v_2(a_1 - b_1) = v_2(a - b) = e \geqslant 1$. Если $e \geqslant 2$, то $v_2\left(a_1^{2^r} - b_1^{2^r}\right) = e + r$, а значит,

$$v_2\left(Q_n(a,b)\right) = v_2\left(\frac{a_1^{2^r} - b_1^{2^r}}{a_1 - b_1}\right) + v_2\left(\frac{a_1 - b_1}{a - b}\right) = r = v_2(n).$$

Однако если $e = 1$, то $v_2\left(a_1^{2^r} - b_1^{2^r}\right) \geqslant r + 1$ (причем неравенство может быть строгим). Итак, мы можем заключить лишь, что $v_2\left(Q_n(a,b)\right) \geqslant v_2(n)$.

(8) Если $a \not\equiv b \pmod 2$, то $a^n \not\equiv b^n \pmod 2$, следовательно, $Q_n(a,b)$ нечетно. Если $a \equiv b \pmod 2$, то, поскольку числа a и b взаимно просты, они нечетны. Отсюда следует, что число $Q_n(a,b) = a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}$ является суммой нечетного числа нечетных слагаемых, а значит, оно нечетно.

(9) Пусть p — простое число, $r \geqslant 1$, причем $p^r \mid Q_n(a,b)$, $p^r \mid \left(a^{2^e n} + b^{2^e n}\right)$. Из утверждения (7) следует, что $p \neq 2$. Так как $p^r \mid (a^n - b^n)$, справедливо сравнение $a^{2^e n} \equiv b^{2^e n} \pmod{p^r}$, следовательно, $p^r \mid 2a^{2^e n}$. Таким образом, p делит a, а значит, и b, что невозможно.

(10) Пусть p — произвольный простой делитель числа n. По предположению $p \mid (a - b)$, поэтому в соответствии с утверждениями (6) или (7) мы получаем $v_p(n) \leqslant v_p\left(Q_n(a,b)\right)$, а следовательно, $v_p(n(a-b)) \leqslant v_p(Q_n(a,b)(a-b)) = v_p(a^n - b^n)$. Так как p произвольно, это значит, что $n(a-b)$ делит $a^n - b^n$. □

Приведем теперь еще один результат, принадлежащий Инкери (1946).

(3С) *Пусть простое число p нечетно, $n \geqslant 1$ и отличные от нуля взаимно простые целые числа a, b таковы, что $a \neq b$. Тогда*

(1) $Q_{p^n}(a,b) = \prod_{m=1}^{n} Q_p(a^{p^{m-1}}, b^{p^{m-1}})$;

(2) *если p не делит $a^{p^n} - b^{p^n}$, то целые числа $a - b$, $Q_p(a,b)$, $Q_p(a^p, b^p), \ldots, Q_p(a^{p^{n-1}}, b^{p^{n-1}})$ попарно взаимно просты;*

(3) *если $p \mid \left(a^{p^n} - b^{p^n}\right)$ и целые числа i, j таковы, что $1 \leqslant i < j \leqslant n$, то*

$$\text{НОД}\left(Q_p\left(a^{p^{i-1}}, b^{p^{i-1}}\right), Q_p\left(a^{p^{j-1}}, b^{p^{j-1}}\right)\right) = p,$$

$$\text{НОД}\left(a - b, Q_p\left(a^{p^{i-1}}, b^{p^{i-1}}\right)\right) = p;$$

(4) *если* $v_p\left(a^{p^n}-b^{p^n}\right)=e\geqslant 1$, *то* $e\geqslant n+1$ *и*

$$v_p(a-b)=e-n.$$

Доказательство. (1) Нетрудно видеть, что

$$Q_{p^n}(a,b)=\prod_{m=1}^{n}\frac{a^{p^m}-b^{p^m}}{a^{p^{m-1}}-b^{p^{m-1}}}=\prod_{m=1}^{n}Q_p\left(a^{p^{m-1}},\,b^{p^{m-1}}\right).$$

(2) Запишем соотношение $a^{p^n}-b^{p^n}=q_0q_1\ldots q_n$, где $q_0=a-b$,

$$q_j=\frac{a^{p^j}-b^{p^j}}{a^{p^{j-1}}-b^{p^{j-1}}}=Q_p\left(a^{p^{j-1}},b^{p^{j-1}}\right).$$

Согласно предположению $p\nmid q_j$ (при $j=0,1,\ldots,n$). Если l — простое число, делящее q_i,q_j (где $0\leqslant i<j\leqslant n$), то $l\neq p$ и $l\mid\left(a^{p^i}-b^{p^i}\right)$. Но так как

$$Q_{p^{j-i}}\left(a^{p^i},b^{p^i}\right)=\frac{a^{p^j}-b^{p^j}}{a^{p^i}-b^{p^i}}=q_{i+1}q_{i+2}\cdots q_j,$$

l делит $Q_{p^{j-1}}(a^{p^i},b^{p^i})$ и из утверждения (3В)(4) следует, что $l=p$. Итак, мы получили противоречие.

(3) Предположим, что l — простое число, $e\geqslant 1$, причем l^e делит q_i и q_j $(0\leqslant i<j\leqslant n)$. Тогда l^e делит бином $a^{p^i}-b^{p^i}$, а также и бином $a^{p^{j-1}}-b^{p^{j-1}}=(a^{p^i}-b^{p^i})q_{i+1}\ldots q_{j-1}$. Так как l^e делит $Q_p(a^{p^{j-1}},b^{p^{j-1}})=q_j$, согласно утверждению (3В)(4) мы можем заключить, что l^e делит p, а значит, $l^e=p$.

(4) Если p делит $a^{p^n}-b^{p^n}$, то $p\nmid a$, $p\nmid b$. Из сравнений

$$a^{p^{n-1}}\equiv\left(a^{p^{n-1}}\right)^p\equiv\left(b^{p^{n-1}}\right)^p\equiv b^{p^{n-1}}\pmod p$$

следует, что $p\mid\left(a^{p^{n-1}}-b^{p^{n-1}}\right)$. По утверждению (3В)(6) мы имеем равенство $v_p(Q_p(a^{p^{n-1}},b^{p^{n-1}}))=1$, а значит, $v_p(a^{p^{n-1}}-b^{p^{n-1}})=e-1$, где $e-1\geqslant 1$. Повторяя это рассуждение, получим $v_p(a-b)=e-n$, где $e\geqslant n+1$. □

Впоследствии нам потребуется следующая оценка.

(3D) *Пусть число* n *нечетно,* $n\geqslant 3$ *и отличные от нуля различные целые числа* a,b *таковы, что* $a+b\geqslant 1$. *Тогда* $Q_n(a,b)\geqslant n$, *причем равенство достигается лишь при* $n=3$, $a=2$, $b=-1$ *или* $n=3$, $a=-1$, $b=2$.

Доказательство. Так как $Q_n(a,b) = Q_n(b,a)$ и $a \neq b$, без ограничения общности можно считать, что $a > b$. Если $b \geqslant 1$, то

$$Q_n(a,b) = a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1} > 1 + 1 + \ldots + 1 = n.$$

Если $b \leqslant -1$, то $a \geqslant 1 - b \geqslant 2$, $b^2 \geqslant 1$ и

$$\begin{aligned} Q_n(a,b) &= (a+b)(a^{n-2} + a^{n-4}b^2 + \ldots + ab^{n-3}) + b^{n-1} \\ &\geqslant 2^{n-2} + 2^{n-4} + \ldots + 2 + 1 \\ &= 2\left(4^{(n-3)/2} + 4^{(n-5)/2} + \ldots + 1\right) + 1 \\ &= 2 \cdot \frac{4^{(n-1)/2} - 1}{4-1} + 1 = \frac{2}{3}\left(2^{n-1} - 1\right) + 1 \\ &= \frac{2^n + 1}{3} \geqslant n \end{aligned}$$

при $n \geqslant 3$. Если $Q_n(a,b) = n$, то мы всюду имеем равенство, следовательно, $n = 3$, $a = 2$, $b = -1$. В силу симметрии $Q_n(a,b) = n$ также при $n = 3$, $a = -1$, $b = 2$. □

Отметим, что если p — нечетное простое число и $a > b \geqslant 1$, то $Q_p(a,b) > p$. Это утверждение является частным случаем доказанного результата, но может быть получено и непосредственно, так как $Q_p(a,b) = a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1} > p$.

Перед тем как перейти к дальнейшему изложению, сделаем ряд замечаний. Если $1 \leqslant b < a$, то из соотношения (2.13) следует, что $\Phi_n(a,b) > 0$. Если n нечетно, $n \geqslant 3$ и числа a и b не являются одновременно четными, то $\Phi_n(a,b)$ нечетно. Далее, если n нечетно, $n \geqslant 3$ и числа a и b не являются одновременно четными, то $\Phi_{2n}(a,b) = \Phi_n(-a,b)$ нечетно.

Пусть a и b — различные взаимно простые целые числа, отличные от нуля, и $n \geqslant 1$. Будем говорить, что простое число p является *примитивным делителем* бинома $a^n - b^n$ (соответственно $a^n + b^n$), если p делит $a^n - b^n$ (соответственно $a^n + b^n$), но не делит $a^m - b^m$ (соответственно $a^m + b^m$) для каждого показателя m, $1 \leqslant m < n$. Прежде всего отметим, что если 2 является примитивным делителем бинома $a^n \pm b^n$, то $n = 1$, так как $a \equiv b \pmod 2$.

Далее докажем следующий результат.

(3E) *Если $n \geqslant 2$, то p является примитивным делителем бинома $a^n + b^n$ тогда и только тогда, когда p есть примитивный делитель бинома $a^{2n} - b^{2n}$.*

Доказательство. Если p — примитивный делитель бинома $a^{2n}-b^{2n}$, то $p \nmid (a^n-b^n)$, а значит, $p \mid (a^n+b^n)$; более того, если $p \mid \left(a^k+b^k\right)$, где $1 \leqslant k \leqslant n$, то $p \mid \left(a^{2k}-b^{2k}\right)$, следовательно. $2k=2n$, так что p есть примитивный делитель бинома a^n+b^n.

Обратно, если p является примитивным делителем бинома a^n+ $+b^n$ (где $n \geqslant 2$), то $p \neq 2$ и $p \mid \left(a^{2n}-b^{2n}\right)$. Если $1 \leqslant k < 2n$ и $p \mid \left(a^k-b^k\right)$, то положим $k=2^e m$, где $e \geqslant 1$ и m нечетно. Тогда

$$a^k-b^k=\left(a^{2^{e-1}m}-b^{2^{e-1}m}\right)\left(a^{2^{e-1}m}+b^{2^{e-1}m}\right).$$

Так как $2^{e-1}m < n$, согласно предположению $p \nmid \left(a^{2^{e-1}m}+b^{2^{e-1}m}\right)$, а значит, $p \mid \left(a^{2^{e-1}m}-b^{2^{e-1}m}\right)$. Повторив это рассуждение, получим, что p делит a^m-b^m, где m нечетно. Таким образом, $a^m \equiv b^m \pmod p$ и $a^n \equiv -b^n \pmod p$. Тогда $a^{mn} \equiv b^{mn} \pmod p$, $a^{nm} \equiv$ $\equiv -b^{nm} \pmod p$, следовательно, $p \mid b$ (потому что $p \neq 2$), а значит, $p \mid a$, что противоречит предположению. Итак, p является примитивным делителем бинома $a^{2n}-b^{2n}$. □

Теперь мы с легкостью можем доказать следующее утверждение.

(3F) *Пусть a, b — (отличные от нуля) взаимно простые целые числа, $n \geqslant 1$ и p — простое число. Тогда следующие утверждения равносильны:*

(1) *p является примитивным делителем бинома a^n-b^n;*
(2) *$p \mid (a^n-b^n)$, но если $1 \leqslant m < n$, $m \mid n$, то $p \nmid (a^m-b^m)$;*
(3) *$p \mid \Phi_n(a,b)$, но если $1 \leqslant m < n$, то $p \nmid \Phi_m(a,b)$;*
(4) *$p \mid \Phi_n(a,b)$, но если $1 \leqslant m < n$, $m \mid n$, то $p \nmid \Phi_m(a,b)$;*
(5) *$p \nmid b$, и если число b' таково, что $bb' \equiv 1 \pmod p$, то порядок числа ab' по модулю p равен n.*

Доказательство. Импликации (1) $\Rightarrow$ (2) и (3) $\Rightarrow$ (4) тривиальны. Эквивалентности (1) $\Leftrightarrow$ (3) и (2) $\Leftrightarrow$ (4) следуют непосредственно из соотношения $a^n-b^n=\prod_{d \mid n} \Phi_d(a,b)$.

Заметим, что $(ab')^d \equiv 1 \pmod p$ тогда и только тогда, когда $p \mid \left(a^d-b^d\right)$. Таким образом, очевидно, что (5) равносильно (1) и (2). □

Пусть простое число p не делит n. Тогда сравнение $X^n-1 \equiv$ $\equiv 0 \pmod p$ не имеет кратных корней, так как производная nX^{n-1} имеет лишь корень 0 по модулю p. Из соотношения (2.5) следует,

что если a — целое число, $a \neq 1$, $p \nmid a$ и $\Phi_{p-1}(a) \equiv 0 \pmod{p}$, то $\Phi_m(a) \not\equiv 0 \pmod{p}$ для каждого целого числа m, $1 \leqslant m < p-1$, делящего $p-1$.

Из этого наблюдения и утверждения (3F) следует, что если $a \neq 1$ и p не делит a, то a является примитивным корнем по модулю p (т. е. порядок числа a по модулю p равен $p-1$) тогда и только тогда, когда $\Phi_{p-1}(a) \equiv 0 \pmod{p}$.

Следующее утверждение появляется в статьях Биркгофа и Вандивера (1904), а затем и в статье Инкери (1946) для случая, когда n — нечетное простое число. Включение $E_1 \subseteq E_2$ впервые было доказано Лежандром (1830).

(3G) *Пусть $n \geqslant 2$. Тогда при сделанных выше предположениях следующие множества простых чисел совпадают:*

E_1 — *множество примитивных делителей бинома $a^n - b^n$;*

E_2 — *множество простых чисел p, таких, что $p \equiv 1 \pmod{n}$ и $p \mid \Phi_n(a,b)$;*

E_3 — *множество простых чисел p, таких, что $p \nmid n$ и $p \mid \Phi_n(a,b)$.*

Доказательство. Покажем, что $E_1 \subseteq E_2$. Согласно предположению $p \mid (a^n - b^n)$, но $p \nmid (a^m - b^m)$ при всех m, $1 \leqslant m < n$. Из утверждения (3F) следует, что если $bb' \equiv 1 \pmod{p}$, то порядок числа ab' по модулю p равен n. Следовательно, $n \mid (p-1)$. Более того, если $1 \leqslant m < n$, $m \mid n$, то $\Phi_m(a,b)$ делит $a^m - b^m$. Так как $p \nmid (a^m - b^m)$, мы заключаем, что $p \nmid \Phi_m(a,b)$. Но p делит $a^n - b^n = \prod_{m|n} \Phi_m(a,b)$, следовательно, p делит $\Phi_n(a,b)$.

Очевидно, что $E_2 \subseteq E_3$. Действительно, если $n \mid (p-1)$, то $n < p$, а значит, $p \nmid n$.

Теперь покажем, что $E_3 \subseteq E_1$. Ясно, что $p \mid (a^n - b^n)$. Предположим, что p не является примитивным делителем бинома $a^n - b^n$. Тогда существует число m, $1 \leqslant m < n$, $m \mid n$, такое, что $p \mid (a^m - b^m)$. Так как

$$a^n - b^n = \Phi_n(a,b)(a^m - b^m) \prod_{d \neq n,\, d \mid n,\, d \nmid m} \Phi_d(a,b),$$

согласно предположению p делит $(a^n - b^n)/(a^m - b^m)$. Положим $n = md$, $a^m = a_1$, $b^m = b_1$. Тогда

$$\frac{a^n - b^n}{a^m - b^m} = \frac{a_1^d - b_1^d}{a_1 - b_1} = \sum_{i=0}^{d-1} a_1^{d-1-i} b_1^i \equiv d a_1^{d-1} \pmod{p}.$$

Но $p \mid (a_1 - b_1)$, так что $p \nmid a_1$, следовательно, $p \mid d$, а значит, $p \mid n$. Полученное противоречие завершает доказательство. □

Докажем еще один результат.

(3H) *Пусть a, b — различные взаимно простые целые числа, отличные от нуля, и $n \geqslant 1$. Пусть, далее, p — примитивный делитель бинома $a^d - b^d$, причем $v_p(a^d - b^d) = r \geqslant 1$. Предположим, что $r \geqslant 2$ для $p = 2$. Тогда*

(1) $v_p(\Phi_d(a,b)) = r$;
(2) *если* $t \geqslant 1$, *то* $v_p(\Phi_{dp^t}(a,b)) = 1$;
(3) *если* $t \geqslant 0$, $k > 1$, $p \nmid k$, *то* $v_p(\Phi_{kdp^t}(a,b)) = 0$.

Доказательство. (1) Утверждение (3F) позволяет заключить, что $p \nmid \Phi_l(a,b)$ при всех l, $1 \leqslant l < d$. Отсюда следует равенство $v_p(\Phi_d(a,b)) = v_p(a^d - b^d)$.

(2) Из соотношения (2.12) следует, что

$$a^{dp^t} - b^{dp^t} = \Phi_{dp^t}(a,b) \cdot \left(a^{dp^{t-1}} - b^{dp^{t-1}}\right) \prod_{e \mid d,\, 1 \leqslant e < d} \Phi_{ep^t}(a,b).$$

Заметим, что $p \nmid \Phi_{ep^t}(a,b)$ при $e < d$, иначе выполнялось бы условие $p \mid \left(a^{ep^t} - b^{ep^t}\right)$. Поскольку p — примитивный делитель бинома $a^d - b^d$, из утверждения (3F)(5) следует, что d делит ep^t. Но $p \nmid d$, а значит, $d \mid e$, что противоречит предположению. Далее, согласно утверждениям (3B)(6) и (3B)(7) мы имеем

$$v_p\left(a^{dp^t} - b^{dp^t}\right) = r + t,$$

$$v_p\left(a^{dp^{t-1}} - b^{dp^{t-1}}\right) = r + t - 1.$$

Таким образом, $v_p(\Phi_{dp^t}(a,b)) = 1$.

(3) Запишем соотношение

$$a^{dkp^t} - b^{dkp^t} = \Phi_{dkp^t}(a,b) \prod_{e \mid dkp^t,\, e \nmid dp^t,\, e < dkp^t} \Phi_e(a,b) \cdot \left(a^{dp^t} - b^{dp^t}\right).$$

Из утверждений (3B)(6) и (3B)(7) следует, что справедливы равенства $v_p(a^{dkp^t} - b^{dkp^t}) = r + t$, $v_p(a^{dp^t} - b^{dp^t}) = r + t$, а значит, $v_p(\Phi_{dkp^t}(a,b)) = 0$. □

Для каждого целого числа $n \geqslant 2$ обозначим через $P[n]$ наибольшее простое число, делящее n.

(3I) *Пусть* $a > b \geqslant 1$, НОД$(a,b) = 1$ *и* $n \geqslant 2$. *Пусть, далее,* p — *примитивный делитель бинома* $a^f - b^f$, *такой, что* $p \mid \Phi_n(a,b)$. *Тогда*

(1) *существует число* $j \geqslant 0$, *такое, что* $n = fp^j$, *причем* $p \nmid f$;
(2) *если* $j > 0$, *то* $p = P[n]$;
(3) *если* $j > 0$ *и* $p^2 \mid \Phi_n(a,b)$, *то* $n = p = 2$;
(4) НОД$(\Phi_n(a,b), n) = 1$ *или* $P[n]$.

Доказательство. (1) Из соотношения (2.11) следует, что $\Phi_n(a,b)$ делит $a^n - b^n$, так что $p \mid (a^n - b^n)$, а значит, $f \mid n$ в силу утверждения (3F). Так как $p \mid (a^{p-1} - b^{p-1})$, мы вновь имеем $f \mid (p-1)$, а значит, $f < p$. Пусть $n = fp^j w$, где $j \geqslant 0$, $p \nmid fw$. Положим $r = fp^j$. Согласно (3.2) справедливо сравнение

$$\frac{a^n - b^n}{a^r - b^r} \equiv wb^{w-1} \pmod{(a^r - b^r)}.$$

Так как $p \mid (a^r - b^r)$ (потому что $f \mid r$),

$$\frac{a^n - b^n}{a^r - b^r} \equiv wb^{w-1} \pmod{p}.$$

Если $n < m$, то $\Phi_n(a,b)$ делит $(a^n - b^n)/(a^r - b^r)$ в соответствии с соотношением (2.12). Так как $p \nmid b$ (поскольку НОД$(a,b) = 1$), мы заключаем, что $p \mid w$, а это невозможно. Таким образом, $n = fp^j$.

(2) Так как $f < p$, при $j > 0$ мы имеем $p = P[n]$.

(3) Пусть $j > 1$ и $s = fp^{j-1}$. Тогда $n = ps$, и мы получаем, что

$$\frac{a^n - b^n}{a^s - b^s} = \frac{[(a^s - b^s) + b^s]^p - b^{sp}}{a^s - b^s}$$

$$= pb^{s(p-1)} + \binom{p}{2}(a^s - b^s)b^{s(p-2)} + \binom{p}{3}(a^s - b^s)^2 b^{s(p-3)}$$

$$+ \ldots + (a^s - b^s)^{p-1}.$$

Если $p \geqslant 3$, то, так как $p \mid (a^s - b^s)$, получим

$$\frac{a^n - b^n}{a^s - b^s} \equiv p \pmod{p^2}.$$

С другой стороны, из соотношения (2.12) следует, что $\Phi_n(a,b)$ делит $(a^n - b^n)/(a^s - b^s)$, а значит, $p^2 \nmid \Phi_n(a,b)$. Таким образом, если $p^2 \mid \Phi_n(a,b)$, то непременно $p = 2$. Значит, если $f \leqslant p-1$, то $f = 1$ и $n = 2^j$, следовательно, $\Phi_n(a,b) \not\equiv 0 \pmod{r}$, что невозможно. А это означает, что $j = 1$ и $n = 2$.

(4) Предположим, что существует простое число p, делящее НОД$(\Phi_n(a,b),n)$. Из утверждений (1) и (2) следует, что $p = P[n]$. Согласно утверждению (3), если $p^2 \mid$ НОД$(\Phi_n(a,b),n)$, то $n = p = 2$, а значит, $p^2 \nmid n$, что и доказывает наше утверждение. □

Частный случай следующей очень интересной теоремы был доказан Бангом (1886). В 1892 г. Зигмонди получил представленный здесь усиленный вариант. Эта теорема была заново доказана Биркгофом и Вандивером (1904), а также многими другими математиками, такими, как Диксон (1905), Кармайкл (1913), Канольд (1950), Артин (1955), Херинг (1974), Люнебург (1981), и, возможно, другими.

(3J) *Пусть* $a > b \geqslant 1$, НОД$(a,b) = 1$, $n \geqslant 1$. *Тогда*

(1) *бином* $a^n - b^n$ *имеет примитивный делитель, за исключением следующих случаев*:

(a) $n = 1$, $a - b = 1$;
(b) $n = 2$, $a + b$ *есть степень числа* 2;
(c) $n = 6$, $a = 2$, $b = 1$;

(2) *бином* $a^n + b^n$ *имеет примитивный делитель, за исключением случая* $n = 3$, $a = 2$, $b = 1$.

Доказательство. (1) Очевидно, что в случаях (a), (b), (c) бином $a^n - b^n$ не имеет примитивных делителей. Если $n = 1$ и $a - b$ не имеет примитивных делителей, то $a - b = 1$.

Пусть $n = 2$. Предположим, что $a^2 - b^2$ не имеет примитивных делителей. Так как $a^2 - b^2 = (a+b)(a-b)$ и НОД$(a+b, a-b) = 1$ или 2, если p — нечетное простое число, делящее $a + b$, то p делит и $a^2 - b^2$. Но p не является примитивным делителем, а значит, $p \mid (a-b)$, следовательно, p делит a и b, что невозможно. Это означает, что $a + b$ есть степень числа 2.

Пусть теперь $n \geqslant 3$. Вновь предположим, что $a^n - b^n$ не имеет примитивных делителей. Пусть $p = P[n]$ и $v_p(\Phi_n(a,b)) = j \geqslant 0$. Положим

$$\Phi_n^*(a,b) = \frac{\Phi_n(a,b)}{p^j}.$$

(1°) Предположим, что $\Phi_n^*(a,b) = 1$. Пусть $\zeta_1, \zeta_2, \ldots, \zeta_{\varphi(n)}$ — примитивные корни степени n из 1. Из неравенства

$$|a - \zeta_i b| = b\left|\frac{a}{b} - \zeta_i\right| > b\left(\frac{a}{b} - 1\right) = a - b$$

и предыдущего замечания следует, что

$$\Phi_n(a,b) = |\Phi_n(a,b)| = \prod_{i=1}^{\varphi(n)} |a - \zeta_i b| > (a-b)^{\varphi(n)} \geqslant 1 = \Phi_n^*(a,b).$$

Значит, $j \geqslant 1$ и $p \mid \Phi_n(a,b)$, следовательно, p делит $a^n - b^n$. Таким образом, p является примитивным делителем бинома $a^f - b^f$, причем f делит n. Согласно утверждению (3I) мы заключаем, что НОД$(n, \Phi_n(a,b)) = p$, а также $p^2 \nmid \Phi_n(a,b)$.

Таким образом, $\Phi_n(a,b) = p$, потому что $\Phi_n^*(a,b) = 1$. Более того, $p-1$ делит $\varphi(n)$, поскольку $p \mid n$. Из этого, в свою очередь, следует, что $p = \Phi_n(a,b) \geqslant (a-b)^{\varphi(n)} \geqslant (a-b)^{p-1}$, а значит, $a - b = 1$.

Если $p^2 \mid n$, положим $n = pm$, так что $p - 1 \leqslant \varphi(m)$ и в силу соотношения (2.14) мы получаем

$$p = \Phi_n(a,b) = \Phi_m(a^p, b^p) > (a^p - b^p)^{\varphi(m)} \geqslant (a^p - b^p)^{p-1},$$

потому что $p \mid m$. Итак, $a^p - b^p = 1$, что противоречит условию $a - b = 1$.

Таким образом, из утверждения (3I) следует, что $n = pf$, $p \nmid f$, где p — примитивный делитель бинома $a^f - b^f$. Заметим также, что $f \mid (p-1)$, а значит, $f < p$. Поскольку $\varphi(n) = (p-1)\varphi(f)$, в силу равенства (2.12) выполняются соотношения

$$p(a^p - b^p) > p(a^f - b^f) \geqslant \Phi_n(a,b)\Phi_f(a,b) = \Phi_f(a^p, b^p) > (a^p - b^p)^{\varphi(f)}.$$

Следовательно, $p > (a^p - b^p)^{\varphi(f)-1}$, поэтому непременно $\varphi(f) = 1$, так что $f = 1$ или $f = 2$, а значит, $n = p$ или $n = 2p$.

Если $n = p$, то $p = \Phi_p(a,b) = a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1} = (a^p - b^p)/(a-b) = a^p - b^p$, а это невозможно, потому что $a - b = 1$.

Если же $n = 2p$, то из неравенства $3 \leqslant p$ и соотношения (2.12) следует, что

$$p = \Phi_{2p}(a,b) = \frac{a^p + b^p}{a+b}.$$

Учитывая утверждение (3D), заключаем, что $a = 2$, $b = 1$ и $p = 3$, следовательно, $n = 6$.

(2°) Предположим, что $a^n - b^n$ не имеет примитивных делителей. Достаточно показать, что $\Phi_n^*(a,b) = 1$, и тогда утверждение будет следовать из (1°). Пусть простое число p делит $\Phi_n(a,b)$, а значит, $p \mid (a^n - b^n)$. Тогда существует число f, делящее n, $1 \leqslant f < n$, такое, что p — примитивный делитель бинома $a^f - b^f$. Согласно утверждению (3I) мы получаем $p = P[n]$ и $\Phi_n(a,b) = p^j$, где $j \geqslant 1$. Следовательно, $\Phi_n^*(a,b) = 1$.

(2) Если $n = 3$, $a = 2$, $b = 1$, то бином $a^n + b^n = 2^3 + 1$ не имеет примитивных делителей. Обратно, если $n = 1$ и $a + b \geqslant 2$, то найдется примитивный делитель.

Если $n = 2$ и a^2+b^2 не имеет примитивных делителей, то $a^2+b^2 = 2^k$ (где $k \geqslant 2$). В самом деле, если нечетное простое число p делит $a^2 + b^2$, то $p \mid (a + b)$, а значит, $p \mid (a^2 - b^2)$, и поэтому $p \mid 2a^2$. Отсюда следует, что $p \mid a$, а также $p \mid b$, что невозможно. Поскольку $a^2 + b^2 = 2^k$ $(k \geqslant 2)$ и НОД$(a, b) = 1$, числа a и b нечетны, а значит, $a^2 + b^2 \equiv 2 \pmod 4$, что невозможно. Итак, бином $a^2 + b^2$ имеет примитивный делитель.

Если $n \geqslant 3$, то из утверждения (1) следует, что бином $a^{2n} - b^{2n}$ имеет примитивный делитель p, за исключением случая, когда $n = 3$, $a = 2$, $b = 1$. Если $p = 2$, то числа a и b нечетны, значит, $2 \mid (a + b)$, а это противоречит утверждению о том, что 2 — примитивный делитель бинома $a^n - b^n$.

Согласно утверждению (3E) мы заключаем, что $a^n + b^n$ имеет примитивный делитель во всех случаях, кроме указанного исключения. □

Из этой теоремы и утверждения (3F) следует, что если $a \geqslant 2$, то каждое число последовательности

$$\Phi_3(a),\ \Phi_4(a),\ \Phi_5(a),\ \Phi_6(a),\ \Phi_7(a), \ldots$$

(при $a = 2$ исключается элемент $\Phi_6(a)$) имеет простой делитель, который не делит ни одно из предыдущих чисел.

Представляют интерес и следующие результаты.

(3K) *Пусть* $1 \leqslant m < n$ *и* $a > b \geqslant 1$, *причем* НОД$(a, b) = 1$. *Если* НОД$(\Phi_m(a, b),\ \Phi_n(a, b)) \neq 1$, *то* $P[n] =$ НОД$(\Phi_m(a, b),\ \Phi_n(a, b))$.

Доказательство. Если $n = 2$, то $m = 1$. Если НОД$(a-b,\ a+b) \neq 1$, то НОД$(a - b,\ a + b) = 2$.

Пусть теперь $n \geqslant 3$, и пусть простое число p и $e \geqslant 1$ таковы, что $p^e \mid \Phi_m(a, b)$, $p^e \mid \Phi_n(a, b)$. Тогда $p \mid (a^m - b^m)$, $p \mid (a^n - b^n)$, а значит, p не является примитивным делителем бинома $a^n - b^n$. Из утверждения (3G) следует, что $p \mid n$, и в силу (3I) мы получаем $p = P[n]$, $\Phi_n(a, b) = pc$, $p \nmid c$, так что $e = 1$. Так как число p выбрано как произвольный общий делитель чисел $\Phi_m(a, b)$, $\Phi_n(a, b)$, мы доказали, что $P[n] =$ НОД$(\Phi_m(a, b), \Phi_n(a, b))$. □

(3L) *Пусть p — простое число, $0 \leqslant i < j$ и $a \geqslant b > 1$,* НОД$(a,b) = 1$. *Тогда*

$$\text{НОД}(\Phi_{p^i}(a,b),\ \Phi_{p^j}(a,b)) = \begin{cases} 1, & \text{если } p \nmid (a-b), \\ p, & \text{если } p \mid (a-b). \end{cases}$$

Доказательство. Из утверждения (3K) следует, что если $d = \text{НОД}(\Phi_{p^i}(a,b),\ \Phi_{p^j}(a,b)) \neq 1$, то $d = p$.

Пусть сначала $p \neq 2$. Если $p \mid (a-b)$, то справедливы сравнения $a^{p^{j-1}} \equiv a \equiv b \equiv b^{p^{j-1}} \pmod{p}$, а значит, согласно утверждению (3B) число p делит $\Phi_{p^j}(a,b) = (a^{p^j} - b^{p^j})/(a^{p^{j-1}} - b^{p^{j-1}})$. Аналогично p делит $\Phi_{p^i}(a,b)$. Наконец, если $p \nmid (a-b)$, то $a^{p^j} \equiv a \not\equiv b \equiv b^{p^j} \pmod{p}$, следовательно, $p \nmid \left(a^{p^j} - b^{p^j}\right)$ и тем более $p \nmid \Phi_{p^j}(a,b)$. Итак, $\text{НОД}(\Phi_{p^i}(a,b),\ \Phi_{p^j}(a,b)) = 1$.

Если $p = 2$, то $\Phi_1(a,b) = a - b$ и $\Phi_{2^k}(a,b) = a^{2^{k-1}} + b^{2^{k-1}}$ (при $k \geqslant 1$). Таким образом, если $a \equiv b \pmod 2$, то 2 делит $\text{НОД}(\Phi_{2^i}(a,b), \Phi_{2^j}(a,b))$, и наоборот. □

Приведем полезное следствие из утверждения (3L).

(3M) *Если a, b, $a > b \geqslant 1$, — целые числа и $n \geqslant 2$, то $P[a^n - b^n] > n$ и $P[a^n + b^n] > 2n$.*

Доказательство. Без ограничения общности можно считать, что $\text{НОД}(a,b) = 1$. Действительно, если $d = \text{НОД}(a,b)$, то, положив $a = da_1$, $b = db_1$, получим $a_1 > b_1 \geqslant 1$ и $\text{НОД}(a_1, b_1) = 1$. Более того, $a^n \pm b^n = d^n(a_1^n \pm b_1^n)$, так что $P[a_1^n \pm b_1^n] \leqslant P[a^n \pm b^n]$. Следовательно, достаточно показать, что $n < P[a_1^n - b_1^n]$ и $2n < P[a_1^n + b_1^n]$. Итак, будем полагать, что $\text{НОД}(a,b) = 1$.

(1) Если $a = 2$, $b = 1$, $n = 6$, то $a^n - b^n = 2^6 - 1 = 63 = 3^2 \times 7$ и $P[2^6 - 1] = 7 > 6$. В прочих случаях в силу утверждения (3L) можем выбрать примитивный делитель p бинома $a^n - b^n$. Из утверждения (3G) следует, что $p \equiv 1 \pmod n$, а значит, $p = 1 + kn$, и поэтому $P[a^n - b^n] \geqslant p > n$.

(2) Согласно (3L) можем выбрать примитивный делитель p бинома $a^{2n} - b^{2n}$. Из утверждения (3G) следует, что $p \equiv 1 \pmod{2n}$, а значит, $p = 1 + 2kn > 2n$. Согласно сделанному замечанию p также является примитивным делителем бинома $a^n + b^n$. Следовательно, $P[a^n + b^n] \geqslant p > 2n$. □

Список литературы

1729 (или ранее) Jacquemet, C., Manuscript in the Bibliothèque Nationale de Paris (see Dickson, *History of the Theory of Numbers*. Vol. II, p. 731).

1738 Euler, L., *Theorematum quorundam arithmeticorum demonstrationes*, Comm. Acad. Sci. Petrop., **10**, 1738 (1747), 125–146; reprinted in *Opera Omnia*, Vol. II, *Comm. Arithmeticae*, Vol. I, pp. 38–58.

1769 Lagrange, J.L., *Résolution des équations numériques*, Mém. Acad. Roy. Sci. Belles-Lettres Berlin, **23** (1769); reprinted in *Oeuvres*, Vol. II, pp. 527–532 and 539–578, Gauthier-Villars, Paris, 1868.

1830 Legendre, A.M., *Théorie des Nombres* (3^e édition), Vol. I, pp. 226–229, Firmin Didot Frères, Paris, 1830; reprinted by A. Blanchard, Paris, 1955.

1837 Kummer, E.E., *De aequatione* $x^{2\lambda} + y^{2\lambda} = z^{2\lambda}$ *per numeros integros resolvenda*, J. Reine Angew. Math., **17** (1837), 203–209; reprinted in *Collected Papers*, Vol. I, pp. 135–141, Springer-Verlag, New York, 1975.

1886 Bang, A.S., *Taltheoretiske Undersøgelser*, Tidskrift Mat., København, Ser. 5, **4** (1886), 70–80 and 130–137.

1888 Sylvester, J.J., *On the divisors of the sum of a geometrical series whose first term is unity and common ratio any positive or negative integer*, Nature, **37** (1888), 417–418; reprinted in *Mathematical Papers*, Vol. IV, pp. 625–629, Cambridge University Press, Cambridge, 1912.

1892 Zsigmondy, K., *Zur Theorie der Potenzreste*, Monatsh. Math., **3** (1892), 265–284.

1897 Lucas, F., *Note relative à la théorie des nombres*, Bull. Soc. Math. France, **25** (1897), 33–35.

1904 Birkhoff, G.D. and Vandiver, H.S., *On the integral divisors of* $a^n - b^n$, Ann. of Math., (2), **5** (1904), 173–180.

1905 Dickson, L.E., *On the cyclotomic function*, Amer. Math. Monthly, **12** (1905), 86–89; reprinted in *Collected Mathematical Papers* (editor A.A. Albert), Vol. 3, pp. 136–139, Chelsea, New York, 1975.

1913 Carmichael, R.D., *On the numerical factors of arithmetical forms* $\alpha^n \pm \beta^n$, Ann. of Math., (2), **15** (1913), 30–70.

1946 Inkeri, K., *Untersuchungen über die Fermatsche Vermutung*, Ann. Acad. Sci. Fenn., Ser. A1, Nr. 33, 1946, 60 pp.

1947 Vivanti, G., *Un teorema di aritmetica e la sua relazione colla ipotesi di Fermat*, Rend. Istit. Lombardo, Milano, Cl. Sci. Mat., **11** (80) (1947), 239–246.

1950 Kanold, H.J., *Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme, II*, J. Reine Angew. Math., **187** (1950), 169–182.

1955 Artin, E., *The orders of linear groups*, Comm. Pure Appl. Math., **8** (1955), 355–366.

1955 Möller, K., *Untere Schranke für die Anzahl der Primzahlen, aus denen x, y, z der Fermatschen Gleichung $x^n + y^n = z^n$ bestehen muss*, Math. Nachr., **14** (1955), 25–28.

1962 Schinzel, A., *On primitive prime factors of $a^n - b^n$*, Proc. Cambridge Philos. Soc., **58** (1962), 555–562.

1964 Kapferer, H., *Verifizierung des symmetrisches Teils der Fermatschen Vermutung für unendlich viele paarweise teilerfremde Exponenten E*, J. Reine Angew. Math., **214/5** (1964), 360–372.

1966 Leopoldt, H.-W., *Lösung einer Aufgabe von Kostrikhin*, J. Reine Angew. Math., **221** (1966), 160–161.

1974 Hering, C., *Transitive linear groups and linear groups which contain irreducible subgroups of prime order*, Geom. Dedicata, **2** (1974), 425–460.

1981 Lüneburg, H., *Ein einfacher Beweis für den Satz von Zsigmondy über primitive Primteiler von $A^n - 1$*. In *Geometries and Groups* (editors M. Aigner and D. Jungnickel), Lecture Notes in Math., **803**, pp. 219–222, Springer-Verlag, New York, 1981.

II.4. Результант и дискриминант многочленов

Пусть

$$F(X,Y) = a_0X^n + a_1X^{n-1}Y + \ldots + a_nY^n \quad (\text{где } a_0 \neq 0),$$
$$G(X,Y) = b_0X^m + b_1X^{m-1}Y + \ldots + b_mY^m \quad (\text{где } b_0 \neq 0)$$

суть бинарные формы с коэффициентами a_i, b_j из области целостности[2] A.

---

[2]Областью целостности называется коммутативное кольцо с единицей, не равной нулю, и без делителей нуля, например кольцо целых чисел. Кольцо классов вычетов по составному модулю не является областью целостности (например, $2 \times 2 = 0$ в $\mathbb{Z}_4$). — *Прим. ред.*

Дадим определение результанта форм F и G, обозначаемого через $R(F,G)$ или $\mathrm{Res}(F,G)$. Прежде всего положим $R(F,b_0)=b_0^n$, если $m=0$, и $R(a_0,G)=a_0^m$, если $n=0$. В частности, $R(a_0,b_0)=1$. Далее, если $m\neq 0$ и $n\neq 0$, будем считать, что $R(F,G)$ равен определителю следующей матрицы порядка $m+n$:

$$\begin{pmatrix} a_0 & a_1 & \dots & \dots & a_n & 0 & 0 \\ 0 & a_0 & a_1 & \dots & \dots & a_n & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & a_0 & a_1 & \dots & a_n \\ b_0 & b_1 & \dots & b_m & 0 & \dots & 0 \\ 0 & b_0 & b_1 & \dots & b_m & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & b_0 & b_1 & \dots & b_m \end{pmatrix}.$$

Заметим, что первые m строк содержат $a_0,\dots,a_n$, а оставшиеся n строк содержат $b_0,\dots,b_m$.

Выражение $R(F,G)$ называется *результантом* бинарных форм $F(X,Y)$ и $G(X,Y)$ и является многочленом с целыми коэффициентами, причем его степень равна m по коэффициентам a_i и равна n по коэффициентам b_j.

Результант формы $\partial F(X,Y)/\partial X$, $\partial F(X,Y)/\partial Y$ называется *дискриминантом* для $F(X,Y)$:

$$\mathrm{Discr}(F)=R\left(\frac{\partial F}{\partial X},\frac{\partial F}{\partial Y}\right).$$

Сформулируем несколько широко известных свойств (см. Боше (1907) или Кон (1974)).

(4A) *Пусть $F(X,Y)$, $G(X,Y)$ — бинарные формы степеней $n\geqslant 1$, $m\geqslant 1$ соответственно. Тогда справедливы следующие утверждения.*

(1) *Форма $F(X,Y)$ имеет (отличный от константы) делитель, пропорциональный некоторому делителю формы $G(X,Y)$, тогда и только тогда, когда $R(F,G)=0$.*

(2) *Если $n\geqslant 2$, то $F(X,Y)$ имеет кратный линейный делитель тогда и только тогда, когда $\mathrm{Discr}(F)=0$.*

(3) *Если $F(X,Y)=\prod_{i=1}^{n}(\alpha_i'X-\alpha_iY)$ и $G(X,Y)=\prod_{j=1}^{m}(\beta_j'X-\beta_jY)$ (где α_i, α_i', β_j, β_j' — элементы поля, содержащего коэффициенты многочленов F и G, причем $\alpha_i'\neq 0$ для всякого*

i и $\beta_j' \neq 0$ при каждом j), то

$$R(F,G) = \prod_{i=1}^{n} G(\alpha_i, \alpha_i') = (-1)^{mn} \prod_{j=1}^{m} F(\beta_j, \beta_j') = \prod_{i,j} (\beta_j'\alpha_i - \beta_j\alpha_i') = (-1)^{mn} \prod_{i,j} (a_i'\beta_j - a_i\beta_j').$$

В частности, $R(G,F) = (-1)^{mn} R(F,G)$.

(4) *Если* $H(X,Y)$ *также является бинарной формой (некоторой степени* l*), то* $R(FG,H) = R(F,H)R(G,H)$ *и* $R(H,FG) = R(H,F)R(H,G)$.

(5) *Если* $n \geqslant m$ *и* $H(X,Y)$ *— форма степени* $\deg(H) = n-m$*, то* $R(F-HG,G) = R(F,G)$. *Аналогичным образом, если* $m \geqslant n$ *и* $K(X,Y)$ *— форма степени* $\deg(K) = m-n$*, то* $R(F,G-KF) = R(F,G)$.

Пусть теперь $f(X)$ и $g(X)$ — произвольные отличные от нуля многочлены степени n и m соответственно. Пусть, далее, $F(X,Y) = Y^n f(X/Y)$, $G(X,Y) = Y^m g(X/Y)$, так что $F(X,Y)$ и $G(X,Y)$ — бинарные формы степеней n и m соответственно.

Результант многочленов f и g по определению равен $R(f,g) = R(F,G)$. *Дискриминант* $\mathrm{Discr}(f)$ многочлена f по определению равен $R(f,f')$.

Если $n \geqslant 1$, $m \geqslant 1$ и $F(X,Y) = \prod_{i=1}^{n} (\alpha_i'X - \alpha_iY)$, $G(X,Y) = \prod_{j=1}^{m} (\beta_j'X - \beta_jY)$ (как в утверждении (4A)), где $\alpha_i' \neq 0$, $\beta_j' \neq 0$, то α_i/α_i' — корни многочлена $f(X)$, β_j/β_j' — корни многочлена $g(X)$.

Если $f(X) = a_0X^n + a_1X^{n-1} + \ldots + a_n$ (где $n \geqslant 1$, $a_0 \neq 0$), положим $F(X,Y) = Y^n f(X/Y) = \prod_{i=1}^{n} (\alpha_i'X - \alpha_iY)$.

Между дискриминантами многочлена $f(X)$ и бинарной формы $F(X,Y)$ существует следующая связь:

$$\mathrm{Discr}(F) = \frac{n^{n-2}}{a_0}\mathrm{Discr}(f). \tag{4.1}$$

Действительно, производная функции $f(X)$ равна

$$f'(X) = na_0X^{n-1} + (n-1)a_1X^{n-2} + \ldots + a_{n-1},$$

и соответствующая ей бинарная форма есть $G(X,Y) = Y^{n-1} \times f'(X/Y)$. С другой стороны, $\partial F/\partial X = Y^{n-1}f'(X/Y) = G(X,Y)$ и $\partial F/\partial Y = nY^{n-1}f(X/Y) - XY^{n-2}f'(X/Y) = (1/Y)[nF(X,Y) - XG(X,Y)]$.

Значит, с одной стороны, мы имеем

$$R\left(\frac{\partial F}{\partial X}, Y\frac{\partial F}{\partial Y}\right) = R\left(\frac{\partial F}{\partial X}, Y\right) R\left(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}\right) = na_0 \operatorname{Discr}(F),$$

а с другой стороны,

$$\begin{aligned} R\left(\frac{\partial F}{\partial X}, Y\frac{\partial F}{\partial Y}\right) &= R(G, nF - XG) = R(G, nF) \\ &= R(G, n) \cdot R(G, F) = n^{n-1}(-1)^{n(n-1)} R(F, G) \\ &= n^{n-1}(-1)^{n(n-1)} R(f, f') = n^{n-1}\operatorname{Discr}(f). \end{aligned}$$

Для удобства читателя укажем явно свойства результанта и дискриминанта многочленов одной переменной.

(4В) *Пусть* f, g, h, k — *многочлены, причем* $\deg(f) = n$, $\deg(g) = m$. *Тогда*

(1) $R(g, f) = (-1)^{mn} R(f, g)$;

(2) *если* $n \leqslant m$ *и* $\deg(h) \leqslant m - n$, *то* $R(f, g) = R(f, g + fh)$;

(3) $R(hk, g) = R(h, g) \cdot R(k, g)$,
$R(g, hk) = R(g, h) \cdot R(g, k)$;

(4) $R(f^s, g) = [R(f, g)]^s$ *для каждого натурального числа* s;

(5) $R((X - a)^s, g) = [g(a)]^s$, *где* $a \in A$, $s \geqslant 1$;

(6) *если* $f = a_0 \prod_{i=1}^{n}(X - \alpha_i)$ *и* $g = b_0 \prod_{j=1}^{m}(X - \beta_j)$, *то*

$$\begin{aligned} R(f, g) &= a_0^m b_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) \\ &= a_0^m \prod_{i=1}^{n} g(\alpha_i) \\ &= (-1)^{mn} b_0^n \prod_{j=1}^{m} f(\beta_j); \end{aligned}$$

(7) *если* $f = a_0 \prod_{i=1}^{n}(X - \alpha_i)$, *то*

$$\operatorname{Discr}(f) = (-1)^{n(n-1)/2} a_0^{2n-1} \prod_{i<j}(\alpha_i - \alpha_j)^2;$$

(8) *если* $f = hk$, $\deg(h) = r$ *и* $\deg(k) = s$, *то*

$$\operatorname{Discr}(f) = (-1)^{rs}\operatorname{Discr}(h)\operatorname{Discr}(k)[R(h, k)]^2.$$

(4C)

(1) *Если многочлены* $f, g \in A[X]$ *отличны от константы и* $R(f,g) \neq 0$, *то* f *и* g *взаимно просты.*

(2) *Если* $A = K$ *— поле и многочлены* $f, g \in K[X]$ *взаимно просты, то* $R(f,g) \neq 0$.

Доказательство. (1) Предположим, что многочлены f и g имеют общий делитель $h \in A[X]$, отличный от константы. Тогда $f = hf_1$ и $g = hg_1$. Согласно (4B)(3) мы получаем

$$R(f,g) = R(h,h) \cdot R(h,g_1) \cdot R(f_1,h) \cdot R(f_1,g_1) = 0.$$

(2) Предположим, что многочлены $f, g \in K[X]$ взаимно просты. По теореме Безу существуют многочлены $f_1, g_1 \in K[X]$, такие, что $g_1 f + f_1 g = 1$; в частности, $\deg(g_1 f) = \deg(f_1 g)$. Согласно (4B)(3) мы имеем

$$R(g_1 f, f_1 g) = R(g_1, f_1) \cdot R(g_1, g) \cdot R(f, f_1) \cdot R(f, g).$$

Если $R(f,g) = 0$, то $R(g_1 f, f_1 g) = 0$. Однако в силу (4B)(2) должны выполняться соотношения

$$R(g_1 f, f_1 g) = R(g_1 f, 1 - g_1 f) = R(g_1 f, 1) = 1,$$

что невозможно. □

Список литературы

1907 Bôcher, M., *Introduction to Higher Algebra*, Macmillan, New York, 1907; reprinted in 1947.

1974 Cohn, P.M., *Algebra*, Vol. I, Wiley, New York, 1974.

Глава III

Алгебраические ограничения на гипотетические решения

Пусть $n > 3$ и x, y, z — отличные от нуля попарно взаимно простые целые числа, такие, что

$$x^n + y^n = z^n.$$

В этой главе мы выведем алгебраические соотношения, которым должны подчиняться числа x, y, z, n. В ряде случаев это приведет к противоречию, означающему, что для рассматриваемого показателя уравнение Ферма имеет лишь тривиальные решения.

III.1. Соотношения Барлоу

Пусть p — нечетное простое число. Предположим, что существуют отличные от нуля попарно взаимно простые целые числа x, y, z, такие, что $x^p + y^p + z^p = 0$. Для начала заметим, что $x + y + z \neq 0$. В самом деле, x, y, z не могут быть одновременно положительны (или отрицательны). Значит, можно считать, что, например, $x > 0$, $y > 0$ и $z < 0$. Тогда $(x + y)^p > x^p + y^p = -z^p$, так что $x + y > -z$ и, таким образом, $x + y + z \neq 0$.

Укажем соотношения, которым должны удовлетворять целые числа x, y, z.

Первый из таких результатов был получен Барлоу (1810, 1811). В 1823 г. Абель независимо получил то же утверждение и изложил его без доказательства в письме к Гольмбо. Доказательство приводимых нами результатов принадлежит Лежандру (1823) и было известно Софи Жермен. Позднее эти утверждения были заново получены Линдеманом (1901, 1907) и содержались в статьях Каталана (1886), Тафельмахера (1892), Флека (1909), Линда (1910), Бахмана (1919), Джеймса (1938), Раклиша (1944) и др.

(1A) *Если существуют отличные от нуля целые числа* x, y, z, *такие, что* $x^p + y^p + z^p = 0$, $\text{НОД}(x, y, z) = 1$, *причем* p *не делит* z, *то существуют такие взаимно простые целые числа* t, t_1, *не кратные* p, *что*

$$x + y = t^p, \qquad \frac{x^p + y^p}{x + y} = t_1^p, \qquad z = -tt_1.$$

Более того, t_1 *нечетно и* $t_1 > 1$.

Доказательство. По предположению числа x, y, z попарно взаимно просты. Рассмотрим целое число

$$Q_p(x, -y) = \frac{x^p + y^p}{x + y} = x^{p-1} - x^{p-2}y + \ldots - xy^{p-2} + y^{p-1}. \qquad (1.1)$$

Так как $x + y + z \equiv x^p + y^p + z^p \equiv 0 \pmod p$ и $p \nmid z$, мы также имеем $p \nmid (x + y)$. Из утверждения (3B) гл. II следует, что $\text{НОД}(x + y, Q_p(x, -y)) = 1$.

Поскольку $(-z)^p = x^p + y^p = (x + y)Q_p(x, -y)$, числа $x + y$ и $Q_p(x, -y)$ являются p-ми степенями, т. е. существуют целые числа t, t_1, такие, что $x + y = t^p$, $Q_p(x, -y) = t_1^p$, следовательно, $-z = tt_1$ и $\text{НОД}(t, t_1) = 1$.

Покажем, что число t_1 нечетно. Из соотношения (1.1) видно, что $Q_p(x, -y)$ есть сумма нечетного числа слагаемых, среди которых x^{p-1} или y^{p-1} нечетно (потому что числа x и y не являются одновременно четными). Таким образом, $Q_p(x, -y)$ должно быть нечетным, а значит, t_1 также нечетно. Наконец, так как $x > y$ (или $y > x$), в силу (1E) мы можем заключить, что $x - y \geqslant 1$ (или $y - x \geqslant 1$), следовательно, $t_1^p = Q_p(x, -y) = Q_p(y, -x) \geqslant p$, так что $t_1 > 0$, а на самом деле даже $t_1 > 1$. □

Если числа x, y, z удовлетворяют уравнению $x^p + y^p + z^p = 0$, причем p не делит x, y, z и $\text{НОД}(x, y, z) = 1$, то согласно предыдущему результату существуют целые числа r, s, t, r_1, s_1, t_1, не кратные p, такие, что

$$\begin{cases} x + y = t^p, & (x^p + y^p)/(x + y) = t_1^p, & z = -tt_1, \\ y + z = r^p, & (y^p + z^p)/(y + z) = r_1^p, & x = -rr_1, \\ z + x = s^p, & (z^p + x^p)/(z + x) = s_1^p, & y = -ss_1. \end{cases} \qquad (1.2)$$

Более того, r, s, t, r_1, s_1, t_1 попарно взаимно просты, r_1, s_1, t_1 нечетны и превосходят 1. Заметим, что $r^p + s^p + t^p = 2(x + y + z) \neq 0$.

Складывая и вычитая равенства, получим, что

$$\begin{cases} x = -r^p + (r^p + s^p + t^p)/2 = (-r^p + s^p + t^p)/2, \\ y = -s^p + (r^p + s^p + t^p)/2 = (r^p - s^p + t^p)/2, \\ z = -t^p + (r^p + s^p + t^p)/2 = (r^p + s^p - t^p)/2. \end{cases} \tag{1.3}$$

Следующее дополнение к (1A) было известно Софи Жермен и приводится Лежандром (1823). Позднее его доказали Флек (1909), Линд (1910), Поме (1923), а также Шпунар (1928), Джеймс (1938), Перес-Качо (1958) и Дрегер (1959) (в иной форме).

(1B) *Если нечетное простое число p не делит z, то каждый простой делитель q числа t_1 сравним с 1 по модулю $2p$. В частности, $t_1 \equiv 1 \pmod{2p}$. Если, кроме того, p не делит xyz, то каждый простой делитель числа $r_1 s_1 t_1$ сравним с 1 по модулю $2p^2$. В частности, $r_1 \equiv 1 \pmod{2p^2}$, $s_1 \equiv 1 \pmod{2p^2}$ и $t_1 \equiv 1 \pmod{2p^2}$.*

Доказательство. Пусть простое число q делит t_1. Тогда q делит $x^p + y^p$, но q не делит $x + y = t^p$, потому что НОД$(t, t_1) = 1$. Из утверждения (3G) гл. II следует, что $q \equiv 1 \pmod{p}$. Так как число $q - 1$ четно, $q \equiv 1 \pmod{2p}$.

Предположим теперь, что $p \nmid xyz$ и что простое число q делит r_1. Тогда q делит x. Следовательно, q не делит yz. Заметим также, что НОД$(r, r_1) = 1$, так что q не делит $y + z$.

Таким образом, $y \equiv t^p \pmod{q}$, $z \equiv s^p \pmod{q}$, следовательно, $t^p + s^p \equiv y + z \not\equiv 0 \pmod{q}$ и $t^{p^2} + s^{p^2} \equiv y^p + z^p \equiv -x^p \equiv 0 \pmod{q}$. Итак, q является примитивным делителем бинома $t^{p^2} + s^{p^2}$. Из утверждения (3E) гл. II следует, что q есть примитивный делитель бинома $t^{2p^2} - s^{2p^2}$, а значит, согласно утверждению (3G) гл. II мы получаем $q \equiv 1 \pmod{2p^2}$. В частности, $r_1 \equiv 1 \pmod{2p^2}$.

Для простых делителей чисел s_1 и t_1 доказательство аналогично. □

Теперь приведем соотношения, которым должны удовлетворять предполагаемые решения во втором случае. Эти факты (включая утверждение о том, что $n \geqslant 2$) были известны Софи Жермен и приводятся Лежандром (1823).

(1C) *Пусть отличные от нуля целые числа x, y, z таковы, что p делит z, $x^p + y^p + z^p = 0$ и НОД$(x, y, z) = 1$. Тогда существуют целое число $n \geqslant 2$ и попарно взаимно простые целые числа r, s, t, r_1, s_1, t_1, не кратные p, такие, что r_1, s_1, t_1 нечетны, превос-*

ходят 1 *и удовлетворяют соотношениям*

$$\begin{cases} x+y=p^{pn-1}t^p, & (x^p+y^p)/(x+y)=pt_1^p, & z=-p^ntt_1, \\ y+z=r^p, & (y^p+z^p)/(y+z)=r_1^p, & x=-rr_1, \\ z+x=s^p, & (z^p+x^p)/(z+x)=s_1^p, & y=-ss_1. \end{cases} \tag{1.4}$$

Более того, если q *— произвольное простое число, делящее* t_1*, то* $q\equiv 1 \pmod{p^2}$*; в частности,* $t_1\equiv 1 \pmod{2p^2}$.

Доказательство. Числа x, y, z попарно взаимно просты. Если p делит z, то p не делит ни x, ни y, и, поскольку $x+y+z\equiv x^p+y^p+z^p\equiv$ $\equiv 0 \pmod{p}$, $x+y\equiv -z\equiv 0 \pmod{p}$.

Пусть $m\geqslant 2$ таково, что $x+y=p^{m-1}t'$, причем p не делит t'. Пусть $Q_p(x,-y)=(x^p+y^p)/(x+y)$. Так как p делит $x+y$, согласно утверждению (3B)(6) гл. II мы получаем $v_p\left(Q_p(x,-y)\right)=v_p(p)=$ $=1$, так что $Q_p(x,-y)=pt_1{}'$, $p\nmid t_1{}'$. Из утверждения (3B)(4) гл. II следует, что $\text{НОД}(x+y,\, Q_p(x,-y))=p$, а значит, $\text{НОД}(t', t_1{}')=1$.

Так как $-z^p=x^p+y^p=p^mt't_1{}'$, в силу единственности разложения на простые множители p делит m и t', $t_1{}'$ являются p-ми степенями целых чисел. Положим $m=pn$. Тогда

$$\begin{aligned} x+y &= p^{pn-1}t^p, \\ \frac{x^p+y^p}{x+y} &= pt_1^p, \\ z &= -p^ntt_1, \end{aligned}$$

где $n\geqslant 1$, $t, t_1\in\mathbb{Z}$, $\text{НОД}(t,t_1)=1$, p не делит ни t, ни t_1.

Так как $p\nmid x$ и $p\nmid y$, согласно утверждению (1A) существуют целые числа r, r_1, s, s_1, не кратные p, такие, что

$$\begin{aligned} y+z=r^p, \quad & (y^p+z^p)/(y+z)=r_1^p, \quad & x=-rr_1, \\ z+x=s^p, \quad & (z^p+x^p)/(z+x)=s_1^p, \quad & y=-ss_1, \end{aligned}$$

причем

$$\text{НОД}(t,r,s)=\text{НОД}(t_1,r_1,s_1)=1,\ \text{НОД}(r,r_1)=\text{НОД}(s,s_1)=1.$$

Доказательство того факта, что числа r_1, s_1, t_1 нечетны, причем $r_1>1$, $s_1>1$, проводится так же, как и для утверждения (1A).

Покажем теперь, что $t_1>1$. Согласно утверждению (3D) гл. II мы имеем $pt_1^p=(x^p+y^p)/(x+y)=Q_p(x,-y)=Q_p(y,-x)\geqslant p$, следовательно, $t_1\geqslant 1$, и достаточно показать, что $t_1\neq 1$. Если $t_1=1$, то мы можем применить то же утверждение, положив, например,

$x > y$, и получим $p = 3$, $x = 2$, $y = 1$, а значит, $2^3 + 1^3 + z^3 = 0$, что невозможно.

Теперь покажем, что если q — произвольный простой делитель числа t_1, то $q \equiv 1 \pmod{p^2}$. Из сравнения $z \equiv 0 \pmod{q}$ следует, что $y \equiv r^p \pmod{q}$, $x \equiv s^p \pmod{q}$ и $0 \equiv x^p + y^p + z^p \equiv r^{p^2} + s^{p^2} \pmod{q}$. С другой стороны, q не делит $r^p + s^p$ (иначе q делило бы $x + y$, а значит, и t, что противоречит условию $\text{НОД}(t, t_1) = 1$). Из утверждения (3D) гл. II следует, что $q \equiv 1 \pmod{p^2}$. А это, в свою очередь, означает, что $t_1 \equiv 1 \pmod{2p^2}$.

Остается лишь показать, что $n \geqslant 2$. В самом деле, $r^p + s^p = 2z + (x + y) = -2p^n t t_1 + p^{pn-1} t^p \equiv 0 \pmod{p}$. Из утверждения (3H) гл. II получаем $r^p + s^p \equiv 0 \pmod{p^2}$. Так как $p \nmid tt_1$, отсюда можем заключить, что $2z = (r^p + s^p) - p^{pn-1} t^p \equiv 0 \pmod{p^2}$, так что $n \geqslant 2$. □

Из равенств (1.4) следует, что $r^p + s^p + p^{pn-1} t^p = 2(x + y + z) \neq 0$.

Утверждение о том, что точная степень числа p, которая делит $x + y$, равна p^{pn-1}, было доказано многими авторами (и даже в 1955 г. Стоуном), которым было неизвестно, что этот результат давно получен.

Запишем соотношения, аналогичные (1.3), для случая, когда $p \mid z$:

$$\begin{cases} x = -r^p + (r^p + s^p + p^{pn-1} t^p)/2 = (-r^p + s^p + p^{pn-1} t^p)/2, \\ y = -s^p + (r^p + s^p + p^{pn-1} t^p)/2 = (r^p - s^p + p^{pn-1} t^p)/2, \\ z = -p^{pn-1} t^p + (r^p + s^p + p^{pn-1} t^p)/2 = (r^p + s^p - p^{pn-1} t^p)/2. \end{cases} \tag{1.5}$$

В случае бесквадратного показателя также найдены соотношения, аналогичные соотношениям Барлоу (см. Стюарт (1977)).

(1D) *Пусть $n > 2$ — бесквадратное целое число и отличные от нуля попарно взаимно простые целые числа x, y, z таковы, что $x^n + y^n = z^n$ (соответственно n нечетно и $x^n - y^n = z^n$). Тогда $z - y = 2^u d^{n-1} a^n$ (соответственно $z + y = 2^u d^{n-1} a^n$), где a, d — натуральные числа, число u равно 0 или 1, причем 2^u и d делят n.*

Доказательство. Сначала рассмотрим случай, когда $x^n + y^n = z^n$. Положим $z - y = a' a^n$, где $a, a' \geqslant 1$ и p-адическое значение числа a' равно $v_p(a') < n$ для каждого простого числа p.

Если простое число p делит a', то p делит и n. Действительно, если $p \nmid n$, то согласно утверждению (3B)(5) гл. II мы мо-

жем заключить, что $p \nmid Q_n(z,y) = (z^n - y^n)/(z-y)$, и тогда $v_p(a') + nv_p(a) = v_p(z-y) = v_p(z^n - y^n) = v_p(x^n) = nv_p(x)$. Следовательно, n делит $v_p(a')$ и $n \leqslant v_p(a')$, что противоречит предположению. Это означает, что $p \mid n$, а значит, $v_p(n) = 1$, поскольку n бесквадратно.

Определим теперь $v_p(a')$ для случая, когда p делит a'. Пусть сначала простое число p нечетно. В силу утверждения (3B)(6) гл. II мы имеем $v_p(Q_n(z,y)) = v_p(n) = 1$. Таким образом, $v_p(a') + nv_p(a) + 1 = v_p(z-y) + v_p(Q_n(z,y)) = v_p(z^n - y^n) = v_p(x^n) = nv_p(x)$. Поэтому $v_p(a') \equiv -1 \pmod{n}$, а следовательно, $v_p(a') = n-1$.

Пусть теперь $p = 2$. Если $4 \mid (z-y)$, то согласно утверждению (3B)(7) гл. II имеем $v_2(Q_n(z,y)) = v_2(n) = 1$, откуда, как и выше, заключаем, что $v_2(a') = n-1$. Если же $2 \mid (z-y)$, но $4 \nmid (z-y)$, то $v_2(a') + nv_2(a) = v_2(z-y) = 1$, так что $v_2(a') = 1$. Итак, мы приходим к выводу, что 2 не делит $z-y$.

Суммируя вышесказанное, получим, что $z - y = 2^u d^{n-1} a^n$, где $u = 0$ или 1, причем 2^u и d делят n. Пусть, далее, n нечетно и $x^n - y^n = z^n$. Тогда $x^n + (-y)^n = z^n$, и согласно первой части доказательства $z + y$ имеет требуемый вид. □

В частности, если целое число $n > 2$ свободно от квадратов и отличные от нуля попарно взаимно простые целые числа x, y, z таковы, что $x^n + y^n = z^n$, то

$$\begin{cases} z - x = 2^{u_1} d_1^{n-1} a_1^n, \\ z - y = 2^{u_2} d_2^{n-1} a_2^n, \end{cases}$$

и, более того, если число n нечетно, то

$$x + y = 2^{u_3} d_3^{n-1} a_3^n,$$

где $a_1, a_2, a_3, d_1, d_2, d_3$ — натуральные числа, показатели u_1, u_2, u_3 равны 0 или 1, причем 2^{u_1}, 2^{u_2}, 2^{u_3}, d_1, d_2, d_3 делят n.

Список литературы

1810 Barlow, P., *Demonstration of a curious numerical proposition*, J. Nat. Phil. Chem. Arts, **27** (1810), 193–205 (this paper is referred to in Dickson's *History of the Theory of Numbers*, Vol. II, p. 733).

1811 Barlow, P., *An Elementary Investigation of Theory of Numbers* (pp. 153–169), J. Johnson, St. Paul's Church-yard, London, 1811.

1823 Abel, N., Extraits de quelques lettres à Holmboe, Copenhague, l'an $\sqrt[3]{6064321219}$ (en comptant la fraction décimale), *Oeuvres*

Complètes, Vol. II, 2nd ed., pp. 254--255, Grondahl, Christiania, 1881.

1823 Legendre, A.M., *Recherches sur quelques objets d'analyse indéterminée, et particulièrement sur le théorème de Fermat*, Mém. Acad. Sci., Institut France, **6** (1823), 1–60; appeared as "Second Supplément" in 1825, to a printing of *Essai sur la Théorie des Nombres* (2^e édition), Courcier, Paris; reprinted in Sphinx-Oedipe, **4** (1909), 97–128.

1886 Catalan, E., *Sur le dernier théorème de Fermat* (Mélanges Mathématiques, CCXV), Mém. Soc. Roy. Sci. Liège Sér. 2, **13** (1886), 387–397.

1892 Tafelmacher, W.L.A., *Sobre el teorema de Fermat de que la ecuación* $x^n + y^n = z^n$ *no tiene solución en numeros enteros* x, y, z *i siendo* $n > 2$, Ann. Univ. Chile, Santiago, **82** (1892), 271–300 and 415–437.

1901 Lindemann, F., *Über den Fermatschen Satz betreffend die Unmöglichkeit der Gleichung* $x^n = y^n + z^n$, Sitzungsber. Akad. Wiss. München, Math., **31** (1901), 185–202; corrigenda p. 495.

1907 Lindemann, F., *Über das sogenannte letzte Fermatsche Theorem*, Sitzungsber. Akad. Wiss. München, Math., **37** (1907), 287–352.

1909 Fleck, A., *Miszellen zum großen Fermatschen Problem*, Sitzungsber. Berliner Math. Ges., **8** (1909), 133–148.

1910 Bachmann, P., *Niedere Zahlentheorie*, Teubner, Leipzig, 1910; reprinted by Chelsea, New York, 1966.

1910 Lind, B., *Über das letzte Fermatsche Theorem*, Abhandl. zur Geschichte d. Math. Wiss., no. 26, 1910, 23–65.

1919 Bachmann, P., *Das Fermatproblem in seiner bisherigen Entwicklung*, W. de Gruyter, Berlin, 1919; reprinted by Springer-Verlag, Berlin, 1976.

1923 Pomey, L., *Sur le dernier théorème de Fermat*, C. R. Acad. Sci. Paris, **177** (1923), 1187–1190.

1928 Spunar, V.M., *On Fermat's last theorem*, J. Washington Acad. Sci., **18** (1928), 385–395.

1938 James, G., *A higher upper limit to the parameters in Fermat's equation*, Amer. Math. Monthly, **45** (1938), 439–445.

1944 Racliş, N., *Démonstration du grand théorème de Fermat pour des grandes valeurs de l'exposant*, Bull. École Polytechnique Bucarest, **15** (1944), 3–19.

1955 Stone, D.E., *On Fermat's last theorem*, Math. Mag., **28** (1955), 295–296.

1958 Pérez-Cacho, L., *Sobre algunas cuestiones de la teoria de números*, Rev. Mat. Hisp.-Amer., (4), **18** (1958), 10–27 and 113–124.

1958/9 Draeger, M., *Das Fermat-Problem*, Wiss. Z. Techn. Hochschule Dresden, **8** (1958/9), 941–946.

1977 Stewart, C.L., *A note on the Fermat equation*, Mathematika, **24** (1977), 130–132.

III.2. Дополнительные соотношения для гипотетических решений

В разделе 1 мы показали, что если отличные от нуля целые числа x, y, z попарно взаимно просты и p — нечетное простое число, причем $x^p + y^p + z^p = 0$, то должны выполняться соотношения Барлоу, в частности, существуют целые числа r, s, t, r_1, s_1, t_1, удовлетворяющие определенным свойствам. В настоящем разделе мы изучим некоторые другие свойства этих целых чисел.

Пусть целые числа m и n отличны от нуля, НОД$(m, n) = 1$ и n нечетно. Обозначим через (m/n) символ Якоби.

Приведенное ниже следствие соотношений Барлоу было впервые получено Пьером в 1943 г.

(2A) *Пусть отличные от нуля взаимно простые целые числа x, y, z таковы, что $x^p + y^p + z^p = 0$. Тогда*

(1) *если $p \nmid xyz$, то*

$$\left(\frac{r_1}{s_1 t_1}\right) = \left(\frac{s_1}{t_1 r_1}\right) = \left(\frac{t_1}{r_1 s_1}\right) = +1;$$

(2) *если $p \mid z$, то*

$$\left(\frac{r_1}{p s_1 t_1}\right) = \left(\frac{s_1}{p t_1 r_1}\right) = \left(\frac{p t_1}{r_1 s_1}\right) = +1.$$

Доказательство. (1) Для начала заметим, что многочлен $pXY(X + Y)$ делит $(X + Y)^p - (X^p + Y^p)$ (в $\mathbb{Z}[X, Y]$) (см. также разд. VII.2).

Согласно утверждению (1A) мы имеем $(x + y)^{p-1} - t_1^p \equiv 0 \pmod{pxy}$. Следовательно, $t_1^p \equiv (x + y)^{p-1} \pmod{r_1 s_1}$, а значит,

$$\left(\frac{t_1}{r_1 s_1}\right) = \left(\frac{t_1^p}{r_1 s_1}\right) = +1.$$

В силу симметрии

$$\left(\frac{r_1}{s_1 t_1}\right) = \left(\frac{s_1}{r_1 t_1}\right) = +1.$$

(2) Если $p \mid z$, то согласно утверждению (1C) мы имеем $(x+y)^{p-1} - pt_1^p \equiv 0 \pmod{pxy}$. Следовательно, $pt_1^p \equiv (x+y)^{p-1} \pmod{r_1 s_1}$. Таким образом,

$$\left(\frac{pt_1}{r_1 s_1}\right) = \left(\frac{pt_1^p}{r_1 s_1}\right) = +1.$$

Как и при доказательстве первой части, мы получаем сравнение $(y+z)^{p-1} - r_1^p \equiv 0 \pmod{pyz}$. Значит,

$$r_1^p \equiv (y+z)^{p-1} \pmod{ps_1 t_1},$$

следовательно,

$$\left(\frac{r_1}{ps_1 t_1}\right) = \left(\frac{r_1^p}{ps_1 t_1}\right) = +1.$$

Аналогично

$$\left(\frac{s_1}{pr_1 t_1}\right) = +1. \quad \square$$

Список литературы

1943 Pierre, C., *Sur le théorème de Fermat* $a^n + b^n = c^n$, C. R. Acad. Sci. Paris, **217** (1943), 37–39.

Глава IV

Теорема Софи Жермен

В этой главе излагается замечательная теорема Софи Жермен для первого случая теоремы Ферма.

IV.1. Теорема Софи Жермен

Софи Жермен, французский математик, современница Коши и Лежандра, доказала теорему существенно нового вида, которая устанавливала "d'un trait de plume"[1] (по выражению Лежандра) первый случай теоремы Ферма для каждого простого числа $p < 100$. Ее метод до сих пор совершенствуется другими математиками. Лежандр развил идеи С. Жермен в своей работе 1823 г.

Начнем с простого наблюдения (утверждение (3) было также доказано Бангом (1935)).

(1A) *Пусть q — простое число и $n \geqslant 3$ — нечетное целое число. Тогда следующие утверждения равносильны.*

(1) *Существуют целые числа a, b, c, не кратные q, такие, что $a^n + b^n + c^n \equiv 0 \pmod{q}$.*

(2) *Существуют целые числа d, e, не кратные q, такие, что $d^n \equiv e^n + 1 \pmod{q}$.*

Более того, если $q - 1 = 2kn$, то эти утверждения эквивалентны следующему.

(3) *Существуют корни u, u' сравнения $X^{2k} - 1 \equiv 0 \pmod{q}$, такие, что $u' \equiv u + 1 \pmod{q}$.*

Доказательство. (1) $\Rightarrow$ (2) Так как $q \nmid c$, существуют числа $d, e \in \mathbb{Z}$, такие, что

$$\begin{cases} dc \equiv -a \pmod{q}, \\ ec \equiv b \pmod{q}. \end{cases}$$

---

[1] «Росчерком пера» (*фр.*). — *Прим. перев.*

Тогда $q \nmid de$, $(dc)^n \equiv (ec)^n + c^n \pmod q$, следовательно, $d^n \equiv e^n + 1 \pmod q$.

(2) $\Rightarrow$ (1) Это очевидно.

Теперь предположим, что $q - 1 = 2kn$.

(2) $\Rightarrow$ (3) Пусть $u = e^n$, $u' = d^n$. Тогда $u^{2k} \equiv e^{q-1} \equiv 1 \pmod q$ и, аналогично, $(u')^{2k} \equiv d^{q-1} \equiv 1 \pmod q$, где $u' \equiv u + 1 \pmod q$.

(3) $\Rightarrow$ (2) Пусть h — первообразный корень по модулю q. Положим $u = h^m$. Тогда $h^{2km} \equiv u^{2k} \equiv 1 \pmod q$, а следовательно, $q - 1 = 2kn$ делит $2km$, так что n делит m. Таким образом, $u \equiv e^n \pmod q$. Аналогично $u' \equiv d^n \pmod q$, и по условию $d^n \equiv e^n + 1 \pmod q$. □

Теперь приведем вариант Лежандра теоремы Софи Жермен[2].

(1B) *Пусть p, q — различные нечетные простые числа. Предположим, что выполнены следующие условия.*

(1) *Если целые числа a, b, c таковы, что $a^p + b^p + c^p \equiv 0 \pmod q$, то $q \mid abc$.*

(2) *Число p несравнимо по модулю q с p-й степенью целого числа.*

Тогда для показателя p имеет место первый случай теоремы Ферма.

Доказательство. Пусть x, y, z — попарно взаимно простые целые числа, не кратные p, такие, что $x^p + y^p + z^p = 0$. Тогда $x^p + y^p + z^p \equiv \equiv 0 \pmod q$ и по предположению (1) мы имеем $q \mid xyz$. Можно считать, что, например, $q \mid x$ и, следовательно, $q \nmid yz$.

Так как $p \nmid xyz$, существуют целые числа r, s, t, r_1, s_1, t_1, удовлетворяющие соотношениям (1.2) и (1.3) гл. III. Так как $q \mid x$, справедливо сравнение $-r^p + s^p + t^p \equiv 0 \pmod q$. По предположению (1) число q делит одно из целых чисел r, s, t. Так как s делит y, t делит z, а q не делит ни yz, ни st, q должно делить r. Но $t_1^p = (x^p + y^p)/(x + y) \equiv y^{p-1} \pmod q$, поскольку $q \mid x$.

---

[2] См. сноску на с. 13 статьи Лежандра 1823 г., где он писал: «Следует согласиться, что это доказательство, принадлежащее госпоже Софи Жермен, весьма изобретательно. Госпожа Жермен успешно работает в физических и математических науках, свидетельством тому награда, которой она удостоена Академией за работу по вибрации упругих пластин. Она также является автором предложения параграфа 13, а кроме того, утверждения, касающегося специального вида простых делителей числа α, приведенного в параграфе 11.» [Здесь они соответствуют утверждениям ((2B), (2C)).]

Так как q делит r, мы получаем, что $y \equiv -z \pmod q$. Таким образом,

$$r_1^p = \frac{y^p + z^p}{y+z} = y^{p-1} + y^{p-2}(-z) + \ldots + (-z)^{p-1}$$
$$\equiv py^{p-1} \equiv pt_1^p \pmod q.$$

Поскольку $t_1 \not\equiv 0 \pmod q$, существует целое число t', такое, что $t't_1 \equiv 1 \pmod q$, а значит, $p \equiv (t'r_1)^p \pmod q$, что противоречит второму предположению. □

Прежде чем перейти к дальнейшему изложению, прокомментируем условия, указанные выше.

В следующем разделе вводится определитель Вендта, с помощью которого можно проверить, существуют ли целые числа x, y, z, не кратные q, такие, что $x^p + y^p + z^p \equiv 0 \pmod q$.

(1C) *Если нечетные простые числа p и q таковы, что $q-1 = 2pk$ для некоторого натурального числа k, то условие* (2) *утверждения* (1B) *эквивалентно каждому из следующих условий:*

(2′) $(2k)^{2k} \not\equiv 1 \pmod q$;

(2″) $p^{2k} \not\equiv 1 \pmod q$.

Доказательство. Прежде всего покажем, что из условия (2) следует (2′). Пусть h — первообразный корень по модулю q, и пусть $p \equiv h^s \pmod q$. Если $(2k)^{2k} \equiv 1 \pmod q$, то $h^{2ks} \equiv p^{2k} \equiv \equiv (2k)^{2k}p^{2k} \equiv (2kp)^{2k} \equiv (q-1)^{2k} \equiv 1 \pmod q$. Следовательно, $q-1 = 2kp$ делит $2ks$, так что $p \mid s$ и $p \equiv a^p \pmod q$, где $a \equiv h^{s/p} \pmod q$.

Теперь докажем, что из условия (2′) следует (2″). Если $p^{2k} \equiv 1 \pmod q$, то $(2k)^{2k} \equiv (2k)^{2k}p^{2k} \equiv (q-1)^{2k} \equiv 1 \pmod q$.

Наконец, покажем, что из условия (2″) следует (2). Если существует такое число a, что $p \equiv a^p \pmod q$, то $p^{2k} \equiv a^{2kp} \equiv a^{q-1} \equiv 1 \pmod q$. □

В табл. 6 (см. Лежандр, 1823) для каждого нечетного простого числа $p < 100$ выбрано простое число q и указаны первообразный корень h по модулю q и множество R вычетов p-х степеней по модулю q. Вычисления, которые достаточно длинны, проведены с использованием первообразного корня по модулю q. Они устанавливают справедливость условия (2).

Для бóльших значений p вычисления становятся затруднительными. Однако беглый взгляд на таблицу показывает, что в каждом

Таблица 6.

p	q	h	R
3	$7 = 2 \times 3 + 1$	3	± 1
5	$11 = 2 \times 5 + 1$	2	± 1
7	$29 = 4 \times 7 + 1$	2	$\pm 1,\ \pm 12$
11	$23 = 2 \times 11 + 1$	5	± 1
13	$53 = 4 \times 13 + 1$	2	$\pm 1,\ \pm 23$
17	$137 = 8 \times 17 + 1$	3	$\pm 1,\ \pm 10,\ \pm 37,\ \pm 41$
19	$191 = 10 \times 19 + 1$	19	$\pm 1,\ \pm 7,\ \pm 39,\ \pm 49,\ \pm 82$
23	$47 = 2 \times 23 + 1$	5	± 1
29	$59 = 2 \times 29 + 1$	2	± 1
31	$311 = 10 \times 31 + 1$	17	$\pm 1,\ \pm 6,\ \pm 36,\ \pm 52,\ \pm 95$
37	$149 = 4 \times 37 + 1$	2	$\pm 1,\ \pm 44$
41	$83 = 2 \times 41 + 1$	2	± 1
43	$173 = 4 \times 43 + 1$	2	$\pm 1,\ \pm 80$
47	$659 = 14 \times 47 + 1$	2	$\pm 1,\ \pm 12,\ \pm 55,\ \pm 144,\ \pm 249$ $\pm 270,\ \pm 307$
53	$107 = 2 \times 53 + 1$	2	± 1
59	$827 = 14 \times 59 + 1$	2	$\pm 1,\ \pm 20,\ \pm 124,\ \pm 270,\ \pm 337$ $\pm 389,\ \pm 400$
61	$977 = 16 \times 61 + 1$	3	$\pm 1,\ \pm 52,\ \pm 80,\ \pm 227,\ \pm 252$ $\pm 357,\ \pm 403,\ \pm 439$
67	$269 = 4 \times 67 + 1$	2	$\pm 1,\ \pm 82$
71	$569 = 8 \times 71 + 1$	3	$\pm 1,\ \pm 76,\ \pm 86,\ \pm 277$
73	$293 = 4 \times 73 + 1$	2	$\pm 1,\ \pm 138$
79	$317 = 4 \times 79 + 1$	2	$\pm 1,\ \pm 114$
83	$167 = 2 \times 83 + 1$	5	± 1
89	$179 = 2 \times 89 + 1$	2	± 1
97	$389 = 4 \times 97 + 1$	2	$\pm 1,\ \pm 115$

случае q выбрано равным $2p+1$, или $4p+1$, или $8p+1$, или $10p+1$, или $14p+1$, или $16p+1$. В самом деле, справедливо такое следствие теоремы Софи Жермен (Лежандр, 1823).

(1D) *Если p — нечетное простое число и число $q = 2p+1$ также простое, то первый случай теоремы Ферма справедлив для показателя p.*

Доказательство. Покажем, что число q удовлетворяет условиям утверждения (1B).

Если целые числа x, y, z не кратны q и $x^p + y^p + z^p \equiv 0 \pmod{q}$, то $x^p \equiv \pm 1 \pmod{q}$, $y^p \equiv \pm 1 \pmod{q}$, $z^p \equiv \pm 1 \pmod{q}$, поскольку $p = (q-1)/2$. Следовательно, $0 \equiv x^p + y^p + z^p \equiv \pm 1 \pm 1 \pm 1 \not\equiv 0 \pmod{q}$, а это противоречит предположению.

Аналогично, если $p \equiv a^p \pmod{q}$, то условие $(2')$ не выполнено, так что $2p+1 = q$ делит $2^2 - 1 = 3$, чего быть не может. □

Лежандр (1823) обобщил этот критерий следующим образом.

(1E) *Если p — простое число, $p > 3$ и число $q = 4p+1$, или $q = 8p+1$, или $q = 10p+1$, или $q = 14p+1$, или $q = 16p+1$ также простое, то первый случай теоремы Ферма справедлив для показателя p.*

Доказательство. Покажем, что в каждом случае q удовлетворяет условиям утверждения (1B).

Случай 1. Пусть $q = 4p+1$.

Если $p \equiv a^p \pmod{q}$, то по условию $(2')$ имеем $4^4 \equiv 1 \pmod{q}$, так что $4p+1 = q$ делит $255 = 3 \times 5 \times 17$, чего быть не может.

Проверим справедливость первого условия. Для этого обозначим через w первообразный корень четвертой степени из 1 по модулю q. Тогда $\{1, w, w^2, w^3\}$ — корни сравнения $X^4 - 1 \equiv 0 \pmod{q}$, причем $w^2 \equiv -1 \pmod{q}$, $w^3 \equiv -w \pmod{q}$. Если первое условие не выполняется, то согласно утверждению (1A) существуют показатели $i \neq j$, $0 \leqslant i, j \leqslant 3$, такие, что $w^j \equiv w^i + 1 \pmod{q}$. Кроме тривиальных случаев, это приводит к одной из следующих возможностей: $w \equiv \pm 2 \pmod{q}$ или $2w \equiv \pm 1 \pmod{q}$. После возведения в квадрат получим, что $q = 5$, а это неверно.

Случай 2. Пусть $q = 8p+1$.

Если $p \equiv a^p \pmod{q}$, то, проведя такие же рассуждения, как и выше, получим, что число $8p+1 = q$ делит $8^8 - 1$, а значит, оно

делит и $8^4 - 1 = 4095 = 3^2 \times 5 \times 7 \times 13$ или $8^4 + 1 = 4097 = 17 \times 241$, чего быть не может.

Если первое условие не выполняется и w — первообразный корень восьмой степени из 1 по модулю q, то найдутся такие показатели $i \neq j$, $0 \leqslant i, j \leqslant 7$, что $w^j \equiv w^i + 1 \pmod{q}$. Так как $w^4 \equiv -1 \pmod{q}$, можно рассматривать сравнения $w^j \equiv \pm w^i \pm 1 \pmod{q}$, где $0 \leqslant i \leqslant 3$. Поскольку первообразные корни восьмой степени из 1 по модулю q равны $\pm w$, $\pm w^3$, причем $w^3 \equiv -w^{-1} \pmod{q}$, изучение сводится к следующим возможностям:

(i) $w^j \equiv \pm 2 \pmod{q}$ $(j = 1, 2)$;
(ii) $w^2 \equiv w \pm 1 \pmod{q}$;
(iii) $2w \equiv \pm 1 \pmod{q}$.

Обсудим эти случаи.

(i) Возведение в четвертую степень приводит к тому, что $q \mid 15$ или $q = 17$, а это противоречит предположению.

(ii) Возведем сравнение в квадрат:

$$-1 \equiv w^2 \pm 2w + 1 \equiv \begin{cases} w + 1 + 2w + 1 \equiv 3w + 2 \pmod{q}, \\ w - 1 - 2w + 1 \equiv -w \pmod{q}. \end{cases}$$

Следовательно, $w \equiv \pm 1 \pmod{q}$, что также противоречит предположению.

(iii) Возводя сравнение в четвертую степень, получим $q = 17$, что вновь означает противоречие.

Случай 3. Пусть $q = 16p + 1$.

Если $p \equiv a^p \pmod{q}$, то, используя тот же самый метод, получим, что $16p+1 = q$ делит $16^{16} - 1 = (16^8+1)(16^4+1)(16^2+1) \times 17 \times 15$. Ясно, что $16p + 1$ не делит 15, 17, 257. Если $16p + 1$ делит число $16^4 + 1 = 65537$, которое является простым (кстати, простым Ферма, $2^{16} + 1$), то $p = 16^3$, чего быть не может. Если $16p + 1$ делит $16^8 + 1 = 2^{32} + 1 = 641 \times 6700417$ (разложение на простые множители найдено Эйлером), то $p = 40$ или 418776, т. е. мы снова приходим к противоречию.

Если первое условие не выполняется и w — первообразный корень шестнадцатой степени из 1 по модулю q, то, так как $\pm w$, $\pm w^3$, $\pm w^5$, $\pm w^7$ являются первообразными корнями шестнадцатой степени из 1 по модулю q и поскольку $w^8 \equiv -1 \pmod{q}$, существуют числа i, j, $0 \leqslant i \leqslant j \leqslant 7$, такие, что $w^j \equiv \pm w^i \pm 1 \pmod{q}$. Это приводит к одному из следующих сравнений со всеми возможными вариантами расстановки знаков:

(i) $w^j \equiv \pm 2 \pmod{q}$ $(j = 1, 2, \ldots, 7)$;
(ii) $w^2 \equiv w \pm 1 \pmod{q}$;
(iii) $w^3 \equiv \pm w + 1 \pmod{q}$;
(iv) $w^4 \equiv w \pm 1 \pmod{q}$;
(v) $w^4 \equiv \pm w^2 \pm 1 \pmod{q}$.

Обсудим все эти возможности.

(i) Возведение в восьмую степень приводит к тому, что $q \mid 257$ или $q \mid 255 = 3 \times 5 \times 17$, что противоречит предположению.

(ii) Возведение в квадрат приводит к сравнению $w^4 \equiv -w \pmod{q}$, что невозможно, или $w^4 \equiv 3w + 2 \pmod{q}$. Во втором случае после повторного возведения в квадрат получаем сравнение $-1 \equiv 9w^2 + 12w + 4 \pmod{q}$, а подставляя $w^2 \equiv w + 1 \pmod{q}$, получим $3w \equiv -2 \pmod{q}$. Следовательно, $w^4 \equiv 3w + 2 \equiv 0 \pmod{q}$, что невозможно.

(iii) Возведем сравнение в куб:

$$-w \equiv \pm w^3 + 3w^2 \pm 3w + 1 \pmod{q}$$

и, сделав замену, получим

$$-w \equiv w \pm 1 + 3w^2 \pm 3w + 1 \pmod{q}.$$

В зависимости от выбора знака имеем $3w^2 + 5w + 2 \equiv 0 \pmod{q}$ или $3w^2 - w \equiv 0 \pmod{q}$.

В первом случае, умножая на w и делая замену, получим $5w^2 + 5w + 3 \equiv 0 \pmod{q}$. Вычитая, приходим к сравнению $2w^2 \equiv -1 \pmod{q}$ и, следовательно, $-2^4 \equiv 1 \pmod{q}$, так что $q \mid 17$, но это невозможно. Если $3w \equiv 1 \pmod{q}$, то $3w^3 \equiv -3w + 3 \equiv 2 \pmod{q}$, так что, возводя в куб, получаем $-3^3 w \equiv 8 \pmod{q}$, а значит, q делит 17, что противоречит предположению.

(iv) Возведем сравнение в квадрат: $-1 \equiv w^2 \pm 2w + 1 \pmod{q}$, а значит, $w^2 \equiv \mp 2w - 2 \pmod{q}$ и, следовательно, $w \pm 1 \equiv w^4 \equiv 4w^2 \pm 8w + 4 \pmod{q}$. В зависимости от выбора знака получим

$$4w^2 \equiv \begin{cases} -7w - 3 \\ 9w - 5 \end{cases} \pmod{q}$$

и, вычитая, придем к сравнениям

$$0 \equiv \begin{cases} w + 5 \\ w + 3 \end{cases} \pmod{q}.$$

Так что $w^4 \equiv w \pm 1 \equiv -4 \pmod{q}$, и, возводя в квадрат, получим $-1 \equiv 16 \pmod{q}$, а значит, $q \mid 17$, что невозможно.

(v) Возводя сравнение в квадрат, получим $-1 \equiv w^4 \pm 2w^2 + 1 \pmod q$. Подставляя $w^4 \equiv \pm w^2 \pm 1 \pmod q$, во всех случаях придем к сравнениям $w^2 \equiv \pm 1 \pmod q$, что невозможно.

Случай 4. Пусть $q = 10p + 1$.

Если $p \equiv a^p \pmod q$, то, проведя аналогичные рассуждения, получим, что $10p + 1 = q$ делит $(10^5 + 1)(10^5 - 1)$. Если q делит $10^5 + 1 = 100\,001 = 11 \times 9091$ (а число 9091 простое), то $p = 909$, что невозможно. Если q делит $10^5 - 1 = 99\,999 = 3^2 \times 41 \times 271$, то $p = 4$ или 27, что также невозможно.

Если первое условие не выполняется и w — первообразный корень десятой степени из 1 по модулю q, то найдутся такие показатели i, j, $0 \leqslant i \leqslant j < 4$, что $w^j \equiv \pm w^i \pm 1 \pmod q$. Указанные выше условия приводят к одному из следующих сравнений:

(i) $w^j \equiv \pm 2 \pmod q$ $(j = 1, 2, 3, 4)$;
(ii) $w^2 \equiv w \pm 1 \pmod q$;
(iii) $w^4 \equiv w \pm 1 \pmod q$.

Обсудим различные возможности.

(i) Возведение в пятую степень приводит к тому, что $q \mid 31$ или $q \mid 33 = 3 \times 11$, а это невозможно.

(ii) Запишем сравнения

$$w^4 \equiv w^2 \pm 2w + 1 \equiv w \pm 1 \pm 2w + 1 \equiv \begin{cases} 3w + 2 \\ -w \end{cases} \pmod q.$$

Второй случай невозможен. В первом случае, умножая на w и подставляя $-1 \equiv 3w^2 + 2w = 3w + 3 + 2w \pmod q$, получим $5w \equiv -4 \pmod q$. Умножая на предыдущее сравнение, имеем $-5 \equiv -12w - 8 \pmod q$, так что $12w \equiv -3 \pmod q$ и $4w \equiv -1 \pmod q$, а следовательно, вычитая, получим $w \equiv -3 \pmod q$ и, таким образом, $q \mid 11$, что противоречит предположению.

(iii) Умножив на w, получим $-1 \equiv w^2 \pm w \pmod q$, следовательно, $w^2 \equiv \mp w - 1 \pmod q$, а это сравнение рассмотрено в случае (ii).

Случай 5. Пусть $q = 14p + 1$.

Если $p \equiv a^p \pmod q$, то мы аналогичным образом получим, что q делит $14^7 + 1$ или $14^7 - 1$. Но $14^7 + 1 = 105\,413\,505 = 3 \times 5 \times 7\,027\,567$ (число 7 027 567 простое). Тогда $p = 501\,969$, что противоречит предположению, так как это число кратно 3. Далее, $14^7 - 1 = 105\,413\,503 = 13 \times 8\,108\,731$ (это последнее число простое). Тогда $p = 579\,195$, чего быть не может.

Если первое условие не выполняется и w — первообразный корень четырнадцатой степени из 1 по модулю q, то существуют показатели $i \neq j$, $0 \leqslant i, j \leqslant 13$, такие, что $w^j \equiv w^i + 1 \pmod q$. Так как $w^7 \equiv -1 \pmod q$, указанные выше условия приводят к одному из следующих сравнений:

(i) $w^j \equiv \pm 2 \pmod q$ $(j = 1, 2, \ldots, 6)$;
(ii) $w^2 \equiv w \pm 1 \pmod q$;
(iii) $w^3 \equiv \pm w + 1 \pmod q$.

Обсудим различные случаи.

(i) Если $-1 \equiv \pm 2^7 \pmod q$, то $q \mid 127$ или $129 = 3 \times 43$, поэтому $p = 3$, а это противоречит условию.

(ii) Если $w^2 \equiv w \pm 1 \pmod q$, то

$$w^4 \equiv w^2 \pm 2w + 1 \equiv w \pm 1 \pm 2w + 1 \equiv \begin{cases} 3w + 2 \\ -w \end{cases} \pmod q.$$

Второй из этих случаев невозможен. В первом случае возведем сравнение в квадрат:

$$-w \equiv 9w^2 + 12w + 4 \equiv 9w + 9 + 12w + 4 \pmod q,$$

следовательно, $22w \equiv -13 \pmod q$. Тогда $22w^2 - 22 \equiv -13 \pmod q$, так что $22w^2 \equiv 9 \pmod q$. Значит, $-13w \equiv 9 \pmod q$, и потому $9w \equiv -4 \pmod q$, $-4w \equiv 5 \pmod q$, $5w \equiv 1 \pmod q$. Таким образом, $25 \equiv -20w \equiv -4 \pmod q$, а следовательно, $q \mid 29$, что невозможно.

(iii) Возводя сравнение $w^3 \equiv \pm w + 1 \pmod q$ в куб, получим

$$-w^2 \equiv \pm w^3 + 3w^2 \pm 3w + 1$$
$$\equiv \pm w + 1 + 3w^2 \pm 3w + 1 \equiv 3w^2 \pm 4w + 2 \pmod q,$$

следовательно, $2w^2 \pm 2w + 1 \equiv 0 \pmod q$, так что $2(\pm w + 1) \pm 2w^2 + \pm w \equiv 0 \pmod q$ и

$$\begin{cases} 2w^2 + 3w + 2 \equiv 0 \pmod q, \\ -2w^2 - w + 2 \equiv 0 \pmod q, \end{cases}$$

а значит,

$$\begin{cases} w + 1 \equiv 0 \pmod q, \\ -3w + 3 \equiv 0 \pmod q, \end{cases}$$

поэтому $w \equiv \mp 1 \pmod q$, что невозможно. □

С помощью этого критерия Лежандр фактически доказал справедливость первого случая теоремы Ферма для каждого просто-

го показателя $p < 197$. Действительно, для каждого такого простого числа p существует простое число $q = 2kp + 1$, где $2k \in$ $\in \{2, 4, 8, 10, 14, 16\}$. С другой стороны, число $38 \times 197 + 1 = 7487$ простое, но $2k \times 197 + 1$ не является простым, если $2k < 38$, $6 \nmid 2k$.

Результаты Лежандра носят ограниченный характер из-за значительного роста величин рассматриваемых чисел. Например, проверка того, не будет ли $p = 197$ p-й степенью по модулю $q = 7487$, приводит к исследованию вопроса, будет ли 7487 делить $38^{19} \pm 1$. Мейе в 1897 г. обобщил результат Лежандра, подняв границу до $p = 211$.

Мириманов использовал метод, основанный на числах Бернулли, и в 1905 г. распространил результаты до $p = 257$.

В 1908 г. Диксон опубликовал две статьи, в которых он развил идеи Лежандра и, проводя более тщательный анализ, включающий в себя сравнения, показал, что первый случай теоремы Ферма справедлив для каждого простого показателя $p < 7000$ (за исключением $p = 6857$, хлопоты по проверке которого он на себя не взял). См. также комментарии Мейе (1908).

Большего успеха в этом направлении добились Краснер (1940), Дене (1951) и Ривуар (1968).

Для простых чисел p, таких, что число $6p + 1$ или $12p + 1$ также простое, этот метод доказательства не применим и не приводит к какому-либо заключению. Заметим, что в 1974 г. Ганди объявил без доказательства, что если числа p и $6p + 1$ — простые, то первый случай имеет место для показателя p. Поскольку доказательство не было опубликовано, есть основания сомневаться в достоверности этого утверждения (см. работу Грэнвилля и Пауэлла (1988)).

Вот интересный, но очень трудный вопрос: существует ли бесконечно много простых чисел p, таких, что число $2p+1$ (или $4p+1$, или $8p + 1$ и т. д.) также является простым. Эта проблема обсуждается в приложении к настоящей главе.

Отметим также следующий результат Вандивера (1926).

(1F) *Пусть p и $q = 2kp+1$ — нечетные простые числа (где $k \geqslant 1$). Если $2k = 2^v p^h$, где $h \geqslant 0$ и p не делит v, а число 2 не является p-й степенью по модулю q, то выполнено условие (2), приведенное выше.*

Доказательство. Покажем справедливость условия $(2')$. Если $(2k)^{2k} \equiv 1 \pmod q$, или, что эквивалентно, $p^{2k} \equiv 1 \pmod q$, то $2^{2kv} \equiv 2^{2kv} p^{2kh} = (2^v p^h)^{2k} \equiv (2k)^{2k} \equiv 1 \pmod q$. Так как p не

делит v, существуют такие целые числа a и b, что $av = 1 + bp$. Тогда

$$1 \equiv 2^{2kva} \equiv 2^{(1+bp)2k} \equiv 2^{2k}(2^{2kp})^b = 2^{2k}(2^{q-1})^b \equiv 2^{2k} \pmod{q}.$$

Если g — первообразный корень по модулю q и $2 \equiv g^s \pmod{q}$, то $1 \equiv 2^{2k} \equiv g^{2ks} \pmod{q}$. Таким образом, $q - 1 = 2kp$ делит $2ks$, а следовательно, $s = ps'$ и $2 \equiv (g^{s'})^p \pmod{q}$, что противоречит предположению. □

Используя утверждение (1B), Вандивер в 1926 г. получил следующий результат, который, впрочем, уже был доказан Вендтом в 1894 г. с использованием его формы теоремы Софи Жермен.

(1G) *Если нечетные простые числа p и $q = 2kp + 1$ таковы, что $2k = 2^v p^h$, $h \geqslant 0$, где v не делится на p, и сравнение $X^p + Y^p + Z^p \equiv 0 \pmod{q}$ имеет лишь тривиальные решения, то первый случай теоремы Ферма справедлив для показателя p.*

Доказательство. В силу результатов (1B) и (1F) достаточно показать, что 2 не является p-й степенью по модулю q. Если $2 \equiv a^p \pmod{q}$, то $a^p + (-1)^p + (-1)^p \equiv 2 + (-1) + (-1) \equiv 0 \pmod{q}$, что противоречит предположению. □

Теорема Софи Жермен, ее следствия и разновидности были получены заново рядом авторов. В 1953 г. Тэбо доказал следующее утверждение.

(1H) *Если целое число $m \geqslant 2$ таково, что $2m + 1$ — простое число, и существуют попарно взаимно простые ненулевые целые числа x, y, z, такие, что $x^m + y^m = z^m$, то $2m + 1$ делит xyz.*

Доказательство. Если $2m + 1$ не делит x, то по малой теореме Ферма $x^{2m} \equiv 1 \pmod{2m + 1}$, откуда следует, что $x^m \equiv \pm 1 \pmod{2m + 1}$.

Аналогичным образом,

$$y^m \equiv \pm 1 \pmod{2m + 1},$$
$$z^m \equiv \pm 1 \pmod{2m + 1},$$

следовательно, $0 = x^m + y^m - z^m \equiv (\pm 1) + (\pm 1) - (\pm 1) \pmod{2m+1}$, что невозможно. □

Этот же самый результат (даже с еще более сильным предположением, что m — простое число) был заново доказан Стоуном в 1963 г. и Ганди в 1966 г. в том же самом журнале[3]!

[3] *Amer. Math. Monthly. — Прим. перев.*

В 1965 г. Ганди доказал такой факт, подобный результату Тэбо.

(1I) *Если целое число $m \geqslant 2$ таково, что $4m+1$ — простое число, и x, y, z — ненулевые попарно взаимно простые целые числа, такие, что $x^m + y^m = z^m$, то $4m+1$ делит xyz.*

Доказательство. Если $m = 3$, то утверждение тривиально (см. разд. I.4).

Пусть $m > 3$. Предположим, что $4m+1$ не делит xyz. Поскольку $x^m + y^m = z^m$, мы можем записать $x^{2m} + y^{2m} + 2x^m y^m = z^{2m}$. Так как $4m+1$ — простое число, не делящее x, по малой теореме Ферма $x^{4m} \equiv 1 \pmod{4m+1}$, а значит, $x^{2m} \equiv \pm 1 \pmod{4m+1}$. Аналогичным образом,

$$y^{2m} \equiv \pm 1 \pmod{4m+1}$$

и

$$z^{2m} \equiv \pm 1 \pmod{4m+1}.$$

Следовательно, $\pm 1 \pm 1 + 2x^m y^m \equiv \pm 1 \pmod{4m+1}$, так что $2x^m y^m \equiv \equiv \pm 1$ или $\pm 3 \pmod{4m+1}$ и $\pm 4 \equiv 4x^{2m} y^{2m} \equiv 1$ или $9 \pmod{4m+1}$. Из этого следует, что $4m+1 = 3, 5$ или 13, а значит, $m = 3$, что противоречит исходному предположению. □

Этот же самый результат (с еще более сильным предположением, что m — простое число) был доказан заново Ганди в 1966 и 1970 гг., а также Кристиллем в 1967 г.

Перисастри (1969) доказал следующие утверждения.

(1J) *Если простое число $p > 51$ таково, что число $8p+1$ также является простым, и x, y, z — ненулевые попарно взаимно простые целые числа, такие, что $x^p + y^p = z^p$, то $8p+1$ делит xyz.*

(1K) *Если целое число $m \geqslant 3$ таково, что $3m+1$ — простое число, и x, y, z — ненулевые попарно взаимно простые числа, такие, что $x^m + y^m = z^m$, то $3m+1$ делит xyz.*

Кришнасастри и Перисастри в 1965 г. доказали следующий результат.

(1L) *Если p — нечетное простое число и целые числа x, y, z таковы, что $x^p + y^p = z^p$, причем p не делит xz, то существует целое число $k \geqslant 1$, такое, что $1 + kp$ делит z.*

Объединяя результат (1C) с теоремой Софи Жермен, получим такое утверждение (см. Стоун (1963), Перисастри (1968)).

(1M) *Пусть p и $2p+1$ — нечетные простые числа. Если ненулевые попарно взаимно простые целые числа x, y, z таковы, что $x^p + y^p + z^p = 0$, то p^2 делит одно (и только одно) из целых чисел x, y, z.*

Доказательство. В силу теоремы Софи Жермен можно полагать, что p делит, например, z. Из утверждения (1C) следует, что p^2 делит z. □

В 1923 и 1925 гг. Поме получил несколько достаточных условий для первого случая теоремы Ферма для простого показателя p, используя при этом подобные методы.

(1N) *Пусть p — нечетное простое число. Предположим, что имеет место какое-либо одно из следующих условий:*

(a) $p \equiv 1 \pmod 4$ *и* $2p+1$ *делит* $2^p + 1$;
(b) $p \equiv 3 \pmod 4$ *и* $2p+1$ *делит* $2^p - 1$;
(c) $4p+1$ *делит* $2^{2p} + 1$;
(d) $4p+1 \equiv 5 \pmod{12}$ *и* $4p+1$ *делит* $3^{3p} + 1$;
(e) $8p+1$ *делит* $2^{4p} - 1$;
(f) $10p+1$ *делит* $5^{5p} - 1$.

Тогда для показателя p справедлив первый случай теоремы Ферма.

Все приведенные выше результаты не являются достаточными для того, чтобы утверждать существование бесконечного числа простых показателей p, для которых справедлив первый случай теоремы Ферма. Лишь в 1985 г. этот факт был впервые доказан Адлеманом и Хиз-Брауном, а также Фуври с использованием аналитических методов.

Ранее, в 1897 г., изучая группу классов кругового поля, Мейе показал, что для каждого нечетного простого числа p существует число e (зависящее от p), такое, что первый случай теоремы Ферма справедлив для показателя p^e. В частности, это влечет за собой существование бесконечного множества попарно взаимно простых показателей, для которых первый случай имеет место. Это последнее утверждение было доказано заново Капферером в 1964 г. Его доказательство не элементарно, так как оно использует теоремы Фуртвенглера, обобщенные Морией (использующие теорию полей классов). В 1978 г. Пауэлл независимо нашел следующее очень простое доказательство.

(10)

(1) *Пусть p — произвольное нечетное простое число, $n = p\times$ $\times(p-1)/2 = 2^u m$, где $u \geqslant 0$, число m нечетно и ненулевые целые числа x, y, z таковы, что $x^n + y^n + z^n = 0$. Тогда* НОД$(m, xyz) \neq 1$.

(2) *Существует бесконечное множество попарно взаимно простых показателей, для которых справедлив первый случай теоремы Ферма.*

Доказательство. (1) Если $p = 3$, то $n = 3$ и условие не выполняется. Пусть $p > 3$. Предположим, что НОД$(m, xyz) = 1$. Тогда $p \nmid xyz$, так что $x^{(p-1)/2} \equiv \pm 1 \pmod p$ и $x^n \equiv \pm 1 \pmod p$. Аналогично, $y^n \equiv \pm 1 \pmod p$, $z^n \equiv \pm 1 \pmod p$, а следовательно, $x^n + y^n + z^n \not\equiv 0 \pmod p$ и тем более $x^n + y^n + z^n \neq 0$.

(2) Предположим, что $n_1, \ldots, n_k$ — попарно взаимно простые показатели, для которых справедлив первый случай теоремы Ферма. Рассмотрим арифметическую прогрессию $\{-1 + 4n_1 n_2 \ldots n_k t \mid t = 0, 1, 2, \ldots\}$. По теореме Дирихле о простых числах в арифметических прогрессиях существует нечетное простое число p, такое, что $p \equiv -1 \pmod{4n_1 n_2 \ldots n_k}$. Пусть $n_{k+1} = p(p-1)/2$, так что n_{k+1} нечетно. Поскольку НОД $(p(p-1)/2, (p+1)/2) = 1$, мы получаем, что НОД$(n_{k+1}, n_1 \ldots n_k) = 1$. В силу утверждения (1) первый случай справедлив для показателя n_{k+1}, а этого достаточно, чтобы завершить доказательство. □

Список литературы

1823 Legendre, A.M., *Recherches sur quelques objets d'analyse indéterminée, et particulièrement sur le théorème de Fermat*, Mém. Acad. Roy. Sci. Institut France, **6** (1823), 1–60; reprinted as "Second Supplément" in 1825, to a printing of *Essai sur la Théorie des Nombres* (2^e édition), Courcier, Paris; reprinted in Sphinx–Oedipe, **4** (1909), 97–128.

1879 Germain, S., *Oeuvres Philosophiques* (editor H. Stupuy), pp. 298–302 and 363–364, P. Ritti, Paris, 1879.

1894 Wendt, E., *Arithmetische Studien über den letzten Fermatschen Satz, welcher aussagt daß die Gleichung $a^n = b^n + c^n$ für $n > 2$ in ganzen Zahlen nicht auflösbar ist*, J. Reine Angew. Math., **113** (1894), 335–346.

1897 Maillet, E., *Sur l'équation indéterminée $ax^{\lambda^t} + by^{\lambda^t} = cz^\lambda$*, Assoc. Francaise Avanc. Sci., St. Etienne, **26** (1897), 156–168.

1905 Mirimanoff, D., *L'équation indéterminée* $x^l + y^l + z^l = 0$ *et le critérium de Kummer*, J. Reine Angew. Math., **128** (1905), 45–68.

1908 Dickson, L.E., *On the last theorem of Fermat*, Messenger Math., **38** (1908), 14–32.

1908 Dickson, L.E., *On the last theorem of Fermat* (second paper), Quart. J. Pure Appl. Math., **40** (1908), 27–45.

1908 Maillet, E., *Question* 612 *de Worms de Romilly*, L'Interm. Math., **15** (1908), 247–248.

1910 Bachmann, P., *Niedere Zahlentheorie*, Teubner, Leipzig, 1910; reprinted by Chelsea, New York, 1966.

1923 Pomey, L., *Sur le dernier théorème de Fermat*, C. R. Acad. Sci. Paris, **177** (1923), 1187–1190.

1925 Pomey, L., *Sur le dernier théorème de Fermat*, J. Math. Pures Appl., (9), **4** (1925), 1–22.

1926 Vandiver, H.S., *Note on trinomial congruences and the first case of Fermat's last theorem*, Ann. of Math., **27** (1926), 54–56.

1935 Bang, A.S., *Om tal af Formen* $a^m + b^m - c^m$, Mat. Tidsskrift, **B** (1935), 49–59.

1940 Krasner, M., *À propos du critère de Sophie Germain–Furtwängler pour le premier cas du théorème de Fermat*, Mathematica (Cluj), **16** (1940), 109–114.

1951 Dénes, P., *An extension of Legendre's criterion in connection with the first case of Fermat's last theorem*, Publ. Math. Debrecen, **2** (1951), 115–120.

1953 Thébault, V., *A note on number theory*, Amer. Math. Monthly, **60** (1953), 322–323.

1963 Stone, D.E., *On Fermat's last theorem*, Amer. Math. Monthly, **70** (1963), 976–977.

1964 Kapferer, H., *Verifizierung des symmetrischen Teils der Fermatschen Vermutung für unendlich viele paarweise teilerfremde Exponenten E*, J. Reine Angew. Math., **214/5** (1964), 360–372.

1965 Gandhi, J.M., *A note on Fermat's last theorem*, Math. Notae, **20** (1965), 107–108.

1965 Krishnasastri, M.S.R. and Perisastri, M., *On some diophantine equations*, Math. Student, **33** (1965), 73–76.

1966 Grosswald, E., *Topics from the Theory of Numbers*, Macmillan, New York, 1966.

1966 Gandhi, J.M., *A note on Fermat's last theorem*, Amer. Math. Monthly, **73** (1966), 1106–1107.

1967 Christilles, W.E., *A note concerning Fermat's conjecture*, Amer. Math. Monthly, **74** (1967), 292–294.
1968 Perisastri, M., *A note on Fermat's last theorem*, Amer. Math. Monthly, **75** (1968), 170.
1968 Rivoire, P., *Dernier Théorème de Fermat et Groupe de Classes dans Certains Corps Quadratiques Imaginaires*, Thèse, Université Clermont-Ferrand, 1968, 59 pp.; reprinted in Ann. Sci. Univ. Clermont-Ferrand II, **68** (1979), 1–35.
1969 Perisastri, M., *On Fermat's last theorem*, Amer. Math. Monthly, **76** (1969), 671–675.
1970 Gandhi, J.M., *On Fermat's last theorem*, An. Ştiinţ. Univ. "Al. I. Cuza" Iaşi, Seçt. I (N.S), **16** (1970), 241–248.
1974 Gandhi, J.M., *On Fermat's last theorem*, Notices Amer. Math. Soc., **21** (1974), A-53.
1978 Powell, B., *Proof of a special case of Fermat's last theorem*, Amer. Math. Monthly, **85** (1978), 750–751.
1985 Adleman, L.M. and Heath-Brown, D.R., *The first case of Fermat's last theorem*, Invent. Math., **79** (1985), 409–416.
1985 Fouvry, E., *Théorème de Brun–Titchmarsh. Application au théorème de Fermat*, Invent. Math., **79** (1985), 383–407.
1988 Granville, A. and Powell, B., *On Sophie Germain's type criteria for Fermat's last theorem*, Acta Arith., **50** (1988), 265–277.

IV.2. Теорема Вендта

В 1894 г. Вендт указал детерминантный критерий существования нетривиального решения сравнения Ферма

$$X^p + Y^p + Z^p \equiv 0 \pmod{q}, \tag{2.1}$$

где p, q — различные нечетные простые числа.

Сначала исключим из нашего обсуждения следующий тривиальный случай (он также справедлив без предположения простоты показателя в сравнении (2.1)).

(2A) *Если простое число q нечетно и натуральное число n таково, что* НОД$(n, q-1) = 1$, *то существуют целые числа x, y, z, не кратные q, такие, что $x^n + y^n + z^n \equiv 0 \pmod{q}$.*

Доказательство. По предположению НОД$(n, q-1) = 1$, а значит, существуют такие целые числа a и b, что $an + b(q-1) = 1$. Пусть x_0, y_0, z_0 — целые числа, не кратные q, такие, что $x_0 + y_0 + z_0 \equiv 0$

(mod q). Тогда

$$\begin{cases} x_0^{an} \equiv x_0 \pmod q, \\ y_0^{an} \equiv y_0 \pmod q, \\ z_0^{an} \equiv z_0 \pmod q, \end{cases}$$

следовательно, $(x_0^a)^n + (y_0^a)^n + (z_0^a)^n \equiv 0 \pmod q$. □

В частности, если $n = p$ — простое число, не делящее $q - 1$, то сравнение (2.1) имеет нетривиальное решение.

Критерий Вендта выражается в терминах циркулянты биномиальных коэффициентов. В общем случае, пусть $n \geqslant 1$, и пусть $\xi_i = \cos 2\pi i/n + \sqrt{-1}\sin 2\pi i/n$ (для $i = 0, 1, \ldots, n-1$) — все n корней степени n из 1. Заметим, что $\xi_0 = 1$. *Циркулянтой* n-набора $(a_0, a_1, \ldots, a_{n-1})$ комплексных чисел a_i называется определитель матрицы

$$C = \begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & \ldots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \ldots & a_0 \end{pmatrix}. \tag{2.2}$$

Обозначим его через $\mathrm{Circ}(a_0, a_1, \ldots, a_{n-1})$. Циркулянта выражается через корни степени n из 1, а также результант двух многочленов (см. разд. II.4). Споттисвуд (1853), а также Штерн (1871) и Муир (1920) доказали такой факт.

Лемма 2.1. *Пусть* $a_0, a_1, \ldots, a_{n-1} \in K$, $G(X) = a_0 + a_1 X + \ldots + a_{n-1}X^{n-1}$ *и* $\xi_0 = 1, \xi_1, \ldots, \xi_{n-1}$ — *корни степени* n *из* 1. *Циркулянта набора* $a_0, a_1, \ldots, a_{n-1}$ *равна*

$$\mathrm{Circ}(a_0, a_1, \ldots, a_{n-1}) = \prod_{i=0}^{n-1} G(\xi_i) = \mathrm{Res}(G(X), X^n - 1)$$

(*где* Res *обозначает результант*).

Доказательство. Пусть

$$A = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

(матрица $n \times n$), так что матрицы $I, A, A^2, \ldots, A^{n-1}$ различны, причем $A^n = I$. Как легко видеть,

$$C = a_0 I + a_1 A + a_2 A^2 + \ldots + a_{n-1} A^{n-1}.$$

Характеристический многочлен матрицы A есть $\det(XA - I) = \pm(X^n - 1)$. Так как он имеет различные корни $\xi_0 = 1, \xi_1, \ldots, \xi_{n-1}$, матрица A диагонализируема, т. е. существует обратимая матрица U (с комплексными элементами), такая, что

$$UAU^{-1} = \begin{pmatrix} \xi_0 & 0 & \ldots & 0 \\ 0 & \xi_1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \xi_{n-1} \end{pmatrix}.$$

Следовательно,

$$UCU^{-1} = \begin{pmatrix} G(\xi_0) & 0 & \ldots & 0 \\ 0 & G(\xi_1) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & G(\xi_{n-1}) \end{pmatrix},$$

где $G(X) = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1}$. Значит, $\mathrm{Circ}(a_0, a_1, \ldots, a_{n-1}) = \det(C) = \det(UCU^{-1}) = \prod_{i=0}^{n-1} G(\xi_i)$. Из утверждения (4B) гл. II также следует, что $\mathrm{Circ}(a_0, a_1, \ldots, a_n) = \mathrm{Res}(G(X), X^n - 1)$. □

Следующий результат Вендта связан с циркулянтой биномиальных коэффициентов. Так, для всех натуральных чисел n положим *определитель Вендта* равным

$$W_n = \mathrm{Circ}\left(1, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}\right). \tag{2.3}$$

Если $G(X) = 1 + \binom{n}{1} X + \binom{n}{2} X^2 + \ldots + \binom{n}{n-1} X^{n-1} = (1+X)^n - X^n$, то согласно лемме мы имеем

$$W_n = \mathrm{Res}(G(X), X^n - 1) = \prod_{i=0}^{n-1} [(1 + \xi_i)^n - 1].$$

Теперь приведем критерий Вендта (1894) (см. также Мэтьюс (1895). Банг (1935) и пояснительное изложение, данное Ривуаром (1968)).

(2B) *Если простое число p нечетно и число $q = 2kp+1$ (где $k \geqslant 1$) также нечетно, то целые числа x, y, z, не кратные q и такие, что*

$x^p + y^p + z^p \equiv 0 \pmod q$, существуют в точности тогда, когда q делит W_{2k}.

Доказательство. В силу утверждения (1A) сравнение Ферма $X^p + Y^p + Z^p \equiv 0 \pmod q$ имеет нетривиальное решение тогда и только тогда, когда система сравнений

$$\begin{cases} X^{2k} \equiv 1 \pmod q, \\ (X+1)^{2k} \equiv 1 \pmod q \end{cases}$$

имеет нетривиальное решение, или, что равносильно, система сравнений

$$\begin{cases} X^{2k} - 1 \equiv 0 \pmod q, \\ (X+1)^{2k} - X^{2k} \equiv 0 \pmod q \end{cases}$$

имеет нетривиальное решение, что будет выполнено в точности тогда, когда результант многочленов $X^{2k} - 1$ и

$$G(X) = (X+1)^{2k} - X^{2k} = 1 + \binom{2k}{1} X + \binom{2k}{2} X^2 + \ldots + \binom{2k}{2k-1} X^{2k-1}$$

сравним с 0 по модулю q. По лемме 2.1 это означает, что $W_{2k} \equiv 0 \pmod q$. □

Теперь обратимся к результатам, связанным с вычислением определителя Вендта

$$W_n = \prod_{j=0}^{n-1} [(1 + \xi_j)^n - 1]. \tag{2.4}$$

Следующее утверждение было предъявлено Вендтом (1894) без доказательства и впоследствии доказано Мэтьюсом (1895), Бангом (1935), Э. Лемером (1935) и Фреймом (1980).

(2C) *Равенство $W_n = 0$ справедливо тогда и только тогда, когда n делится на* 6.

Доказательство. Предположим, что n кратно шести, и пусть

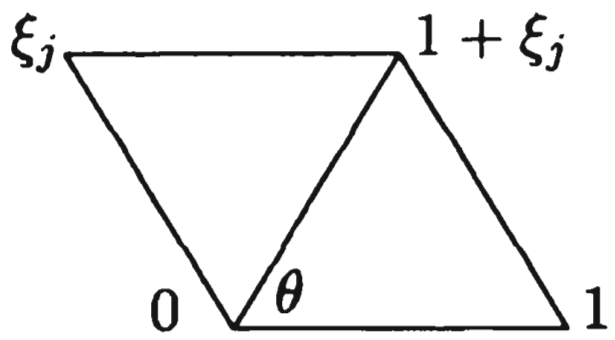
$$\xi = \xi_1 = \cos 2\pi/n + \sqrt{-1} \sin 2\pi/n.$$

Положим $l = n/3$, так что $\omega = \xi^l$ — первообразный кубический корень из 1. Тогда $1 + \omega + \omega^2 = 0$, следовательно, $1 + \xi^l = -\xi^{2l}$ и $(1 + \xi^l)^n = 1$. Таким образом, $W_n = 0$.

Обратно, если $W_n = 0$, то найдется такой индекс j, что

$$(1 + \xi_j)^r = 1,$$

а значит, ξ_j и $1+\xi_j$ — корни степени n из 1, и, поскольку треугольник с вершинами в точках 0, 1, $1+\xi_j$



является равносторонним, $\theta = 2\pi/6$ (или $\theta = -2\pi/6$) и $1+\xi_j$ — первообразный корень шестой степени из 1. Но $(1+\xi_j)^n = 1$, так что 6 делит n. □

Как следствие получаем такой результат.

(2D) *Если p и $6mp+1 = q$ — простые числа, то сравнение $X^p + Y^p + Z^p \equiv 0 \pmod q$ имеет нетривиальное решение.*

Доказательство. Утверждение следует непосредственно из результатов (2B) и (2C). □

Если n делится на 6, то, ввиду результата (2C), выражение для определителя Вендта обычно записывают в несколько измененном виде:

$$W_n = \prod_{i=0}^{n-1} G(\xi_i),$$

где

$$G(X) = \frac{(X+1)^n - X^n}{X^2 + X + 1}. \tag{2.5}$$

В 1935 г. Э. Лемер сформулировал без доказательства следующее утверждение.

(2E) *Если d делит n, то W_d делит W_n.*

Доказательство. Можно полагать, что $W_d \neq 0$, т. е. что $6 \nmid d$. Заметим, что, поскольку $d \mid n$, каждый корень из 1 степени d одновременно является и корнем из 1 степени n. Так как $W_d \neq 0$, мы получаем

$$\frac{W_n}{W_d} = \prod_{\xi_j^d = 1} \frac{(1+\xi_j)^n - 1}{(1+\xi_j)^d - 1} \times \prod_{\xi_i^n = 1, \xi_i^d \neq 1} [(1+\xi_i)^n - 1].$$

Если $n = de$, то

$$\frac{(1+\xi_j)^n - 1}{(1+\xi_j)^d - 1} = (1+\xi_j)^{d(e-1)} + \ldots + (1+\xi_j)^d + 1.$$

Таким образом, отношение W_n/W_d является целым алгебраическим числом, а так как оно еще и рационально, это число есть рациональное целое. □

Следующее свойство было также указано Э. Лемером без доказательства. Последнее появилось лишь в статье Фрейма (1980) (но не такое, как приведенное ниже). Более слабое утверждение, что $2^n - 1$ делит W_n, было доказано Бангом (1935).

(2F) *Если* $n \geqslant 1$, *то* $W_n = (-1)^{n-1}(2^n - 1)u^2$, *где* u — *целое число.*

Доказательство. Запишем выражение для определителя Вендта

$$W_n = \prod_{j=0}^{n-1} [(1+\xi^j)^n - 1],$$

где $\xi = \cos 2\pi/n + \sqrt{-1}\sin 2\pi/n$. Значит, в состав произведения для W_n входит множитель вида $2^n - 1$ (при $j = 0$), а если число n четно, то и множитель -1 (при $j = n/2$). Итак,

$$W_n = (-1)^{n-1}(2^n - 1) \prod_{j \neq 0, n/2} [(1+\xi^j)^n - 1].$$

Положим $u = \prod_{0<j<n/2}[(1+\xi^j)^n - 1]$. Заметим, что для каждого $j \neq 0,\ n/2$ выполнены равенства

$$(1+\xi^{-j})^n - 1 = \left[\xi^{-j}(1+\xi^j)\right]^n - 1 = (1+\xi^j)^n - 1,$$

поэтому $u \in \mathbb{R}$, $W_n = (-1)^{n-1}(2^n - 1)u^2$ и остается лишь показать, что $u \in \mathbb{Z}$. Пусть σ — произвольный автоморфизм поля $\mathbb{Q}(\xi)$, так что $\sigma(\xi) = \xi^l$, где $1 \leqslant l < n$ и НОД$(l, n) = 1$. Значит, $\sigma\left[(1+\xi^j)^n - 1\right] = (1+\xi^k)^n - 1$, где $0 < k < n/2$ и $jl \equiv \pm k \pmod n$, поскольку $(1+\xi^{-k})^n - 1 = (1+\xi^k)^n - 1$. Если $0 < j,\ j' < n/2$, то выберем числа $k,\ k'$ такими, что $0 < k,\ k' < n/2$ и $jl \equiv \pm k \pmod n$, $j'l \equiv \pm k' \pmod n$. Ясно, что если $j \neq j'$, то $k \neq k'$, поскольку если $jl \equiv \pm j'l \pmod n$, то $j \equiv \pm j' \pmod n$, откуда следует равенство $j = j'$. Итак, образы различных делителей числа u при отображении σ не совпадают, а значит, $\sigma(u) = u$, поэтому $u \in \mathbb{Q}$ и u неподвижно при автоморфизмах поля $\mathbb{Q}(\xi)$. Но число u является также и алгебраическим целым, а следовательно, $u \in \mathbb{Z}$. □

Для случая четного номера n Фрейм (1980) получил такой результат.

(2G) *Если четное число n не кратно 3, то*

$$W_n = -3((2^n - 1)/3)^3 u^6,$$

где u — целое число. В частности, если число p простое, $p \equiv 5 \pmod 6$, то $W_{p-1} = -3((2^{p-1} - 1)/3)^3 u^6$, где u — целое число.

Доказательство. Положим $n = 2m$. Поскольку $3 \nmid n$, число $\rho = \xi^3$ также является первообразным корнем степени n из 1. Так как $\rho^m = -1$, по формуле (2.4) получим[4]

$$W_n = \prod_{j=0}^{2m-1} \prod_{k=0}^{2m-1} (1 + \rho^{m+j} + \rho^{m+k}).$$

Если $j = m$, то $\prod_{k=0}^{2m-1}(2 + \rho^{m+k}) = 2^{2m} - 1$, и аналогично, если $k = m$, то $\prod_{j=0}^{2m-1}(2 + \rho^{m+j}) = 2^{2m} - 1$, а при $j = k$ имеем $\prod_{j=0}^{2m-1}(1 - 2\rho^j) = 1 - 2^{2m}$. Не принимая в расчет повторение множителей с одинаковыми слагаемыми и замечая, что при $j = k = m$ соответствующий множитель равен 3, получим, что $W_n = -3((2^n - 1)/3)^3 v$, где

$$v = \prod{}' (1 + \rho^{m+j} + \rho^{m+k})$$

(символ $\prod'$ обозначает произведение по всем парам (j, k), для которых $0 \leqslant j, k \leqslant 2m - 1$, $j \neq m$, $k \neq m$ и $j \neq k$).

Среднее геометрическое чисел $1, \rho^{m+j}, \rho^{m+k}$ равно ξ^{j+k} (поскольку $\rho = \xi^3$). Разделив каждый множитель рассматриваемого произведения на среднее геометрическое его слагаемых, получим

$$v = \prod{}' \xi^{j+k} \prod{}' (\xi^{-j-k} + \xi^{m+2j-k} + \xi^{m+2k-j}).$$

Первое произведение равно

$$\prod_{j \neq m} \prod_{k \neq m, k \neq j} \xi^j \xi^k = \prod_{j \neq m} \xi^{j(2m-2)} \prod_{k \neq m, k \neq j} \xi^k$$

$$= \prod_{j \neq m} (-1) \xi^{j(2m-3)} \prod_{j=0}^{2m-1} \xi^k$$

---

[4] Чтобы доказать следующую формулу, достаточно раскрыть внутреннее произведение, воспользоваться тем, что j постоянно, и применить теорему Виета. — *Прим. перев.*

$$= \prod_{j\neq m}(-1)\xi^{j(2m-3)}\xi^{(2m-1)2m/2}$$

$$= \prod_{j\neq m}\xi^{j(2m-3)}$$

$$= (-1)^{2m-3}\prod_{j=0}^{2m-1}\xi^{j(2m-3)}$$

$$= -\xi^{(2m-3)(2m-1)2m/2}$$

$$= (-1)^{(2m-3)(2m-1)+1} = 1.$$

Второе произведение равно $\prod''(\xi^e + \xi^f + \xi^g)$, где $\prod''$ обозначает произведение по всем тройкам (e, f, g), для которых $0 \leqslant e, f, g \leqslant 2m-1$, причем числа e, f, g различны и $e + f + g \equiv 0 \pmod{2m}$. В самом деле, поскольку $j \neq k$, $j \neq m$, $k \neq m$ и $3 \nmid m$, выбрав числа e, f, g такими, что $0 \leqslant e, f, g \leqslant 2m-1$ и

$$\begin{cases} e \equiv -j-k \pmod{2m}, \\ f \equiv m+2j-k \pmod{2m}, \\ g \equiv m+2k-j \pmod{2m}, \end{cases}$$

получим, что e, f, g различны и $e + f + g \equiv 0 \pmod{2m}$.

Обратно, для каждой рассматриваемой тройки (e, f, g) определим числа j, k так, что $0 \leqslant j, k \leqslant 2m-1$ и

$$\begin{aligned} j &\equiv f-e-m \pmod{2m}, \\ k &\equiv g-e-m \pmod{2m}, \end{aligned}$$

откуда следует, что $j \neq m$, $k \neq m$ и $j \neq k$.

Положим $u = \prod''(\xi^e + \xi^f + \xi^g)$, где $\prod''$ обозначает произведение по всем тройкам (e, f, g), для которых $0 \leqslant e < f < g \leqslant 2m-1$ и $e + f + g \equiv 0 \pmod{2m}$. Покажем, что число u неподвижно относительно любого автоморфизма σ поля $\mathbb{Q}(\xi)$. Если $\sigma(\xi) = \xi^l$, где $\text{НОД}(l, n) = 1$, $1 \leqslant l < n$, то $\sigma(\xi^e + \xi^f + \xi^g)$ равно $\xi^{el} + \xi^{fl} + \xi^{gl}$ и является делителем числа u. Если $(e', f', g') \neq (e, f, g)$, то числа el, fl, gl не могут быть сравнимы по модулю $2m$ с $e'l$, $f'l$, $g'l$ соответственно, а также с этими числами в любом порядке. Итак, различные делители числа u при отображении σ не склеиваются, а значит, $\sigma(u) = u$, т. е. целое алгебраическое число u является рациональным, поэтому $u \in \mathbb{Z}$. Но $v = u^6$, поскольку каждый делитель $\xi^e + \xi^f + \xi^g$ числа v равен делителю $\xi^{e'} + \xi^{f'} + \xi^{g'}$ числа u, где тройка (e', f', g') получается перестановкой элементов тройки (e, f, g).

Следовательно, $W_n = -3((2^n-1)/3)^3 u^6$. $\square$

Для доказательства следующего результата потребуется такая лемма.

Лемма 2.2. *Пусть число n таково, что $2n+1=p$ — простое число, $\xi=\cos 2\pi/n+\sqrt{-1}\sin 2\pi/n$ и P — любой примарный идеал кругового поля $\mathbb{Q}(\xi)$, который делит p, т. е. $P\cap\mathbb{Z}=\mathbb{Z}p$. Тогда существует такой первообразный корень s по модулю p, что $\xi\equiv s^2 \pmod P$.*

Доказательство. Действительно, пусть g — произвольный первообразный корень по модулю p, т. е. g имеет порядок $p-1=2n$ по модулю p, так что g^2 имеет порядок n по модулю p и множество элементов порядка n по модулю p есть $\{g^{2j} \pmod p \mid 1\leqslant j<n,$ $\text{НОД}(j,n)=1\}$. Если $1\leqslant j,k<n$, $\text{НОД}(j,n)=\text{НОД}(k,n)=1$ и $j\neq k$, то $g^{2j}\not\equiv g^{2k} \pmod p$. Согласно утверждению (3F) гл. II для всех таких показателей j справедливо сравнение $\Phi_n(g^{2j})\equiv 0 \pmod p$. С другой стороны, $\Phi_n(\xi^j)=0$, так что $\Phi_n(\xi^j)\equiv 0 \pmod P$ для всех j, $1\leqslant j<n$, $\text{НОД}(j,n)=1$. Следовательно, существует такой показатель j, что $\xi\equiv g^{2j} \pmod P$, и нам остается лишь выбрать s таким, что $s\equiv\pm g^j \pmod p$, $1\leqslant s<p$. □

Фрейм доказал также следующее утверждение (а Банг в 1935 г. заметил, что $p\mid W_n$).

(2H) *Если $2n+1=p$ — простое число, то $p^{[(n-1)/2]}$ делит W_n.*

Доказательство. Сначала положим $\xi=\cos 2\pi/n+\sqrt{-1}\sin 2\pi/n$. Выберем числа u,v, $1\leqslant u,v<n$, $\text{НОД}(u,n)=\text{НОД}(v,n)=1$, и для каждого индекса j, $1\leqslant j<n$, такого, что $\text{НОД}(j,n)=1$, определим $f_j=1-\xi^{ju}-\xi^{jv}$.

Положим $d_{u,v}=\prod_{\text{НОД}\,(j,n)=1} f_j$. Покажем, что $d_{u,v}\in\mathbb{Z}$. В самом деле, пусть σ — произвольный автоморфизм поля $\mathbb{Q}(\xi)$, так что $\sigma(\xi)=\xi^l$, где $\text{НОД}(l,n)=1$. Тогда $\sigma(1-\xi^{ju}-\xi^{jv})=1-\xi^{ku}-\xi^{kv}$, где $1\leqslant k<n$ и $k\equiv jl \pmod n$, т. е. $\sigma(f_j)=f_k$. Поскольку таким образом можно получить каждый делитель f_k числа $d_{u,v}$, отображение σ задает перестановку на множестве делителей f_j чисел $d_{u,v}$. Следовательно,

$$\sigma(d_{u,v})=\prod_{\text{НОД}\,(j,n)=1}\sigma(f_j)=\prod_{\text{НОД}\,(j,n)=1} f_j=d_{u,v}.$$

Тем самым показано, что $d_{u,v}\in\mathbb{Q}$, а так как $d_{u,v}$ — алгебраическое целое число, $d_{u,v}\in\mathbb{Z}$. Если P — произвольный примарный идеал

поля $\mathbb{Q}(\xi)$, для которого $P \cap \mathbb{Z} = \mathbb{Z}p$, и s — такой первообразный корень по модулю p, что $\xi \equiv s^2 \pmod P$, то

$$d_{u,v} \equiv \prod_{\text{НОД}\,(j,n)=1} (1 - s^{2ju} - s^{2jv}) \pmod P,$$

следовательно,

$$d_{u,v} \equiv \prod_{\text{НОД}\,(j,n)=1} (1 - s^{2ju} - s^{2jv}) \pmod p.$$

Для каждого числа h, $2 \leqslant h \leqslant p-2$, такого, что $h^2 \not\equiv -1 \pmod p$ при $p \equiv 1 \pmod 4$, определим числа $a_h, b_h, 0 \leqslant a_h, b_h \leqslant p-1$, из системы сравнений

$$\begin{cases} a_h \equiv 2h/(h^2+1) \pmod p, \\ b_h \equiv -(h^2-1)/(h^2+1) \pmod p. \end{cases}$$

Тогда $a_h \not\equiv 0, 1 \pmod p$ и $b_h \not\equiv 0, 1 \pmod p$. Следовательно, существуют такие числа $u = u_h$, $v = v_h$, что $1 \leqslant u, v \leqslant p-1$ и

$$\begin{cases} a_h \equiv s^u \pmod p, \\ b_h \equiv s^v \pmod p. \end{cases}$$

Справедливо сравнение $a_h^2 + b_h^2 \equiv 1 \pmod p$, следовательно, $1 - s^{2u} - s^{2v} \equiv 0 \pmod p$, а значит, p делит $d_{u,v}$.

Если числа h, h', $2 \leqslant h, h' \leqslant p-2$, таковы, что $h^2 \not\equiv -1 \pmod p$, $h'^2 \not\equiv -1 \pmod p$ при $p \equiv 1 \pmod 4$, причем $h' \equiv \pm h$ или $\pm\overline{h} \pmod p$, где $h\overline{h} \equiv 1 \pmod p$, то, как легко проверить, $a_{h'} \equiv \pm a_h \pmod p$ или $a_{h'} \equiv \pm b_h \pmod p$, в то время как $b_{h'} \equiv \pm b_h \pmod p$ или $b_{h'} \equiv \pm a_h \pmod p$ соответственно. Тогда, используя очевидные обозначения, мы можем записать $1 - s^{2u} - s^{2v} = 1 - s^{2u'} - s^{2v'}$. Обратно, если числа h, h' таковы, что $1 - s^{2u} - s^{2v} = 1 - s^{2u'} - s^{2v'}$, то или $a_h \equiv \pm a_{h'} \pmod p$, $b_h \equiv \pm b_{h'} \pmod p$, или $a_h \equiv \pm b_{h'} \pmod p$, $b_h \equiv \pm a_{h'} \pmod p$. Во всех возможных случаях это приводит к сравнению $h' \equiv \pm h$ или $\pm\overline{h} \pmod p$.

Если $p \not\equiv 1 \pmod 4$, то количество возможных значений числа h равно $p - 3 = 2n - 2$, а значит, существует $[(2n-2)/4] = [(n-1)/2]$ делителей $1 - s^{2u} - s^{2v}$, кратных p.

Если $p \equiv 1 \pmod 4$, то количество возможных значений числа h равно $p - 5 = 2n - 4$, а значит, существует $[(2n-4)/4] = [(n-1)/2]$ (потому что n четно) делителей $1 - s^{2u} - s^{2v}$, кратных p.

Итак, во всех случаях $p^{[(n-1)/2]}$ делит $\prod_{u,v} d_{u,v}$. Так как $W_n = \prod_{u,v} d_{u,v} t$, где $t \in \mathbb{Z}$ (поскольку t — алгебраическое целое число и $t \in \mathbb{Q}$), $p^{[(n-1)/2]}$ делит W_n. $\square$

Например, 47^{11} делит W_{23} и 101^{24} делит W_{50}.

Следующий результат связан с делимостью на числа Люка. Для удобства читателя напомним ряд необходимых фактов, касающихся чисел Фибоначчи и Люка (см. также разд. V.3).

Числа Фибоначчи F_n $(n \geqslant 0)$ определяются следующим образом:

$$F_0 = 0, \qquad F_1 = 1,$$

а если $n \geqslant 2$, то

$$F_n = F_{n-1} + F_{n-2}.$$

Аналогичным образом, *числа Люка* L_n $(n \geqslant 0)$ определяются так:

$$L_0 = 2, \qquad L_1 = 1,$$

а если $n \geqslant 2$, то

$$L_n = L_{n-1} + L_{n-2}.$$

Пусть α, β — корни многочлена $X^2 - X - 1$, т. е.

$$\alpha = \frac{1+\sqrt{5}}{2} = 1.6180\ldots,$$

$$\beta = \frac{1-\sqrt{5}}{2} = -0.6180\ldots$$

и

$$\alpha + \beta = 1, \qquad \alpha - \beta = \sqrt{5}, \qquad \alpha\beta = -1.$$

Как известно, α называется *золотым числом* (или *золотым сечением*).

Следующая лемма принадлежит Бине (1843).

Лемма 2.3. *Для всех* $n \geqslant 0$ *выполнены равенства*

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad L_n = \alpha^n + \beta^n.$$

Доказательство. Поскольку $\alpha^2 = \alpha + 1$, $\beta^2 = \beta + 1$, мы получаем, что $\alpha^n = \alpha^{n-1} + \alpha^{n-2}$, а также $\beta^n = \beta^{n-1} + \beta^{n-2}$ (при $n \geqslant 2$).

Положим $T_n = (\alpha^n - \beta^n)/(\alpha - \beta)$. Тогда $T_0 = 0$, $T_1 = 1$ и

$$T_{n-1} + T_{n-2} = \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} + \frac{\alpha^{n-2} - \beta^{n-2}}{\alpha - \beta} = \frac{\alpha^n - \beta^n}{\alpha - \beta} = T_n$$

(при $n \geqslant 2$). Таким образом, последовательность чисел $\{T_n \mid n \geqslant 0\}$ совпадает с последовательностью Фибоначчи. Аналогично положим $U_n = \alpha^n + \beta^n$, тогда $U_0 = 2, U_1 = 1$ и $U_{n-1} + U_{n-2} = \alpha^{n-1} + \beta^{n-1} + \alpha^{n-2} + \beta^{n-2} = \alpha^n + \beta^n = U_n$ (при $n \geqslant 2$). Это означает, что

последовательность $\{U_n \mid n \geqslant 0\}$ совпадает с последовательностью чисел Люка. □

Дальнейшие результаты, касающиеся чисел Фибоначчи и Люка, можно найти, например, в книгах Воробьева (1961), Хоггатта (1969) или Рибенбойма (1995).

Фрейм доказал следующее утверждение.

(2I) *Если число n нечетно, то L_n^2 делит W_n.*

Доказательство. В силу утверждения (2C) можно считать, что $3 \nmid n$. Используя предыдущую лемму, получаем

$$\begin{aligned}\prod_{j=0}^{n-1}(1-\xi^j-\xi^{2j}) &= -\prod_{j=0}^{n-1}(1-\xi^j\alpha)(1-\xi^j\beta)\\ &= -(1-\alpha^n)(1-\beta^n)\\ &= -1+(\alpha^n+\beta^n)-(-1)^n\\ &= L_n,\end{aligned}$$

поскольку n нечетно. Аналогично $\prod_{k=1}^{n-1}(1-\xi^{2k}-\xi^k) = L_n$. Теперь заметим, что если $1 \leqslant j,\ k \leqslant n-1$, то пары $(j \bmod n,\ 2j \bmod n)$ и $(2k \bmod n,\ k \bmod n)$ различны. В самом деле, в противном случае выполнялись бы сравнения $j \equiv 2k \pmod n$ и $2j \equiv k \pmod n$, а следовательно, и сравнения $3j \equiv 3k \pmod n$ и $j \equiv -k \pmod n$. Таким образом, мы заключаем, что $j = k$ и $j = n-k$, так что число $n = 2k$ четно, а это противоречит предположению.

Тем самым доказано, что $W_n = L_n^2 v$, где $v \in \mathbb{Q}$, причем v — алгебраическое целое число, а значит, $v \in \mathbb{Z}$. □

К примеру, квадраты чисел Люка

$$L_{47} = 6\,643\,838\,879$$

и

$$L_{53} = 119\,218\,851\,371$$

(которые, как известно, являются простыми) делят W_{47} и W_{53} соответственно.

Улучшая результат Любельского (1935), Э. Лемер независимо от Банга (1935) в том же 1935 г. доказал следующее свойство определителя Вендта.

(2J) *Если p — нечетное простое число, то $p^{p-2}(2^{p-1}-1)/p$ делит W_{p-1}.*

Доказательство. Рассмотрим матрицу C, определитель которой равен W_{p-1}:

$$C = \begin{pmatrix} 1 & \binom{p-1}{1} & \binom{p-1}{2} & \dots & \binom{p-1}{p-2} \\ \binom{p-1}{p-2} & 1 & \binom{p-1}{1} & \dots & \binom{p-1}{p-3} \\ \binom{p-1}{p-3} & \binom{p-1}{p-2} & 1 & \dots & \binom{p-1}{p-4} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \binom{p-1}{1} & \binom{p-1}{2} & \binom{p-1}{3} & \dots & 1 \end{pmatrix}.$$

Прибавив все столбцы матрицы C к ее последнему столбцу, получим матрицу C', все элементы последнего столбца которой равны

$$1 + \binom{p-1}{1} + \binom{p-1}{2} + \ldots + \binom{p-1}{p-2} = 2^{p-1} - 1.$$

Прибавляя к каждому столбцу матрицы C' (вплоть до столбца с номером $p-3$) следующий столбец, получим матрицу C'', все элементы первых $p-3$ столбцов которой имеют вид

$$\binom{p-1}{k} + \binom{p-1}{k+1} = \binom{p}{k+1},$$

$k = 0, 1, \ldots, p-2$. Все эти элементы кратны p. Таким образом, $W_{p-1} = \det C''$ делится на $p^{p-3}(2^{p-1} - 1) = p^{p-2}(2^{p-1} - 1)/p$. □

Новый результат в этой области получен Алу (1997).

Фрейм установил, что если $n \leqslant 50$ и $6 \nmid n$, то

$$\left|\log_{10} |W_n| - n^2 \log_{10} c\right| < 0.33,$$

где

$$\log c = \frac{2}{\pi} \int_0^{\pi/3} \log(2 \cos\theta) \mathrm{d}\theta,$$

так что $\log_{10} c = 0.140305\ldots$ Таким образом, число W_n содержит примерно $0.1403\, n^2$ разрядов. Знание величины числа W_n, а также некоторых его простых делителей может свидетельствовать, что разложение числа W_n на простые множители уже закончено.

В 1982 г. Бойд показал, что последовательность $\{\Delta_n\}$, где

$$\Delta_n = \log_{10} |W_n| - n^2 \log_{10} c,$$

является ограниченной и имеет ровно три предельные точки 0, $\frac{1}{2}\log_{10} 3$, $\frac{2}{3}\log_{10} 2$, отвечающих соответственно номерам $n \equiv \pm 1, \pm 2$ или $3 \pmod 6$.

Приведенные ниже значения определителя Вендта W_n для $n = 2k \geqslant 20$ были любезно предоставлены Дж. С. Фреймом.

$$
\begin{aligned}
W_1 &= 1,\\
W_2 &= -3,\\
W_3 &= 28 = 2^2 \times 7,\\
W_4 &= -375 = -3 \times 5^3,\\
W_5 &= 3751 = 11^2 \times 31,\\
W_6 &= 0,\\
W_7 &= 2^6 \times 29^2 \times 127,\\
W_8 &= -3^7 \times 5^3 \times 17^3,\\
W_9 &= 2^2 \times 7 \times 19^4 \times 37^2 \times 73,\\
W_{10} &= -3 \times 11^9 \times 31^3,\\
W_{11} &= 23^5 \times 67^2 \times 89 \times 199^2,\\
W_{12} &= 0,\\
W_{13} &= 3^6 \times 53^2 \times 79^2 \times 131^2 \times 521^2 \times 8191,\\
W_{14} &= -2^{24} \times 3 \times 29^6 \times 43^3 \times 127^3,\\
W_{15} &= 2^{14} \times 7 \times 11^2 \times 31^7 \times 61^4 \times 151 \times 271^2,\\
W_{16} &= -3^7 \times 5^3 \times 7^6 \times 17^{15} \times 257^3,\\
W_{20} &= -3 \times 5^{24} \times 11^9 \times 31^3 \times 41^9 \times 61^6,\\
W_{22} &= -3 \times 23^{21} \times 67^6 \times 89^3 \times 199^6 \times 683^3,\\
W_{26} &= -3^{25} \times 53^{12} \times 79^6 \times 131^6 \times 521^6 \times 2731^3 \times 8191^{31},\\
W_{28} &= -2^{60} \times 3 \times 5^3 \times 13^6 \times 29^{27} \times 43^3 \times 113^9 \times 127^3 \times 197^{61},\\
W_{32} &= -3^7 \times 5^3 \times 7^6 \times 17^{15} \times 47^6 \times 97^{12} \times 193^6 \times 257^9 \times 353^6\\
&\quad \times 449^6 \times 65537^{31},\\
W_{34} &= -3 \times 103^{12} \times 137^{12} \times 239^6 \times 307^6 \times 409^6 \times 613^6 \times 3571^6\\
&\quad \times 43691^3 \times 131071^3,\\
W_{38} &= -3 \times 7^6 \times 191^{12} \times 229^{12} \times 419^6 \times 457^6 \times 647^6 \times 761^6\\
&\quad \times 1483^6 \times 9349^6 \times 174763^3 \times 524287^3,\\
W_{40} &= -3^{19} \times 5^{24} \times 11^{15} \times 17^3 \times 31^9 \times 41^{39} \times 61^6 \times 241^6 \times 281^{12}\\
&\quad \times 641^6 \times 881^6 \times 61681^{31},\\
W_{44} &= -3 \times 5^3 \times 23^{21} \times 67^6 \times 89^{21} \times 199^6 \times 353^6 \times 397^9 \times 617^6\\
&\quad \times 683^3 \times 1013^6 \times 2113^9 \times 2333^6 \times 3257^6 \times 4357^{61},\\
W_{46} &= -3 \times 47^{45} \times 139^{12} \times 461^6 \times 599^{12} \times 691^{12} \times 829^6 \times 1151^6\\
&\quad \times 2347^6 \times 3313^6 \times 178481^3 \times 2796203^3,
\end{aligned}
$$

$$W_{50} = -3 \times 11^9 \times 31^3 \times 101^{24} \times 151^{18} \times 251^9 \times 401^6 \times 601^3 \times 1151^{12} \times 1301^6 \times 1601^6 \times 1801^3 \times 1951^6 \times 3851^6 \times 4051^3 \times 4651^6 \times 5801^6 \times 6101^6,$$

$$W_{52} = -3^{25} \times 5^3 \times 53^{51} \times 79^6 \times 131^6 \times 157^{15} \times 233^6 \times 313^{12} \times 521^6 \times 677^6 \times 1301^6 \times 1613^9 \times 2731^3 \times 6709^6 \times 8191^3 \times 13417^6 \times 20593^6.$$

В 1991 г. Фи и Грэнвилль нашли делители (измененного) определителя Вендта W_n для всех четных номеров $n \leqslant 200$ (включая номера, кратные 6). Их результаты позволяют сформулировать следующее утверждение.

(2K) *Если $k \leqslant 100$ и числа p, $2kp+1$ являются простыми, то для показателя p справедлив первый случай последней теоремы Ферма.*

Доказательство. Справедливость утверждения устанавливается с помощью явной записи разложения W_{2k} на множители (при $2k \leqslant \leqslant 200$) и проверки выполнения условий утверждения (2B). □

Значения W_{2k} (для $2k = 2, 4, 8, 16$) позволяют утверждать, что сравнение Ферма $X^p + Y^p + Z^p \equiv 0 \pmod q$, где p и $q = 2kp + +1$ — нечетные простые числа, имеет лишь тривиальные решения. Однако сравнения $X^3 + Y^3 + Z^3 \equiv 0 \pmod{31}$ и $X^3 + Y^3 + Z^3 \equiv 0 \pmod{43}$ имеют нетривиальные решения, поскольку $31 \mid W_{10}$ и $43 \mid W_{14}$.

Согласно результату Диксона (1909) (см. утверждение (2C) гл. X), если p и q — простые числа, причем $q \geqslant (p-1)^2(p-2)^2 + 6p - 2$, то сравнение (2.1) имеет нетривиальное решение. Таким образом, если $q = 2kp + 1$ и $6 \not| 2k$, то $q \mid W_{2k}$ в силу утверждения (2B).

В завершение этого раздела сошлемся на результаты Ганди (1975, 1976), полученные в предположении, что первый случай теоремы Ферма не имеет места для показателя p. Эти утверждения сформулированы в терминах подходящих циклических определителей, однако доказательствам было не суждено увидеть свет из-за безвременной кончины Ганди.

Список литературы

1843 Binet, J., *Mémoire sur l'intégration des équations linéaires aux différences finies d'un ordre quelconque à coefficients variables*. C. R. Acad. Sci. Paris, **17** (1843), 559–567.

1853 Spottiswoode, W., *Elementary theorems relating to determinants* (rewritten and much enlarged by the author), J. Reine Angew. Math., **51** (1853), 209–271 and 328–381.

1871 Stern, M.A., *Einige Bemerkungen über eine Determinante*, J. Reine Angew. Math., **73** (1871), 374–380.

1894 Wendt, E., *Arithmetische Studien über den letzten Fermatschen Satz, welcher aussagt, daß die Gleichung* $a^n = b^n + c^n$ *für* $n > 2$ *in ganzen Zahlen nicht auflösbar ist*, J. Reine Angew. Math., **113** (1894), 335–346.

1895 Matthews, G.B., *A note in connexion with Fermat's last theorem*, Messenger Math., **24** (1895), 97–99.

1909 Dickson, L.E., *On the congruence* $x^n + y^n + z^n \equiv 0 \pmod{p}$, J. Reine Angew. Math., **135** (1909), 134–141.

1909 Dickson, L.E., *Lower limit for the number of sets of solutions of* $x^e + y^e + z^e \equiv 0 \pmod{p}$, J. Reine Angew. Math., **135** (1909), 181–188.

1910 Bachmann, P., *Niedere Zahlentheorie*, Teubner, Leipzig, 1910; reprinted by Chelsea, New York, 1966.

1920 Muir, T., *The Theory of Determinants in the Historical Order of Development*, Vol. III, Macmillan, London, 1920.

1935 Bang, A.S., *Om tal af Formen* $a^m + b^m - c^m$, Mat. Tidsskrift, **B** (1935), 49–59.

1935 Lehmer, E., *On a resultant connected with Fermat's last theorem*, Bull. Amer. Math. Soc., **41** (1935), 864–867.

1935 Lubelski, S., *Studien über den großen Fermat'schen Satz*, Prace Matematyczne Fyz., **42** (1935), 11–44.

1961 Vorob'ev, N.N., *Fibonacci Numbers*, Blaisdell, New York, 1961.

1968 Rivoire, P., *Dernier Théorème de Fermat et Groupe de Classes dans Certains Corps Quadratiques Imaginaires*, Thèse, Université Clermont-Ferrand, 1968, 59 pp.; reprinted in Ann. Sci. Univ. Clermont-Ferrand II, **68** (1979), 1–35.

1969 Hoggatt, V.E., *Fibonacci and Lucas Numbers*, Houghton-Mifflin, Boston, 1969.

1975 Gandhi, J.M., *Fermat's last theorem, II: A new circulant condition for the first case*, Notices Amer. Math. Soc., **22** (1975), A-450.

1975 Gandhi, J.M., *Fermat's last theorem, III: A new circulant condition for the first case, for primes of the form* $6m - 1$, Notices Amer. Math. Soc., **22** (1975), A-502.

1975 Gandhi, J.M., *Fermat's last theorem, IV: A new circulant condition for the first case, for primes of the form* $6m+1$, Notices Amer. Math. Soc., **22** (1975), A-541.

1976 Gandhi, J.M., *Fermat's last theorem, V*, Notices Amer. Math. Soc., **23** (1976), A-56.

1980 Frame, J.S., *Factors of the binomial circulant determinant*, Fibonacci Quart., **18** (1980), 9–23.

1982 Boyd, D.W., *The asymptotic behaviour of the binomial circulant determinant*, J. Math. Anal. Appl., **86** (1982), 30–32.

1991 Fee, G. and Granville, A., *The prime factors of Wendt's binomial circulant determinant*, Math. Comp., **57** (1991), 839–848.

1995 Ribenboim, P., *The New Book of Prime Number Records*, Springer-Verlag, New York, 1995.

1997 Helou, C., *On Wendt's determinant*, Math. Comp., **66** (1997), 1341–1346.

IV.3. Приложение: простые числа Жермен

Как уже отмечалось, проблема существования бесконечного количества таких простых чисел p, для которых число $2p+1$ (или $4p+1$, или $8p+1$, и т. д.) также является простым, очень сложна. Мы приведем эвристическое рассуждение, которое указывает на справедливость гораздо более общего утверждения.

Для каждого положительного числа x обозначим через $\pi(x)$ количество простых чисел, не превосходящих x. Знаменитая теорема о простых числах Адамара и Валле Пуссена (1899) утверждает, что

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1,$$

то есть $\pi(x) \sim x/\log x$.

Согласно теореме Дирихле, если натуральные числа a и m взаимно просты, то в арифметической прогрессии $\{a + km \mid k \geqslant 0\}$ содержится бесконечно много простых чисел. Пусть $\pi_{a,m}(x)$ обозначает количество простых чисел в этой прогрессии, не превосходящих x. Тогда

$$\lim_{x\to\infty} \frac{\pi_{a,m}(x)}{\pi(x)} = \frac{1}{\varphi(m)},$$

то есть

$$\pi_{a,m}(x) \sim \frac{1}{\varphi(m)} \cdot \frac{x}{\log x}.$$

Рассмотрим многочлен $f(X) = mX + a$. Заметим, что значение $\pi_{a,m}(x)$ равно количеству чисел n, $1 \leqslant n \leqslant (x-a)/m$, для которых $f(n)$ — простое число.

Можно рассмотреть следующую более общую ситуацию. Пусть $f_1(X)$, $f_2(X)$, ..., $f_k(X)$ — многочлены с целыми коэффициентами и положительным коэффициентом при старшем члене. Обозначим через $d_j \geqslant 1$ степень многочлена $f_j(X)$. Потребуем также, чтобы эти многочлены были неприводимы над $\mathbb{Q}$ и чтобы ни один из них не был постоянным делителем другого. Для всякого натурального числа N обозначим через $Q(N) = Q_{f_1,\ldots,f_k}(N)$ количество целых чисел n, $1 \leqslant n \leqslant N$, для которых $f_1(n)$, $f_2(n)$, ..., $f_k(n)$ — простые числа.

В силу теоремы о простых числах вероятность того, что большое натуральное число m окажется простым, равна $\pi(m)/m \sim 1/\log m$.

Несмотря на то, что нас будут интересовать значения многочленов $f_1(X), f_2(X), \ldots, f_k(X)$, мы не должны брать в расчет тот факт, что наборы этих значений не являются распределенными случайным образом.

Для каждого простого числа p обозначим через s_p вероятность того события, что ни одно из k чисел такого случайного набора не кратно p. Тогда

$$s_p = \left(\frac{p-1}{p}\right)^k = \left(1 - \frac{1}{p}\right)^k.$$

Аналогично, пусть r_p — вероятность того, что для случайного числа n ни одно из чисел $f_1(n), f_2(n), \ldots, f_k(n)$ не кратно p. Если $w(p)$ обозначает число решений сравнения

$$f_1(X) f_2(X) \ldots f_k(X) \equiv 0 \pmod{p},$$

то $r_p = (p - w(p))/p = 1 - w(p)/p$. Можно показать, что произведение $\prod_p r_p/s_p$ сходится. Обозначим его предел через $C = C(f_1, \ldots, f_k)$. Если считать, что этим числом измеряется степень того, насколько значения набора $f_1(X), \ldots, f_k(X)$ не случайны, то вероятность того, что все числа $f_1(n)$, $f_2(n), \ldots, f_k(n)$ являются простыми (для больших n), равна

$$C(f_1, \ldots, f_n) \frac{1}{\log f_1(n) \ldots \log f_k(n)}$$
$$\sim \quad C(f_1, \ldots, f_n) \frac{1}{d_1 \ldots d_k} \cdot \frac{1}{(\log n)^k},$$

поскольку $\log f_i(n) \sim d_i \log n$. Тогда

$$Q(N) \sim C(f_1, \ldots, f_k) \frac{1}{d_1 \ldots d_k} \sum_{n=2}^{N} \frac{1}{(\log n)^k}.$$

В частности, $\lim_{N\to\infty} Q(N) = \infty$. Таким образом, мы попытались эвристически объяснить, что при $C \neq 0$ должно существовать бесконечно много простых чисел p с заданными свойствами.

Теперь рассмотрим следующие частные случаи:

(1) $f_1(X) = X$, $f_2(X) = 2X + 1$;
(2) $f_1(X) = X$, $f_2(X) = X + 2$.

Случай (1) соответствует простым числам Жермен, в то время как случай (2) относится к простым близнецам. В обоих случаях $w(2) = 1$ и $w(p) = 2$ при $p > 2$. Таким образом, константа равна

$$C = \frac{1 - \frac{1}{2}}{\left(1 - \frac{1}{2}\right)^2} \prod_{p>2} \frac{1 - \frac{2}{p}}{\left(1 - \frac{1}{p}\right)^2} = 1.3203236\ldots,$$

так что

$$Q(N) \sim 1.3203236\ldots \cdot \sum_{n=2}^{N} \frac{1}{(\log n)^2}.$$

В 1923 г. это предположение было высказано Харди и Литтлвудом для количества простых близнецов, не превосходящих N. Оно достаточно точно соответствует реальному числу простых близнецов (см. Секстон (1954), Ренч (1961), Шенкс (1962) и Брент (1975)).

Список литературы

1923 Hardy, G.H. and Littlewood, J.E., *Some problems of "partitio numerorum", III. On the expression of a number as a sum of primes*, Acta. Math., **44** (1923), 1–70.

1954 Sexton, C.R., *Counts of twin primes less than* 100000, Math. Tables and Aids to Comp., **8** (1954), 47–49.

1961 Wrench, J.W., *Evaluation of Artin's constant and the twin prime constant*, Math. Comp., **15** (1961), 396–398.

1962 Bateman, P.T. and Horn, R.A., *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp., 16 (1962), 363–367.

1962 Shanks, D., *Solved and Unsolved Problems in Number Theory*, Vol. I, Spartan, Washington, DC, 1962; reprinted by Chelsea, New York, 1979.

1963 Schinzel, A., *A remark on a paper by Bateman and Horn*, Math. Comp., **17** (1963), 445–447.

1965 Bateman, P.T. and Horn, R.A., *Primes represented by irreducible polynomials in one variable*, Proc. Symposia in Pure Mathematics, Theory of Numbers, Amer. Math. Soc, Vol. 8, 1965, pp. 119–132.

1975 Brent, R.P., *Irregularities in the distribution of primes and twin primes*, Math. Comp., **29** (1975), 43–56.

Глава V

Эпизоды 5 и 6

В этой главе мы продолжаем изложение вспомогательного материала.

V.1. p-адические числа

Для изучения свойств делимости на простое число p удобно рассматривать разложение целого числа по основанию p:

$$a = a_0 + a_1 p + \ldots + a_m p^m,$$

где $0 \leqslant a_i \leqslant p-1$, $p^m \leqslant a < p^{m+1}$.

Гензель ввел также бесконечные p-адические разложения, называемые *p-адическими целыми числами*. Он описал операции сложения и умножения p-адических целых чисел и доказал очень важную теорему о существовании p-адических целых чисел, являющихся корнями некоторого многочлена. Можно рассматривать p-адическое число как предел последовательности целых чисел по p-адической метрике. Это позволяет применить методы анализа для изучения свойств делимости.

А. Поле p-адических чисел

Здесь мы кратко опишем свойства p-адических чисел и результаты, необходимые для изучения уравнения Ферма.

В разделе П.1 мы для каждого простого числа p определили p-адическое нормирование v_p поля $\mathbb{Q}$. Напомним определение множества p-целых рациональных чисел:

$$\mathbb{Z}_p = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0, p \nmid b, \text{НОД}\,(a,b) = 1 \right\}.$$

Это подкольцо в $\mathbb{Q}$, содержащее $\mathbb{Z}$. Более того, неравенство $v_p(r) \geqslant 0$ выполняется для рационального числа r тогда и только тогда, когда $r \in \mathbb{Z}_p$.

Множество $\mathbb{Z}_p$ называется *кольцом нормирования* для v_p. Единственный максимальный идеал в $\mathbb{Z}_p$ совпадает с $\mathbb{Z}_p p = \{a/b \in \mathbb{Z}_p \mid a$ кратно $p\}$. Поле $\mathbb{Z}_p/\mathbb{Z}_p p$, изоморфное полю $\mathbb{F}_p$ (состоящему из p элементов), называется *полем вычетов* для v_p.

По нормированию v_p построим функцию двух рациональных аргументов d_p. Если $a,\ b \in \mathbb{Q}$, то

$$\begin{cases} d_p(a,b) = p^{-v_p(a-b)} & \text{при } a \neq b, \\ d_p(a,a) = 0. \end{cases}$$

Легко убедиться в справедливости следующих свойств:

$$\begin{aligned} d_p(a,b) &\geqslant 0, \\ d_p(a,b) &= d_p(b,a), \\ d_p(a,b) &= d_p(a-b,0), \\ d_p(a+c,b+c) &= d_p(a,b), \\ d_p(a,b) &\leqslant \max\{d_p(a,c),\ d_p(b,c)\} \leqslant \\ &\leqslant d_p(a,c) + d_p(b,c). \end{aligned}$$

Итак, d_p — метрика, согласованная с операцией сложения. Она называется *p-адической метрикой* в $\mathbb{Q}$.

Пополнение поля $\mathbb{Q}$ по p-адической метрике есть снова поле, обозначаемое через $\hat{\mathbb{Q}}_p$ и называемое *полем p-адических чисел*. Каждый отличный от нуля элемент α из $\hat{\mathbb{Q}}_p$ представляется в виде p-адического разложения

$$\alpha = \sum_{i=m}^{\infty} a_i p^i,$$

где $0 \leqslant a_i \leqslant p-1$, $m \in \mathbb{Z}$ и $a_m \neq 0$. Если $\alpha_n = \sum_{i=m}^{n} a_i p^i$ (где $n \geqslant m$), то $\alpha = \lim_{n\to\infty} \alpha_n$ (предел понимается в смысле сходимости по p-адической метрике).

Можно продолжить по непрерывности p-адическое нормирование на поле $\hat{\mathbb{Q}}_p$, положив

$$\hat{v}_p\left(\sum_{i=m}^{\infty} a_i p^i\right) = m \quad (\text{при } a_m \neq 0).$$

Тогда множество значений функции $\hat{v}_p$ есть снова целые числа и бесконечность.

Топологическое замыкание кольца $\mathbb{Z}_p$ в поле $\hat{\mathbb{Q}}_p$ есть кольцо, обозначаемое через $\hat{\mathbb{Z}}_p$. Его элементы называются *p-адическими це-*

лыми числами. Таким образом, $\alpha \in \hat{\mathbb{Q}}_p$ является p-адическим целым числом в точности тогда, когда $\hat{v}_p(\alpha) \geqslant 0$. Ясно также, что $\hat{\mathbb{Z}}_p \cap \mathbb{Q} = \mathbb{Z}_p$. Единственным ненулевым простым идеалом в $\hat{\mathbb{Z}}_p$ является идеал $\hat{\mathbb{Z}}_p p$, состоящий из чисел, кратных p. Поле вычетов нормирования $\hat{v}_p$ совпадает с полем $\hat{\mathbb{Z}}_p/\hat{\mathbb{Z}}_p p$, изоморфным полю $\mathbb{F}_p$.

Пусть $\alpha, \beta \in \hat{\mathbb{Q}}_p$. Тогда мы будем говорить, что α *делит* β, если найдется такой элемент $\gamma \in \hat{\mathbb{Z}}_p$, что $\alpha\beta = \gamma$. Это означает, что $\hat{v}_p(\alpha) \leqslant \hat{v}_p(\beta)$. Назовем элемент $\alpha \in \hat{\mathbb{Z}}_p$ *единицей* в $\hat{\mathbb{Z}}_p$, если α делит 1, т. е. $\hat{v}_p(\alpha) = 0$. Множество всех единиц $U_p \subset \hat{\mathbb{Z}}_p$ является группой по умножению.

Пусть $\alpha, \beta, \gamma \in \hat{\mathbb{Q}}_p$, $\gamma \neq 0$. Тогда мы будем говорить, что $\alpha \equiv \beta \pmod{\gamma}$, если γ делит $\alpha - \beta$. Аналогичным образом, если $\gamma \in \hat{\mathbb{Q}}_p$, $\gamma \neq 0$, и $F(X), G(X) \in \hat{\mathbb{Q}}_p[X]$, то мы будем писать $F(X) \equiv G(X) \pmod{\gamma}$, если γ делит каждый коэффициент разности $F(X) - G(X)$.

Для этих сравнений остаются в силе свойства сравнений целых чисел.

B. Многочлены с p-адическими коэффициентами

Здесь мы кратко коснемся теории многочленов с коэффициентами из $\hat{\mathbb{Q}}_p$.

Пусть $f(X) = a_0 X^n + a_1 X^{n-1} + \ldots + a_n \in \hat{\mathbb{Q}}_p[X]$. Положим $\tilde{v}_p(f) = \min_{0 \leqslant i \leqslant n}\{v_p(a_i)\}$. Для всех многочленов $f, g \in \hat{\mathbb{Q}}_p[X]$, $g \neq 0$, определим функцию

$$\tilde{v}_p\left(\frac{f}{g}\right) = \tilde{v}_p(f) - \tilde{v}_p(g).$$

Легко видеть, что данное определение корректно. Тогда $\tilde{v}_p$ суть нормирование кольца $\hat{\mathbb{Q}}_p[X]$, сужение которого на $\mathbb{Q}_p$ есть v_p. Для простоты обозначений будем писать v_p вместо $\tilde{v}_p$.

Пусть $f, g \in \hat{\mathbb{Q}}_p[X]$. Тогда мы будем писать $f \equiv g \pmod{p^n}$, если $v_p(f-g) \geqslant n$, или, что то же самое, p^n делит каждый коэффициент разности $f - g$. Для каждого многочлена $f = \sum_{i=0}^{m} a_i X^i \in \mathbb{Z}_p[X]$ обозначим через $\bar{f} = f \pmod{p}$ многочлен $\bar{f} = \sum_{i=0}^{m} \bar{a}_i X^i \in \mathbb{F}_p[X]$.

Напомним несколько известных фактов, касающихся многочленов из $\hat{\mathbb{Q}}_p[X]$. Многочлен $f \in \hat{\mathbb{Z}}_p[X]$ называется *примитивным*, если $v_p(f) = 0$. Каждый многочлен $f \in \hat{\mathbb{Z}}_p[X]$ может быть представлен в виде $f = af_1$, где $a \in \mathbb{Z}$, $f_1 \in \hat{\mathbb{Z}}_p[X]$ и многочлен f_1 примитивен.

(1A) Лемма Гаусса. *Произведение $f \cdot g$ примитивных многочленов $f, g \in \hat{\mathbb{Z}}_p[X]$ есть снова примитивный многочлен.*

(1B) *Пусть примитивный многочлен $f \in \hat{\mathbb{Z}}_p[X]$ представляется в виде $f = g \cdot h$, где $g, h \in \hat{\mathbb{Q}}_p[X]$. Тогда существуют примитивные многочлены $g_1, h_1 \in \mathbb{Z}_p[X]$, такие, что $f = g_1 \cdot h_1$ и* $\deg g_1 = \deg g$, $\deg h_1 = \deg h$.

Отличный от константы многочлен $f \in \hat{\mathbb{Z}}_p[X]$ (соответственно $f \in \hat{\mathbb{Q}}_p[X]$) называется *неприводимым* над $\hat{\mathbb{Z}}_p[X]$ ($\hat{\mathbb{Q}}_p[X]$), если он не представим в виде $f = g \cdot h$, где g и f — многочлены из $\hat{\mathbb{Z}}_p[X]$ ($\hat{\mathbb{Q}}_p[X]$), отличные от константы.

(1C) *Многочлен $f \in \hat{\mathbb{Z}}_p[X]$ неприводим над $\hat{\mathbb{Z}}_p[X]$ тогда и только тогда, когда он неприводим над $\hat{\mathbb{Q}}_p[X]$.*

Многочлены $f, g \in \hat{\mathbb{Z}}_p[X]$ называются *взаимно простыми*, если все их общие делители из $\hat{\mathbb{Z}}_p[X]$ суть постоянные, т. е. степень этих делителей равна нулю.

(1D) *Если отличный от константы неприводимый многочлен $f \in \hat{\mathbb{Z}}_p[X]$ не делит многочлен $g \in \hat{\mathbb{Z}}_p[X]$, также отличный от константы, то f и g взаимно просты.*

(1E) *Пусть многочлены $f, g \in \hat{\mathbb{Z}}_p[X]$ взаимно просты. Тогда найдутся такие многочлены $s, t \in \hat{\mathbb{Z}}_p[X]$, что $s \cdot f + t \cdot g$ есть отличный от нуля элемент кольца $\hat{\mathbb{Z}}_p$.*

(1F) *Пусть $f, g, h \in \hat{\mathbb{Z}}_p[X]$, многочлен f неприводим и делит произведение $g \cdot h$. Тогда хотя бы один из многочленов g и h делится на f.*

(1G) *Пусть многочлены $g, h \in \hat{\mathbb{Z}}_p[X]$ отличны от константы и взаимно просты. Тогда если хотя бы один из них примитивен и каждый их них делит f, то произведение $g \cdot h$ делит f.*

(1H) *Каждый ненулевой многочлен $f \in \hat{\mathbb{Z}}_p[X]$ можно представить в виде $f = a g_1 \dots g_n$, где $a \in \hat{\mathbb{Z}}_p$, $g_1, \dots, g_n \in \hat{\mathbb{Z}}_p[X]$ — примитивные неприводимые многочлены и $n \geqslant 0$. Более того, a и $g_1, \dots, g_n$ определены единственным образом с точностью до умножения на единицу в $\hat{\mathbb{Z}}_p$.*

Теперь рассмотрим результант и дискриминант многочленов из $\hat{\mathbb{Z}}_p[X]$.

(1I) *Пусть f и g — многочлены из $\hat{\mathbb{Z}}_p[X]$, отличные от константы. Тогда следующие утверждения эквивалентны.*

(a) *Существует отличный от константы многочлен $h \in \hat{\mathbb{Z}}_p[X]$, делящий f и g.*

(b) *Существуют ненулевые многочлены $f_1, g_1 \in \hat{\mathbb{Z}}_p[X]$, такие, что* $\deg f_1 < \deg f$, $\deg g_1 < \deg g$ *и*

$$g_1 \cdot f + f_1 \cdot g = 0.$$

Доказательство. (a) $\Rightarrow$ (b) По определению делимости найдутся многочлены $f_1, g_1 \in \hat{\mathbb{Z}}_p[X]$, такие, что $f = h \cdot f_1$ и $g = -h \cdot g_1$. Очевидно, что f_1 и g_1 отличны от нуля, $\deg f_1 < \deg f$, $\deg g_1 < \deg g$ и $g_1 \cdot f + f_1 \cdot g = 0$.

(b) $\Rightarrow$ (a) Обратно, предположим, что существуют многочлены $f_1, g_1 \in \hat{\mathbb{Z}}_p[X]$, такие, что $\deg f_1 < \deg f$, $\deg g_1 < \deg g$ и $g_1 f + f_1 g = 0$. Если бы f и g были взаимно просты, то по утверждению (1E) нашлись бы многочлены $s, t \in \hat{\mathbb{Z}}_p[X]$, такие, что $s \cdot f + t \cdot g = c \in \hat{\mathbb{Z}}_p$, $c \neq 0$. Исключая g из двух полученных соотношений, придем к равенству $f(sf_1 - tg_1) = cf_1$. Так как степень левой части больше степени правой, получаем противоречие. Следовательно, многочлены f и g не являются взаимно простыми. □

(1J) *Для того чтобы многочлены*

$$f = \sum_{i=0} a_i X^{m-i} \quad \text{и} \quad g = \sum_{i=0} b_i X^{n-i}$$

(где $m, n > 0$ и $f, g \in \hat{\mathbb{Z}}_p[X]$) имели общий делитель, отличный от константы, необходимо и достаточно, чтобы выполнялось условие $R(f, g) = 0$.

Доказательство. Как следует из утверждения (4B) гл. II, если f и g имеют общий делитель, отличный от константы, то $R(f, g) = 0$.

Покажем, что условие $R(f, g) = 0$ является достаточным. Согласно утверждению (1I) достаточно доказать существование таких ненулевых многочленов $f_1, g_1 \in \hat{\mathbb{Z}}_p[X]$, $f_1 = \sum_{i=0}^{m-1} c_i X^{m-1-i}$, $g_1 = \sum_{j=0}^{n-j} d_i X^{n-1-j}$, что $g_1 \cdot f + f_1 \cdot g = 0$ (случай $c_0 = d_0 = 0$ не исключается). Это соотношение равносильно следующей системе из

$m+n$ уравнений с неизвестными $c_0, \ldots, c_{m-1}, d_0, \ldots, d_{n-1}$ (полученной приравниванием к нулю коэффициентов при степенях переменной X):

$$\begin{cases} d_0a_0 + c_0b_0 = 0, \\ d_0a_1 + d_1a_0 + c_0b_1 + c_1b_0 = 0, \\ d_0a_2 + d_1a_1 + d_2a_0 + c_0b_2 + c_1b_1 + c_2b_0 = 0, \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \end{cases}$$

Эта линейная однородная система имеет в $\hat{\mathbb{Q}}_p$ ненулевое решение тогда и только тогда, когда ее определитель равен нулю, или, что то же самое, определитель транспонированной системы равен нулю. Этот определитель есть не что иное, как $R(f,g)$. Для завершения доказательства заметим, что из существования ненулевого решения системы в $\hat{\mathbb{Q}}_p$ следует существование ненулевого решения в $\hat{\mathbb{Z}}_p$, получаемого домножением на общий знаменатель. □

(1K) *Пусть взаимно простые отличные от константы многочлены $f, g \in \mathbb{Z}_p[X]$ таковы, что $v_p(R(f,g)) = \rho$. Тогда любой ненулевой многочлен $h \in \hat{\mathbb{Z}}_p[X]$, такой, что $v_p(h) \geqslant \rho$ и $\deg h < \deg f + \deg g$, можно единственным способом представить в виде $h = g_1 \cdot f + f_1 \cdot g$, где $f_1, g_1 \in \hat{\mathbb{Z}}_p[X]$, $v_p(f_1) \geqslant v_p(h) - \rho$, $v_p(g_1) \geqslant v_p(h) - \rho$, $\deg f_1 < \deg f$ и $\deg g_1 < \deg g$.*

Доказательство. Пусть

$$f = \sum_{i=0}^{m} a_i X^{m-i},$$

$$g = \sum_{i=0}^{n} b_i X^{n-i},$$

$$h = \sum_{i=0}^{m+n-1} e_1 X^{m+n-i}.$$

Наша цель — найти такие многочлены $f_1 = \sum_{i=0}^{m-1} c_i X^{m-1-i}$, $g_1 = \sum_{j=0}^{n-1} d_j X^{n-1-j}$ из $\hat{\mathbb{Z}}_p[X]$, что $h = g_1 \cdot f + f_1 \cdot g$. Приравняв коэффициенты при соответствующих степенях переменной X в обеих частях этого соотношения, получим линейную систему из $m+n$ уравнений с $m+n$ неизвестными c_i, d_j, определитель которой есть в точности $R(f,g)$.

Так как f и g взаимно просты, согласно утверждению (1J) мы заключаем, что $R(f,g) \neq 0$. Следовательно, рассматриваемая система имеет единственное решение.

Коэффициенты c_i, d_j можно найти по правилу Крамера. Их числители суть линейные формы от e_i с коэффициентами из $\hat{\mathbb{Z}}_p$ (так как $f, g \in \hat{\mathbb{Z}}_p[X]$), а знаменатели равны $R(f,g)$. Поскольку $v_p(e_i) \geqslant v_p(h) \geqslant \rho = v_p(R(f,g))$, мы получаем $v_p(c_i) \geqslant 0, v_p(d_j) \geqslant 0$, так что $f_1, g_1 \in \hat{\mathbb{Z}}_p[X]$ и $v_p(f_1) \geqslant v_p(h) - \rho$, $v_p(g_1) \geqslant v_p(h) - \rho$. □

(1L) *Пусть $f \in \hat{\mathbb{Z}}_p[X]$ — многочлен, отличный от константы. Тогда для того, чтобы существовал многочлен $g \in \mathbb{Z}_p[X]$, отличный от константы, квадрат которого делит f, необходимо и достаточно, чтобы выполнялось условие* $\operatorname{Discr}(f) = 0$.

Доказательство. Если g^2 делит f, то g делит f и f', а значит, $\operatorname{Discr}(f) = R(f,f') = 0$. Обратно, если $\operatorname{Discr}(f) = 0$, то согласно утверждению (1J) существует отличный от константы многочлен $g \in \hat{\mathbb{Z}}_p[X]$, делящий f и f'. Учитывая утверждение (1H), можно считать, что многочлен g неприводим. Мы можем записать $f = g \cdot h$, откуда получим, что $f' = g' \cdot h + g \cdot h'$. Поскольку многочлен g делит f', он должен делить и $g' \cdot h$. Но из неравенства $\deg g' < \deg g$ следует, что g не делит g', а значит, g делит h. Таким образом, g^2 делит f. □

Исследуем теперь поведение результанта $R(f,g)$ при замене f и g на многочлены, достаточно близкие им по метрике, определенной нормированием v_p на $\hat{\mathbb{Q}}_p[X]$.

(1M) *Пусть $f, g, f_1, g_1 \in \hat{\mathbb{Z}}_p[X]$ — многочлены, отличные от константы, $v_p(f_1 - f) \geqslant \alpha$ и $v_p(g_1 - g) \geqslant \beta$. Тогда $v_p(R(f_1,g_1) - R(f,g)) \geqslant \min\{\alpha, \beta\}$.*

Доказательство. Пусть элемент $a \in \hat{\mathbb{Z}}_p$ таков, что $v_p(a) = \min\{v_p(f_1 - f), v_p(g_1 - g)\}$. Тогда $f_1 = f + ah$, $g_1 = g + ak$ для некоторых $h, k \in \hat{\mathbb{Z}}_p[X]$. Ясно, что $R(f_1,g_1) = R(f + ah, g + ak)$. Записав исключающую матрицу для $f + ah$, $g + ak$ и вычислив ее определитель, получим $R(f,g) + as$, где $s \in \hat{\mathbb{Z}}_p$ — некоторая сумма произведений множителей, равных a или коэффициентам многочленов f, h, g, k. Следовательно,

$$v_p(R(f_1,g_1) - R(f,g)) \geqslant v_p(a) \geqslant \min\{\alpha, \beta\}. \quad \square$$

(1N) *Пусть $f, f_1 \in \hat{\mathbb{Z}}_p[X]$ — многочлены, отличные от константы, причем $v_p(f_1 - f) \geqslant \alpha$. Тогда $v_p(\mathrm{Discr}(f) - \mathrm{Discr}(f_1)) \geqslant \alpha$.*

Доказательство. Так как $\mathrm{Discr}(f) = R(f, f')$, $\mathrm{Discr}(f_1) = R(f_1, f_1')$, остается лишь заметить, что из неравенства $v_p(f_1 - f) \geqslant \alpha$ следует, что $v_p(f_1' - f') \geqslant \alpha$. Действительно, если $m = \max\{\deg f, \deg f_1\}$, $f = \sum_{i=0}^{m} a_i X^{m-i}$ и $f_1 = \sum_{i=0}^{m} b_i X^{m-i}$, то

$$f' = \sum_{i=0}^{m-1} (m-i)\, a_i\, X^{m-1-i}, \qquad {f_1}' = \sum_{i=0}^{m-1} (m-i)\, b_i\, X^{m-1-i}.$$

Поэтому $v_p((m-i)(b_i - a_i)) \geqslant v_p(b_i - a_i)$ для всех $i = 0, \ldots, m-1$, а значит, $v_p(f_1' - f') \geqslant \min\{v_p(b_i - a_i) \mid i = 0, \ldots, m-1\} \geqslant v_p(f_1 - f) \geqslant \alpha$. $\square$

Отсюда немедленно следует такое утверждение.

(1O) *Пусть $f, g \in \hat{\mathbb{Z}}_p[X]$, причем $\overline{f} = f \bmod p$, $\overline{g} = g \bmod p$. Тогда результант $R(\overline{f}, \overline{g})$ многочленов $\overline{f}$ и $\overline{g}$ (вычисленный в $\mathbb{F}_p[X]$) равен $\overline{R(f, g)}$, а дискриминант $\mathrm{Discr}(\overline{f})$ многочлена $\overline{f}$ (вычисленный в $\mathbb{F}_p[X]$) равен $\overline{\mathrm{Discr}(f)}$.*

Будем говорить, что многочлены $f, g \in \hat{\mathbb{Z}}_p[X]$ *взаимно просты по модулю p*, если $\overline{f}$ и $\overline{g}$ взаимно просты в $\mathbb{F}_p[X]$. Аналогично многочлен f называется *неприводимым по модулю p*, если $\overline{f} \in \mathbb{F}_p[X]$ неприводим. Каждый многочлен $f \in \hat{\mathbb{Z}}_p[X]$ сравним по модулю p с произведением неприводимых по модулю p многочленов из $\hat{\mathbb{Z}}_p[X]$, причем последние определены единственным образом по модулю p.

С учетом данных определений сформулируем следующий результат.

(1P) *Многочлены $f, g \in \hat{\mathbb{Z}}_p[X]$ взаимно просты по модулю p тогда и только тогда, когда их результант является единицей в $\hat{\mathbb{Z}}_p$, т. е. $v_p(R(f, g)) = 0$.*

Доказательство. По определению взаимной простоты $\overline{f}$ и $\overline{g}$ взаимно просты в $\mathbb{F}_p[X]$. По утверждению (4B) гл. II это означает, что $R(\overline{f}, \overline{g}) \neq 0$. Согласно утверждению (1O) это условие равносильно неравенству $\overline{R(f, g)} \neq 0$, т. е. p не делит $R(f, g)$, или, что то же самое, $v_p(R(f, g)) = 0$. $\square$

(1Q) *Пусть многочлены $f, g \in \mathbb{Z}_p[X]$ неприводимы по модулю простого числа p. Тогда p делит $R(f, g)$ в том и только в том случае, когда $f \equiv \varepsilon g \pmod p$, где ε — единица кольца $\hat{\mathbb{Z}}_p$.*

Доказательство. Действительно, p делит $R(f,g)$ в точности тогда, когда f и g не взаимно просты по модулю p. Но тогда существует такой отличный от константы многочлен $h \in \mathbb{Z}_p[X]$, что $f \equiv h \cdot f_1 \pmod p$ и $g \equiv h \cdot g_1 \pmod p$. По предположению $f \equiv h \pmod p$ и $g \equiv h \pmod p$, следовательно, $\overline{f} \mid \overline{g}$ и $\overline{g} \mid \overline{h}$, так что $f \equiv \varepsilon g \pmod p$, где ε — единица кольца $\hat{\mathbb{Z}}_p$. Обратное утверждение очевидно. □

Заметим, что если $f = \sum_{i=0}^{m} a_i X^i \in \mathbb{Z}_p[X]$ и f' делится на p, то $f \equiv \sum_{i \geqslant 0} a_{pi} X^{pi} \pmod p$. В самом деле, коэффициенты многочлена f' равны $j a_j$. Поэтому если p делит f', но не делит j, то p делит a_j. Следовательно,

$$f \equiv \left(\sum_{i \geqslant 0} a_{pi} X^i \right)^p \pmod p.$$

В частности, если многочлен f неприводим по модулю p, то $\overline{f'} \neq 0$, так что мы можем рассматривать дискриминант многочлена f по модулю p.

(1R) *Пусть многочлен $f \in \hat{\mathbb{Z}}_p[X]$ неприводим по модулю p. Тогда p не делит* $\operatorname{Discr}(f)$.

Доказательство. Представим f в виде $f = f_1 + p f_2$, где ни один из коэффициентов многочлена f_1 не делится на p. Тогда $f' = f_1' + p f_2'$ и согласно утверждению (1N) мы получаем $\operatorname{Discr}(f) \equiv \operatorname{Discr}(f_1) \pmod p$. Поэтому если p делит $\operatorname{Discr}(f)$, то и $\operatorname{Discr}(f_1) = R(f_1, f_1')$ делится на p. В силу утверждения (1P) существует такой многочлен $h \in \hat{\mathbb{Z}}_p[X]$, что многочлен $\overline{h}$ отличен от константы и является общим делителем многочленов $\overline{f_1}$ и $\overline{f_1}'$. Отсюда $\overline{f_1} = \overline{h} \cdot \overline{g}$, $\overline{f_1}' = \overline{h} \cdot \overline{k}$, где $g, k \in \hat{\mathbb{Z}}_p[X]$. Так как многочлен $\overline{f_1} = \overline{f}$ неприводим, мы заключаем, что $\overline{g} = \overline{c}$ для некоторого $c \in \hat{\mathbb{Z}}_p$. Тогда $\overline{c} \cdot \overline{f_1}' = \overline{f_1} \cdot \overline{k}$. Следовательно,

$$\deg(\overline{f}_1{}') \leqslant \deg(f_1') < \deg(f_1) = \deg(\overline{f}_1) \leqslant \deg(\overline{f}_1 \cdot \overline{k}) = \deg(\overline{f}_1{}'),$$

чего быть не может. □

(1S) *Пусть дан многочлен $f \in \hat{\mathbb{Z}}_p[X]$, такой, что многочлен $\overline{f}$ отличен от константы. Тогда все неприводимые делители многочлена f сравнимы между собой по модулю p в том и только в том случае, когда p делит* $\operatorname{Discr}(f)$.

Доказательство. Справедливо сравнение $f \equiv g_1 g_2 \dots g_n \pmod p$, где $g_1, g_2, \dots, g_n$ неприводимы по модулю p. Следовательно, по

утверждениям (1M) настоящей главы и (4D) гл. II мы получаем

$$\begin{aligned}\operatorname{Discr}(f) &\equiv \operatorname{Discr}(g_1 g_2 \dots g_n)\\ &= \pm \prod_{i=1}^{n} \operatorname{Discr}(g_i) \cdot \prod_{i<j} [R(g_i, g_j)]^2 \pmod{p}.\end{aligned}$$

Согласно утверждению (1R) число p не делит $\operatorname{Discr}(g_i)$ при $1 \leqslant \leqslant i \leqslant n$. Поэтому p делит $\operatorname{Discr}(f)$ тогда и только тогда, когда существуют индексы $i < j$, для которых p делит $R(g_i, g_j)$. Но согласно утверждению (1Q) это означает, что $g_i \equiv g_j \pmod{p}$. □

C. Лемма К. Гензеля

Этот важнейший результат, полученный Гензелем в 1908 г., безусловно является *raison d'être*[1] p-адических чисел. Он утверждает существование, при определенных условиях, p-адических корней многочленов. Мы докажем лемму Гензеля в сильной формулировке.

(1T) *Пусть многочлены $F, g, h \in \hat{\mathbb{Z}}_p[X]$ таковы, что*

(i) $\deg g = m > 0$, $\deg h = n > 0$, $\deg F = m + n$, *многочлен g приведен* (*т. е. старший коэффициент многочлена g равен* 1) *и* $\deg(F - gh) < \deg F$;

(ii) $v_p(R(g, h)) = \rho \geqslant 0$ *и*

(iii) $v_p(F - gh) = \alpha > 2\rho$.

Тогда существуют многочлены $G, H \in \hat{\mathbb{Z}}_p[X]$, такие, что $v_p(G - g) \geqslant \alpha - \rho$, $v_p(H - h) \geqslant \alpha - \rho$, $\deg G = \deg g$, $\deg H = \deg h$, многочлен G приведен, многочлены H и h имеют одинаковые коэффициенты при старшем члене и, наконец, $F = G \cdot H$.

Доказательство. Мы докажем следующее утверждение. Зафиксируем произвольное $j \geqslant 0$.

(*) Пусть $g, h \in \hat{\mathbb{Z}}_p[X]$, $\deg g = m$, $\deg h = n$, многочлен g приведен, $\deg(F - gh) < \deg F$, $v_p(F - gh) \geqslant \alpha + j$ и $v_p(R(g, h)) = \rho$. Тогда существуют многочлены $g^*, h^* \in \hat{\mathbb{Z}}_p[X]$, такие, что $\deg g^* < m$, $\deg h^* < n$, $v_p(g^*) \geqslant \alpha + j - \rho$, $v_p(h^*) \geqslant \alpha + j - \rho$ и $v_p(F - (g + g^*)(h - h^*)) \geqslant \alpha + j + 1$.

Действительно, $R(g, h) \neq 0$, так как $v_p(R(g, h)) = \rho$. Согласно утверждению (1J) многочлены g и h взаимно просты.

---

[1] Смыслом появления (*фр.*). — *Прим. перев.*

Заметим, что $v_p(F - gh) \geqslant \alpha + j \geqslant \rho$ и $\deg(F - gh) < \deg F = \deg f + \deg h$, а из утверждения (1K) следует, что существуют определенные единственным образом многочлены $g^*, h^* \in \hat{\mathbb{Z}}_p[X]$, такие, что

$$F - gh = h^*g + g^*h,$$
$$v_p(g^*) \geqslant v_p(F - gh) - \rho \geqslant \alpha + j - \rho,$$
$$v_p(h^*) \geqslant v_p(F - gh) - \rho \geqslant \alpha + j - \rho,$$
$$\deg(g^*) < \deg(g),$$
$$\deg(h^*) < \deg(h).$$

Следовательно,

$$\begin{aligned} v_p(F - (g + g^*)(h + h^*)) &= v_p((F - gh) - (h^*g + g^*h) - g^*h^*) \\ &= v_p(g^*h^*) \\ &\geqslant 2(\alpha + j - \rho) \\ &= (\alpha - 2\rho) + (\alpha + 2j) \\ &\geqslant \alpha + j + 1. \end{aligned}$$

Перейдем к доказательству основного утверждения. Сначала применим доказанные соотношения утверждения (*) к $g = g_0$, $h = h_0$, $j = 0$, полагая $g_1 = g_0 + g_0^*$, $h_1 = h_0 + h_0^*$. Затем применим этот результат к $g_1, h_1, j = 1$, обозначая $g_2 = g_1 + g_1^*$, $h_2 = h_1 + h_1^*$ и т. д.

Необходимо заметить, что

$$v_p(R(g_{j+1}, h_{j+1})) = v_p(R(g_j, h_j)) = \rho$$

при всех $j \geqslant 0$, поскольку, как видно из утверждения (1M) и условия (iii),

$$\begin{aligned} v_p\left[R(g_{j+1}, h_{j+1}) - R(g_j, h_j)\right] &\geqslant \min\{v_p(g^*), v_p(h^*)\} \\ &\geqslant \alpha + j - \rho > \rho. \end{aligned}$$

Итак, имеются такие последовательности многочленов $(g_j)_{j\geqslant 0}$ и $(h_j)_{j\geqslant 0}$, что $\deg g_j = m$, $\deg h_j = n$, каждый многочлен g_j имеет старший коэффициент 1, h_j и h имеют одинаковые коэффициенты при старшем члене и, наконец,

$$v_p(g_{j+1} - g_j) \geqslant \alpha + j - \rho, \quad v_p(h_{j+1} - h_j) \geqslant \alpha + j - \rho.$$

Следовательно, $(g_j)_{j\geqslant 0}$ и $(h_j)_{j\geqslant 0}$ суть последовательности Коши[2] многочленов степени m и n соответственно. Это означает, что если

$$g_j = \sum_{i=0}^{m} b_{ij} X^i \quad \text{и} \quad h_j = \sum_{i=0}^{n} c_{ij} X^i,$$

то последовательности $(b_{ij})_{j\geqslant 0}$ и $(c_{ij})_{j\geqslant 0}$ являются последовательностями Коши в $\hat{\mathbb{Q}}_p$ для каждого i. В силу полноты[3] пространства $\hat{\mathbb{Q}}_p$ можем определить $b_i = \lim b_{ij}$, $c_i = \lim c_{ij}$ и $G = \sum_{i=0}^{m} b_i X^i$, $H = \sum_{i=0}^{n} c_i X^i$.

Тогда $v_p(G - g_j) \geqslant \alpha + j - \rho$, потому что[4]

$$G - g_j = \lim_{s\to\infty} \left(\sum_{i=0}^{s} g^*_{j+i} \right)$$

и

$$v_p \left(\sum_{i=0}^{s} g^*_{j+i} \right) \geqslant \alpha + j - \rho$$

для всех $s \geqslant 1$. Аналогичным образом, $v_p(H - h_j) \geqslant \alpha + j - \rho$ для всех $j \geqslant 0$. Наконец,

$$\begin{aligned} v_p(F - GH) &= v_p[(F - g_j h_j) + (g_j - G)H + g_j(h_j - H)] \\ &\geqslant \min\{v_p(F - g_j h_j), v_p(g_j - G) + v_p(H), \\ &\qquad v_p(g_j) + v_p(h_j - H)\} \\ &\geqslant \alpha + j - \rho \end{aligned}$$

для всех $j \geqslant 0$. Отсюда следует, что $F = G \cdot H$ и многочлен G приведен, причем многочлены H и h имеют одинаковые коэффициенты при старшем члене. $\square$

---

[2] *Последовательностью Коши* или *фундаментальной последовательностью* (в пространстве с метрикой d) называется такая последовательность $(\gamma_j)_{j\geqslant 0}$, что для любого $\varepsilon > 0$ существует номер $N \in \mathbb{N}$ (зависящий от ε, т. е. $N = N(\varepsilon)$), для которого при любых $n > N(\varepsilon)$ и $q > 0$ $(n, q \in \mathbb{N})$ выполнено неравенство $d(\gamma_{n+q}, \gamma_n) < \varepsilon$. Метрика в кольце многочленов $\hat{\mathbb{Q}}_p[X]$ строится по нормированию $\tilde{v}_p$ этого кольца аналогично метрике в поле $\hat{\mathbb{Q}}_p$ (см. п. А настоящего раздела и начало п. В). — *Прим. перев.*

[3] *Полным* называется пространство с метрикой, в котором любая последовательность Коши имеет предел.

См. также книгу Г. И. Архипов, В. А. Садовничий, В. Н. Чубариков, *Лекции по математическому анализу*, *2-е изд.* — М.: Высшая школа, 2000. — *Прим. перев.*

[4] Следующее равенство справедливо в силу соотношений $g_3 = g_2 + g^*_2 = g_1 + g^*_1 + g^*_2$ и т. д. — *Прим. перев.*

Приведем теперь более традиционную формулировку леммы Гензеля.

(1U) *Пусть многочлены* $F, g, h \in \hat{\mathbb{Z}}_p[X]$ *таковы, что*

(i) $\deg g = m > 0$, $\deg h = n > 0$, $\deg F = m + n$, *многочлен* g *приведен и* $\deg(F - gh) < \deg F$;

(ii) g *и* h *взаимно просты по модулю* p;

(iii) $F \equiv g \cdot h \pmod{p}$.

Тогда существуют многочлены $G, H \in \hat{\mathbb{Z}}_p[X]$, *такие, что* $G \equiv g \pmod{p}$, $H \equiv h \pmod{p}$, $\deg G = \deg g$, $\deg H = \deg h$, *многочлен* G *приведен, многочлены* H *и* h *имеют одинаковые коэффициенты при старшем члене и* $F = G \cdot H$.

Доказательство. Утверждение немедленно вытекает из предыдущего. В самом деле, согласно результату (1P) справедливо равенство $v_p(R(g,h)) = 0$, а так как $v_p(F - gh) \geqslant 1$, применимо утверждение (1T). □

Еще одна часто встречающаяся формулировка леммы Гензеля связана с поднятием корней по модулю p.

(1V) *Пусть* $F \in \hat{\mathbb{Z}}_p[X]$, $\deg F \geqslant 1$. *Пусть, далее,* $a \in \hat{\mathbb{Z}}_p$ — *простой корень сравнения* $F(X) \equiv 0 \pmod{p}$. *Тогда существует число* $b \in \hat{\mathbb{Z}}_p$, *такое, что* $\bar{b} = \bar{a}$ *и* $F(b) = 0$.

Доказательство. По условию $F \equiv (X - a)h \pmod{p}$, причем $h(a) \not\equiv 0 \pmod{p}$. Следовательно, многочлены $X - a$ и h взаимно просты по модулю p. Тогда по предыдущему утверждению $F = G \cdot H$, где многочлен G приведен, $\deg G = 1$, $\overline{G} = X - a$, следовательно, $G = X - b$, $b \in \hat{\mathbb{Z}}_p$, $\bar{b} = \bar{a}$, а значит, $F(b) = 0$. □

Применим лемму Гензеля к многочлену $X^{p-1} - 1$.

(1W) *Для каждого простого числа* p *кольцо* $\hat{\mathbb{Z}}_p$ *содержит* $(p-1)$ *корень из единицы степени* $(p-1)$. *Более точно, для каждого* $j = 1, \ldots, p-1$ *существует единственный элемент* $w_j \in \hat{\mathbb{Z}}_p$, *такой, что* $w_j^{p-1} = 1$ *и* $w_j \equiv j \pmod{p}$.

Доказательство. Для всех $j = 1, \ldots, p-1$ справедливо сравнение $j^{p-1} \equiv 1 \pmod{p}$. Поэтому $X^{p-1} - 1 \equiv \prod_{j=1}^{p-1}(X - j) \pmod{p}$. Таким образом, все корни сравнения суть $1, 2, \ldots, p-1$, причем все они просты. Воспользовавшись предыдущим утверждением, получим, что для каждого j найдется элемент $w_j \in \hat{\mathbb{Z}}_p$, такой, что $w_j^{p-1} = 1$ и $w_j \equiv j \pmod{p}$.

Для доказательства единственности заметим, что если $w \in \hat{\mathbb{Z}}_p$, $w^{p-1} = 1$ и $w \equiv k \pmod p$, то w должно совпадать с одним из корней многочлена $X^{p-1} - 1$, скажем, $w = w_j$. Но тогда $j \equiv w_j \equiv \equiv w \equiv k \pmod p$, и поэтому $j = k$, т. е. $w = w_k$. □

Для простого числа p обозначим через $(\hat{\mathbb{Z}}/p)^\times$ мультипликативную группу ненулевых классов вычетов по модулю p. Пусть Ω обозначает мультипликативную группу корней из единицы степени $(p-1)$ в $\hat{\mathbb{Z}}_p$.

Как следствие получаем такой результат.

(1X) *Отображение, ставящее в соответствие каждому ненулевому классу вычетов j по модулю p корень степени $(p-1)$ из единицы ω_j в $\hat{\mathbb{Z}}_p$, такой, что $\omega_j \equiv j \pmod p$, устанавливает изоморфизм между мультипликативными группами $(\mathbb{Z}/p)^\times$ и Ω. Более того, элемент ω_g порождает Ω тогда и только тогда, когда g является первообразным корнем по модулю p.*

Доказательство. Действительно, если $1 \leqslant j, k, h \leqslant p-1$ и $jk \equiv h \pmod p$, то по утверждению (1W) отсюда следует, что $\omega_j \omega_k \equiv \omega_h \pmod p$. Так как $\omega_j \equiv j \pmod p$, отображение $(j \bmod p) \mapsto \omega_j$ есть изоморфизм. Последнее утверждение тривиально. □

(1Y) *Во введенных обозначениях справедливы следующие утверждения:*

(1) *если $(p-1) \nmid r$, то $\sum_{\omega \in \Omega} \omega^r = 0$;*
(2) *если $(p-1) \mid r$, то $\sum_{\omega \in \Omega} \omega^r = p-1$.*

Доказательство. (1) Пусть g является первообразным корнем по модулю p. Тогда ω_g порождает Ω. Следовательно, если $(p-1) \nmid r$, то

$$\sum_{\omega \in \Omega} \omega^r = \sum_{j=0}^{p-2} \omega_g^{jr} = \frac{1 - \omega_g^{(p-1)r}}{1 - \omega_g^r} = 0.$$

(2) Если $(p-1) \mid r$, то $\omega^r = 1$ для любого $\omega \in \Omega$, следовательно, $\sum_{\omega \in \Omega} \omega^r = p-1$. □

Список литературы

1908 Hensel, K., *Theorie der algebraischen Zahlen*, Teubner, Leipzig, 1908.

1999 Ribenboim, P., *The Theory of Classical Valuations*, Springer–Verlag, New York, 1999.

V.2. Линейные рекуррентные последовательности второго порядка

Пусть A и B — отличные от нуля целые числа, такие, что $D = A^2 - 4B \neq 0$. Для данных целых чисел R_0 и R_1 и каждого $k \geqslant 2$ положим $R_k = AR_{k-1} - BR_{k-2}$.

Если $A = 1$, $B = -1$ и $R_0 = 0$, $R_1 = 1$, то R_k есть k-е *число Фибоначчи*. Если $A = 1$, $B = -1$ и $R_0 = 2$, $R_1 = 1$, то R_k есть k-е *число Люка*. Об этих числовых последовательностях кратко говорилось в разд. IV.2.

Рассмотрим некоторые элементарные свойства числовых последовательностей $(R_k)_{k\geqslant 0}$. Для удобства будем полагать, что $R_0 = 0$ и $R_1 = 1$. Аналогичные результаты справедливы и при $R_0 = 2$, $R_1 = A$.

Утверждение (1) следующей леммы доказал Г. Зибек (1846). Оно является обобщением результата Ж. Бине для чисел Фибоначчи (гл. IV, лемма 2.3). В 1878 г. Люка опубликовал классическую работу по этой тематике (см. также Д. Г. Лемер (1930)). Дальнейшие результаты теории рекурентных последовательностей можно найти в книге Л. Е. Диксона (1920, т. I, с. 393–411).

ЛЕММА 2.1. *Во введенных обозначениях и при сделанных допущениях справедливы следующие утверждения:*

(1) *если* α *и* β *— корни уравнения* $X^2 - AX + B = 0$, *т. е.*

$$\alpha = \frac{A + \sqrt{A^2 - 4B}}{2}, \qquad \beta = \frac{A - \sqrt{A^2 - 4B}}{2},$$

то для всех $k \geqslant 0$ *выполнено равенство*

$$R_k = \frac{\alpha^k - \beta^k}{\alpha - \beta};$$

(2) *если* $k, h \geqslant 1$, *то* $R_{k+h} = R_k R_{h+1} - BR_{k-1}R_h$;
(3) $(\alpha^h + \beta^h)^2 = DR_h^2 + 4B^h$;
(4) *если* $k \mid h$, *то* $R_k \mid R_h$;
(5) $AR_h + (\alpha^h + \beta^h) = 2R_{h+1}$ *при* $h \geqslant 0$,
$AR_h - (\alpha^h + \beta^h) = 2BR_{h-1}$ *при* $h \geqslant 1$;
(6) *если* $k \geqslant 1$ *нечетно, то*

$$2^{k-1}R_k = \sum_{h=0}^{(k-1)/2} \binom{k}{2h+1} A^{k-2h-1} D^h,$$

$$2^{k-1}(\alpha^k + \beta^k) = \sum_{h=0}^{(k-1)/2} \binom{k}{2h} A^{k-2h} D^h;$$

(7) *если* $k \geqslant 1$ *нечетно и* $n \geqslant 1$, *то*

$$R_{nk} = D^{(k-1)/2} R_n^k + \sum_{h=1}^{(k-1)/2} \frac{k}{h} \binom{k-h-1}{h-1} B^{nh} D^{(k-2h-1)/2} R_n^{k-2h}.$$

Доказательство. (1) Из соотношения $\alpha^2 - A\alpha + B = 0$ следует, что $\alpha^{k+2} = A\alpha^{k+1} - B\alpha^k$ и аналогично $\beta^{k+2} = A\beta^{k+1} - B\beta^k$. Замечая, что $\alpha \neq \beta$, так как $A^2 - 4B \neq 0$, вычитая и деля на $\alpha - \beta$, получим

$$\frac{\alpha^{k+2} - \beta^{k+2}}{\alpha - \beta} = A\frac{\alpha^{k+1} - \beta^{k+1}}{\alpha - \beta} - B\frac{\alpha^k - \beta^k}{\alpha - \beta}.$$

Положим $R'_k = (\alpha^k - \beta^k)/(\alpha - \beta)$ для каждого $k \geqslant 0$. Тогда $R'_{k+2} = AR'_{k+1} - BR'_k$ при $k \geqslant 0$. Так как последовательности $(R_k)_{k\geqslant 0}$, $(R'_k)_{k\geqslant 0}$ удовлетворяют одному и тому же рекуррентному соотношению, причем $R'_0 = R_0 = 0$, $R'_1 = R_1 = 1$, мы можем заключить, что $R_k = R'_k = (\alpha^k - \beta^k)/(\alpha - k)$ для всех $k \geqslant 0$.

(2) Утверждение следует из соотношений

$$\begin{aligned} R_k R_{h+1} - BR_{k-1}R_h &= \frac{(\alpha^k - \beta^k)(\alpha^{h+1} - \beta^{h+1}) - \alpha\beta(\alpha^{k-1} - \beta^{k-1})(\alpha^h - \beta^h)}{(\alpha - \beta)^2} \\ &= \frac{\alpha^{k+h} - \beta^{k+h}}{\alpha - \beta} = R_{k+h}. \end{aligned}$$

(3) Так как $(\alpha - \beta)^2 = D$, $\alpha\beta = B$, мы получаем

$$\begin{aligned} (\alpha^h + \beta^h)^2 - DR_h^2 &= \alpha^{2h} + 2\alpha^h\beta^h + \beta^{2h} - D\left(\frac{\alpha^h - \beta^h}{\alpha - \beta}\right)^2 \\ &= \alpha^{2h} + 2\alpha^h\beta^h + \beta^{2h} - (\alpha^{2h} - 2\alpha^h\beta^h + \beta^{2h}) \\ &= 4\alpha^h\beta^h = 4B^h. \end{aligned}$$

(4) Пусть $h = nk$. Для $n = 1$ утверждение очевидно, а далее по индукции заключаем, что

$$R_{(n+1)k} = R_{nk}R_{k+1} - BR_{nk-1}R_k$$

делится на R_k.

(5) Так как $A = \alpha + \beta$, согласно (1) получаем

$$\begin{aligned} AR_h + (\alpha^h + \beta^h) \\ &= (\alpha+\beta)\frac{\alpha^h - \beta^h}{\alpha - \beta} + (\alpha^h + \beta^h) \\ &= \frac{\alpha^{h+1} - \alpha\beta^h + \alpha^h\beta - \beta^{h+1} + \alpha^{h+1} + \alpha\beta^h - \alpha^h\beta - \beta^{h+1}}{\alpha - \beta} \\ &= 2\frac{\alpha^{h+1} - \beta^{h+1}}{\alpha - \beta} = 2R_{h+1}. \end{aligned}$$

Аналогичным образом,

$$\begin{aligned} AR_h - (\alpha^h + \beta^h) \\ &= (\alpha+\beta)\frac{\alpha^h - \beta^h}{\alpha - \beta} - (\alpha^h + \beta^h) \\ &= \frac{\alpha^{h+1} - \alpha\beta^h + \alpha^h\beta - \beta^{h+1} - \alpha^{h+1} - \alpha\beta^h + \alpha^h\beta + \beta^{h+1}}{\alpha - \beta} \\ &= 2\alpha\beta\frac{\alpha^{h-1} - \beta^{h-1}}{\alpha - \beta} = 2BR_{h-1}. \end{aligned}$$

(6) Пусть $k \geqslant 1$ нечетно. Возводя соотношения

$$\begin{cases} 2\alpha = A + \sqrt{D}, \\ 2\beta = A - \sqrt{D} \end{cases}$$

в степень k и вычитая, получим

$$2^k(\alpha^k - \beta^k) = 2\left[\sum_{h=0}^{(k-1)/2} \binom{k}{2h+1} A^{k-2h-1} D^{(2h+1)/2}\right].$$

Разделив на $2(\alpha - \beta) = 2\sqrt{D}$, получаем

$$2^{k-1}R_k = \sum_{h=0}^{(k-1)/2} \binom{k}{2h+1} A^{k-2h-1} D^h.$$

Аналогично, возводя выражения для 2α и 2β в степень k, складывая и деля на 2, получим

$$2^{k-1}(\alpha^k + \beta^k) = \sum_{h=0}^{(k-1)/2} \binom{k}{2h} A^{k-2h} D^h.$$

(7) Согласно утверждению (1D) гл. VII справедливо равенство

$$X^k + Y^k = (X+Y)^k + \sum_{h=1}^{(k-1)/2} (-1)^h \frac{k}{h} \binom{k-h-1}{h-1} X^h Y^h (X+Y)^{k-2h}.$$

Положим $X = \alpha^n$, $Y = -\beta^n$. Тогда, так как число k нечетно,

$$\alpha^{nk} - \beta^{nk} = (\alpha^n - \beta^n)^k + \sum_{h=1}^{(k-1)/2} \frac{k}{h} \binom{k-h-1}{h-1} (\alpha\beta)^{nh} (\alpha^n - \beta^n)^{k-2h}.$$

Разделив на $\alpha - \beta$, учитывая, что $\alpha\beta = B$ и $\alpha - \beta = \sqrt{D}$, и используя (1), получим

$$R_{nk} = D^{(k-1)/2} R_n^k + \sum_{h=1}^{(k-1)/2} \frac{k}{h} \binom{k-h-1}{n-1} B^{nh} D^{(k-2h-1)/2} R_n^{k-2h}. \quad \square$$

Исследуем теперь свойства делимости членов рекуррентной последовательности $(R_k)_{k \geqslant 0}$.

Пусть $m \geqslant 1$ и найдется такой индекс k, что m делит R_k. Наименьшее из таких k называется *рангом вхождения* числа m в последовательность $(R_k)_{k \geqslant 0}$ и обозначается через $r(m)$.

Лемма 2.2.

(1) *Пусть* $m \geqslant 1$ *и* НОД$(m, B) = 1$. *Тогда существует ранг вхождения числа* m.

(2) *Если* $m \geqslant 1$ *и* НОД$(m, B) = 1$, *то* m *делит* R_k *тогда и только тогда, когда* $r(m)$ *делит* k.

(3) *Пусть* $m, n \geqslant 1$, НОД$(m, B) =$ НОД$(n, B) =$ НОД$(m, n) = 1$. *Тогда* $r(mn) =$ НОК$(r(m), r(n))$.

(4) *Пусть* p — *нечетное простое число,* $p \nmid B$. *Тогда* $R_p \equiv (D/r) \pmod p$ (*где через* (D/p) *обозначен символ Якоби*).

(5) *Пусть* p — *нечетное простое число,* $p \nmid B$. *Тогда* $r(p)$ *делит* $\big(p - (D/p)\big)$.

(6) *Пусть* p — *нечетное простое число,* $p \nmid B$, $k = v_p\big(R_{r(p)}\big)$ *и* $e \geqslant k$. *Тогда* $r(p^e) = p^{e-k} r(p)$.

(7) *Пусть* $k \geqslant 1$, $h \geqslant 1$. *Тогда* $R_{kh+1} \equiv R_{h+1}^k \pmod{R_h^2}$.

(8) *Пусть* $k \geqslant 1$, $h \geqslant 1$. *Тогда* $R_{kh} \equiv k R_h R_{h+1}^{k-1} \pmod{R_h^2}$.

Доказательство. (1) Рассмотрим множество пар

$$\{(R_k \mod m,\ R_{k-1} \mod m) \mid k = 1, 2, \ldots\}.$$

Так как существует лишь конечное число пар классов вычетов по модулю m, найдутся такие целые числа k и l, $k < l$, что

$$\begin{cases} R_k \equiv R_l \pmod m, \\ R_{k-1} \equiv R_{l-1} \pmod m. \end{cases}$$

Так как $BR_{k-2} = AR_{k-1} - R_k$, мы заключаем, что $BR_{k-2} \equiv BR_{l-2} \pmod m$, откуда, поскольку НОД$(m, B) = 1$, следует сравнение $R_{k-2} \equiv R_{l-2} \pmod m$. Повторение этого рассуждения приводит к тому, что $0 = R_0 \equiv R_{l-k} \pmod m$, т. е. существует такое натуральное число $l - k$, что $m \mid R_{l-k}$. Отсюда заключаем, что найдется наименьший номер $r(m)$, для которого $m \mid R_{r(m)}$.

(2) Заметим сначала, что если m делит R_k, то НОД$(m, R_{k-1}) = 1$ для каждого $k \geqslant 2$. Действительно, иначе нашлось бы простое число p, делящее m, R_k и R_{k-1}. Из соотношений $R_k = AR_{k-1} - BR_{k-2}$ и НОД$(m, B) = 1$ следует, что $p \mid R_{k-2}$. Повторение этого рассуждения приводит к тому, что $p \mid R_1 = 1$, а это противоречит предположению.

Пусть теперь S — множество всех чисел k, для которых m делит R_k. Согласно (1) мы имеем $S \neq \varnothing$. Более того, если $k, h \in S$, то $k + h \in S$. Действительно, из утверждения (2) леммы 2.1 следует, что $m \mid (k + h)$.

Аналогично, если $k, h \in S, k < h$, то $h - k \in S$. В самом деле, $R_h = R_{k+(h-k)} = R_k R_{h-k+1} - BR_{k-1}R_{h-k}$, следовательно, $m \mid BR_{k-1}R_{h-k}$. Но НОД$(m, B) = 1$ и, как показано выше, НОД$(m, R_{k-1}) = 1$, а значит, $m \mid R_{h-k}$.

Этого достаточно, чтобы показать, что S есть множество чисел, кратных наименьшему его элементу, а именно $r(m)$.

(3) Из условий $m \mid mn$ и $mn \mid R_{r(mn)}$ следует, что $m \mid R_{r(mn)}$, поэтому $r(m) \mid r(mn)$. Аналогично $r(n) \mid r(mn)$, а значит, $l = \text{НОК}(r(m), r(n))$ делит $r(mn)$.

С другой стороны, $m \mid R_{r(m)}$ и $r(m) \mid l$, следовательно, $m \mid R_l$. Аналогично доказывается, что $n \mid R_l$. Тогда с учетом равенства НОД$(m, n) = 1$ получаем $mn \mid R_l$, т. е. $r(mn) \mid l$.

(4) Согласно утверждению (3.3) гл. II мы имеем

$$R_p = \frac{\alpha^p - \beta^p}{\alpha - \beta} = (\alpha - \beta)^{p-1} + pf = D^{(p-1)/2} + pf.$$

Так как $D^{(p-1)/2} \equiv (D/p) \pmod p$, мы заключаем, что $R_p \equiv \left(\frac{D}{p}\right) \pmod p$.

(5) Если $p \mid D$, то $(D/p) = 0$ и $R_p \equiv 0 \pmod{p}$. Пусть $(D/p) = 1$. Покажем, что тогда $R_{p-1} \equiv 0 \pmod{p}$, откуда согласно (2) можно заключить, что $r(p) \mid (p-1)$. Действительно, согласно лемме 2.1 (5) и доказанному выше утверждению (4) мы имеем

$$2BR_{p-1} = AR_p - (\alpha^p + \beta^p) \equiv A - (\alpha^p + \alpha^p) \pmod{p}.$$

По лемме 2.1 (6) получаем $2^{p-1}(\alpha^p + \beta^p) \equiv A^p \pmod{p}$. Следовательно,

$$2BR_{p-1} \equiv 2^p BR_{p-1} \equiv 2^{p-1}A - A^p \equiv A - A^p \equiv 0 \pmod{p}.$$

Так как $p \nmid B$, $p \neq 2$, справедливо сравнение $R_{p-1} \equiv 0 \pmod{p}$.

Пусть теперь $(D/p) = -1$. Покажем, что $R_{p+1} \equiv 0 \pmod{p}$, откуда согласно (2) можно заключить, что $r(p) \mid (p+1)$. Действительно, по лемме 2.1 (5) и доказанному выше утверждению (4) мы имеем

$$2R_{p+1} = AR_p + (\alpha^p + \beta^p) \equiv -A + (\alpha^p + \beta^p) \pmod{p}.$$

По лемме 2.1 (6) получаем $2^{p-1}(\alpha^p + \beta^p) \equiv A^p \pmod{p}$, так что

$$2R_{p+1} \equiv 2^p R_{p+1} \equiv -2^{p-1}A + A^p \equiv -A + A^p \equiv 0 \pmod{p}.$$

Поскольку $p \neq 2$, должно выполняться сравнение $R_{p+1} \equiv 0 \pmod{p}$.

(6) Пусть $R_{r(p)} = p^k t$, где $p \nmid t$, $k \geqslant 1$. По лемме 2.1(7) для $m \geqslant 1$ имеем

$$\begin{aligned} R_{r(p)p^m} &= D^{(p^m-1)/2} R_{r(p)}^{p^m} \\ &+ \sum_{h=1}^{(p^m-1)/2} \frac{p^m}{h} \binom{p^m - h - 1}{h-1} B^{r(p)h} D^{(p^m-2h-1)/2} R_{r(p)}^{p^m-2h}. \end{aligned}$$

Для $h = (p^m - 1)/2$ слагаемое с номером h равно $p^m B^{r(p)(p^m-1)/2} \times$ $\times R_{r(p)}$, причем его p-адическое значение есть $m + k$, поскольку $p \nmid B$.

Если $0 < h < (p^m - 1)/2$, то

$$\begin{aligned} &v_p\left(\frac{p^m}{h}\binom{p^m - h - 1}{h-1} B^{r(p)h} D^{(p^m-2h-1)/2} R_{r(p)}^{p^m-2h}\right) \\ &\quad \geqslant v_p\left(\frac{p^m}{h} R_{r(p)}^{p^m-2h}\right) = m + (p^m - 2h)k - v_p(h). \end{aligned}$$

Однако если $m \geqslant 1$ и $0 < h < (p^m - 1)/2$, то $p^m > 2h + v_p(h) + 1$. Действительно, $2h = p^m - p^s r$, где $p \nmid r$, $0 \leqslant s < m$, и если $s = 0$,

то $r > 1$. Тогда $2h + v_p(h) + 1 = p^m - p^s r + s + 1 < p^m$, потому что $s + 1 < p^s r$ (так как $p \neq 2$). Следовательно,

$$m + (p^m - 2h)k - v_p(h) > m + v_p(h)(k-1) + k \geqslant m + k.$$

При $m \geqslant 1$ справедливы неравенства

$$v_p\left(D^{(p^m-1)/2} R_{r(p)}^{p^m}\right) \geqslant p^m k > m + k$$

(так как $p \neq 2$). Таким образом, для $m \geqslant 1$ имеем $v_p\left(R_{r(p)p^m}\right) = m + k$, что справедливо и при $m = 0$.

Положим $m = e - k \geqslant 0$. Тогда $v_p\left(R_{r(p)p^{e-k}}\right) = e$, так что $p^e \mid R_{r(p)p^{e-k}}$ и, следовательно, согласно (2) мы получаем, что $r(p^e) \mid r(p)p^{e-k}$. Так как $p^e \mid R_{r(p^e)}$, мы заключаем, что $r(p) \mid r(p^e)$. Отсюда следует, что $r(p^e) = r(p)p^m$ при $0 \leqslant m \leqslant e - k$. Если $m < e - k$, то $v_p(R_{r(p)p^m}) = m + k < e$, так что $p^e \nmid R_{r(p)p^m}$, следовательно, $r(p^e) \neq r(p)p^m$. Отсюда видно, что $r(p^e) = r(p)p^{e-k}$.

(7) Доказательство проведем методом математической индукции. Для $k = 1$ утверждение очевидно. Далее, по лемме 2.1 (2) и индуктивному предположению

$$\begin{aligned} R_{(k+1)h+1} &= R_{(kh+1)+h} \\ &= R_{kh+1}R_{h+1} - BR_{kh}R_h \\ &\equiv R_{kh+1}R_{h+1} \\ &\equiv R_{h+1}^{k+1} \pmod{R_h^2}, \end{aligned}$$

так как R_h делит R_{kh} (по лемме 2.1 (4)).

(8) Также воспользуемся методом математической индукции. Для $k = 1$ утверждение очевидно. Далее, принимая во внимание утверждение (7), лемму 2.1 (2) и (4), получим

$$\begin{aligned} R_{(k+1)h} &= R_{kh+h} = R_h R_{kh+1} - BR_{h-1}R_{kh} \\ &\equiv R_h R_{h+1}^k - BR_{h-1}kR_h R_{h+1}^{k-1} \\ &\equiv R_h R_{h+1}^{k-1}[R_{h+1} - BkR_{h-1}] \\ &\equiv R_h R_{h+1}^{k-1}(k+1)R_{h+1} \equiv (k+1)R_h R_{h+1}^k \pmod{R_h^2}, \end{aligned}$$

поскольку

$$R_{h+1} = R_h R_2 - BR_{h-1} \equiv -BR_{h-1} \pmod{R_h}. \quad \square$$

Список литературы

1843 Binet, J., *Mémoire sur l'intégration des équations linéaires aux différences finies d'un ordre quelconque à coefficients variables*, C. R. Acad. Sci. Paris, **17** (1843), 559–567.

1846 Siebeck, H., *Die recurrenten Reihen vom Standpunkt der Zahlentheorie aus betrachtet*, J. Reine Angew. Math., **33** (1846), 71–77.

1878 Lucas, E., *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math., **1** (1878), 184–239 and 289–321.

1920 Dickson, L.E., *History of the Theory of Numbers*, Vol. I. Carnegie Institution, Washington, DC, 1920; reprinted by Chelsea, New York, 1952.

1930 Lehmer, D.H., *An extended theory of Lucas' functions*, Ann. of Math., **31** (1930), 419–448.

1995 Ribenboim, P., *The Fibonacci numbers and the Arctic Ocean*, Sympos. Gaussiana, Conf. A (editors M. Behara, R. Fritsch, and R.G. Lintz), W. de Gruyter, Berlin, 1995, pp. 41–83.

Глава VI

Арифметические ограничения на гипотетические решения и показатель степени

Пусть p — нечетное простое число и x, y, z — отличные от нуля попарно взаимно простые целые числа, удовлетворяющие уравнению $x^p + y^p + z^p = 0$.

В этой главе мы рассмотрим сравнения и свойства делимости, присущие некоторым выражениям, содержащим числа x, y, z и p. В ряде случаев будут получены противоречия, показывающие справедливость теоремы Ферма (или ее первого случая) для определенных показателей p. В разделе 3 мы остановимся на гипотезе Абеля, полное прямое доказательство которой до сих пор неизвестно.

VI.1. Сравнения

Итак, пусть p — нечетное простое число, и пусть числа x, y, z — отличные от нуля попарно взаимно простые решения уравнения $x^p + y^p + z^p = 0$. Для удобства ссылок приведем необходимые утверждения из разд. III.1.

Пусть $p \nmid xyz$. Тогда существуют отличные от нуля целые числа r, s, t, r_1, s_1 и t_1, такие, что

$$\begin{cases} x + y = t^p, & (x^p + y^p)/(x + y) = t_1^p, & z = -tt_1, \\ y + z = r^p, & (y^p + z^p)/(y + z) = r_1^p, & x = -rr_1, \\ z + x = s^p, & (z^p + x^p)/(z + x) = s_1^p, & y = -ss_1, \end{cases} \tag{1.1}$$

причем $p \nmid rstr_1s_1t_1$ и r, s, t, r_1, s_1, t_1 попарно просты. Более того, $r^p + s^p + t^p \neq 0$.

Если $p \nmid xy$, но $p \mid z$, то найдутся такие отличные от нуля целые числа r, s, t, r_1, s_1, t_1 и $n \geqslant 2$, что

$$\begin{cases} x + y = p^{pn-1}t^p, & (x^p + y^p)/(x+y) = pt_1^p, & z = -p^n t t_1, \\ y + z = r^p, & (y^p + z^p)/(x+y) = r_1^p, & x = -r r_1, \\ x + y = s^p, & (z^p + x^p)/(x+y) = s_1^p, & y = -s s_1, \end{cases} \tag{1.2}$$

$p \nmid rstr_1s_1t_1$ и r, s, t, r_1, s_1, t_1 попарно взаимно просты, причем $r^p + s^p + p^{pn-1}t^p \neq 0$.

Более того, если $p \nmid xyz$, то $r_1 \equiv 1 \pmod{2p^2}$, $s_1 \equiv 1 \pmod{2p^2}$ и $t_1 \equiv 1 \pmod{2p^2}$. Если $p \mid z$, $p \nmid xy$, то $r_1 \equiv 1 \pmod{2p}$, $s_1 \equiv 1 \pmod{2p}$ и $t_1 \equiv 1 \pmod{2p^2}$. Если $p \nmid xyz$, то

$$\begin{cases} x = -r^p + k, \\ y = -s^p + k, \\ z = -t^p + k, \end{cases} \tag{1.3}$$

где $k = (r^p + s^p + t^p)/2$. Если $p \mid z$, $p \nmid xy$, то

$$\begin{cases} x = -r^p + k, \\ y = -s^p + k, \\ z = -p^{pn-1}t^p + k, \end{cases} \tag{1.4}$$

где $k = (r^p + s^p + p^{pn-1}t^p)/2$.

Начнем с простого сравнения, а затем рассмотрим его более сильную форму. Из сравнений $x^p \equiv x \pmod{p}$, $y^p \equiv y \pmod{p}$, $z^p \equiv z \pmod{p}$ следует, что $-z \equiv -z^p = x^p + y^p \equiv x + y \pmod{p}$, а значит, $x^p + y^p = -z^p \equiv (x+y)^p \pmod{p^2}$.

Первый результат принадлежит Флеку (1909). В более слабой форме он был получен Линдом в 1910 г. Впоследствии утверждение было заново доказано Фробениусом в 1914 г., Вандивером (1914), Поме (1923) и Перес-Качо (1958).

(1A) *Пусть p — нечетное простое число и x, y, z — отличные от нуля взаимно простые решения уравнения $x^p + y^p + z^p = 0$. Тогда*

(1) *если p не делит x, то $x^{p-1} \equiv 1 \pmod{p^3}$;*

(2) *если $p \nmid xyz$, то $(x+y)^p \equiv x^p + y^p \pmod{p^4}$.*

Доказательство. (1) *Случай* 1: p не делит yz. Как указано выше, тогда $r_1 \equiv 1 \pmod{p^2}$. Следовательно, $x = -rr_1 \equiv -r \pmod{p^2}$ и $x^p \equiv -r^p \pmod{p^3}$.

В силу симметрии имеем также $y^p \equiv -s^p \pmod{p^3}$ и $z^p \equiv -t^p \pmod{p^3}$. Так как $x^p + y^p + z^p = 0$, мы заключаем, что $r^p + s^p + t^p \equiv 0$

$(\mathrm{mod}\ p^3)$. Из соотношений (1.3) вытекает, что $x \equiv -r^p\ (\mathrm{mod}\ p^3)$. Следовательно, $x^p \equiv x\ (\mathrm{mod}\ p^3)$ и $x^{p-1} \equiv 1\ (\mathrm{mod}\ p^3)$.

Случай 2: z кратно p. В этом случае p не делит y. Как отмечалось выше, тогда $t_1 \equiv 1\ (\mathrm{mod}\ p^2)$, а значит, $t_1^p \equiv 1\ (\mathrm{mod}\ p^3)$.

С другой стороны, $pn - 1 \geqslant 4$, поэтому $x \equiv -y\ (\mathrm{mod}\ p^4)$ и $pt_1^p = (x^p + y^p)/(x+y) = x^{p-1} - x^{p-2}y + \ldots - xy^{p-2} + y^{p-1} \equiv px^{p-1}\ (\mathrm{mod}\ p^4)$, а следовательно, $x^{p-1} \equiv t_1^p \equiv 1\ (\mathrm{mod}\ p^3)$.

(2) Из соотношений $0 = x^p + y^p + z^p \equiv x + y + z\ (\mathrm{mod}\ p^3)$ следует, что $x+y \equiv -z\ (\mathrm{mod}\ p^3)$, а значит, $(x+y)^p \equiv -z^p \equiv x^p + y^p\ (\mathrm{mod}\ p^4)$. □

Воспользовавшись теорией полей классов, Вандивер вывел приведенное ниже следствие из теорем Фуртвенглера (1914, 1919).

(1B) *Во введенных обозначениях справедливы сравнения* $x^p \equiv x\ (\mathrm{mod}\ p^3)$, $y^p \equiv y\ (\mathrm{mod}\ p^3)$, $z^p \equiv z\ (\mathrm{mod}\ p^3)$ *и* $x+y+z \equiv 0\ (\mathrm{mod}\ p^3)$.

Следующий результат также принадлежит Флеку (1909). Его частные случаи были получены заново Поме (1923), Вандивером (1925), Джеймсом (1934), Невядомским (1938) и Инкери (1946).

(1C) *Пусть отличные от нуля взаимно простые целые числа* x, y, z *таковы, что* $x^p + y^p + z^p = 0$. *Тогда*

(1) *если* $p \nmid xyz$, *то* $x+y+z$ *делится на* 6 *и на* $rstp^3$, *а* $r+s+t$ *кратно* p^2;

(2) *если* $p \mid z$, *то* $x+y+z$ *делится на* 6 *и на* $rstp^2$, *а* $r+s$ *кратно* p, *в то время как* $r+s+t$ *не делится на* p.

Доказательство. Из соотношений (1.1) (соответственно (1.2)) следует, что в обоих случаях числа r, s, t делят $x+y+z$. Но число $x+y+z$ четно и $x^p \equiv x\ (\mathrm{mod}\ 3)$, $y^p \equiv y\ (\mathrm{mod}\ 3)$, $z^p \equiv z\ (\mathrm{mod}\ 3)$, следовательно, $x+y+z \equiv x^p + y^p + z^p = 0\ (\mathrm{mod}\ 3)$.

В первом случае согласно утверждению (1A) получим $x^p \equiv x\ (\mathrm{mod}\ p^3)$, $y^p \equiv y\ (\mathrm{mod}\ p^3)$, $z^p \equiv z\ (\mathrm{mod}\ p^3)$, а значит, $x+y+z \equiv 0\ (\mathrm{mod}\ p^3)$. Так как $p \nmid rst$, мы заключаем, что $rstp^3$ делит $x+y+z$.

Как указывалось выше, $r_1 \equiv 1\ (\mathrm{mod}\ p^2)$, $s_1 \equiv 1\ (\mathrm{mod}\ p^2)$, $t_1 \equiv 1\ (\mathrm{mod}\ p^2)$. Из соотношений (1.1) следует, что $x \equiv -r\ (\mathrm{mod}\ p^2)$, $y \equiv -s\ (\mathrm{mod}\ p^2)$, $z \equiv -t\ (\mathrm{mod}\ p^2)$, а значит, $r+s+t \equiv 0\ (\mathrm{mod}\ p^2)$.

Пусть теперь $p \mid z$. Тогда $p \nmid xy$, откуда, учитывая (1.2), получим, что p^n делит z и $x+y$ (при $n \geqslant 2$), а значит, p^2 делит $x+y+z$. Так как $p \nmid rst$, число $x+y+z$ кратно p^2rst.

Как указывалось выше, $r_1 \equiv 1 \pmod p$, $s_1 \equiv 1 \pmod p$, откуда, учитывая (1.2), получим, что $x \equiv -r \pmod p$, $y \equiv -s \pmod p$. Следовательно, $r + s \equiv -(x + y) \equiv z \equiv 0 \pmod p$. Таким образом, $r + s + t \equiv t \not\equiv 0 \pmod p$. □

Первая часть следующего предложения была доказана Шпунаром (1929) и Джеймсом (1934). Более простое доказательство нашел Сегал (1938).

(1D) *Пусть отличные от нуля взаимно простые целые числа* x, y, z *таковы, что* $x^p + y^p + z^p = 0$. *Тогда*

(1) *если* $p \nmid xyz$, *то* $r + s + t \neq 0$;

(2) *если* $p \mid z$, *то* $r + s + p^n t \neq 0$ *и* $r + s + t \neq 0$ (*где показатель* n *определен в* (1.2)).

Доказательство. (1) Предположим, что $p \nmid xyz$ и $r + s + t = 0$. Так как $(r, s, t) = 1$, без ограничения общности можно считать, что r и s нечетны, а t четно. Тогда $r^p + s^p = (y+z)+(z+x) = x+y+2z = = t^p - 2tt_1$ (согласно (1.1)). Отсюда

$$\frac{r^p + s^p}{r + s} = -\frac{r^p + s^p}{t} = 2t_1 - t^{p-1}.$$

Левая часть этого соотношения равна $r^{p-1} - r^{p-2}s + \ldots - rs^{p-2} + + s^{p-1}$. Она нечетна как сумма p нечетных чисел. С другой стороны, $2t_1 - t^{p-1}$ четно, что невозможно. Следовательно, в первом случае $r + s + t \neq 0$.

(2) Если $p \mid z$, то $p \nmid xy$ и с учетом равенств (1.2) мы получаем, что $r^p + s^p = (y+z)+(z+x) = x+y+2z = p^{pn-1}t^p - 2p^n t t_1$. Значит, если $r + s + p^n t = 0$, то

$$\frac{r^p + s^p}{r + s} = -\frac{r^p + s^p}{p^n t} = 2t_1 - p^{pn-n-1}t^{p-1}.$$

Поскольку $p \nmid t_1$ и $n \geqslant 2$, число p не делит $(r^p + s^p)/(r + s)$. С другой стороны, согласно утверждению (3R)(4) гл. II справедливо соотношение $\text{НОД}(p, r + s) = \text{НОД}(r + s, (r^p + s^p)/(r + s))$. В силу утверждения (1C) сумма $(r + s)$ кратна p, а значит, p делит $(r^p + s^p)/(r + s)$. Итак, мы получили противоречие. Наконец, так как $p \nmid (r + s + t)$, из утверждения (1C) следует, что $r + s + t \neq 0$. □

В связи с этим результатом Раклиш в 1944 г. рассмотрел следующее предположение относительно нечетного простого показателя p.

(R'_p) *Пусть a, b, c — ненулевые целые числа и $pabc$ делит $a^p + b^p + c^p$. Тогда $a + b + c = 0$ или $a^p + b^p + c^p = 0$.*

Раклиш доказал такой результат.

(1E) *Если условие (R'_p) справедливо для некоторого нечетного простого числа p, то для показателя p справедливо утверждение первого случая теоремы Ферма.*

Доказательство. Предположим, что не кратные p взаимно простые целые числа x, y, z таковы, что $x^p + y^p + z^p = 0$. Определим ненулевые целые числа r, s, t из соотношений (1.1). Согласно замечанию после формулы (1.1) мы получаем, что $r^p + s^p + t^p \neq 0$, а как следует из утверждения (1D), $r + s + t \neq 0$. По утверждению (1C) мы получаем, что p делит $r + s + t$. Согласно (1.1) и (1.3) числа r, s, t делят $r^p + s^p + t^p$, а так как числа p, r, s и t попарно взаимно просты, $prst$ делит $r^p + s^p + t^p$, из чего следует, что условие (R'_p) не выполняется. □

Однако, вообще говоря, утверждение (R'_p) неверно. Для (R'_3) и (R'_5) найдены контрпримеры: $p = 3$, $a = b = c = 1$ и $p = 5$, $a = 33$, $b = -2$, $c = -1$ соответственно.

Аналогичным образом рассмотрим следующее утверждение.

(R''_p) *Пусть отличные от нуля целые числа a, b, c таковы, что $pabc$ делит $a^p + b^p + p^{pn-1}c^p$ (для некоторого $n \geqslant 2$). Тогда $a + b + p^n c = 0$ или $a^p + b^p + p^{pn-1}c^p = 0$.*

Справедлива следующая импликация.

(1F) *Если утверждение (R''_p) выполнено для некоторого нечетного простого числа p, то выполнено и утверждение второго случая теоремы Ферма для показателя p.*

Доказательство. Предположим, что x, y, z — такие взаимно простые целые числа, что $p \mid z$ и $x^p + y^p + z^p = 0$. Определим ненулевые целые числа r, s, t, n из соотношений (1.2), $n \geqslant 2$. Тогда, как следует из утверждения (1D), $r + s + p^n t \neq 0$, и с учетом замечания после (1.2) мы получаем, что $r^p + s^p + p^{pn-1}t^p \neq 0$.

Однако, как мы видели в утверждении (1C), $r + s \equiv 0 \pmod{p}$, так что p делит $r^p + s^p + p^{pn-1}t^p$. Согласно соотношениям (1.4) числа r, s, t делят $r^p + s^p + p^{pn-1}t^p$, а так как p, r, s и t взаимно просты, $prst$ делит $r^p + s^p + p^{pn-1}t^p$. Это противоречит предположению (R''_p). □

В 1946 г. Инкери обобщил утверждение (1A). Он также получил соответствующий результат для второго случая, применив более сильный метод из теории полей классов.

(1G) *Пусть p — нечетное простое число, $n \geqslant 1$, ненулевые целые числа x, y, z взаимно просты, причем $x^{p^n} + y^{p^n} + z^{p^n} = 0$ и x не кратно p. Тогда $x^{p-1} \equiv 1 \pmod{p^{2n+1}}$.*

Доказательство. В силу того что числа x, y, z попарно взаимно просты, можно без ограничения общности полагать, что $p \nmid y$. Тогда

$$-x^{p^n} = y^{p^n} + z^{p^n} = (y+z) \prod_{m=1}^{n} Q_p\left(y^{p^{m-1}}, -z^{p^{m-1}}\right).$$

Согласно утверждению (3C)(2) гл. II множители в правой части этого равенства попарно взаимно просты, следовательно, $y + z = a^{p^n}$, где $a \mid x$ и $p \nmid a$. Аналогично $x + z = b^{p^n}$, где $b \mid y$ и $p \nmid b$.

Если $p \nmid z$, то, используя такие же рассуждения, получим $x+y = c^{p^n}$, где $c \mid z, p \nmid c$, и $(x^p + y^p)/(x+y) = d^{p^n}$, где $d \mid z$, $p \nmid d$ и НОД $(c, d) = 1$. Однако если $p \mid z$, то исходя из утверждения (3C)(3) гл. II мы можем записать $x + y = p^h c^{p^n}$ и $(x^p + y^p)/(x+y) = pd^{p^n}$, где $c \mid z$, $d \mid z$, $p \nmid c$, $p \nmid d$, НОД $(c, d) = 1$ и $h \geqslant 1$.

Покажем, что если q — любое простое число, делящее d (и при $p \mid z$, и при $p \nmid z$), то $q \equiv 1 \pmod{p^{n+1}}$. Действительно, так как $q \mid d$, мы заключаем, что $q \mid (x^p + y^p)$, $q \mid z$, $q \neq p$ и $q \nmid c$, следовательно, $q \nmid (x+y)$. Тогда

$$\begin{cases} y \equiv a^{p^n} \pmod{q}, \\ x \equiv b^{p^n} \pmod{q}, \end{cases}$$

а значит, $q \nmid \left(a^{p^n} + b^{p^n}\right)$. Но $a^{p^{n+1}} + b^{p^{n+1}} \equiv x^p + y^p \equiv 0 \pmod{q}$. Следовательно, q является примитивным делителем бинома $a^{p^{n+1}} + b^{p^{n+1}}$. Из утверждения (3G) гл. II следует, что $q \equiv 1 \pmod{p^{n+1}}$, поэтому $d \equiv 1 \pmod{p^{n+1}}$, а значит, $d^{p^n} \equiv 1 \pmod{p^{2n+1}}$.

Для завершения доказательства изучим два случая.

Если $p \nmid x$, то $(x^p+y^p)/(x+y) \equiv 1 \pmod{p^{2n+1}}$, поэтому $x^p+y^p \equiv x+y \pmod{p^{2n+1}}$. В силу симметрии $y^p+z^p \equiv y+z \pmod{p^{2n+1}}$ и $x^p+z^p \equiv x+z \pmod{p^{2n+1}}$. Сложив эти сравнения, разделив на 2 и вычитая из полученного сравнения второе из исходных сравнений, получим $x^p \equiv x \pmod{p^{2n+1}}$, следовательно, $x^{p-1} \equiv 1 \pmod{p^{2n+1}}$.

Если $p \mid z$, положим $v_p(z) = k \geqslant 1$, так что $v_p\left(z^{p^n}\right) = p^n k \geqslant n+1$. Согласно утверждению (3C)(4) гл. II мы имеем $v_p(x+y) = p^n k - n$,

так что $x \equiv -y \pmod{p^{kp^n - n}}$. Следовательно,

$$pd^{p^n} = \frac{x^p + y^p}{x + y} = x^{p-1} - x^{p-2}y + \ldots - xy^{p-2} + y^{p-1} \equiv px^{p-1} \pmod{p^{kp^n - n}}.$$

Но $kp^n - n \geqslant 2n + 2$, потому что $p > 3$ (иначе предположение не выполнено). Итак, $x^{p-1} \equiv d^{p^n} \equiv 1 \pmod{p^{2n+1}}$. □

Дальнейшие результаты связаны со сравнениями вида

$$(1 + x)^{p^k} \equiv 1 + x^{p^k} \pmod{p^{k+1}}.$$

Прежде чем перейти к их изучению, докажем следующую лемму, которую явно сформулировала Ферентину-Николакопулу (1965).

Лемма 1.1. *Пусть нечетное простое число p не делит a. Тогда*

(1) *если $n > m \geqslant 0$, то $a^{p^n} \equiv a^{p^{n-m}} \pmod{p^{n-m+1}}$;*

(2) *если $k \geqslant 1$, то $a^{p^k} - a^{p^{k-1}} \equiv ap^{k-1}(a^{p-1} - 1) \pmod{p^{k+1}}$.*

Пусть p также не делит $(a + 1)$. Тогда

(3) *если $k \geqslant 1$, то $[(a+1)^{p^k} - a^{p^k} - 1] - [(a+1)^{p^{k-1}} - a^{p^{k-1}} - 1] \equiv \equiv p^{k-1}[(a+1)^p - a^p - 1] \pmod{p^{k+1}}$;*

(4) *если $k \geqslant 2$, то $(a+1)^{p^k} \equiv a^{p^k} + 1 \pmod{p^{k+1}}$ тогда и только тогда, когда $(a+1)^{p^{k-1}} \equiv a^{p^{k-1}} + 1 \pmod{p^{k+1}}$;*

(5) *если $k \geqslant 1$ и $(a+1)^{p^k} \equiv a^{p^k} + 1 \pmod{p^{k+2}}$, то $(a+1)^{p^{k-1}} \equiv \equiv a^{p^{k-1}} + 1 \pmod{p^{k+1}}$.*

Доказательство. (1) Возведем сравнения $a^{p^m} \equiv \ldots \equiv a^p \equiv a \pmod{p}$ в степень p^{n-m}:

$$a^{p^n} \equiv a^{p^{n-m}} \pmod{p^{n-m+1}}.$$

(2) Запишем соотношение $a^{p^k} - a^{p^{k-1}} = a^{p^{k-1}}[a^{p^{k-1}(p-1)} - 1]$. Если $a^{p-1} = 1 + bp$, то

$$\left(a^{p-1}\right)^{p^{k-1}} \equiv 1 + bp^k \pmod{p^{k+1}},$$

следовательно,

$$\left(a^{p-1}\right)^{p^{k-1}} - 1 \equiv bp^k \equiv \left(a^{p-1} - 1\right)p^{k-1} \pmod{p^{k+1}}.$$

Так как $a^{p^{k-1}} \equiv a \pmod{p}$, мы заключаем, что

$$a^{p^k} - a^{p^{k-1}} \equiv a(a^{p-1} - 1)p^{k-1} \pmod{p^{k+1}}.$$

(3) Применив утверждение (2) и учитывая то обстоятельство, что по предположению p не делит $a+1$, получим

$$(a+1)^{p^k} - (a+1)^{p^{k-1}} \equiv (a+1)p^{k-1}((a+1)^{p-1} - 1) \pmod{p^{k+1}}$$

и аналогично

$$a^{p^k} - a^{p^{k-1}} \equiv ap^{k-1}(a^{p-1} - 1) \pmod{p^{k+1}}.$$

Вычитая эти сравнения, получим

$$\begin{aligned}[(a+1)^{p^k} - a^{p^k} - 1] - [(a+1)^{p^{k-1}} - a^{p^{k-1}} - 1] \\ \equiv p^{k-1}[(a+1)^p - a^p - 1] \pmod{p^{k+1}}.\end{aligned}$$

(4) Прежде всего заметим, что если $k \geqslant 2$, то $a^{p^k} \equiv a^{p^{k-1}} \equiv \equiv \ldots \equiv a^p \pmod{p^2}$ и

$$(a+1)^{p^k} \equiv (a+1)^{p^{k-1}} \equiv (a+1)^p \pmod{p^2}.$$

Таким образом,

$$\begin{aligned}(a+1)^{p^k} - a^{p^k} - 1 &\equiv (a+1)^{p^{k-1}} - a^{p^{k-1}} - 1 \\ &\equiv (a+1)^p - a^p - 1 \pmod{p^2}.\end{aligned}$$

Если

$$(a+1)^{p^k} - a^{p^k} - 1 \equiv 0 \pmod{p^{k+1}},$$

то, очевидно,

$$(a+1)^{p^k} - a^{p^k} - 1 \equiv 0 \pmod{p^2},$$

так что $(a+1)^p - a^p - 1 \equiv 0 \pmod{p^2}$. Исходя из утверждения (3) получаем

$$(a+1)^{p^{k-1}} - a^{p^{k-1}} - 1 \equiv 0 \pmod{p^{k+1}}.$$

Обратное утверждение доказывается аналогично.

(5) Из предположения следует, что $(a+1)^{p^k} \equiv a^{p^k} + 1 \pmod{p^{k+1}}$, а значит, $(a+1)^{p^{k-1}} \equiv a^{p^{k-1}} + 1 \pmod{p^{k+1}}$. □

В частности, как было отмечено Биркгофом и как показал Кармайкл в своей статье «Вторая заметка по последней теореме Ферма» (1913), если простое число p не делит ни a, ни $(a+1)$, то $(1+a)^p \equiv \equiv 1 + a^p \pmod{p^3}$ тогда и только тогда, когда $(1+a)^{p^2} \equiv 1 + a^{p^2} \pmod{p^3}$.

Следующий результат получен Клёсгеном в 1970 г.

(1H) *Пусть p — нечетное простое число и $m \geqslant 1$. Тогда следующие утверждения равносильны.*

(1) *Существуют целые числа* x, y, z, *не кратные* p, *удовлетворяющие сравнению*

$$x^{p^m} + y^{p^m} + z^{p^m} \equiv 0 \pmod{p^{m+1}}.$$

(2) *Существует целое число* a, $1 \leqslant a \leqslant (p-3)/2$, *такое, что*

$$1 + a^{p^m} \equiv (1+a)^{p^m} \pmod{p^{m+1}}.$$

Более того, если какие-либо два из чисел x, y, z *сравнимы по модулю* p, *то* $2^{p^m-1} \equiv 1 \pmod{p^{m+1}}$.

Доказательство. Достаточно доказать, что из (1) следует (2), поскольку обратное утверждение очевидно. Пусть z' — такое целое число, что $z'z \equiv 1 \pmod{p}$. Пусть, далее, $a \equiv z'x \pmod{p}$, $-b \equiv z'y \pmod{p}$, где $1 \leqslant a \leqslant p-1$, $1 \leqslant b \leqslant p-1$. Тогда

$$a^{p^m} \equiv z'^{p^m} x^{p^m} \pmod{p^{m+1}}, \qquad -b^{p^m} \equiv z'^{p^m} y^{p^m} \pmod{p^{m+1}},$$

так что $a^{p^m} + 1 \equiv b^{p^m} \pmod{p^{m+1}}$. Если $b \equiv a + t \pmod{p}$, то $a^{p^m} + 1 \equiv b^{p^m} \equiv (a+t)^{p^m} \equiv a + t \pmod{p}$, поэтому $t \equiv 1 \pmod{p}$ и $a^{p^m} + 1 \equiv (a+1)^{p^m} \pmod{p^{m+1}}$, где $1 \leqslant a < a+1 \leqslant p-1$.

Если $a = (p-1)/2$, то $a + 1 = (p+1)/2 \equiv -(p-1)/2 \pmod{p}$, поэтому

$$(p-1)^{p^m} + 2^{p^m} \equiv -(p-1)^{p^m} \pmod{p^{m+1}},$$

следовательно, $2^{p^m} \equiv 2 \pmod{p^{m+1}}$ и можно положить $a = 1$, так как $1^{p^m} + 1 \equiv (1+1)^{p^m} \pmod{p^{m+1}}$. Если $(p-1)/2 < a \leqslant p-2$, то, полагая $a_1 = p - 1 - a$, получим $1 \leqslant a_1 \leqslant (p-3)/2$ и

$$1 + a_1^{p^m} \equiv (1+a_1)^{p^m} \pmod{p^{m+1}}.$$

Чтобы доказать заключительное утверждение, предположим, что, например, $x \equiv y \pmod{p}$. В ходе доказательства мы получили сравнения $a \equiv z'x \equiv z'y \equiv -b \pmod{p}$, $b \equiv a + 1 \pmod{p}$, из которых следует, что $2a \equiv -1 \pmod{p}$, а значит, $a = (p-1)/2$. Таким образом, $2^{p^m-1} \equiv 1 \pmod{p^{m+1}}$. □

Получим прямое следствие из этого результата.

Если для некоторого показателя p не выполнен первый случай теоремы Ферма, то есть если найдутся целые числа x, y, z, не кратные p, такие, что $x^p + y^p + z^p = 0$, то непременно $x^p + y^p + z^p \equiv 0 \pmod{p^2}$. Следовательно, мы получаем, что существует такое число a, $1 \leqslant a \leqslant (p-3)/2$, что $1 + a^p \equiv (1+a)^p \pmod{p^2}$. Кармайкл (1913) и Мейснер (1914) получили более сильные результаты (первое утверждение доказал также Ганди (1975)).

(1I) *Пусть отличные от нуля взаимно простые целые числа* x, y, z *таковы, что* $x^p + y^p + z^p = 0$. *Тогда*

(1) *если* $p \nmid xyz$, *то существует такое целое число* a, $1 \leqslant a \leqslant (p-3)/2$, *что*

$$(1+a)^p \equiv 1 + a^{p^2} \pmod{p^3},$$

или, что равносильно, $(1+a)^p \equiv 1 + a^p \pmod{p^3}$;

(2) *если* $p \mid xyz$, *то существует такое целое число* a. $1 \leqslant a \leqslant (p-3)/2$, *что* $(1+a)^p \equiv 1 + a^p \pmod{p^2}$.

Доказательство. (1) Из утверждения (1A) следует, что $x^p \equiv x \pmod{p^3}$, поэтому $x^{p^2} \equiv x^p \equiv x \pmod{p^3}$. Аналогично $y^{p^2} \equiv y \pmod{p^3}$ и $z^{p^2} \equiv z \pmod{p^3}$. Следовательно, принимая во внимание утверждение (1C), мы получаем $x^{p^2} + y^{p^2} + z^{p^2} \equiv x + y + z \equiv 0 \pmod{p^3}$.

В силу утверждения (1H) существует такое число a, $1 \leqslant a \leqslant (p-3)/2$, что $(1+a)^{p^2} \equiv 1 + a^{p^2} \pmod{p^3}$, и с учетом замечания Биркгофа после леммы 1.1 мы можем заключить, что $(1+a)^p \equiv 1 + a^p \pmod{p^3}$.

(2) Если $p \mid xyz$, то можно считать, например, что $p \nmid xy$, $p \mid z$. Согласно утверждению (1C) справедливо сравнение $x + y + z \equiv 0 \pmod{p^2}$, следовательно, $(x+y)^p \equiv -z^p = x^p + y^p \pmod{p^3}$. Так как $x \not\equiv 0 \pmod{p}$, $y \not\equiv 0 \pmod{p}$, найдется такое целое число b, $1 \leqslant b \leqslant p-1$, что $y \equiv bx \pmod{p}$. Тогда $y^p \equiv b^p x^p \pmod{p^2}$ и $(x+y)^p \equiv x^p(1+b)^p \pmod{p^2}$. Таким образом, $x^p(1+b)^p \equiv x^p(1+b^p) \pmod{p^2}$. Поскольку $p \nmid x$, должно выполняться сравнение $(1+b)^p \equiv 1 + b^p \pmod{p^2}$.

Как и при доказательстве утверждения (1H), если $1 \leqslant b \leqslant (p-3)/2$, положим $a = b$, в случае когда $(p-1)/2 < b \leqslant p-1$, возьмем $a = p - 1 - b$, а если $b = (p-1)/2$, то положим $a = 1$. □

Заметим, что, как отметил Биркгоф (см. упоминавшуюся статью Кармайкла (1913)), утверждение (1I) не применимо для первого случая при $p \equiv 1 \pmod{6}$. Убедимся в этом, рассмотрев следующую несложную лемму.

Лемма 1.2. *Нечетное простое число* p *сравнимо с* $1 \pmod{6}$ *тогда и только тогда, когда* $p \neq 3$ *и существует такое целое число* t, $1 \leqslant t \leqslant p-1$, *что* $t^2 + t + 1 \equiv 0 \pmod{p}$.

Доказательство. Пусть $p = 6k+1$ и g — первообразный корень по модулю p. Пусть, далее, число t таково, что $1 \leqslant t \leqslant p-1$ и $t \equiv g^{2k}$

$(\mathrm{mod}\ p)$. Тогда $t \not\equiv 1\ (\mathrm{mod}\ p)$, но $t^3 \equiv 1\ (\mathrm{mod}\ p)$. Следовательно, $t^2+t+1 = (t^3-1)/(t-1) \equiv 0\ (\mathrm{mod}\ p)$.

Обратно, если $t^2+t+1 \equiv 0\ (\mathrm{mod}\ p)$, то $(2t+1)^2 = 4t^2+4t+1 = 4(t^2+t+1)-3 \equiv -3\ (\mathrm{mod}\ p)$. Таким образом, -3 есть квадратичный вычет по модулю $p \neq 3$. Отсюда следует, что $1 = (-3/p) = (p/3)$, так что $p \equiv 1\ (\mathrm{mod}\ 3)$, а значит, $p \equiv 1\ (\mathrm{mod}\ 6)$. □

Применим теперь следующее утверждение, доказанное Коши (1841): если $p \equiv 1\ (\mathrm{mod}\ 6)$, то многочлен $pX(X+1)(X^2+X+1)^2$ делит $(X+1)^p - X^p - 1$ (см. утверждение (2A), гл. VII).

Итак, если $p \equiv 1\ (\mathrm{mod}\ 6)$, то по лемме 1.2 найдется такое число t, $1 \leqslant t \leqslant p-1$, что $t^2+t+1 \equiv 0\ (\mathrm{mod}\ p)$. Отсюда следует, что $(1+t)^p \equiv 1+t^p\ (\mathrm{mod}\ p^3)$ и согласно замечанию Биркгофа $(1+t)^{p^2} \equiv 1+t^{p^2}\ (\mathrm{mod}\ p^3)$. Продолжая рассуждения, аналогичные доказательству утверждения (1H), мы придем к выводу, что существует такое a, $1 \leqslant a \leqslant (p-3)/2$, что $(1+a)^{p^2} \equiv 1+a^{p^2}\ (\mathrm{mod}\ p^3)$.

Отсюда видно, что предложение (1I) не применимо для первого случая при $p \equiv 1\ (\mathrm{mod}\ 6)$.

В 1975 г. Вагштаф установил, что для всех простых показателей p, $p < 100\,000$, $p \equiv -1\ (\mathrm{mod}\ 6)$, сравнение $(1+x)^p \equiv 1+x^p\ (\mathrm{mod}\ p^3)$ не разрешимо в целых числах $a, 1 \leqslant a \leqslant (p-3)/2$. Таким образом, первый случай для этих показателей был доказан (см. также Джонсон (1977)).

В том же 1975 г. Ганди независимо провел эти вычисления. Утверждение (1I) можно переформулировать так.

(1J) *Пусть g — первообразный корень по модулю p. Тогда*

(1) *если $1+g^{jp^2}+g^{kp^2} \not\equiv 0\ (\mathrm{mod}\ p^3)$ для всех $j,k = 1,\ldots,p-1$, то для показателя p справедлив первый случай теоремы Ферма;*

(2) *если $1+g^{jp}+g^{kp} \not\equiv 0\ (\mathrm{mod}\ p^2)$ для всех $j,k = 1,\ldots,p-1$, то теорема Ферма справедлива для показателя p.*

Доказательство. (1) Если для показателя p не выполнен первый случай теоремы Ферма, то должно существовать такое целое число a, $1 \leqslant a \leqslant (p-3)/2$, что $(1+a)^{p^2} \equiv 1+a^{p^2}\ (\mathrm{mod}\ p^3)$. Заметим, что $a \not\equiv 0, -1\ (\mathrm{mod}\ p)$. Пусть числа j,k таковы, что $a \equiv g^j\ (\mathrm{mod}\ p)$, $-(1+a) \equiv g^k\ (\mathrm{mod}\ p)$. Тогда $a^{p^2} \equiv g^{jp^2}\ (\mathrm{mod}\ p^3)$, $(1+a)^{p^2} \equiv -g^{kp^2}\ (\mathrm{mod}\ p^3)$ и, следовательно, $1+g^{jp^2}+g^{kp^2} \equiv 0\ (\mathrm{mod}\ p^3)$.

(2) Если для показателя p не выполнена теорема Ферма, то должно существовать такое число a, $1 \leqslant a \leqslant (p-3)/2$, что $(1+a)^p \equiv$

$\equiv 1+a^p \pmod{p^2}$. Тогда аналогичным образом заключаем, что найдутся такие числа j, k, что $1 + g^{jp} + g^{kp} \equiv 0 \pmod{p^2}$. □

В 1950 г. Трипанис предположил (без доказательства), что справедливо следующее усиление результата Кармайкла, которое было заново найдено Ферентину-Николакопулу в 1965 г. (мы приводим ее доказательство), а в 1970 г. обобщено Клёсгеном (см. (1J)).

(1K) *Если первый случай теоремы Ферма не выполнен для показателя $p > 5$, то существует целое число a, $1 \leqslant a \leqslant (p-5)/2$, такое, что*

$$(1+a)^{p^2} \equiv 1 + a^{p^2} \pmod{p^4},$$

или, что равносильно,

$$(1+a)^{p^3} \equiv 1 + a^{p^3} \pmod{p^4}.$$

Доказательство. Предположим, что положительные целые числа x, y, z, не кратные p, таковы, что

$$x^p + y^p = z^p.$$

Пусть t обозначает порядок числа p по модулю z, то есть такое наименьшее натуральное число, что

$$p^t \equiv 1 \pmod{z}.$$

Тогда $p^t - 1 = dz$ для некоторого натурального числа d. Ясно, что p не делит d. Положим $m = dx, n = dy$. Тогда p не делит m и n, причем

$$m^p + n^p = (p^t - 1)^p.$$

Таким образом, числа m, n и $-(p^t - 1)$ удовлетворяют уравнению Ферма. По утверждению (1C) мы имеем $m + n \equiv p^t - 1 \pmod{p^3}$.

Заметим, что числа m и n меньше чем $p^t - 1$, а так как $(m+n)^p > m^p + n^p$, мы получаем, что $m+n > p^t - 1$, поэтому $p^t < m+n+1 < 2p^t$. Отсюда следует, что $t \geqslant 4$, потому что если $t \leqslant 3$, то

$$m + n \equiv p^t - 1 \pmod{p^t},$$

т. е. $m + n + 1 \equiv 0 \pmod{p^t}$, что невозможно.

Так как $m + n \equiv -1 \pmod{p^3}$, выполняется сравнение $(n+1)^p \equiv -m^p \pmod{p^4}$. Из соотношения $m^p + n^p = (p^t - 1)^p$ следует, что

$$n^p + 1 \equiv -m^p \pmod{p^{t+1}},$$

а значит, $n^p+1 \equiv -m^p \pmod{p^5}$, и с учетом предыдущего сравнения мы получаем

$$(n+1)^p \equiv n^p + 1 \pmod{p^4}.$$

Согласно утверждению (1A) мы имеем $m^{p-1} \equiv n^{p-1} \equiv (p^t-1)^{p-1} \equiv$ $\equiv 1 \pmod{p^3}$, и, поскольку $n+1 \equiv -m \pmod{p^3}$,

$$(n+1)^{p-1} \equiv m^{p-1} \equiv n^{p-1} \equiv 1 \pmod{p^3}.$$

Как известно, существует в точности $\varphi(p^3) = p^2(p-1)$ обратимых классов вычетов по модулю p^3, образующих циклическую мультипликативную группу. Пусть класс вычетов w по модулю p^3 порождает эту группу. Тогда из сравнений

$$n^{p-1} \equiv 1 \pmod{p^3} \qquad \text{и} \qquad (n+1)^{p-1} \equiv 1 \pmod{p^3}$$

следует, что порядки классов вычетов $n \pmod{p^3}$ и $(n+1) \pmod{p^3}$ делят $p-1$. Поэтому существуют такие целые числа h, k, $0 \leqslant h, k \leqslant p-2$, что

$$n \equiv w^{hp^2} \pmod{p^3}$$

и

$$n+1 \equiv w^{kp^2} \pmod{p^3}.$$

Пусть $b \equiv w^h \pmod{p}$. Тогда

$$n \equiv b^{p^2} \equiv b \pmod{p}$$

и

$$n+1 \equiv w^{kp^2} \equiv w^k \pmod{p},$$

следовательно, $w^k \equiv b+1 \pmod{p}$, так что

$$n^p \equiv b^{p^3} \pmod{p^4}$$

и

$$(n+1)^p \equiv (b+1)^{p^3} \pmod{p^4}.$$

Поскольку $(n+1)^p \equiv n^p + 1 \pmod{p^4}$, мы получаем, что

$$(b+1)^{p^3} \equiv b^{p^3} + 1 \pmod{p^4}.$$

Заметим, что p не делит ни b, ни $b+1$. Если $1 \leqslant b \leqslant (p-5)/2$, положим $a = b$. При $b = (p-3)/2$ из сравнения

$$\left(\frac{p-1}{2}\right)^{p^3} \equiv \left(\frac{p-3}{2}\right)^{p^3} + 1 \pmod{p^4}$$

следует, что

$$-1 \equiv -3^{p^3} + 2^{p^3} \pmod{p^4},$$

а значит, можно взять $a = 2$. Если $b = (p-1)/2$, то

$$\left(\frac{p+1}{2}\right)^{p^3} \equiv \left(\frac{p-1}{2}\right)^{p^3} + 1 \pmod{p^4},$$

откуда следует, что

$$1 \equiv -1 + 2^{p^3} \pmod{p^4},$$

поэтому можно положить $a = 1$. Если $(p+1)/2 \leqslant b < p-1$, то, полагая $a = p-1-b$, получим $1 \leqslant a \leqslant (p-3)/2$ и

$$(a+1)^{p^3} \equiv -b^{p^3} \equiv 1 - (b+1)^{p^3} \equiv 1 + a^{p^3} \pmod{p^4}.$$

По лемме 1.1(4) мы получаем

$$(a+1)^{p^2} \equiv a^{p^2} + 1 \pmod{p^4}. \quad \square$$

Заметим, что ввиду леммы 1.1(5) утверждение (1K) и в самом деле является усилением (1I).

Получим прямое следствие из приведенных результатов, указанное Ганди (1976).

(1L) *Пусть утверждение первого случая теоремы Ферма не выполнено для некоторого показателя p. Тогда существует такое целое число b, не кратное p, что* $(1+b)^p \equiv 1 + b^p \pmod{p^4}$.

Доказательство. Согласно утверждению (1J) найдется такое целое число a, не кратное p, что

$$(1+a)^{p^2} \equiv 1 + a^{p^2} \pmod{p^4}.$$

По лемме 1.1 мы имеем

$$(1+a)^p \equiv 1 + a^p \pmod{p^3}.$$

Возводя это сравнение в степень p, получим

$$(1+a)^{p^2} \equiv (1+a^p)^p \pmod{p^4},$$

следовательно,

$$(1+a^p)^p \equiv 1 + a^{p^2} \pmod{p^4}.$$

Положив $b = a^p$, получим $(1+b)^p \equiv 1 + b^p \pmod{p^4}$. $\square$

Брчич-Костич в 1952 г. получил подобный результат при некоторых дополнительных ограничениях на простой показатель p. В 1970 г. Клёсген доказал следующее обобщение утверждения (1K).

(1M) *Пусть $n \geqslant 1$ и целые числа x, y, z, не кратные данному простому нечетному числу p, таковы, что $x^{p^n} + y^{p^n} + z^{p^n} = 0$. Тогда*

$$x^{p^{3n}} + y^{p^{3n}} + z^{p^{3n}} \equiv 0 \pmod{p^{3n+1}},$$

или, что равносильно, существует такое целое число a, $1 \leqslant a \leqslant (p-3)/2$, что

$$(1+a)^{p^{3n}} \equiv 1 + a^{p^{3n}} \pmod{p^{3n+1}}.$$

Доказательство. Согласно утверждению (1G) мы имеем $x^p \equiv x \pmod{p^{2n+1}}$. Возводя это сравнение в степень p^n, получим $x^{p^{n+1}} \equiv x^{p^n} \pmod{p^{3n+1}}$. Еще одно возведение в степень p^n приведет к сравнениям $x^{p^{n+2}} \equiv x^{p^{n+1}} \equiv x^{p^n} \pmod{p^{3n+1}}$. Повторяя эту операцию, мы получим $x^{p^{3n}} \equiv x^{p^n} \pmod{p^{3n+1}}$. Аналогично $y^{p^{3n}} \equiv y^{p^n} \pmod{p^{3n+1}}$ и $z^{p^{3n}} \equiv z^{p^n} \pmod{p^{3n+1}}$. Следовательно,

$$x^{p^{3n}} + y^{p^{3n}} + z^{p^{3n}} \equiv x^{p^n} + y^{p^n} + z^{p^n} = 0 \pmod{p^{3n+1}}.$$

Последнее утверждение следует из (1H). □

При $n = 1$ получим утверждение (1J).

Джонсон (1977) исследовал возможность дальнейшего усиления сравнений Кармайкла и Трипаниса по модулю каждой степени p^{n+2} ($n \geqslant 1$). В подобных ситуациях обычно применяют p-адические методы.

Обозначим через $\alpha_j \in \hat{\mathbb{Z}}_p$ единственное p-адическое целое число, являющееся корнем степени $(p-1)$ из единицы, такое, что $\alpha_j \equiv j \pmod{p}$ для всех $j = 1, 2, \ldots, p-1$ (см. (1W), гл. V).

(1N) *Пусть p — простое число, $p > 3$, и целое число a таково, что p не делит ни a, ни $a+1$. Тогда следующие условия равносильны:*

(1) *для всех $n \geqslant 1$ справедливо сравнение* $(1+a)^{p^n} \equiv 1 + a^{p^n} \pmod{p^{n+2}}$;
(2) $1 + \alpha_a = \alpha_{1+a}$;
(3) $a^2 + a + 1 \equiv 0 \pmod{p}$.

Доказательство. Заметим, что p-адическое разложение числа α_a имеет вид $\alpha_a = a + \rho_a p$, где $\rho_a \in \hat{\mathbb{Z}}_p$, причем ρ_a определяется по α_a единственным образом. Покажем, что для всех $n \geqslant 0$ выполнено сравнение

$$\alpha_a \equiv a^{p^n} + \rho_a p^{n+1} \pmod{p^{n+2}}. \tag{1.5}$$

Для $n = 0$ это очевидно. Пусть сравнение (1.5) выполнено для некоторого n. Тогда из равенства $\alpha_a^{p-1} = 1$ следует, что

$$\begin{aligned}\alpha_a &= (\alpha_a)^p \equiv (a^{p^n} + \rho_a p^{n+1})^p \\ &\equiv a^{p^{n+1}} + \rho_a p^{n+2} a^{p^n(p-1)} \\ &\equiv a^{p^{n+1}} + \rho_a p^{n+2} \pmod{p^{n+3}},\end{aligned}$$

поскольку $a^{p^n(p-1)} \equiv 1 \pmod{p}$.

Теперь мы готовы доказать равносильность утверждений (1), (2) и (3).

(1) $\Rightarrow$ (2) Пусть для всех $n \geqslant 1$ выполнено условие $1 + a^{p^n} \equiv (1+a)^{p^n} \pmod{p^{n+2}}$. Следовательно, с учетом (1.5) можно записать сравнения

$$1 + \alpha_a \equiv 1 + a^{p^n} + \rho_a p^{n+1} \equiv (1+a)^{p^n} + \rho_a p^{n+1} \pmod{p^{n+2}}.$$

С другой стороны, $\alpha_{1+a} \equiv (1+a)^{p^n} + \rho_{1+a} p^{n+1} \pmod{p^{n+2}}$, поэтому $1 + \alpha_a \equiv \alpha_{1+a} \pmod{p^{n+1}}$ для всех $n \geqslant 1$. Из единственности p-адического разложения следует, что $1 + \alpha_a = \alpha_{1+a}$.

(2) $\Rightarrow$ (1) Воспользуемся сравнениями

$$\alpha_{1+a} \equiv (1+a)^{p^n} + \rho_{1+a} p^{n+1} \pmod{p^{n+2}}$$

и

$$1 + \alpha_a \equiv 1 + a^{p^n} + \rho_a p^{n+1} \pmod{p^{n+2}}.$$

Согласно предположению $\alpha_{1+a} = 1 + \alpha_a$, так что $(1+a) + \rho_{1+a} p = 1 + (a + \rho_a p)$. Из единственности p-адического разложения заключаем, что $\rho_{1+a} = \rho_a$, а значит, $(1+a)^{p^n} \equiv 1 + a^{p^n} \pmod{p^{n+2}}$.

(2) $\Rightarrow$ (3) Заметим, что p-адические корни из единицы степени $(p-1)$ образуют циклическую мультипликативную группу. Пусть α_j — ее порождающий элемент. Рассмотрим подполе $\mathbb{Q}(\alpha_j) \subset \hat{\mathbb{Q}}_p$, являющееся расширением Галуа поля $\mathbb{Q}$. Пусть σ — такой автоморфизм, что $\sigma(\alpha_j) = \alpha_j^{-1}$. Так как $\alpha_a = (\alpha_j)^k$ (для некоторого k), справедливы равенства $\sigma(\alpha_a) = (\alpha_j)^{-k} = \alpha_a^{-1}$. Аналогично $\sigma(\alpha_{1+a}) = \alpha_{1+a}^{-1}$.

По предположению $1 + \alpha_a = \alpha_{1+a}$. Применив автоморфизм σ, получим $1 + \alpha_a^{-1} = \alpha_{1+a}^{-1}$. Следовательно,

$$\alpha_a \alpha_{1+a} + \alpha_{1+a} = \alpha_a,$$

так что

$$\alpha_a + \alpha_a^2 + 1 + \alpha_a = \alpha_a$$

и

$$\alpha_a^2 + \alpha_a + 1 = 0.$$

Так как $\alpha_a \equiv a \pmod p$, мы можем заключить, что $a^2 + a + 1 \equiv 0 \pmod p$.

(3) $\Rightarrow$ (2) Поскольку $p \neq 3$ и $a^2 + a + 1 \equiv 0 \pmod p$, мы получаем, что $a \not\equiv 1 \pmod p$. Умножив на $(a-1)$, получим $a^3 \equiv 1 \pmod p$. Следовательно, $(\alpha_a)^3 \equiv 1 \pmod p$. Но $(\alpha_a^3)^{p-1} = 1$, поэтому $\alpha_a^3 = 1$, а это единственный корень из единицы степени $(p-1)$ в $\hat{\mathbb{Z}}_p$, сравнимый с 1 по модулю p. Так как $\alpha_a \neq 1$, число α_a суть первообразный кубический корень из 1, а значит,

$$\alpha_a^2 + \alpha_a + 1 = 0.$$

Таким образом, $\alpha_a + 1 = -\alpha_a^2 \equiv -a^2 \equiv a + 1 \pmod p$, а следовательно, $\alpha_a + 1 \equiv \alpha_{a+1}$ есть единственный корень из единицы степени $(p-1)$ в $\hat{\mathbb{Z}}_p$, сравнимый с $a+1$ по модулю p. □

Заметим, что ввиду леммы 1.1 вышеуказанное условие (1) равносильно следующему:

(1′) *для всех* $n \geqslant 1$ *справедливо сравнение* $(1+a)^{p^{n+1}} \equiv 1 + a^{p^{n+1}} \pmod{p^{n+2}}$.

Из леммы 1.2 следует, что при $p > 3$ целое число a, $1 \leqslant a \leqslant p-1$, удовлетворяющее эквивалентным условиям из утверждения (1N), существует тогда и только тогда, когда $p \equiv 1 \pmod 6$.

Как следствие получаем такой результат.

(1O) *Пусть* p *— простое число,* $p \equiv 5 \pmod 6$. *Тогда существует такое целое число* $n_0 > 0$, *что при* $n \geqslant n_0$ *и* $a = 1, 2, \ldots, p-2$ *выполнено условие*

$$(1+a)^{p^n} \not\equiv 1 + a^{p^n} \pmod{p^{n+2}}.$$

Доказательство. Из леммы 1.2 следует, что если $a = 1, 2, \ldots, p-2$, то $a^2 + a + 1 \not\equiv 0 \pmod p$. Согласно утверждению (1N) для всех a существует такое число $n(a)$, что

$$(1+a)^{p^{n(a)}} \not\equiv 1 + a^{p^{n(a)}} \pmod{p^{n(a)+2}}.$$

В силу леммы 1.1(5) мы заключаем, что если $n \geqslant n_0 = \max\{n(a) \mid a = 1, 2, \ldots, p-2\}$, то

$$(1+a)^{p^n} \not\equiv 1 + a^{p^n} \pmod{p^{n+2}}$$

для всех $a = 1, 2, \ldots, p-1$. □

Было бы интересно установить справедливость следующего утверждения.

(I) *Пусть для всех* $a = 1, 2, \ldots, p-2$ *выполняется сравнение* $(1+a)^p \equiv 1 + a^p \pmod{p^3}$. *Тогда* $a^2 + a + 1 \equiv 0 \pmod{p}$.

Дело в том, что если утверждение (I) справедливо, то и первый случай теоремы Ферма справедлив для всех показателей $p \equiv 5 \pmod 6$. Действительно, иначе согласно утверждению (1I) нашlось бы такое число a, $1 \leqslant a \leqslant p-2$, что $(1+a)^p \equiv 1 + a^p \pmod{p^3}$. Но тогда ввиду утверждения (I) должно выполняться сравнение $a^2 + a + 1 \equiv 0 \pmod p$, а значит, $p \equiv 1 \pmod 6$, что противоречит предположению.

Арвин в 1920 г. показал, что существуют такие целые числа a и простые числа p, что $(1+a)^p \equiv 1 + a^p \pmod{p^2}$, но в то же время $a^2 + a + 1 \not\equiv 0 \pmod p$. Так что кажущееся естественным усиление утверждения (I) неверно.

Список литературы

1841 Cauchy, A., *Exercices d'analyse et de physique mathématique*, **2** (1841), 137–144 (Notes sur quelques théorèmes d'algèbre); *Oeuvres Complètes*, (2), Vol. XII, pp. 157–166, Gauthier-Villars, Paris, 1916.

1909 Fleck, A., *Miszellen zum großen Fermatschen Problem*, Sitzungsber. Berliner Math. Ges., **8** (1909), 133–148.

1910 Lind, B., *Über das letzte Fermatsche Theorem*, Abh. Geschichte Math. Wiss, **26** (1910), 23–65.

1913 Carmichael, R.D., *Note on Fermat's last theorem*, Bull. Amer. Math. Soc., **19** (1913), 233–236.

1913 Carmichael, R.D., *Second note on Fermat's last theorem*, Bull. Amer. Math. Soc., **19** (1913), 402–403.

1914 Frobenius, G., *Über den Fermatschen Satz, III*, Sitzungsber. Königl. Preussischen Akad. Wiss., Berlin, **22** (1914), 653–681; reprinted in *Collected Works*, Vol. 3, pp. 648–676, Springer-Verlag, Berlin, 1968.

1914 Vandiver, H.S., *A note on Fermat's last theorem*, Trans. Amer. Math. Soc., **15** (1914), 202–204.

1914 Meissner, W., *Über die Lösungen der Kongruenz* $x^{p-1} \equiv 1 \pmod{p^m}$ *und ihre Verwertung zur Periodenbestimmung mod* p^k, Sitzungsber. Berliner Math. Ges., **13** (1914), 96–107.

1917 Pollaczek, F., *Über den großen Fermat'schen Satz*, Sitzungsber. Akad. Wiss., Wien, Abt. IIa, **126** (1917), 45–59.

1919 Vandiver, H.S., *A property of cyclotomic numbers and its relation to Fermat's last theorem*, Ann. of Math., **21** (1919), 73–80.

1920 Arwin, A., *Über die Lösung der Kongruenz* $(\lambda+1)^p - \lambda^p - 1 \equiv 0 \pmod{p^2}$, Acta Math., **42** (1920), 173–190.

1923 Pomey, L., *Sur le dernier théorème de Fermat*, C. R. Acad. Sci. Paris, **177** (1923), 1187–1190.

1925 Vandiver, H.S., *A property of cyclotomic integers and its relation to Fermat's last theorem*, Ann. of Math., **26** (1925), 217–232.

1929 Spunar, V.A., *On Fermat's last theorem, II*, J. Washington Acad. Sci., **19** (1929), 395–401.

1934 James, G., *On Fermat's last theorem*, Amer. Math. Monthly, **41** (1934), 419–424.

1938 Segal, D., *A note on Fermat's last theorem*, Amer. Math. Monthly, **45** (1938), 438–439.

1938 Niewiadomski, R., *Sur la grandeur absolue et relation mutuelle des nombres entiers qui peuvent résoudre l'équation* $x^p + y^p = z^p$ (in Polish), Wiadom. Mat., **44** (1938), 113–127.

1944 Racliş, N., *Démonstration du grand théorème de Fermat pour des grandes valeurs de l'exposant*, Bull. École Polytechnique Bucarest, **15** (1944), 45–61.

1946 Inkeri, K., *Untersuchungen über die Fermatsche Vermutung*, Ann. Acad. Sci. Fenn., Ser. AI, **33** (1946), 1–60.

1950 Trypanis, A.A., *On Fermat's last theorem*, Proc. Intern. Congress Math., Cambridge, 1950, Vol. 1, 301–302.

1952 Brčić-Kostić, M., *L'extension de la congruence* $(a+b)^n - a^n - b^n \equiv 0 \pmod{n}$ (*n un nombre premier*) (in Croatian, French summary), Hrvatsko Prirodoslovno Društvo, Glas. Mat. Ser. II, **7** (1952), 7–11.

1958 Pérez-Cacho, L., *Sobre algunas cuestiones de la teoria de números*, Rev. Mat. Hisp.-Amer., (4), **18** (1958), 10–27 and 113–124.

1965 Ferentinou-Nicolacopoulou, J., *A new necessary condition for the existence of a solution to the equation* $x^p + y^p = z^p$ *of Fermat* (Greek, French summary), Bull. Soc. Math. Grèce (N.S.), **6** (1965), 222–236.

1965 Ferentinou-Nicolacopoulou, J., *Remarks on the preceding article* (Greek, French summary), Bull. Soc. Math. Grèce (N.S.), **6** (1965), 356–357.

1970 Klösgen, W., *Untersuchungen über Fermatsche Kongruenzen*, Gesellschaft Math. Datenverarbeitung, Bonn, No. 37, 1970, 124 pp.

1975 Everett, C.J. and Metropolis, N., *On the roots of* $x^m \pm 1$ *in the p-adic field* $\mathbb{Q}_p$, Notices Amer. Math. Soc., **22** (1975), A-619; preprint, Los Alamos Sci. Lab., LA-UR-74-1835.

1975 Gandhi, J.M., *Fermat's last theorem, I*, Notices Amer. Math. Soc., **22** (1975), A-486.

1975 Wagstaff, S., *Fermat's last theorem is true for any exponent less than* 100 000, Notices Amer. Math. Soc., **23** (1975), A-53, Abstract 731-10-35.

1976 Gandhi, J.M., *On the first case of Fermat's last theorem*, preprint.

1977 Johnson, W., *On the congruences related to the first case of Fermat's last theorem*, Math. Comp., **31** (1977), 519–526.

VI.2. Условия делимости

Пусть p — нечетное простое число и отличные от нуля взаимно простые целые числа x, y, z таковы, что $x^p + y^p + z^p = 0$. В этом разделе мы выведем некоторые условия делимости для чисел x, y, z и выражений, содержащих эти числа.

Следующее предложение было сформулировано Перес-Качо в 1958 г., однако утверждение (2) было ранее доказано Массутье в 1931 г. Более простое доказательство дано Поме в том же 1931 г.

(2A) *Пусть p — нечетное простое число и ненулевые попарно взаимно простые целые числа x, y, z таковы, что $x^p + y^p + z^p = 0$. Тогда*

(1) *если xyz не кратно 3, то $x \equiv y \equiv z \not\equiv 0 \pmod 3$, целые числа $x^2 - yz$, $y^2 - xz$, $z^2 - xy$ кратны 3, но не делятся на 9, и для всякого простого числа $q \neq 3$, делящего ровно одно из чисел $x^2 - yz$, $y^2 - xz$, $z^2 - xy$, справедливо сравнение $q \equiv 1 \pmod 6$;*

(2) *если $p \equiv -1 \pmod 6$, то xyz кратно 3.*

Доказательство. (1) Поскольку $3 \nmid xyz$, числа x, y, z сравнимы с 1 или с -1 по модулю 3. Из сравнения $(\pm 1)^p + (\pm 1)^p + (\pm 1)^p \equiv 0 \pmod 3$ следует, что непременно $x \equiv y \equiv z \not\equiv 0 \pmod 3$. Поэтому $x^2 \equiv yz \pmod 3$, так что $x^2 - yz$ кратно 3, и аналогично числа $y^2 - xz$ и $z^2 - xy$ кратны 3.

Заметим, что ровно одно из чисел x, y, z четно. Поэтому $x^2 \neq yz$, $y^2 \neq xz$, $z^2 \neq xy$.

Покажем, что $9 \nmid (z^2 - xy)$. Из соотношений $x^{2p}+x^py^p+x^pz^p = 0$ и $xy = (xy - z^2) + z^2$ следует, что $-(x^{2p} + x^pz^p) = x^py^p = \left[(xy - z^2) + z^2\right]^p \equiv p(xy - z^2)z^{2(p-1)} + z^{2p} \pmod{(z^2 - xy)^2}$. Заметив, что числа x, y, z различны (так как 2 не есть p-я степень), получим

$$Q_3(x^p, z^p) = x^{2p} + x^pz^p + z^{2p} \equiv p(z^2 - xy)z^{2(p-1)} \pmod{(z^2 - xy)^2}.$$

Так как $3 \mid (x^p - z^p)$, в силу утверждения (3B)(6) гл. II мы имеем $v_3(Q_3(x^p, z^p)) = v_3(3) = 1$. Таким образом, $9 \nmid (z^2 - xy)$.

Из последнего сравнения следует также, что $x^{2p} + x^pz^p + z^{2p}$ кратно $z^2 - xy$. Пусть теперь простое число q, $q \neq 3$, делит $x^{2p} + x^pz^p + z^{2p}$. Тогда $q \nmid x$ или $q \nmid z$, поскольку НОД$(x, z) = 1$. Без ограничения общности можно считать, что $q \nmid z$. Пусть число z' таково, что $zz' \equiv 1 \pmod{q}$. Умножив на z'^{2p}, получим $(x^pz'^p)^2 + (x^pz'^p) + 1 \equiv 0 \pmod{q}$. По лемме 1.2 мы имеем $q \equiv 1 \pmod{6}$.

В частности, каждый простой делитель $q \neq 3$ числа $z^2 - xy$ удовлетворяет сравнению $q \equiv 1 \pmod{6}$. Доказательство для простых делителей чисел $x^2 - yz$ и $y^2 - xz$ совершенно аналогично.

(2) Пусть $3 \nmid xyz$ и $p \nmid z$ (случаи $p \nmid x$ и $p \nmid y$ рассматриваются аналогично).

Поскольку числа $x^{2p} + x^pz^p + z^{2p}$ и $z^2 - xy$ положительны и кратны 3, но не делятся на 9, из первой части доказательства следует, что

$$\frac{x^{2p} + x^pz^p + z^{2p}}{z^2 - xy} \equiv 1 \pmod{3}.$$

С другой стороны, сравнение из первой части доказательства позволяет заключить, что

$$\frac{x^{2p} + x^pz^p + z^{2p}}{z^2 - xy} \equiv pz^{2(p-1)} \pmod{z^2 - xy}.$$

Следовательно, так как $3 \mid (z^2 - xy)$, справедливо сравнение $p \equiv 1 \pmod{3}$. □

Поме в 1931 г. заявил, что для каждого показателя p он доказал, что если x, y, z отличны от нуля и $x^p + y^p + z^p = 0$, то xyz кратно 3. В 1934 г. он добавил, что к тому же xyz кратно 5. Однако эти доказательства содержали ошибку (см. Брауэр, 1934).

В 1946 г. Инкери доказал следующее утверждение.

(2В) *Пусть p — нечетное простое число, $p \not\equiv 1, 9 \pmod{20}$, целые числа x, y, z отличны от нуля и $x^p + y^p + z^p = 0$. Тогда 5 делит xyz.*

Доказательство. Из утверждения (6В) гл. I следует, что $p \neq 5$. Можно полагать, что числа x, y, z взаимно просты.

Если $5 \nmid xyz$, то x^p, y^p, z^p сравнимы с ± 1, ± 2 по модулю 5. При необходимости изменив обозначения и знаки, будем считать, что $x^p \equiv y^p \equiv 2 \pmod 5$.

Пусть целое число h таково, что $ph \equiv 1 \pmod 4$. Если $p \equiv 3 \pmod 4$, положим $h = 3$. Возводя сравнение $x^p \equiv y^p \pmod 5$ в степень h, получим, что $x \equiv y \pmod 5$. Так как $z^p = -x^p - y^p \equiv \equiv -2y^p \pmod 5$, мы вновь можем записать $z^{2p} \equiv 4y^{2p} \equiv -x^p y^p \equiv \equiv (-xy) \pmod 5$, а следовательно, возводя в степень h, получим $z^2 \equiv -xy \pmod 5$. В частности, так как $x \equiv y \equiv \pm 1$ или $\pm 2 \pmod 5$, $z^2 \equiv \pm 1 \pmod 5$.

Рассмотрим теперь число $z^{2p} + x^p y^p$. Оно нечетно, так как ровно одно из чисел x, y, z четно.

Покажем, что если простое число $q \neq 5$ делит $z^{2p} + x^p y^p$, то $q \equiv \equiv \pm 1 \pmod 5$. В самом деле, верны соотношения $(2x^p + 3y^p)^2 - -5y^{2p} = 4(x^{2p} + 3x^p y^p + y^{2p}) = 4(z^{2p} + x^p y^p)$. Поэтому для простого числа $q \neq 5$ мы имеем $(2x^p + 3y^p)^2 \equiv 5y^{2p} \pmod q$, а значит, 5 является квадратичным вычетом по модулю q. По квадратичному закону взаимности

$$1 = \left(\frac{5}{q}\right) = \left(\frac{q}{5}\right), \quad \text{следовательно,} \quad q \equiv \pm 1 \pmod 5.$$

Из сказанного следует, что любой делитель k числа $z^{2p} + x^p y^p$, не кратный 5, должен быть сравним с $\pm 1 \pmod 5$. Возьмем

$$k = \frac{z^{2p} + x^p y^p}{z^p + xy} = z^{2(p-1)} - z^{2(p-2)}xy + z^{2(p-3)}(xy)^2 - \ldots + (xy)^{p-1}.$$

Так как $z^2 \equiv -xy \pmod 5$, мы получаем $k \equiv pz^{2(p-1)} \equiv p \pmod 5$, потому что $z^2 \equiv \pm 1 \pmod 5$. Таким образом, $k \not\equiv 0 \pmod 5$ и, следовательно, $k \equiv \pm 1 \pmod 5$.

Итак, $p \equiv \pm 1 \pmod 5$.

Осталось показать, что $p \equiv 1 \pmod 4$. Если предположить, что $p \equiv 3 \pmod 4$, то $3p \equiv 1 \pmod 4$, а значит, $z \equiv z^{3p} \equiv (-2)^3 y^{3p} \equiv 2y \pmod 5$. Рассматривая соотношение

$$(2z^p + 3y^p)^2 - 5y^{2p} = 4(z^{2p} + 3y^p z^p + y^{2p}) = 4(x^{2p} + y^p z^p),$$

как и раньше, можем показать, что каждый простой делитель $q \neq 5$ числа $x^{2p}+y^pz^p$ должен быть сравним с $\pm 1 \pmod 5$. Следовательно, каждый делитель k числа $x^{2p}+y^pz^p$, $k \not\equiv 0 \pmod 5$, также должен быть сравним с $\pm 1 \pmod 5$.

В частности, положив $k = x^2 + yz$, если $p \equiv 3 \pmod 4$, мы получим $y \equiv -2z \pmod 5$, а значит, $x^2 \equiv y^2 \equiv -2yz \pmod 5$, так что $k = x^2+yz \equiv -yz \not\equiv 0 \pmod 5$. Следовательно, $k \equiv \pm 1 \pmod 5$. Однако, с другой стороны, $k \equiv x^2 + yz \equiv y^2 + 2y^2 = 3y^2 \equiv \pm 2 \pmod 5$, чего быть не может. Тем самым доказано, что $p \equiv 1 \pmod 4$.

Таким образом, мы получили, что $p \equiv 1$ или $9 \pmod{20}$. Это противоречит предположению, а значит, $5 \mid xyz$. □

Перес-Качо в 1958 г. доказал такое предложение.

(2C) *Пусть p — нечетное простое число и ненулевые взаимно простые целые числа x, y, z таковы, что $x^p + y^p + z^p = 0$. Тогда*

(1) *если $q \neq 5$ — простой делитель числа $(x^2 - yz)(y^2 - zx)\times$ $\times(z^2 - xy)$, то $q \equiv \pm 1 \pmod{10}$;*
(2) *ни одно из чисел $x^2 - yz$, $y^2 - zx$, $z^2 - xy$ не кратно 25.*

В 1946 г. Инкери получил также следующий результат.

(2D) *Пусть p — нечетное простое число и ненулевые взаимно простые целые числа x, y, z таковы, что $x^{p^n} + y^{p^n} + z^{p^n} = 0$ (где $n \geqslant 1$). Тогда*

(1) *$xyz(x-y)(x-z)(y-z)$ кратно 5;*
(2) *$xyz(x-y)(x-z)(y-z)(x^2-yz)(y^2-xz)(z^2-xy)$ кратно 7 (при $p > 3$);*
(3) *$xyz(x-y)(x-z)(y-z)(x^2+yz)(y^2+xz)(z^2+xy)$ кратно 11 (при $p > 5$).*

Доказательство. Прежде всего заметим, что если l — простое число, $p \not| (l-1)$ и ненулевые числа a, b взаимно просты, то $l \mid (a+b)$ тогда и только тогда, когда $l \mid (a^p + b^p)$. Действительно, если a или b кратно l, то это очевидно.

Пусть $l \not| ab$. Ясно, что если $l \mid (a+b)$, то $l \mid (a^p + b^p)$. Обратно, если $l \mid (a^p + b^p)$, но $l \not| (a+b)$, то l является примитивным делителем бинома $a^p + b^p$, а тогда согласно утверждению (3G) гл. II мы получаем $l \equiv 1 \pmod p$, чего быть не может.

Пусть $u = x^{p^n}$, $v = y^{p^n}$, $w = z^{p^n}$. Тогда $u + v + w = 0$ и нам надо показать (ввиду сделанного выше замечания и так как $p > 2$, $p > 3$ и $p > 5$ соответственно), что

(1) $uvw(u-v)(u-w)(v-w)$ кратно 5;
(2) $uvw(u-v)(u-w)(v-w)(u^2-vw)(v^2-uw)(w^2-uv)$ кратно 7;
(3) $uvw(u-v)(u-w)(v-w)(u^2+vw)(v^2+uw)(w^2+uv)$ кратно 11.

Пусть $l = 5, 7$ или 11.

Так как $(u, v, w) = 1$, можно полагать, что, например, $l \nmid v$. Пусть **число** v' таково, что $v'v \equiv 1 \pmod{l}$. Следовательно, умножив на v', получим, что $t + t' \equiv 1 \pmod{l}$, где $t \equiv -v'u \pmod{l}$, $t' \equiv -v'w \pmod{l}$. Пусть

$$\begin{aligned}
T_1 &= t,\\
T_2 &= t-1,\\
T_3 &= t+1,\\
T_4 &= 2t-1,\\
T_5 &= t-2,\\
T_6 &= t^2-t+1,\\
T_7 &= t^2+t-1,\\
T_8 &= t^2-t-1,\\
T_9 &= t^2-3t+1.
\end{aligned}$$

Тогда

$$\begin{aligned}
vT_1 &\equiv -u \pmod{l},\\
vT_2 &\equiv -u-v \equiv w \pmod{l},\\
vT_3 &\equiv -u+v \pmod{l},\\
vT_4 &\equiv -2u-v \equiv -u+w \pmod{l},\\
vT_5 &\equiv -u-2v \equiv w-v \pmod{l},\\
v^2T_6 &\equiv u^2+vu+v^2 \equiv u^2-vw\\
&\equiv v^2-uw \equiv w^2-vu \pmod{l},\\
v^2T_7 &\equiv u^2-vu-v^2 \equiv u^2+vw \pmod{l},\\
v^2T_8 &\equiv u^2+vu-v^2 \equiv -v^2-uw \pmod{l},\\
v^2T_9 &\equiv u^2+3vu+v^2 \equiv w^2+uv \pmod{l}.
\end{aligned}$$

(1) Пусть $l = 5$. Тогда легко проверить следующие импликации:

$$\begin{aligned}
t \equiv 0 \pmod 5 &\quad\Rightarrow\quad 5 \mid T_1,\\
t \equiv 1 \pmod 5 &\quad\Rightarrow\quad 5 \mid T_2,\\
t \equiv 2 \pmod 5 &\quad\Rightarrow\quad 5 \mid T_5,\\
t \equiv -1 \pmod 5 &\quad\Rightarrow\quad 5 \mid T_3,\\
t \equiv -2 \pmod 5 &\quad\Rightarrow\quad 5 \mid T_4.
\end{aligned}$$

Таким образом, $uvw(u-v)(u-w)(v-w)$ кратно 5.

(2) Пусть $l = 7$. Тогда легко проверить, что если $t \equiv -3, -2, -1, 0, 1, 2, 3 \pmod 7$, то 7 делит $T_4, T_6, T_3, T_1, T_2, T_5, T_6$ соответственно. Таким образом, $uvw(u-v)(u-w)(v-w)(u^2-vw)(v^2-uw)(w^2-vu)$ кратно 7.

(3) Пусть $l = 11$. Тогда если $t \equiv -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5 \pmod{11}$, то 11 делит $T_4, T_7, T_8, T_9, T_3, T_1, T_2, T_5, T_7, T_8, T_9$ соответственно. Значит, число $uvw(u-v)(u-w)(v-w)(u^2+vw)\times$ $\times(v^2+uw)(w^2+uv)$ кратно 11. □

Заметим, что это рассуждение нельзя обобщить на случай $l > 11$. Действительно, если $t \equiv -2 \pmod l$ для $l > 11$, то значения T_i $(1 \leqslant i \leqslant 9)$ по модулю l отличны от 0 и по абсолютному значению не превосходят 11.

Приведем результат Пьера (1943), касающийся делимости на 4, предварительно доказав лемму о символе Якоби.

Лемма 2.1. *Пусть попарно взаимно простые нечетные целые числа a, b, c таковы, что*

$$\left(\frac{a}{bc}\right) = \left(\frac{b}{ac}\right) = \left(\frac{c}{ab}\right) = +1.$$

Тогда не более одного из чисел a, b, c сравнимо с 3 по модулю 4.

Доказательство. Предположим, что $a \equiv b \equiv 3 \pmod 4$. Тогда по квадратичному закону взаимности

$$1 = \left(\frac{c}{ab}\right) = \left(\frac{ab}{c}\right)(-1)^{(c-1)/2\times(ab-1)/2} = \left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right),$$

$$1 = \left(\frac{b}{ac}\right) = \left(\frac{b}{a}\right)\left(\frac{b}{c}\right),$$

$$1 = \left(\frac{a}{bc}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{c}\right).$$

Следовательно, $(a/b) = (a/c) = (b/c) = (b/a)$. Однако

$$\left(\frac{b}{a}\right) = \left(\frac{a}{b}\right)(-1)^{(b-1)/2\times(a-1)/2} = -\left(\frac{a}{b}\right).$$

Полученное противоречие завершает доказательство. □

(2E) *Пусть p — нечетное простое число и ненулевые взаимно простые целые числа x, y, z таковы, что $x^p + y^p + z^p = 0$. Тогда ровно одно из чисел x, y, z кратно 4.*

Доказательство. Будем считать, что число z четно, а x, y нечетны. Предположим, что $z \equiv 2 \pmod 4$, и придем к противоречию.

Случай 1: $p \nmid xyz$.

Согласно соотношениям (1.2) мы получаем

$$\begin{aligned} s_1^p &= \frac{z^p + x^p}{z + x} \\ &= z^{p-1} - z^{p-2}x + \ldots + z^2x^{p-3} - zx^{p-2} + x^{p-1} \\ &\equiv -2x^{p-2} + x^{p-1} \pmod 4. \end{aligned}$$

Так как число x нечетно, $x^{p-1} \equiv 1 \pmod 4$. Следовательно, $s_1^p \equiv -2x^{p-2} + 1 \equiv -2(4k \pm 1)^{p-2} + 1 \equiv \mp 2 + 1 \equiv 3 \pmod 4$, а значит, $s_1 \equiv 3 \pmod 4$. Аналогично $r_1^p = (z^p + y^p)/(z + y) \equiv 3 \pmod 4$, поэтому $r_1 \equiv 3 \pmod 4$.

Как следует из утверждения (3A) гл. II, $(r_1/s_1t_1) = (s_1/r_1t_1) = (t_1/s_1r_1) = 1$, так что в силу леммы 2.1 не более чем одно из чисел r_1, s_1, t_1 сравнимо с 3 по модулю 4. Противоречие получено.

Случай 2: $p \mid xyz$.

Сначала рассмотрим случай $p \mid z$. Как и в предыдущем случае, $s_1 \equiv 3 \pmod 4$, $r_1 \equiv 3 \pmod 4$.

По утверждению (2A) гл. III нечетные числа r_1, s_1, pt_1 удовлетворяют соотношениям $(r_1/pt_1s_1) = (s_1/pt_1r_1) = (pt_1/r_1s_1) = 1$, что противоречит лемме 2.2.

Предположим теперь, что $p \nmid z$ и, например, $p \mid x$. Продолжая аналогичные рассуждения, из соотношений (1.2) получим, что $pr_1^p \equiv 3 \pmod 4$, а так как r_1 нечетно, $r_1^{p-1} \equiv 1 \pmod 4$, так что $pr_1 \equiv 3 \pmod 4$. Более того, $s_1 \equiv 3 \pmod 4$, и согласно утверждению (2A) гл. III нечетные целые числа pr_1, s_1, t_1 удовлетворяют соотношениям $(pr_1/s_1t_1) = (s_1/pr_1t_1) = (t_1/pr_1s_1) = +1$, что противоречит лемме 2.1. □

В 1910 г. Линд заявил, что 9 делит $x + y + z$, но предъявленное доказательство было неполным, и поэтому ряд уравнений и неравенств в его работе вызывают сомнение (см. Диксон (1920, с. 769)).

После рассмотрения свойств делимости на небольшие числа обратимся к результатам, которые связаны с выражениями, содержащими гипотетические решения уравнения Ферма x, y, z.

В 1913 г. Невядомский доказал такой факт.

(2F) *Пусть p — нечетное простое число и ненулевые взаимно простые числа x, y, z таковы, что $x^p + y^p + z^p = 0$. Тогда $x^{2p+1} + y^{2p+1} + z^{2p+1}$ делится на $(x + y)(y + z)(z + x)$.*

Доказательство. Как легко проверить,

$$x^{2p+1}+y^{2p+1}+z^{2p+1}=\left(\frac{x+y}{x^p+y^p}+\frac{y+z}{y^p+z^p}+\frac{z+x}{z^p+x^p}\right)x^py^pz^p.$$

Следовательно,

$$\frac{x^{2p+1}+y^{2p+1}+z^{2p+1}}{(x+y)(y+z)(z+x)}=-\frac{(y^p+z^p)(z^p+x^p)}{(y+z)(z+x)}-\frac{(x^p+y^p)(z^p+x^p)}{(x+y)(z+x)}-\frac{(x^p+y^p)(y^p+z^p)}{(x+y)(y+z)},$$

и это число является целым. □

Следующий результат Рамесвара Рао (1969) также достаточно прост.

(2G) *Пусть p — нечетное простое число и ненулевые попарно взаимно простые числа x, y, z таковы, что $x^p+y^p+z^p=0$. Тогда $x+y$ делит d^p, где $d=\text{НОД}(x+y,z)$ (в силу симметрии аналогичные утверждения имеют место для $x+z, y+z$).*

Доказательство. Поскольку $x+y+z\equiv 0 \pmod p$, существует такое число $k\neq 0$, что $x+y+z=kp$. Так как p нечетно, $x+y=kp-z$ делит числа $x^p+y^p=-z^p$ и $(kp)^p-z^p$, а значит, $kp-z$ делит $(kp)^p$. Поскольку $d=\text{НОД}(kp,z)$, положим $kp=ud$, $z=vd$, где числа u и v взаимно просты. Но $u-v$ делит оба числа u^pd^{p-1}, v^pd^{p-1}. Следовательно, $(u-v)d=x+y$ делит d^p. □

Следующий результат, появившийся в работе Симмонса (1966), был приписан Г. Рейсу; утверждение (1) заново доказал Роллеро (1981).

(2H) *Пусть p — нечетное простое число и попарно взаимно простые положительные числа x, y, z таковы, что $x^p+y^p=z^p$. Тогда существуют определенные единственным образом натуральные числа k, a, b, такие, что $x=k+a$, $y=k+b$, $z=k+a+b$.*

Более того, при этом

(1) *pab делит k^p;*
(2) $\text{НОД}(a,b)=1$;
(3) *если $a\neq 1$, то* $\text{НОД}(k,a)\neq 1$; *если $p\nmid a$, то* $\text{НОД}(k,a)\neq a$;
(4) *если $b\neq 1$, то* $\text{НОД}(k,b)\neq 1$; *если $p\nmid b$, то* $\text{НОД}(k,b)\neq b$.

Доказательство. Можно полагать, что $0<x<y<z$. Так как $z<x+y$, определим k из равенства $x+y=z+k$. Из неравенства

$y < z$ следует, что $k < x < y$. Пусть числа a и b находятся из соотношений $x = k + a$, $y = k + b$. Тогда $z = k + a + b$.

Ясно, что числа k, a, b определены единственным образом: если $x = k' + a'$, $y = k' + b'$ и $z = k' + a' + b'$, то $0 = (k - k') + (a - a') = (k - k') + (b - b') = (k - k') + (a - a') + (b - b')$, а значит, $k = k'$, $a = a'$, $b = b'$. Перепишем соотношение $x^p + y^p = z^p$ в виде

$$(k + a)^p + (k + b)^p = (k + a + b)^p. \tag{2.1}$$

Легко видеть, что НОД$(k + a, k + b, k + a + b) = 1$, потому что НОД$(x, y, z) = 1$. Таким образом, числа $k + a$, $k + b$ и $k + a + b$ попарно взаимно просты.

Из соотношения $(k + a + b)^p = (k + a)^p + p(k + a)^{p-1}b + \ldots + b^p$ следует, что $(k + b)^p = p(k + a)^{p-1}b + \ldots + b^p$. Таким образом, $k^p + pk^{p-1}b + \binom{p}{2}k^{p-2}b^2 + \ldots + b^p = p(k + a)^{p-1}b + \ldots + b^p$, так что

$$k^p = pb[(k + a)^{p-1} - k^{p-1}] + \binom{p}{2}[(k + a)^{p-2} - k^{p-2}]b^2 + \ldots + \binom{p}{p-1}ab^{p-1}. \tag{2.2}$$

Каждое выражение в квадратных скобках кратно a, а значит, и k^p кратно pab. Если $a \neq 1$, то НОД$(k, a) \neq 1$, а если $b \neq 1$, то НОД$(k, b) \neq 1$. Итак, НОД$(a, b) = 1$, так как если простое число q делит a и b, то оно также делит и k, а значит, и $k + a$, и $k + b$.

Если $p \nmid a$, то НОД$(k, a) \neq a$, так как в противном случае $k = al$, где l — целое число, и, разделив (2.2) на a, мы получим, что

$$a^{p-1}l^p = pba^{p-2}[(l + 1)^{p-1} - l^{p-1}] + \binom{p}{2}a^{p-3}\left[(l + 1)^{p-2} - l^{p-2}\right]b^2 + \ldots + pb^{p-1}.$$

Таким образом, a делит последнее слагаемое pb^{p-1}. Но $p \nmid a$, и, следовательно, a делит b^{p-1}, чего быть не может. Аналогично, если $p \nmid b$, то НОД$(k, b) \neq b$. □

Пусть p — нечетное простое число и ненулевые попарно взаимно простые целые числа x, y, z таковы, что $x^p + y^p + z^p = 0$.

Флек (1909, 1910) начал более систематическое изучение свойств делимости следующих чисел, построенных на основе гипотетическо-

го решения (x, y, z):

$$A = y^2 + yz + z^2,$$
$$B = z^2 + zx + x^2,$$
$$C = x^2 + xy + y^2,$$

$$A_1 = x^2 - yz, \quad A_2 = x^2 + yz,$$
$$B_1 = y^2 - zx, \quad B_2 = y^2 + zx,$$
$$C_1 = z^2 - xy, \quad C_2 = z^2 + xy,$$
$$S = x + y + z, \quad T = -(xy + yz + zx),$$
$$U = xyz, \quad 2V = x^2 + y^2 + z^2.$$

Пусть числа r, s и t определены из соотношений Барлоу (см. разд. III.1).

(2I) *Во введенных обозначениях и при сделанных допущениях существуют такие ненулевые числа* $G, M, J, K, L, J_1, K_1, L_1$, *что*

(1)
$$S = \begin{cases} -rstp^3GM & (\textit{в первом случае}), \\ -rstp^2GM & (\textit{во втором случае}); \end{cases}$$

(2) $A = GJ, B = GK, C = GL, A_1 = GJ_1, B_1 = GK_1, C_1 = GL_1$;
(3) *G есть наибольший общий делитель числа S и этих шести чисел*;
(4) *числа J, K, L, J_1, K_1, L_1 попарно взаимно просты*;
(5) *простые делители чисел J, K, L имеют вид $6hp + 1$*;
(6) *простые делители чисел J_1, K_1, L_1 имеют вид $6hp^2 + 1$*;
(7) $x^{3p} \equiv y^{3p} \equiv z^{3p} \pmod{GJKLJ_1K_1L_1}$.

В 1979 г. Инкери внес ряд поправок в доказательства Флека и получил дальнейшие результаты в этом направлении.

В заключение этого раздела приведем результат Поллачека, полученный в 1917 г., элементарное доказательство которого неизвестно. Оригинальное доказательство опиралось на сравнения, полученные Куммером в 1857 г., которые справедливы в предположении, что первый случай теоремы Ферма не выполнен для показателя p. При доказательстве этих сравнений Куммер подробно рассмотрел арифметические свойства кругового поля $\mathbb{Q}(\zeta_p)$, где ζ_p — примитивный корень из 1 степени p. Таким образом, это выходит за рамки нашей книги.

Вот результат Поллачека.

(2J) *Пусть p — нечетное простое число, и пусть существуют такие попарно взаимно простые ненулевые целые числа x, y, z, что $x^p + y^p + z^p = 0$. Тогда числа $A = y^2 + yz + z^2$, $B = z^2 + zx + x^2$ и $C = x^2 + xy + y^2$ не делятся на p.*

Список литературы

1857 Kummer, E.E., *Einige Sätze über die aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten complexen Zahlen, für den Fall daß die Klassenzahl durch λ theilbar ist, nebst Anwendungen derselben auf einen weiteren Beweis des letztes Fermat'schen Lehrsatzes*, Math. Abh. Königl. Akad. Wiss. zu Berlin, 1857, pp. 41–74.

1909 Fleck, A., *Miszellen zum großen Fermatschen Problem*, Sitzungsber. Berliner Math. Ges., **8** (1909), 133–148.

1910 Fleck, A., *Bemerkung zum großen Fermatschen Problem*, Sitzungsber. Berliner Math. Ges., **9** (1910), 50–53.

1910 Lind, B., *Über das letzte Fermatsche Theorem*, Abh. Geschichte Math. Wiss., no. 26, 1910, pp. 23–65.

1913 Niewiadomski, R., *Question 4194*, L'Interm. Math., **20** (1913), 76.

1917 Pollaczek, F., *Über den großen Fermat'schen Satz*, Sitzungsber. Akad. Wiss., Wien, Abt. IIa, **126** (1917), 45–59.

1920 Dickson, L.E., *History of the Theory of Numbers*, Vol. II, Carnegie Institution, Washington, DC, 1920; reprinted by Chelsea, New York, 1971.

1931 Massoutié, L., *Sur le dernier théorème de Fermat*, C. R. Acad. Sci. Paris, **193** (1931), 502–504.

1931 Pomey, L., *Nouvelles remarques relatives au dernier théorème de Fermat*, C. R. Acad. Sci. Paris, **193** (1931), 563–564.

1934 Pomey, L., *Sur le dernier théorème de Fermat (divisibilité par* 3 *et par* 5), C. R. Acad. Sci. Paris, **199** (1934), 1562–1564.

1934 Brauer, A., *Review of the above paper by L. Pomey*, Jahrbuch Fortschritte Math., **60**, II (1934), 928.

1943 Pierre C., *Sur le théorème de Fermat $a^n + b^n = c^n$*, C. R. Acad. Sci. Paris, **217** (1943), 37–39.

1946 Inkeri, K., *Untersuchungen über die Fermatsche Vermutung*, Ann. Acad. Sci. Fenn., Ser. AI, **33** (1946), 60 pp.

1958 Pérez-Cacho, L., *Sobre alcunas cuestiones de la teoría de números*, Rev. Mat. Hisp.-Amer., (4), **18** (1958), 10–27 and 113–124.

1966 Simmons, G.J., *Some results pertaining to Fermat's conjecture*, Math. Mag., **39** (1966), 18–21.
1969 Rameswar Rao, D., *Some theorems on Fermat's last theorem*, Math. Student, **37** (1969), 208–210.
1981 Rollero, A., *Un'osservazione sull'ultimo teorema di Fermat*, Atti Accad. Ligure Sci. Lett., **38** (1981), 3–9.
1979 Inkeri, K., *On some expressions associated with Fermat's last theorem*, J. Reine Angew. Math., **311/312** (1979), 178–190.

VI.3. Гипотеза Абеля

В 1823 г. Абель высказал предположение, что если отличные от нуля взаимно простые целые числа x, y, z таковы, что $0 < x < y < z$ и $x^n + y^n = z^n$ $(n > 2)$, то ни одно из чисел x, y, z не является степенью простого числа. Прямое доказательство этого утверждения до сих пор не найдено, однако известно, что оно выполнено, если число n либо не является простым, либо, будучи простым, не делит xyz. Доказательство последнего утверждения мы не приводим, так как оно требует привлечения аналитических методов.

Множество частичных результатов, полученных различными авторами, объединены в табл. 7.

В 1887 г. Мансьон заявил, что им получен следующий результат: если показатель является нечетным простым числом, то x – составное число. Доказательство содержало ошибку. В 1891 г. Люка опубликовал доказательство того факта, что для произвольного n число x не может быть степенью простого числа; но доказательство было неполным, как указал в 1895 г. Марков. В 1955 г. Мёллер сформулировал теорему, включавшую все приведенные результаты. Однако доказательство на с. 27 его статьи нельзя считать удовлетворительным. Мы приведем более простое и корректное доказательство.

(3A) *Пусть нечетное число $n \geqslant 3$ имеет в точности r различных простых делителей. Тогда если целые числа x, y, $1 \leqslant x < y$, взаимно просты и $a = y^n + x^n$, $b = y^n - x^n$, то*

(1) *числа a, b имеют не менее r различных простых делителей;*
(2) *если a имеет ровно r различных простых делителей, то $a = 2^3 + 1^3$ (так что $n = 3$, $r = 1$);*
(3) *если b имеет ровно r различных простых делителей, то $y = x + 1$, $b = (x+1)^n - x^n$.*

Таблица 7.

Год	Автор	Показатель $n > 2$	Результат
1857	Тэлбот	произвольный	(I) y, z — составные числа (II) если x — простое число, то $z - y = 1$
1884	Жонкюре	произвольный	(I) и (II)
1887	Борлетти	нечетный простой	z — составное число
		четный	x, y, z — составные числа
1901	Гамбиоли	произвольный, не степень 2	(II), z не есть степень простого числа
1905	Зауэр	произвольный	y, z — не степени простого числа
1932	Нетаньяху–Милей-ковский	произвольный	y, z — не степени простого числа
		не простой	(III) x не степень простого числа
1949	Извеков	произвольный	(I)
1952	Бини	нечетный	z не является степенью простого числа и $z \neq nq$, где q — простое число, не равное n
		нечетный простой	z не кратно n и не равно $q_1 q_2 \dots q_r$, где числа q_i, $q_1 < q_2 < \dots < q_r$, простые и $q_1^n > 2q_1 q_2 \dots q_r$.

Доказательство. (1) Пусть $p_1, \dots, p_r$ — различные простые делители числа n. Так как $y \pm x \neq 0$, согласно утверждению (3В)(3) гл. II число $y^n \pm x^n = (y \pm x) \cdot Q_n(y, \mp x)$ кратно $(y \pm x) \times$ $\times \prod_{i=1}^{r} Q_{p_i}(y, \mp x)$. Как следует из части (2) того же утверждения, целые числа $Q_{p_i}(y, \mp x)$ (при $i = 1, \dots, r$) попарно взаимно просты.

Заметим, что $x^{p_i} + y^{p_i} > x + y$ и $(x^{p_i} - y^{p_i})/(x - y) = x^{p_i - 1} +$ $+ x^{p_i - 2} y + \dots + y^{p_i - 1} > 1$. Поэтому каждое число $Q_{p_i}(y, \mp x)$ имеет по крайней мере один простой делитель. Следовательно, числа a и b имеют не менее r различных простых делителей.

(2) Пусть m есть произведение r различных простых делителей числа n, так что $m \mid n$. Покажем сначала, что $n = m$. Воспользуемся равенством $a = (y^m + x^m)(y^n + x^n)/(y^m + x^m)$. Согласно части (1) и по предположению число $y^m + x^m$ имеет ровно r различных простых делителей, в точности совпадающих с простыми делителями числа a. Если $n > m$, то a не имеет примитивных делителей. Как следует из утверждения (3J) гл. II, $a = 2^3 + 1^3$, а значит, $n = 3 = m$, что противоречит предположению. Таким образом, $n = m$, т. е. n есть произведение r различных простых чисел.

Пусть $r = 1, n = p$. Тогда $a = (y + x)Q_p(y, -x)$. По предположению a есть степень некоторого простого числа q. Так как q делит $y + x$ и $Q_p(y, -x) > 1$, согласно утверждению (3B)(4) гл. II мы заключаем, что $q = p$, а в соответствии с частью (6) того же утверждения $Q_p(y, -x) = p$. Из утверждения (3D) гл. II следует, что $p = 3, y = 2, x = 1$.

Пусть $r > 1, n = ph$, p — простое число, $p \nmid h$. Тогда h есть произведение $r - 1$ различных простых чисел. Так как $a = (y^h + x^h)Q_p(y^h, -x^h)$, в силу утверждения (1) и по предположению число $y^h + x^h$ имеет $r - 1$ или r различных простых делителей. Проведем индукцию по r. Если $y^h + x^h$ имеет ровно $r - 1$ различных простых делителей, то $h = 3, y = 2, x = 1$. Тогда $n = 3p$ (где $p > 3$), $r = 2$ и $2^{3p} + 1 = (2^p + 1)Q_3(2^p, -1)$.

Если существует такое простое число $q \neq 3$, что $q \mid (2^p + 1)$, то, как следует из утверждения (3B)(6) гл. II, $v_q(Q_3(2^p, -1)) = v_q(3) = 0$, а значит, $q \nmid Q_3(2^p, -1)$. Так как $r = 2$ и $3 \mid (2^p + 1)$, число $Q_3(2^p, -1)$ есть степень числа 3. Тогда, применяя то же утверждение (3B)(6) гл. II, мы получаем $Q_3(2^p, -1) = 3$, значит, в соответствии с утверждением (3D) гл. II, $2^p = 2$, что невозможно.

Если $2^p + 1 = 3^s$, то $3^s \equiv 1 \pmod 8$, потому что $p > 3$. Таким образом, $s = 2s'$. Тогда $2^p = 3^s - 1 = (3^{s'} + 1)(3^{s'} - 1)$, а следовательно, $3^{s'} + 1 = 2^{p-c}$, $3^{s'} - 1 = 2^c$, где $p - c > c \geqslant 0$. Вычитая, получим $2 = 2^{p-c} - 2^c = 2^c(2^{p-2c} - 1)$, а значит, $c = 1$, $p - 2c = 1$, т. е. $p = 3$, что невозможно.

Если $y^h + x^h$ имеет ровно r различных простых делителей, то каждый простой делитель q числа $Q_p(y^h, -x^h)$ делит $y^h + x^h$. Из утверждения (3B)(4) гл. II следует, что $q = p$. Но $Q_p(y^h, -x^h) > 1$, а значит, $Q_p(y^h, -x^h)$ есть степень числа p, причем согласно части (6) того же утверждения $Q_p(y^h, -x^h) = p$, и по утверждению (3D) гл. II мы получаем $p = 3$, $y^h = 2$, $x^h = 1$, следовательно, $h = 1$ и $n = 3$, что и завершает доказательство.

(3) Если число $b = y^n - x^n$ имеет ровно r различных простых делителей, то по утверждениям (3B)(2), (3) гл. II мы заключаем, что $y^n - x^n$ кратно $(y-x)\prod_{i=1}^{r} Q_{p_i}(y,x)$, причем целые числа $Q_{p_i}(y,x) > 1$ попарно взаимно просты. Следовательно, по предположению они являются степенями простых чисел. Если $y - x > 1$ и простое число q делит $y - x$, то существует такое число i, что $q \mid Q_{p_i}(y,x)$. Согласно части (4) того же утверждения $q = p_i$, и согласно части (6) мы получаем, что $Q_{p_i}(y,x) = p_i$. Из утверждения (3D) гл. II следует, что $p_i = 3$, $y = 2$, $x = -1$. Полученное противоречие означает, что $y = x + 1$. □

Как следствие получаем такой результат.

(3B) *Пусть натуральное число $n \geqslant 3$ имеет в точности r различных нечетных простых делителей. Если взаимно простые натуральные числа x, y, z, $x < y < z$, таковы, что $x^n + y^n = z^n$, то z и y имеют не менее $r+1$ различных простых делителей, а x имеет не менее r различных простых делителей. Более того, если x имеет ровно r таких делителей, то n нечетно и $z - y = 1$.*

Доказательство. Согласно результатам гл. I число n не кратно 3 и не является степенью числа 2, следовательно, $r \geqslant 1$. Пусть $n = 2^u m$, где $u \geqslant 0$ и нечетное число m имеет ровно r различных простых делителей. Положим $x_1 = x^{2^u}$, $y_1 = y^{2^u}$ и $z_1 = z^{2^u}$. Так как $z^n = z_1^m = x_1^m + y_1^m$, $y^n = y_1^m = z_1^m - x_1^m$, $m \neq 3$ и $z_1 - x_1 > 1$, из утверждения (3A) следует, что числа z^n и y^n, а значит, z и y имеют не менее $r+1$ различных простых делителей.

Аналогично $x^n = x_1^m = z_1^m - y_1^m$, так что x^n, а следовательно, и x имеют не менее r различных простых делителей. Если x имеет ровно r таких делителей, то согласно утверждению (3A) мы получаем $z_1 = y_1 + 1$, т. е. $z^{2^u} = y^{2^u} + 1$. Отсюда $u = 0, z = y + 1$ и n нечетно. □

Докажем еще одно предложение.

(3C) *Пусть $n > 2$ и взаимно простые натуральные числа x, y, z, $x < y < z$, таковы, что $x^n + y^n = z^n$. Тогда*

(1) *числа y, z не являются степенями простых чисел;*
(2) *если x — степень простого числа, то $z = y + 1$, причем n — нечетное простое число.*

Доказательство. (1) Если z или y является степенью простого числа, то таково и $z^n = x^n + y^n$ или $y^n = z^n - x^n$ соответственно. То-

гда согласно утверждению (3B) число n есть степень числа 2 и $n \geqslant$ $\geqslant 4$, а это противоречит предположению о том, что теорема Ферма справедлива для таких показателей.

(2) Если x есть степень простого числа q, то, как следует из утверждения (3B), $z = y + 1$ и $n = p^e$, где $e \geqslant 1$, p — нечетное простое число. Покажем, что $e = 1$.

Если $e > 1$, то, так как $z^p - y^p > 1$ и $Q_{p^e-1}(z^p, y^p) = (z^{p^e} - y^{p^e})/$ $/(z^p - y^p) > 1$ и поскольку $x^{p^e} = z^{p^e} - y^{p^e} = (z^p - y^p) \times$ $\times Q_{p^e-1}(z^p, y^p)$, оба множителя в правой части суть степени числа q, большие чем 1, а следовательно, кратные q. По утверждению (3B)(4) гл. II число q делит $(z^p - y^p, Q_{p^e-1}(z^p, y^p)) = (p^{e-1}, z^p - y^p)$, а значит, $q = p$.

С другой стороны, $z = y + 1$, следовательно, $z^p - y^p = py^{p-1} +$ $+ \binom{p}{2} y^{p-2} + \ldots + \binom{p}{p-1} y + 1$, а значит, $p = q$ не делит $z^p - y^p$, что противоречит предположению. □

Мёллер получил следующее дополнение к (3A).

(3D) *Если нечетное число $m > 3$ имеет ровно r различных простых делителей, а натуральные числа x, y, $x < y$, взаимно просты, то число $b = y^{2m} - x^{2m}$ имеет не менее $2r + 1$ различных простых делителей.*

Доказательство. Из разложения $b = (y^m - x^m)(y^m + x^m)$ и условия НОД$(x, y) = 1$ следует, что $d =$ НОД$(y^m - x^m, y^m + x^m) = 1$ или 2. Согласно утверждению (3A) числа $y^m - x^m$ и $y^m + x^m$ имеют не менее r различных простых делителей. Так как $m > 3$, в силу утверждения (3A) число $y^m + x^m$ имеет не менее $r + 1$ различных простых делителей.

Если $y^m - x^m$ имеет ровно r различных простых делителей, то из утверждения (3A) следует, что $y = x + 1$, а значит, $y^m - x^m$ нечетно. Таким образом, $d = 1$ и b имеет не менее $2r + 1$ различных простых делителей. Если $y^m - x^m$ имеет не менее $r + 1$ различных простых делителей, то, поскольку $d = 1$ или 2, число b имеет не менее $2(r + 1) - 1 = 2r + 1$ различных простых делителей. □

В частности, если нечетное число $m > 3$ имеет ровно r различных простых делителей и натуральные числа x, y, z, $x < y < z$, взаимно просты, причем $x^{2m} + y^{2m} = z^{2m}$, то x, y имеют не менее $2r + 1$ различных простых делителей. Это было показано Мёллером в 1955 г. Отсюда с учетом утверждения (3B) получим, что для такого показателя $2m$ числа x, y, z не могут быть степенями простого.

Инкери в 1946 г. показал, что если $0 < x < y < z$, число p простое, $p \nmid xyz$ и $x^p + y^p = z^p$, то $z - y > 1$. Следовательно, согласно утверждению (3С) число x не является степенью простого числа. Итак, мы получили прямое доказательство гипотезы Абеля в случае, когда $p \nmid xyz$. При $p \mid xyz$ прямое доказательство того факта, что x не является степенью простого числа, а значит, и неравенства $z > y + 1$, остается неизвестным.

В 1886 г. Каталан изучил следствия из этого допущения.

(3Е) *Пусть p — нечетное простое число и натуральные числа x, y, $x < y$, таковы, что $x^p + y^p = (y+1)^p$. Тогда*

(1) *$py(y+1)$ делит $x^p - 1$;*

(2) *$p \nmid x$, $p \mid (x-1)$;*

(3) *если простое число q делит $y + 1 - x$, то q делит и $x - 1$;*

(4) НОД$(x+y, y+1-x) = 1$;

(5) НОД$(2x-1, 2y+1) = 1$;

(6) *x — единственное такое целое число, что*

$$(py^{p-1})^{1/p} < x < \left(p(y+1)^{p-1}\right)^{1/p}.$$

Доказательство. (1) Многочлен $(Y+1)^p - Y^p - 1$ делится на p, Y и $Y+1$. Следовательно, $x^p - 1 = (y+1)^p - y^p - 1 = py(y+1)h$, где $h \in \mathbb{Z}$.

(2) Так как $p \mid (x^p - 1)$, мы получаем, что $p \nmid x$. Из сравнения $x^p \equiv x \pmod p$ следует, что $p \mid (x-1)$.

(3) Из соотношений $y^p = (y+1)^p - x^p = (y+1-x)k$, где $k \in \mathbb{Z}$, следует, что если $q \mid (y+1-x)$, то $q \mid y$, так что $q \mid (x-1)$.

(4) Если простое число q делит $x+y$ и $y+1-x$, то $q \mid (x-1)$, а значит, $q \mid y$. Следовательно, $q \mid x$, но, поскольку $x^p + y^p = (y+1)^p$, мы получаем, что НОД$(x, y) = 1$, а это противоречит предположению.

(5) Если простое число q делит $2x-1$ и $2y+1$, то оно делит и их сумму $2(x+y)$, и их разность $2(y-x+1)$, но q нечетно, так что $q \mid (y-x+1)$, $q \mid (x+1)$. Итак, мы пришли к противоречию.

(6) Воспользовавшись соотношениями

$$\begin{aligned} x^p &= (y+1)^p - y^p = \frac{(y+1)^p - y^p}{(y+1) - y} \\ &= (y+1)^{p-1} + (y+1)^{p-2}y + \ldots + (y+1)y^{p-2} + y^{p-1}, \end{aligned}$$

получим

$$py^{p-1} < x^p < p(y+1)^{p-1},$$

откуда следуют доказываемые неравенства.

Наконец, заметим, что если целые числа x_1, x_2 таковы, что

$$(py^{p-1})^{1/p} < x_1 < x_2 < \left(p(y+1)^{p-1}\right)^{1/p},$$

то

$$y < x_1\left(\frac{x_1}{p}\right)^{1/(p-1)} \quad \text{и} \quad x_2\left(\frac{x_2}{p}\right)^{1/(p-1)} < y+1,$$

а значит,

$$(x_2-x_1)\left(\frac{x_1}{p}\right)^{1/(p-1)} < x_2\left(\frac{x_2}{p}\right)^{1/(p-1)} - x_1\left(\frac{x_1}{p}\right)^{1/(p-1)} < 1.$$

Но $1 \leqslant x_2 - x_1$ и $p = (p^p)^{1/p} < (py^{p-1})^{1/p} < x_1$, так как согласно п. (2) справедливы неравенства $p \leqslant x - 1 < x < y$. Следовательно, $1 < (x_1/p)^{1/(p-1)}$, а значит, $1 < (x_2 - x_1)(x_1/p)^{1/(p-1)}$. Полученное противоречие завершает доказательство. □

Воспользуемся теперь соотношениями Барлоу из разд. III.1 с очевидной сменой обозначений, так как мы рассматриваем уравнение $x^p + y^p = z^p$ (где $0 < x < y < z$) вместо $x^p + y^p + z^p = 0$. В частности, рассмотрим целые числа r, s, t, определенные в этих формулах. Следующие факты были доказаны Дитманом в 1964 г.

(3F) *Пусть p — нечетное простое число и натуральные числа x, y, $x < y$, таковы, что $x^p + y^p = (y+1)^p$ (следовательно, x, y взаимно просты). Тогда*

(1) *если $p \mid (y+1)$, то $v_p(-s+1) = v_p(y+1) - 1$;*
(2) *если $p \mid y$, то $v_p(t-1) = v_p(y) - 1$.*

Доказательство. (1) Пусть $z = y+1$ и $z - x = -s^p$. Тогда $s \neq -1$. По утверждению (1C) гл. III выполнено неравенство $n = v_p(y+1) \geqslant 2$ и p^n делит z и $x+y$, поэтому p^n делит $2z - (x+y) = z - x + 1 = -s^p + 1$. Так как $s^p \equiv s \pmod p$, мы получаем $p \mid (-s+1)$. Пусть $v_p(-s+1) = l \geqslant 1$. По утверждению (3B)(6) гл. II имеем неравенство $n \leqslant v_p(-s^p+1) = l+1$, откуда следует, что $l \geqslant n-1$.

Если $v_p(-s+1) \geqslant n$, то в соответствии с тем же утверждением (3B)(6) гл. II мы получаем $v_p(-s^p+1) \geqslant n+1$, а следовательно, p^{n+1} делит $-s^p + 1 = 2z - (x+y)$. Согласно соотношениям (1.2) число p^{pn-1} делит $x+y$, а значит, p^{n+1} делит $2z$, откуда следует,

что $p^{n+1} \mid z = y + 1$, а это противоречит предположению. Таким образом, $v_p(-s+1) = n-1$.

(2) Пусть $v_p(y) = n$. Тогда по утверждению (3B) гл. II мы имеем $n \geqslant 2$ и, как следует из соотношений (1.2), p^n делит числа y и $y + 1 - x = 2y - (x + y - 1)$. Значит, p^n делит $x + y - 1 = t^p - 1$. Так как $t^p \equiv t \pmod p$, p делит $t - 1$. Пусть $v_p(t-1) = l \geqslant 1$; тогда по утверждению (3B)(6) гл. II справедливо неравенство $n \leqslant v_p(t^p - 1) = l + 1$, а следовательно, $l \geqslant n - 1$.

Если $v_p(t-1) \geqslant n$, то $v_p(t^p - 1) \geqslant n + 1$, так что p^{n+1} делит $t^p - 1 = 2y - (y + 1 - x)$. Но p^{pn-1} делит $z - x = y + 1 - x$, поэтому p^{n+1} делит $2y$, откуда следует, что $p^{n+1} \mid y$, а это противоречит предположению. □

Вопрос, затронутый в предыдущем утверждении, пока не удалось разрешить с помощью прямого доказательства. Используя другие методы, можно показать, что при предположениях из утверждения (3E) p непременно делит y или $y + 1$.

Дитман также изучил возможность существования такого решения уравнения Ферма, для которого $y = x + 1$, получив следующий результат.

(3G) *Пусть p — нечетное простое число и натуральные числа x, z таковы, что $x^p + (x+1)^p = z^p$. Тогда*

(1) $p \mid x(x+1)$;

(2) *если* $p \mid (x+1)$, *то* $-r = \left[-p^{n-1/p}s\right]$ *и* $r \equiv 1 \pmod p$;

(3) *если* $p \mid x$, *то* $-s = \left[-p^{n-1/p}r\right] + 1$ *и* $-s \equiv 1 \pmod p$.

Доказательство. (1) Если $p \nmid x(x+1)$, то по утверждению (1C) гл. III мы имеем $z - x = -s^p$ и $z - (x+1) = -r^p$, откуда следует, что $1 = r^p - s^p$, а это невозможно, так как r и s отличны от нуля.

(2) Если $p \mid (x+1)$, то $p \nmid xz$, откуда по утверждению (1C) гл. III следует, что $z - x = -p^{pn-1}s^p$ и $z - (x+1) = -r^p$. Таким образом, $1 = r^p - p^{pn-1}s^p$, а значит, $r \equiv 1 \pmod p$ и $-r^p < -p^{pn-1}s^p$, так что $-r < -p^{n-1/p}s$.

Если $-r < -p^{n-1/p}s - 1$, то $r > p^{n-1/p}s + 1$. Следовательно, $r^p > p^{pn-1}s + 1$, что противоречит предположению. Значит, $-r = [-p^{n-1/p}s]$.

(3) Если $p \mid x$, то $p \nmid (x+1)z$, откуда по утверждению (1C) гл. III мы получаем, что $z - x = -s^p$, $z - (x+1) = -p^{pn-1}r^p$. Следовательно, $1 = p^{pn-1}r^p - s^p$, поэтому $-s \equiv 1 \pmod p$ и $-s^p > -p^{pn-1}r^p$, а значит, $-s > -p^{n-1/p}r$.

Если $-s > -p^{n-1/p}r + 1$, то $s + 1 < p^{n-1/p}r$, так что $s^p + 1 < p^{pn-1}r^p$, что противоречит предположению. Таким образом, $-s = [-p^{n-1/p}r] + 1$. □

Список литературы

1881 Abel, N.H., Extraits de quelques lettres à Holmboe, *Oeuvres Complètes*, Vol. II, 2nd ed., pp. 254–255, Grondahl, Christiania, 1881.

1857 Talbot, W.H.F., *On Fermat's theorem*, Trans. Roy. Soc. Edinburgh, **21** (1857), 403–406.

1884 Jonquières, E. de, *Sur le dernier théorème de Fermat*, Atti Accad. Pont. Nuovi Lincei, **37** (1883/4), 146–149; reprinted in Sphinx-Oedipe, **5** (1910), 29–32.

1884 Jonquières, E. de, *Sur le dernier théorème de Fermat*, C. R. Acad. Sci. Paris, **98** (1884), 863–864.

1886 Catalan, E., *Sur le dernier théorème de Fermat*, Bull. Acad. Roy. Sci. Lett. Beaux-Arts Belgique, (3), **12** (1886), 498–500.

1886 Catalan, E., *Sur le dernier théorème de Fermat* (Mélanges Mathématiques, CCXV), Mém. Soc. Roy. Sci. Liège Sér. 2, **13** (1886), 387–397.

1887 Borletti, F., *Sopra il teorema di Fermat relativo all'equazione* $x^n + y^n = z^n$, Rend. Istit. Lombardo, (2), **20** (1887), 222–224.

1887 Mansion, P., *Sur le dernier théorème de Fermat*, Bull. Acad. Roy. Sci. Lett. Beaux-Arts Belgique, (3), **13** (1887), 16–17 and 225.

1891 Lucas, E., *Théorie des Nombres*, reprinted by A. Blanchard, Paris, 1961.

1895 Markoff, V., *Question 477*, L'Interm. Math. Sér. I, **2** (1895), 23.

1901 Gambioli, D., *Memoria bibliografica sull'ultimo teorema di Fermat*, Period. Mat., **16** (1901), 145–192.

1905 Sauer, R., *Eine polynomische Verallgemeinerung des Fermatschen Satzes*, Dissertation, Giessen, 1905.

1932 Netanjahu-Mileikowsky, E.M., *Elementarer Beitrag zur Fermatschen Vermutung*, J. Reine Angew. Math., **166** (1932), 116–117.

1946 Inkeri, K., *Untersuchungen über die Fermatsche Vermutung*, Ann. Acad. Sci. Fenn. Ser. A, **33** (1946), 1–60.

1949 Izvekoff, J., *Sur une propriété des nombres premiers*, Bull. Soc. Math. Phys. Serbie, **1** (1949), 41–43.

1952 Bini, U., *La risoluzione delle equazioni* $x^n \pm y^n = M$ *e l'ultimo teorema di Fermat*, Archimede, **4** (1952), 50–57.

1955 Möller, K., *Untere Schranke für die Anzahl der Primzahlen, aus denen x, y, z der Fermatschen Gleichung $x^n + y^n = z^n$ bestehen muss*, Math. Nachr., **14** (1955), 25–28.

1964 Dittmann, G., *Untersuchungen über höhere Potenzen natürlicher Zahlen*, Thesis, Potsdam, 1964, 56 pp.

VI.4. Первый случай для четных показателей

В этом разделе мы приводим доказательство первого случая теоремы Ферма для четных показателей, принадлежащее Тержаняну (1977, см. также 1978). Достаточно рассмотреть показатели вида $2p$, где p — нечетное простое число. Доказательство потребует лишь элементарных соображений, так что остается только удивляться, почему оно не было найдено ранее.

Различные авторы изучали уравнение Ферма с четными показателями, однако рассуждение Тержаняна включило в себя все их прямые доказательства. Тем не менее мы приведем, а в некоторых случаях и докажем эти утверждения.

Начнем с письма Софи Жермен Гауссу (1804), в котором утверждалось без доказательства, что если p — простое число, $p \equiv 7 \pmod 8$, то уравнение $X^{p-1} + Y^{p-1} = Z^{p-1}$ не имеет решений в отличных от нуля целых числах.

В первой из длинного ряда статей по теореме Ферма Куммер (1837) доказал следующий факт, который был заново получен Нидермайером в 1943 г., а затем Гризелем (1953) и Эконому (1956). Мы приведем доказательство Гризеля.

(4A) *Пусть n — целое число, $n \geqslant 2$. Если существуют такие ненулевые целые числа x, y, z, что $x^{2n} + y^{2n} = z^{2n}$ и* НОД$(n, xyz) = 1$, *то $n \equiv 1 \pmod 8$.*

Доказательство. Так как теорема Ферма справедлива для показателя 4, будем считать число n нечетным, $n \geqslant 3$. Согласно замечанию в начале разд. I.1 можно также полагать, что числа x, y, z попарно взаимно просты и положительны, причем x четно, а y, z нечетны. Тогда, используя обозначения из разд. 1, получим

$$\begin{aligned} x^{2n} &= z^{2n} - y^{2n} \\ &= (z^2 - y^2)(z^{2(n-1)} + y^2 z^{2(n-2)} + \ldots + y^{2(n-2)} z^2 + y^{2(n-1)}) \\ &= (z^2 - y^2) \cdot Q_n(z^2, y^2). \end{aligned}$$

По утверждению (3B)(4) гл. II мы имеем НОД$(z^2-y^2, Q_n(z^2,y^2)) =$ $=$ НОД(z^2-y^2, n). Если простое число p делит числа n и z^2-y^2, то оно тем более делит x, что противоречит предположению. Таким образом, числа z^2-y^2 и $Q_n(z^2,y^2)$ взаимно просты.

Итак, z^2-y^2 и $Q_n(z^2,y^2)$ суть степени целых чисел, и показатель степени равен $2n$. Более того, число z^2-y^2 четно, а $Q_n(z^2,y^2)$ нечетно. Поэтому существует такое нечетное число k, что

$$z^{2(n-1)} + z^{2(n-2)}y^2 + z^{2(n-3)}y^4 + \ldots + y^{2(n-1)} = k^{2n}.$$

Каждое слагаемое этого равенства является квадратом нечетного числа, т. е. имеет вид $(2a+1)^2 = 4a(a+1)+1 \equiv 1 \pmod 8$. Таким образом, справедливо сравнение $n \equiv 1 \pmod 8$. □

Отсюда получаем такое следствие.

(4B) *Множество простых чисел p, таких, что первый случай теоремы Ферма справедлив для показателя $2p$, бесконечно.*

Доказательство. Согласно теореме Дирихле о простых числах в арифметической прогрессии каждому из сравнений $p \equiv 3 \pmod 8$, $p \equiv 5 \pmod 8$, $p \equiv 7 \pmod 8$ удовлетворяет бесконечно много простых чисел. Но если для числа p выполнены эти сравнения, то в силу утверждения (4A) первый случай теоремы Ферма справедлив для показателя $2p$. □

Отметим следующее усиление утверждения (4A). Часть (1) принадлежит Нидермайеру (1944), а утверждение (2) — Грею (1954).

(4C) *Пусть p — нечетное простое число и ненулевые взаимно простые целые числа x, y, z таковы, что $x^{2p}+y^{2p}=z^{2p}$. Тогда*

(1) *если $3p$ не делит x, y, z, то $p \equiv 1 \pmod 3$;*

(2) *если $2p$ не делит x, y, z, то $p = 24a+1$ (для некоторого целого числа a), причем число $12a+1$ не имеет делителей, сравнимых с 3 по модулю 4.*

Приведем еще одно усиление результата (4A) (утверждение (1) доказано Нидермайером в 1944 г., а (2) — Лонгом в 1960 г.).

(4D) *Пусть m — целое число, $m \geqslant 3$, и ненулевые целые числа x, y, z таковы, что $x^{2m}+y^{2m}=z^{2m}$ Тогда*

(1) *если $m = p$ — простое число, причем $5p$ не делит x, y, z. то $p \equiv \pm 1 \pmod 5$;*

(2) *если $(m, xyz) = 1$, то $m \equiv 1$ или $49 \pmod{120}$.*

Как следствие получаем такой результат.

(4E) *Если число $n = 2m$ оканчивается на* 4 *или* 6 (*в десятичной записи*), *то не существует таких отличных от нуля целых чисел* x, y, z, *что* $(m, xyz) = 1$ *и* $x^n + y^n = z^n$.

ДОКАЗАТЕЛЬСТВО. Поскольку $m \equiv \pm 2 \pmod 5$, мы получаем, что $m \not\equiv 1$ или $49 \pmod{120}$, и утверждение следует из (4D). □

Лонг (1961) расширил свой метод и доказал такой результат.

(4F) *Пусть p — простое число, $p \equiv -1 \pmod{10}$, и взаимно простые целые числа x, y, z, не кратные p, таковы, что $x^{2p} + y^{2p} = z^{2p}$. Тогда p есть квадрат по модулю* 11, *а следовательно, $p \equiv$* $\equiv 49$, 169, 289, 529 *или* $889 \pmod{1320}$.

Следующие результаты, связанные с символом Лежандра, были получены Эконому в 1956 г.

(4G) *Пусть нечетное целое число n, $n > 1$, и нечетное простое число q таковы, что*

(a) $(q - 1, n) = 1$;

(b) $(n/q) = -1$;

(c) *если* $0 < m < (q-1)/2$, *где* $n \equiv m \pmod{(q-1)/2}$, *и целые числа a, b, c удовлетворяют сравнению* $a^{2m} + b^{2m} \equiv c^{2m} \pmod q$, *причем*

$$\left(\frac{a^2 + b^2}{q}\right) = 1, \qquad \left(\frac{c^2 - a^2}{q}\right) = 1, \qquad \left(\frac{c^2 - b^2}{q}\right) = 1,$$

то $abc \equiv 0 \pmod q$.

Тогда не существует таких взаимно простых отличных от нуля целых чисел x, y, z, что НОД$(n, xyz) = 1$ *и* $x^{2n} + y^{2n} = z^{2n}$.

Существует много способов выбора чисел q, m, удовлетворяющих этим условиям. Так, в каждом из следующих примеров первый случай теоремы Ферма справедлив для показателя $2n$:

(a) $n \equiv -1 \pmod 3$;

(b) $n \equiv \pm 2 \pmod 5$;

(c) $(n/11) = -1$ и $n \equiv 4 \pmod 5$;

(d) $(n/19) = -1$ и $n \equiv 4$ или $7 \pmod 9$;

(e) $(n/23) = -1$ и $n \equiv 2$, или 3, или 4, или $10 \pmod{11}$;

(f) $(n/29) = -1$ и $n \equiv 3$, или 5, или 9, или $11 \pmod{14}$ и т. д.

Подобным образом Эконому доказал справедливость первого случая теоремы Ферма для всех четных показателей, меньших 200 000 (с возможными исключениями 108 722 и 188 018).

Ганди в 1966 г. доказал такое утверждение.

(4H) *Пусть простое число p, $p \geqslant 5$, и попарно взаимно простые целые числа x, y, z таковы, что $x^{p-1} + y^{p-1} = z^{p-1}$. Тогда z нечетно, и p делит ровно одно из чисел x, y (то, которое является четным), а следовательно, p не делит z.*

Доказательство. Так как число $p-1$ четно, согласно замечанию в начале разд. I.1 число z нечетно, а x и y имеют различную четность, например, x нечетно, а y четно.

Если $p \nmid xy$, то $x^{p-1} \equiv y^{p-1} \equiv 1 \pmod{p}$, в то время как $z^{p-1} \equiv 0 \pmod{p}$ или $z^{p-1} \equiv 1 \pmod{p}$. Тогда $2 \equiv x^{p-1} + y^{p-1} \equiv 0$ или $1 \pmod{p}$, что невозможно. Предположим, что $p \mid x$, $p \nmid y$, и придем к противоречию. Положив $m = (p-1)/2$, получим

$$x^{p-1} = z^{p-1} - y^{p-1} = (z^m - y^m)(z^m + y^m).$$

Оба множителя в правой части этого равенства взаимно просты, поскольку они нечетны. Следовательно, каждый их них есть степень целого числа, показатель которой равен $(p-1)$:

$$\begin{cases} z^m - y^m = a^{p-1}, \\ z^m + y^m = b^{p-1}, \end{cases}$$

а значит, $x = ab$ и $2z^m = a^{p-1} + b^{p-1}$. Но $p \mid x$ и НОД$(a, b) = 1$, так что p делит ровно одно из чисел a, b. Следовательно, $2z^m \equiv 1 \pmod{p}$. Возводя это сравнение в квадрат, получим $4 \equiv 1 \pmod{p}$, что невозможно.

Таким образом, p делит y. Следовательно, p не делит z. □

В 1969 г. Раина получил следующий результат.

(4I) *Пусть простое число p, $p \geqslant 5$, и натуральные попарно взаимно простые числа x, y, z таковы, что $x^{p-1} + y^{p-1} = z^{p-1}$. Тогда z является квадратичным вычетом по модулю p.*

Доказательство. Одно из чисел x, y четно, другое нечетно. Пусть y четно. Согласно утверждению (4H) число z нечетно и p делит y.

Положим $m = (p-1)/2$. Поскольку $(x^m)^2 + (y^m)^2 = (z^m)^2$, принимая во внимание утверждение (1A) гл. I, получим, что существуют такие натуральные числа a и b различной четности, что

НОД$(a,b)=1$ и

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

Пусть сначала b нечетно, тогда a четно. Так как НОД$(2a,b)=1$, найдутся такие целые числа h и k, что

$$\begin{cases} 2a = h^m, \\ b = k^m. \end{cases}$$

Таким образом, $4z^m = h^{p-1} + 4k^{p-1}$. Если $p \mid k$, то $p \nmid h$, поэтому $4z^m \equiv 1 \pmod p$. Следовательно, возведя это сравнение в квадрат, получим $16 \equiv 1 \pmod p$, а значит, $p=5$, что невозможно, так как уравнение $X^4 + Y^4 = Z^4$ неразрешимо в натуральных числах (утверждение (2С), гл. I).

Итак, $p \nmid k$, и, поскольку $p \mid y$, мы получаем $p \mid h$. Таким образом, $h^{p-1} = 4a^2 \equiv 0 \pmod{16p}$ и $z^{(p-1)/2} \equiv k^{p-1} \equiv 1 \pmod p$.

Пусть теперь b четно, в то время как a нечетно. Проводя аналогичные рассуждения, получим, что $z^{(p-1)/2} \equiv 1 \pmod p$. Итак, z является квадратичным вычетом по модулю p. □

Дальнейший результат в статье Раины не находит применения, так как его посылка никогда не выполняется (а именно, z не может быть простым числом в силу утверждения (3С)).

В 1955 г. Беккер опубликовал статью, в которой утверждалась справедливость теоремы Ферма для всех четных показателей, больших двух. Однако можно с уверенностью сказать, что приведенное доказательство неверно.

Приведем теперь доказательство теоремы Тержаняна, из которой следуют все вышеприведенные результаты. Мы снова будем рассматривать частное $Q_n(z,y) = (z^n - y^n)/(z-y)$, где n — нечетное натуральное число, а z, y — различные ненулевые целые числа (не обязательно положительные).

Для удобства читателя напомним, что если m и n — отличные от нуля нечетные целые числа, $n > 0$, НОД$(m,n)=1$, то определен символ Якоби (m/n). Если $m > 0$, то символ (n/m) также определен, причем справедлив так называемый квадратичный закон взаимности:

$$\left(\frac{m}{n}\right) = (-1)^{(m-1)/2 \times (n-1)/2} \left(\frac{n}{m}\right). \qquad (4.1)$$

Более того,

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}. \tag{4.2}$$

(4J) *Пусть различные нечетные числа y, z таковы, что $y \equiv z \pmod 4$ и* НОД$(y, z) = 1$. *Пусть, далее, m и n нечетны, причем $m \geqslant 1, n \geqslant 1$ и* НОД$(m, n) = 1$. *Тогда*

(1) $Q_m(z, y) \equiv m \pmod 4$ *и, в частности, $Q_m(z, y)$ нечетно;*

(2) *символы Якоби $(Q_m(z, y)/Q_n(z, y))$ и (m/n) определены и равны.*

Доказательство. (1) Пусть $z = y + 4t$. Тогда

$$\begin{aligned} Q_m(z, y) &= \frac{(y+4t)^m - y^m}{4t} = \binom{m}{1} y^{m-1} + \binom{m}{2} y^{m-2} 4t + \dots \\ &\equiv m y^{m-1} \equiv m \pmod 4, \end{aligned}$$

поскольку число $(m-1)$ четно и y нечетно, а значит, $y^{m-1} \equiv 1 \pmod 4$.

(2) Заметим сначала, что, так как НОД$(m, n) = 1$, символ Якоби (m/n) определен. Аналогично, поскольку НОД$(y, z) = 1$, из утверждения (3В)(2) гл. II следует, что

$$\text{НОД}(Q_m(z, y), Q_n(z, y)) = 1.$$

Так как $Q_n(z, y) > 0$, символ Якоби $(Q_m(z, y)/Q_n(z, y))$ также имеет смысл.

Равенство символов Якоби докажем индукцией по $k = \min\{m, n\}$. При $k = 1$ утверждение очевидно. Пусть $k > 1$. Тогда $m \neq n$, поскольку НОД$(m, n) = 1$.

Если $m > n$, то существуют такие нечетные целые числа r, $0 < r < n = k$, и q, что $m = qn + r$ или $m = qn - r$. Если $m = qn + r$, то число $m - r$ четно, откуда по утверждению (3В)(1) гл. II следует, что

$$\left(\frac{Q_m(z, y)}{Q_n(z, y)}\right) = \left(\frac{y^{m-r} Q_r(z, y)}{Q_n(z, y)}\right) = \left(\frac{Q_r(z, y)}{Q_n(z, y)}\right) = \left(\frac{r}{n}\right) = \left(\frac{m}{n}\right).$$

Если $m = qn - r$, то числа $m - n, n - r$ четны, откуда, используя утверждение (3В)(1) гл. II и свойства символа Якоби, по индукции

получим

$$\left(\frac{Q_m(z,y)}{Q_n(z,y)}\right) = \left(\frac{-y^{m-n}z^{n-r}Q_r(z,y)}{Q_n(z,y)}\right)$$
$$= \left(\frac{-Q_r(z,y)}{Q_n(z,y)}\right) = \left(\frac{-1}{Q_n(z,y)}\right)\left(\frac{Q_r(z,y)}{Q_n(z,y)}\right)$$
$$= \left(\frac{-1}{Q_n(z,y)}\right)\left(\frac{r}{n}\right).$$

Так как $Q_n(z,y) \equiv n \pmod 4$ согласно части (1),

$$(Q_n(z,y)-1)/2 \equiv (n-1)/2 \pmod 2,$$

следовательно, в соответствии с соотношениями (4.2) мы получаем $(-1/Q_n(z,y)) = (-1/n)$. Таким образом,

$$\left(\frac{Q_m(z,y)}{Q_n(z,y)}\right) = \left(\frac{-1}{n}\right)\left(\frac{r}{n}\right) = \left(\frac{m}{n}\right).$$

Если $m < n$, то по закону взаимности (4.1) для символа Якоби, используя проведенное выше доказательство, получаем

$$\left(\frac{Q_m(z,y)}{Q_n(z,y)}\right) = (-1)^{(Q_m(z,y)-1)/2\times(Q_n(z,y)-1)/2}\left(\frac{Q_n(z,y)}{Q_m(z,y)}\right)$$
$$= (-1)^{(m-1)/2\times(n-1)/2}\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right). \quad \square$$

Теперь мы с легкостью можем получить результат Тержаняна.

(4K) *Пусть p — нечетное простое число. Если отличные от нуля целые числа x, y, z таковы, что $x^{2p} + y^{2p} = z^{2p}$, то $2p$ делит x или y.*

Доказательство. Без ограничения общности будем полагать, что числа x, y, z попарно взаимно просты. Далее, числа x, y не могут быть оба нечетны, так как показатель $2p$ четен (см. замечание в начале разд. I.1). Пусть число x четно, а y, z нечетны. Тогда

$$x^{2p} = z^{2p} - y^{2p} = (z^2 - y^2)\frac{z^{2p} - y^{2p}}{z^2 - y^2}.$$

По утверждению (3B)(4) гл. II мы имеем

$$\text{НОД}\left(z^2 - y^2, \frac{z^{2p} - y^{2p}}{z^2 - y^2}\right) = p \quad \text{или} \quad 1.$$

Если этот наибольший общий делитель равен p, то p делит x^{2p}, а значит, $2p$ делит x.

Покажем теперь, что числа z^2-y^2 и $(z^{2p}-y^{2p})/(z^2-y^2)$ не могут быть взаимно простыми. Действительно, если эти числа взаимно просты, то они должны быть квадратами целых чисел. Но

$$\frac{z^{2p}-y^{2p}}{z^2-y^2}=\frac{z^p-y^p}{z-y}\times\frac{z^p+y^p}{z+y}=Q_p(z,y)\times Q_p(z,-y),$$

причем два множителя в правой части взаимно просты, поскольку НОД$(y,z)=1$, а числа y,z нечетны. Таким образом, $Q_p(z,y)$ и $Q_p(z,-y)$ также являются квадратами целых чисел. Так как p не является квадратом целого числа, существует такое нечетное простое число q, что p не является квадратом по модулю q.

Предположим сначала, что $z\equiv y\pmod 4$. Согласно (4.1) мы имеем

$$-1=\left(\frac{p}{q}\right)=\left(\frac{Q_p(z,y)}{Q_q(z,y)}\right),$$

что невозможно, потому что $Q_p(z,y)$ — квадрат целого числа. Если $z\not\equiv y\pmod 4$, то $z\equiv -y\pmod 4$ и, следовательно, мы вновь получаем

$$-1=\left(\frac{p}{q}\right)=\left(\frac{Q_p(z,-y)}{Q_q(z,-y)}\right),$$

что также невозможно. Полученное противоречие завершает доказательство. □

В 1981 г. Роткевич получил следующее усиление результата Тержаняна.

(4L) *Пусть p — нечетное простое число. Если натуральные числа x,y,z таковы, что $x^{2p}+y^{2p}=z^{2p}$, то $8p^3$ делит x или y.*

Доказательство. Можно считать, что числа x,y,z попарно взаимно просты, причем x четно, а y,z нечетны. Тогда по теореме Тержаняна $2p$ делит x.

Покажем, что 8 делит x. Нетрудно видеть, что НОД$(z^p-x^p,\ z^p+x^p)=1$, так как НОД$(x,z)=1$, x четно и z нечетно. Так как $y^{2p}=z^{2p}-x^{2p}=(z^p-x^p)(z^p+x^p)$, мы получаем, что $z^p-x^p=[(z^p-x^p)/(z-x)](z-x)=a^{2p}$, где a — нечетное натуральное число. Поскольку $p\mid x$, можно заключить, что $p\nmid z$, а значит, $p\nmid(z-x)$. По утверждению (3B)(5) гл. II мы имеем НОД$((z^p-x^p)/(z-x),\ z-x)=1$, а следовательно, $(z^p-x^p)/(z-x)=b^2$, где b — нечетное натуральное число (так как z нечетно). Таким образом, $b^2=(2b_1+1)^2+1=4b_1(b_1+1)\equiv 1\pmod 8$

и $z^{p-1} + z^{p-2}x + z^{p-3}x^2 \equiv 1 \pmod 8$, потому что x четно. Но z нечетно, и мы снова имеем $z^{p-1} \equiv 1 \pmod 8$, откуда следует, что $z^{p-3}x(z+x) \equiv 0 \pmod 8$. Таким образом, $x \equiv 0 \pmod 8$, так как числа $z, z+x$ нечетны.

Тот факт, что p^3 делит x, следует из результата Вандивера (1B). Мы также можем записать $z^p + x^p = c^{2p}$, где c — нечетное натуральное число. Согласно теореме Вандивера $x^p \equiv x \pmod{p^3}$. Поскольку $p \mid x$ и $p \geqslant 3$, мы заключаем, что p^3 делит x, а значит, x делится и на $8p^3$. □

В 1950 г. Гут воспользовался соображениями Куммера и Мириманова и, применив методы теории полей классов, получил критерий справедливости первого случая теоремы Ферма с показателем $2p$, использующий числа Эйлера. Конечно, теперь этот результат не актуален.

В заключение укажем один простой факт, которым воспользуемся позже.

(4M) *Пусть x, y, z — ненулевые взаимно простые целые числа, $n \geqslant 3$ и $x^{2n} + y^{2n} = z^{2n}$. Тогда $2 \mid xy$ и $3 \mid xy$.*

Доказательство. Если числа x, y нечетны, то $x^{2n} + y^{2n} \equiv 2 \pmod 4$, но тогда число z четно, причем $z^{2n} \equiv 0 \pmod 4$, что невозможно. Если $3 \nmid xy$, то $x^{2n} \equiv y^{2n} \equiv 1 \pmod 3$, но $z^{2n} \equiv 0$ или $1 \pmod 3$, так что соотношение $x^{2n} + y^{2n} = z^{2n}$ не может быть справедливым. □

Список литературы

1804 Germain, S., *Letter to Gauss, Nov. 21, 1804*; reprinted in *Oeuvres Philosophiques*, p. 298 (editées par H. Stupuy), Ritti, Paris, 1879.

1837 Kummer, E.E., *De aequatione $x^{2\lambda} + y^{2\lambda} = z^{2\lambda}$ per numeros integros resolvenda*, J. Reine Angew. Math., **17** (1837), 203–209; reprinted in *Collected Papers*, Vol. I, pp. 135–141.

1943 Niedermeier, F., *Ein elementarer Beitrag zur Fermatschen Vermutung*, J. Reine Angew. Math., **185** (1943), 111–112.

1944 Niedermeier, F., *Zwei Erweiterungen eines Kummerschen Kriteriums für die Fermatsche Gleichung*, Deutsche Math., **7** (1944), 518–519.

1950 Gut, M., *Eulersche Zahlen und großer Fermatscher Satz*, Comment. Math. Helv., **24** (1950), 73–99.

1953 Griselle, T., *Proof of Fermat's last theorem for* $n = 2(8a + 1)$, Math. Mag., **26** (1953), 263.

1954 Grey, L.D., *A note on Fermat's last theorem*, Math. Mag., **27** (1954), 274–277.

1955 Becker, H.W., *Proof of F.L.T. for all even powers*, Math. Mag., **28** (1955), 297–298; and **29** (1956), 125.

1956 Oeconomou, G., *Sur le premier cas du théorème de Fermat pour les exposants pairs*, C. R. Acad. Sci. Paris, **243** (1956), 1588–1591.

1960 Long, L., *A note on Fermat's theorem*, Math. Gaz., **44** (1960), 261–262.

1961 Long, L., *On Fermat's last theorem*, Math. Gaz., **45** (1961), 319–321.

1966 Gandhi, J.M., *On Fermat's last theorem*, Math. Gaz., **50** (1966), 36–37.

1969 Raina, B.L., *On Fermat's last theorem*, Amer. Math. Monthly, **76** (1969), 49–51.

1977 Terjanian, G., *Sur l'équation* $x^{2p} + y^{2p} = z^{2p}$, C. R. Acad. Sci. Paris, **285** (1977), 973–975.

1978 Terjanian, G., *L'équation* $x^p - y^p = az^2$ *et le théorème de Fermat*, Sém. Th. des Nombres, Bordeaux, exposé no. 29, 1978, 7 pp.

1981 Rotkiewicz, A., *On Fermat's equation with exponent* $2p$, Colloq. Math., **45** (1981), 101–102.

Глава VII

Эпизоды 7 и 8

В этой главе рассматриваются многочлены, имеющие прямое отношение к уравнению Ферма.

VII.1. Некоторые важные полиномиальные тождества

Здесь мы приводим некоторые алгебраические тождества, которые используются в исследованиях уравнения Ферма. Многие предыдущие попытки доказать теорему Ферма опирались на известные полиномиальные тождества.

Вначале укажем следующие тождества, которые были использованы Ламе в 1840 г. (см. также В. А. Лебег (1847), Меншен (1847), Каталан (1885)). К. Ф. Гаусс (1863) рассмотрел частные случаи, когда $n = 3, 5, 7$ (см. также Ребу (1877) и Брокар (1878)).

(1A) *Если X, Y, Z — переменные и число n нечетно, то*

$$(X+Y+Z)^n - (X+Y-Z)^n - (X-Y+Z)^n - (-X+Y+Z)^n$$
$$= 4nXYZ \sum_{\substack{i+j+k=(n-3)/2 \\ i,j,k \geqslant 0}} \frac{(n-1)!}{(2i+1)!\,(2j+1)!\,(2k+1)!} X^{2i} Y^{2j} Z^{2k}.$$

Доказательство. Выписывая явно степени с показателем n в левой части равенства, получим

$$(X+Y+Z)^n - (X+Y-Z)^n - (X-Y+Z)^n - (-X+Y+Z)^n$$
$$= \sum_{\substack{a+b+c=n \\ a,b,c \geqslant 0}} \frac{n!}{a!\,b!\,c!} X^a Y^b Z^c [1 - (-1)^c - (-1)^b - (-1)^a].$$

Так как n нечетно и $a + b + c = n$, ровно одно или же все три целых числа a, b, c тоже нечетны. Если только одно из них нечетно, то

$1-(-1)^a-(-1)^b-(-1)^c=0$. Таким образом, мы можем рассматривать только слагаемые, для которых $a=2i+1$, $b=2j+1$, $c=2k+1$, а значит, $i+j+k=(n-3)/2$ и $1-(-1)^a-(-1)^b-(-1)^c=4$.

Отсюда вытекает справедливость нашего утверждения. □

Как следствие имеем такой результат (см. А. С. Веребрюсов, 1908).

(1B) *Если X, Y, Z — переменные и число n нечетно, то*

$$(X+Y+Z)^n-X^n-Y^n-Z^n=\frac{4n}{2^n}(X+Y)(Y+Z)(Z+X)\times\sum_{\substack{i+j+k=(n-3)/2\\ i,j,k\geqslant 0}}\frac{(n-1)!\,(X+Y)^{2i}(Y+Z)^{2j}(Z+X)^{2k}}{(2i+1)!\,(2j+1)!\,(2k+1)!}.$$

Доказательство. В тождестве (1A) заменим X, Y, Z на U, V, W, где $U=(X+Y)/2$, $V=(Y+Z)/2$, $W=(Z+X)/2$. Тогда

$$\begin{aligned}U+V+W&=X+Y+Z,\\ U+V-W&=Y,\\ U-V+W&=X,\\ -U+V+W&=Z,\end{aligned}$$

и (1A) превращается в равенство

$$(X+Y+Z)^n-X^n-Y^n-Z^n=\frac{4n}{2^n}(X+Y)(Y+Z)(Z+X)\times\sum_{\substack{i+j+k=(n-3)/2\\ i,j,k\geqslant 0}}\frac{(n-1)!\,(X+Y)^{2i}(Y+Z)^{2j}(Z+X)^{2k}}{(2i+1)!\,(2j+1)!\,(2k+1)!}.$$ □

Рассмотрим следующий частный случай.

(1C) *Если X, Y — переменные и число n нечетно, то*

$$(X+Y)^n-X^n-Y^n=\frac{4n}{2^n}(X+Y)XY\times\sum_{\substack{i+j+k=(n-3)/2\\ i,j,k\geqslant 0}}\frac{(n-1)!}{(2i+1)!\,(2j+1)!\,(2k+1)!}(X+Y)^{2i}Y^{2j}X^{2k}.$$

Доказательство. Доказываемое равенство получается, если заменить Z на 0 в тождестве (1B). □

Уже в 1837 г. Куммер использовал следующее тождество для многочлена $(X+Y)^n-(X^n+Y^n)$ (см. также Меншен (1847), Вашет (1861), Баризьен (1906), Бутен и Гонсалес Кихано (1907), Бини (1907), Роуз (1907) и Бахман (1910)).

(1D) *Если X, Y — переменные и $n \geqslant 1$, то*

$$(X+Y)^n-(X^n+Y^n)=\sum_{i=1}^{\infty}(-1)^{i-1}\frac{n}{i}\binom{n-i-1}{i-1}X^iY^i(X+Y)^{n-2i}$$

(будем считать, что при $2i>n$ члены в этой сумме равны нулю).

Доказательство. Докажем тождество

$$X^n+Y^n=(X+Y)^n+\sum_{i=1}^{\infty}(-1)^i\frac{n}{i}\binom{n-i-1}{i-1}X^iY^i(X+Y)^{n-2i}$$

по индукции. Для $n=1,2$ оно очевидно. Далее,

$$\begin{aligned}X^{n+1}+Y^{n+1}&=(X^n+Y^n)(X+Y)-XY(X^{n-1}+Y^{n-1})\\&=(X+Y)^{n+1}\\&\quad+\sum_{i=1}^{\infty}(-1)^i\frac{n}{i}\binom{n-i-1}{i-1}X^iY^i(X+Y)^{n+1-2i}\\&\quad-XY(X+Y)^{n-1}\\&\quad-\sum_{i=1}^{\infty}(-1)^i\frac{n-1}{i}\binom{n-i-2}{i-1}X^{i+1}Y^{i+1}(X+Y)^{n-1-2i}\\&=(X+Y)^{n+1}+\sum_{i=1}^{\infty}(-1)^ic_iX^iY^i(X+Y)^{n+1-2i},\end{aligned}$$

где $c_1=n+1$ и если $i\geqslant 2$, то

$$c_i=\frac{n}{i}\binom{n-i-1}{i-1}+\frac{n-1}{i-1}\binom{n-i-1}{i-2}=\frac{n+1}{i}\binom{n-i}{i-1}.\ \square$$

В 1885 г. (а затем и в 1886 г.) Каталан привел другую форму тождества (1B).

(1E) *Если X, Y, Z — переменные и число n нечетно, то*

$$\frac{(X+Y+Z)^n - X^n - Y^n - Z^n}{(X+Y)(Y+Z)(Z+X)} = P^{n-3} + H_1 P^{n-4} + H_2 P^{n-5} + \ldots + H_{n-3} + 2H^{(2)}_{(n-3)/2},$$

где $P = X+Y+Z = H_1$ и при $i \geqslant 1$ многочлен H_i является суммой всех одночленов степени i с коэффициентом 1 от переменных X, Y, Z, а $H^{(2)}_{(n-3)/2}$ является суммой всех одночленов степени $(n-3)/2$ с коэффициентом 1 от переменных X^2, Y^2, Z^2 (таким образом, степень самого этого многочлена равна $n-3$), т. е. $H^{(2)}_{(n-3)/2} = H_{(n-3)/2}(X^2, Y^2, Z^2)$.

Доказательство. Нетрудно видеть, что справедливы соотношения

$$\begin{aligned} Q_1 &= \frac{P^n - (X^n + Y^n + Z^n)}{X+Y} = \frac{P^n - Z^n}{P-Z} - \frac{X^n + Y^n}{X+Y} \\ &= (P^{n-1} + ZP^{n-2} + Z^2P^{n-3} + \ldots + Z^{n-1}) \\ &\quad - (X^{n-1} - YX^{n-2} + Y^2X^{n-3} - \ldots + Y^{n-1}). \end{aligned}$$

Но согласно алгоритму Евклида, так как $Y + Z = P - X$, мы получаем

$$\begin{aligned} &\frac{P^{n-1} + ZP^{n-2} + Z^2P^{n-3} + \ldots + Z^{n-1}}{Y+Z} \\ &= P^{n-2} + H_1(X,Z)P^{n-3} + H_2(X,Z)P^{n-4} + \ldots + H_{n-2}(X,Z) \\ &\quad + \frac{X^{n-1} + ZX^{n-2} + \ldots + Z^{n-1}}{Y+Z}, \end{aligned}$$

где $H_i(X, Z)$ является суммой всех одночленов степени i с коэффициентом 1 от переменных X, Z. Следовательно,

$$\begin{aligned} Q_2 &= \frac{Q_1}{Y+Z} \\ &= (P^{n-2} + H_1(X,Z)P^{n-3} + H_2(X,Z)P^{n-4} + \ldots + H_{n-2}(X,Z)) \\ &\quad + \frac{1}{Y+Z}[(Y+Z)X^{n-2} - (Y^2 - Z^2)X^{n-3} + (Y^3 + Z^3)X^{n-4} \\ &\qquad - \ldots - (Y^{n-1} - Z^{n-1})] \\ &= (P^{n-2} + H_1(X,Z)P^{n-3} + H_2(X,Z)P^{n-4} + \ldots + H_{n-2}(X,Z)) \\ &\quad + (X^{n-2} - (Y-Z)X^{n-3} + (Y^2 - ZY + Z^2)X^{n-4} - \ldots \\ &\qquad - (Y^{n-2} - ZY^{n-3} + Z^2Y^{n-4} - \ldots - Z^{n-2})). \end{aligned}$$

Снова применив алгоритм Евклида, получим

$$\frac{P^{n-2}+H_1(X,Z)P^{n-3}+H_2(X,Z)P^{n-4}+\ldots+H_{n-2}(X,Z)}{Z+X}$$

$$= P^{n-3}+H_1P^{n-4}+H_2P^{n-5}+\ldots+H_{n-3}$$

$$+\frac{Y^{n-2}+H_1(X,Z)Y^{n-3}+H_2(X,Z)Y^{n-4}+\ldots+H_{n-2}(X,Z)}{Z+X},$$

где H_i имеет такой вид, как указано в формулировке. Далее,

$$Q_3 = \frac{Q_2}{Z+X}$$

$$= P^{n-3}+H_1P^{n-4}+H_2P^{n-5}+\ldots+H_{n-3}$$

$$+\frac{1}{Z+X}[Y^{n-2}+H_1(X,Z)Y^{n-3}+H_2(X,Z)Y^{n-4}$$

$$+\ldots+H_{n-2}(X,Z)+X^{n-2}-(Y-Z)X^{n-3}$$

$$+(Y^2-ZY+Z^2)X^{n-4}-\ldots$$

$$-(Y^{n-2}-ZY^{n-3}+Z^2Y^{n-4}-\ldots-Z^{n-2})].$$

Но

$$\frac{H_1(X,Z)}{Z+X} = 1,$$

$$\frac{H_3(X,Z)}{Z+X} = X^2+Z^2 = H_1^{(2)}(X,Z),$$

$$\frac{H_5(X,Z)}{Z+X} = X^4+X^2Z^2+Z^4 = H_2^{(2)}(X,Z)$$

и т. д. Следовательно,

$$Q_3 = P^{n-3}+H_1P^{n-4}+H_2P^{n-5}+\ldots+H_{n-3}+Y^{n-3}$$

$$+H_1^{(2)}(X,Z)Y^{n-5}+H_2^{(2)}(X,Z)Y^{n-7}+\ldots+H_{(n-3)/2}^{(2)}(X,Z)$$

$$+\frac{1}{Z+X}[Y^{n-2}+H_2(X,Z)Y^{n-4}+H_4(X,Z)Y^{n-6}+$$

$$\ldots+H_{n-3}(X,Z)Y+X^{n-2}-(Y-Z)X^{n-3}$$

$$+(Y^2-YZ+Z^2)X^{n-4}-\ldots$$

$$-(Y^{n-2}-ZY^{n-3}+Z^2Y^{n-4}-\ldots-Z^{n-2})].$$

Выражение в квадратных скобках равно

$$\begin{aligned}
&YX^{n-3}+YZX^{n-4}+(YZ^2+Y^3)X^{n-5}\\
&\quad+(YZ^3+Y^3Z)X^{n-6}+(YZ^4+Y^3Z^2+Y^5)X^{n-7}+\ldots\\
&\quad+(YZ^{n-3}+Y^3Z^{n-5}+\ldots+Y^{n-4}Z^2+Y^{n-2})\\
&\quad+X^{n-2}-(Y-Z)X^{n-3}+(Y^2-YZ+Z^2)X^{n-4}-\ldots\\
&\quad-(Y^{n-2}-ZY^{n-3}+Z^2Y^{n-4}-\ldots-Z^{n-2})\\
=\;&X^{n-2}+ZX^{n-3}+(Y^2+Z^2)X^{n-4}+(Y^2Z+Z^3)X^{n-5}\\
&\quad+(Y^4+Y^2Z^2+Z^4)X^{n-6}+(Y^4Z+Y^2Z^3+Z^5)X^{n-7}\\
&\quad+\ldots+(Y^{n-3}Z+Y^{n-5}Z^3+\ldots+Z^{n-2})\\
=\;&X^{n-2}+ZX^{n-3}+H_1^{(2)}(Y,Z)X^{n-4}+H_1^{(2)}(Y,Z)ZX^{n-5}\\
&\quad+H_2^{(2)}(Y,Z)X^{n-6}+H_2^{(2)}(Y,Z)ZX^{n-7}+\ldots+H_{(n-3)/2}^{(2)}(Y,Z)Z.
\end{aligned}$$

Таким образом,

$$\begin{aligned}
Q_3 \;=\;&P^{n-3}+H_1P^{n-4}+H_2P^{n-5}+\ldots+H_{n-3}+Y^{n-3}+\\
&H_1^{(2)}(X,Z)Y^{n-5}+H_2^{(2)}(X,Z)Y^{n-7}+\ldots+H_{(n-3)/2}^{(2)}(X,Z)\\
&+X^{n-3}+H_1^{(2)}(Y,Z)X^{n-5}+\ldots+H_{(n-3)/2}^{(2)}(Y,Z)\\
&=P^{n-3}+H_1P^{n-4}+H_2P^{n-5}+\ldots+H_{n-3}+2H_{(n-3)/2}^{(2)},
\end{aligned}$$

так как каждая из двух последних строк равна $H_{(n-3)/2}^{(2)}$. □

Список литературы

1782 Waring, E., *Meditationes Algebraicae* (3rd ed.), Cambridge University Press, Cambridge, 1782.

1837 Kummer, E.E., *De aequatione* $x^{2\lambda}+y^{2\lambda}=z^{2\lambda}$ *per numeros integros resolvenda*, J. Reine Angew. Math., **17** (1837), 203–209; reprinted in *Collected Papers*, Vol. I, pp. 135–141, Springer-Verlag, Berlin, 1975.

1840 Lamé, G., *Mémoire d'analyse indéterminée démontrant que l'équation* $x^7+y^7=z^7$ *est impossible en nombres entiers*, J. Math. Pures Appl., **5** (1840), 195–211.

1847 Lamé, G., *Mémoire sur la résolution en nombres complexes de l'équation* $A^n+B^n+C^n=0$, J. Math. Pures Appl., **12** (1847), 172–184.

1847 Lebesgue, V.A., *Sur la question* 70^e, Nouv. Ann. Math., **6** (1847), 427–431.

1847 Mention, J., *Solution de la question 70*, Nouv. Ann. Math., **6** (1847), 399–400.

1861 Vachette, A., *Note sur certains développements et solution des questions 461, 468, et 479*, Nouv. Ann. Math., **20** (1861), 155–174.

1863 Gauss, C.F., *Zur Theorie der complexen Zahlen.* (I) *Neue Theorie der Zerlegung der Cuben, Werke*, Vol. II, pp. 387–391.

1877 Rebout, E., *Formation d'un cube entier qui soit égal à la somme de quatre cubes entiers*, Nouv. Ann. Math., (2), **16** (1877), 272–273.

1878 Brocard, H., *Sur divers articles de la Nouvelle Correspondance* (*Question 286*), Nouv. Corr. Math., **4** (1878), 136–138.

1885 Serret, J.A., *Algèbre Supérieure*, Vol. I, p. 449 (5^e édition), Gauthier-Villars, Paris, 1885.

1885 Catalan, E., *Sur le théorème de Fermat (1861)*, Mélanges Mathématiques XLVII, Mém. Soc. Roy. Sci. Liège, (2), **12** (1885), 179–187.

1886 Catalan, E., *Sur le dernier théorème de Fermat*, Mém. Soc. Roy. Sci. Liège, (2), **13** (1886), 387–397.

1906 Barisien, E.N., *Questions 3076 et 3077*, L'Interm. Math., **13** (1906), 142.

1907 Bini, U., *Sopra alcune congruenze*, Period. Mat., (3), **22** (1907), 180–183.

1907 Boutin, A. and Gonzalez Quijano, P.M., *Sur la question 3076* (*de Barisien*), L'Interm. Math., **14** (1907), 22–23.

1907 Rose, J., *Sur la question 3076* (*de Barisien*), L'Interm. Math., **14** (1907), 92–93.

1908 Werebrusow, A.S., *Question 3406*, L'Interm. Math., **15** (1908), 12.

1909 Dubouis, E., *Sur la question 3406* (*de Werebrusow*), L'Interm. Math., **16** (1909), 79–80.

1910 Bachmann, P., *Niedere Zahlentheorie*, Teubner, Leipzig, 1910; reprinted by Chelsea, New York, 1966.

1951 Perron, O., *Algebra*, Vol. I, W. de Gruyter, Berlin, 1951.

1959 Rédei, L., *Algebra*, Vol. I, Akademie Verlag, Geest & Portig, Leipzig, 1959.

VII.2. Многочлены Коши

В своем доказательстве теоремы Ферма для показателя 7 Ламе (1839, 1840) использовал полиномиальное тождество седьмой степени. Изучая работы Ламе, Коши и Лиувилль привели более общее полиномиальное тождество (1839), из которого получены следующие частные случаи (Коши, 1841):

$$(X+Y)^5 - X^5 - Y^5 = 5XY(X+Y)(X^2+XY+Y^2),$$
$$(X+Y)^7 - X^7 - Y^7 = 7XY(X+Y)(X^2+XY+Y^2)^2.$$

Так началось изучение многочлена $(X+Y)^n - X^n - Y^n$.

Если показатель $n \geqslant 3$ нечетен, то этот многочлен делится на $X, Y, X+Y$. Кроме того, если показатель равен нечетному простому числу p, то наш многочлен также кратен и p.

(2A) *Пусть* $n \equiv \pm 1 \pmod 6$. *Тогда многочлен* $(X+Y)^n - (X^n + Y^n)$ *делится на* $\left(X^2+XY+Y^2\right)^e$, *но не делится на* $\left(X^2+XY+Y^2\right)^{e+1}$, *где*

$$e = \begin{cases} 1, & \text{если} \quad n \equiv -1 \pmod 6, \\ 2, & \text{если} \quad n \equiv 1 \pmod 6. \end{cases}$$

Доказательство. Покажем, что

$$(X+1)^n - (X^n+1) = (X^2+X+1)^e H_n(X),$$

где показатель e определен выше, $H_n(X) \in \mathbb{Z}[X]$ и X^2+X+1 не делит $H_n(X)$. Отсюда, приведя многочлен к однородному виду, получим справедливость утверждения (2A).

Пусть $G_n(X) = (X+1)^n - (X^n+1)$, и пусть ω — первообразный корень из 1 третьей степени, $\omega = (-1+\sqrt{-3})/2$. Тогда $\omega^2+\omega+1=0$ и мы можем записать $G_n(\omega) = (\omega+1)^n - (\omega^n+1) = -(\omega^{2n}+\omega^n+1) = -(\omega^{3n}-1)/(\omega^n-1) = 0$.

Таким образом, $G_n(X)$ делится на минимальный многочлен X^2+X+1 для ω. Разделив $G_n(X)$ с остатком, получим, что $G_n(X) = F(X)(X^2+X+1) + (aX+b)$, где $F(X) \in \mathbb{Z}[X]$ и $a, b \in \mathbb{Z}$. Значит, $0 = G_n(\omega) = F(\omega)(\omega^2+\omega+1) + a\omega + b = a\omega + b$, откуда следует, что $a=0$ (иначе выполнялось бы условие $\omega = -b/a \in \mathbb{Q}$, что неверно) и $b=0$.

Далее, $(X^2+X+1)^2$ делит $G_n(X)$ тогда и только тогда, когда ω является корнем многочлена $G_n(X)$ кратности 2, а значит, ω — корень его производной $G_n'(X) = n((X+1)^{n-1} - X^{n-1})$, т. е.

$n\left[(\omega+1)^{n-1}-\omega^{n-1}\right]=0$. Поскольку $\omega+1=-\omega^2$, это условие эквивалентно равенству $(\omega^{n-1}-1)\omega^{n-1}=0$, т. е. $\omega^{n-1}=1$. А это равенство верно тогда и только тогда, когда $n-1$ кратно 3, т. е. $n\equiv 1 \pmod 6$.

Покажем, что $(X^2+X+1)^3$ не делит $G_n(X)$. Действительно, предположим, что $G_n(X)$ делится на $(X^2+X+1)^3$. Тогда должно выполняться сравнение $n\equiv 1 \pmod 6$ и, более того, многочлен X^2+X+1 должен делить $G_n''(X)=n(n-1)((X+1)^{n-2}-X^{n-2})$. Значит, $G_n''(\omega)=0$, и потому $(\omega+1)^{n-2}=\omega^{n-2}$ и $-\omega^{2(n-2)}=\omega^{n-2}$. Следовательно, $\omega^{n-2}=-1$ и $\omega^{2(n-2)}=1$. Это означает, что 3 делит $2(n-2)$, т. е. $n\equiv 2 \pmod 3$, откуда следует, что $n\equiv -1 \pmod 6$, так что мы пришли к противоречию. □

Из сказанного выше следует такое утверждение: если $n\equiv\pm1 \pmod 6$, то

$$(X+Y)^n-(X^n+Y^n)=XY(X+Y)(X^2+XY+Y^2)^eE_n(X,Y), \quad (2.1)$$

и если $n=p>3$ — простое число, то

$$(X+Y)^p-(X^p+Y^p)=pXY(X+Y)(X^2+XY+Y^2)^eC_p(X,Y), \quad (2.2)$$

где $E_p(X,Y)=pC_p(X,Y)$ и $e=1$ или 2, в зависимости от того, сравнимо ли n с -1 или с 1 $\pmod 6$.

В математической литературе встречаются многочисленные доказательства этого утверждения (или его вариантов) (см., например, Кэли (1878), Глейшер (1878, 1879), Муир (1878), Каталан (1884, 1885, 1886), Люка (1888, 1891), Баризьен (1906), Топен и Реталь (1907), Урсус и Григорьев (1907), Кандидо (1907) и Брчич-Костич (1952)).

В 1878 г. Глейшер сформулировал это утверждение так.

(2B) *Если число n нечетно, то $(X-Y)^n+(Y-Z)^n+(Z-X)^n$ делится на*

$$\frac{1}{3}[(X-Y)^3+(Y-Z)^3+(Z-X)^3].$$

Если $n\equiv -1 \pmod 6$, то $(X-Y)^n+(Y-Z)^n+(Z-X)^n$ делится на

$$\frac{1}{2}[(X-Y)^2+(Y-Z)^2+(Z-X)^2].$$

Если же $n\equiv 1 \pmod 6$, то $(X-Y)^n+(Y-Z)^n+(Z-X)^n$ делится на

$$\frac{1}{2}[(X-Y)^4+(Y-Z)^4+(Z-X)^4].$$

Доказательство. Пусть A, B — переменные и число $n \geqslant 3$ нечетно. Тогда $AB(A+B)$ делит $(A+B)^n - A^n - B^n$.

Положим $A = Z-Y$, $B = X-Z$. Тогда $A+B = X-Y$ и многочлен $AB(A+B) = (Z-Y)(X-Z)(X-Y) = \frac{1}{3}[(Y-Z)^3+(Z-X)^3+(X-Y)^3]$ делит $(X-Y)^n + (Y-Z)^n + (Z-X)^n$. Далее,

$$\begin{aligned} A^2 + AB + B^2 &= (Z-Y)^2 + (Z-Y)(X-Z) + (X-Z)^2 \\ &= \frac{1}{2}[(Y-Z)^2 + (Z-X)^2 + (X-Y)^2] \end{aligned}$$

и

$$\begin{aligned} (A^2 + AB + B^2)^2 &= \frac{1}{4}[(Y-Z)^2 + (Z-X)^2 + (X-Y)^2]^2 \\ &= \frac{1}{2}[(Y-Z)^4 + (Z-X)^4 + (X-Y)^4]. \end{aligned}$$

Таким образом, из утверждения (2A) следует, что если $n \equiv -1 \pmod 6$, то многочлен $(X-Y)^n + (Y-Z)^n + (Z-X)^n$ делится на $\frac{1}{2}[(X-Y)^2 + (Y-Z)^2 + (Z-X)^2]$, а если $n \equiv 1 \pmod 6$, то $(X-Y)^n + (Y-Z)^n + (Z-X)^n$ делится на $\frac{1}{2}[(X-Y)^4 + (Y-Z)^4 + + (Z-X)^4]$. □

Следующее важное утверждение было в явном виде получено Каталаном (1884, 1885), Джероно (1885), Нестером (1907), Вельшем (1909) и Брокаром (1910).

(2C) *Пусть p — простое число. Тогда*

(1) *если* $(X+Y)^p - X^p - Y^p = pXY(X+Y)P^2$, *где* $P \in \mathbb{Z}[X,Y]$, *то* $p = 3$, $P = 1$ *или* $p = 7$, $P = X^2 + XY + Y^2$;

(2) *если* $2^{p-1} - 1 = pN^2$, *где число* N *целое, то* $p = 3$, $N = 1$ *или* $p = 7$, $N = 3$.

Доказательство. Докажем эти два утверждения одновременно. Во-первых, заметим, что $p \neq 2$. Полагая $X = Y = 1$, получим $2^p - - 2 = 2pN^2$, где $N = P(1,1) \in \mathbb{Z}$.

Если $p = 3$, то $N = 1$. Предположим теперь, что $p \neq 3$. Запишем соотношение $(2^{(p-1)/2} + 1)(2^{(p-1)/2} - 1) = pN^2$. Оба множителя в левой части нечетны, а следовательно, они взаимно просты. Значит, один из множителей является квадратом целого числа, а другой есть произведение простого числа p на квадрат целого числа.

Но $2^{(p-1)/2} - 1 \equiv 3 \pmod 4$, поскольку $(p-1)/2 \geqslant 2$, и, таким образом, $2^{(p-1)/2} - 1$ не является квадратом целого числа. Отсюда следует, что $2^{(p-1)/2} + 1 = M^2$, где число M целое. Так как $2^{(p-1)/2} =$

$= M^2 - 1 = (M-1)(M+1)$, числа $M-1$, $M+1$ являются степенями числа 2. Но $(M+1)-(M-1)=2$, а значит, $M-1=2$, $M=3$ и при этом $p=7$, $N=3$. Следовательно,

$$P^2 = \frac{(X+Y)^7 - X^7 - Y^7}{7XY(X+Y)} = (X^2+XY+Y^2)^2. \quad \square$$

Мы будем обозначать многочлен $C_p(X,1)$ через $C_p(X)$ и называть его *многочленом Коши* для простого числа $p \geqslant 5$. Если $p = 6k \pm 1$, то $C_p(X)$ имеет степень $6(k-1)$. Обратим внимание на следующие частные случаи:

$$\begin{aligned}
C_5(X,Y) &= 1,\\
C_7(X,Y) &= 1,\\
C_{11}(X,Y) &= X^6+3X^5Y+7X^4Y^2+9X^3Y^3+7X^2Y^4+3XY^5+Y^6\\
&= (X^2+XY+Y^2)^3+[XY(X+Y)]^2,\\
C_{13}(X,Y) &= X^6+3X^5Y+8X^4Y^2+11X^3Y^3+8X^2Y^4+3XY^5+Y^6\\
&= (X^2+XY+Y^2)^3+2[XY(X+Y)]^2.
\end{aligned}$$

Эти выражения от $XY(X+Y)$ и X^2+XY+Y^2 будут вскоре обобщены для произвольных значений p.

Многочлены Коши удовлетворяют следующим свойствам при $p = 6k \pm 1$ (см. Мириманов (1903), Клёсген (1970)).

(2D) *Пусть $C_p(X)$ — многочлен Коши. Тогда*

(1) $C_p(X) = X^{6(k-1)}C_p(1/X)$,
$C_p(X) = C_p(-1-X)$;

(2) $C_p(0) = C_p(-1) = 1$;

(3) *$C_p(X)$ не имеет действительных корней;*

(4) *все (мнимые) корни многочлена $C_p(X)$ просты и принадлежат непересекающимся множествам в количестве $k-1$, каждое из которых состоит из шести различных корней*

$$\left\{z, \frac{1}{z}, -(1+z), -\frac{1}{1+z}, -\frac{z}{1+z}, -\frac{1+z}{z}\right\}.$$

Доказательство. (1) Так как

$$C_p(X) = \frac{(X+1)^p - X^p - 1}{pX(X+1)(X^2+X+1)^e}$$

(где $e = 1$ или 2), мы получаем

$$C_p(1/X) = X^{-p+2e+3}C_p(X).$$

Поскольку

$$e = \begin{cases} 1, & \text{если} \quad p = 6k-1, \\ 2, & \text{если} \quad p = 6k+1, \end{cases}$$

справедливо равенство $C_p(X) = X^{6(k-1)}C_p(1/X)$. Точно так же получим, что $C_p(X) = C_p(-1-X)$.

(2) Так как $C_p(X)$ — симметричный многочлен со старшим коэффициентом 1, $C_p(0) = 1$. К тому же из утверждения п. (1) имеем $C_p(-1) = C_p(0) = 1$.

(3) Если $z > 0$ — действительный корень многочлена $C_p(X)$, то $(z+1)^p = z^p+1$, что невозможно. Если $z < -1$ — действительный корень многочлена $C_p(X)$, то число $-(1+z) > 0$ должно быть положительным действительным корнем многочлена $C_p(-1-X) = C_p(X)$, что противоречит предположению. И наконец, если z, $-1 < z < 0$, есть действительный корень многочлена $C_p(X)$, то число $1/z < -1$ тоже должно быть действительным корнем многочлена $C_p(X)$, что невозможно.

(4) Пусть z — произвольный корень многочлена $C_p(X)$. Из п. (1) следует, что числа $1/z$ и $-(1+z)$ тоже являются корнями многочлена $C_p(X)$, а значит, $-(1+1/z) = -(z+1)/z$, $-1/(1+z)$ и $-z/(z+1)$ также являются корнями этого многочлена. Множества корней, приведенные выше, либо совпадают, либо не пересекаются. В самом деле, если

$$t \in M_z = \left\{ z, \frac{1}{z}, -(1+z), -\frac{1}{1+z}, -\frac{z}{1+z}, -\frac{1+z}{z} \right\},$$

то, как легко проверить, $M_t = M_z$.

Пусть z — мнимый корень многочлена $C_p(X)$. Предположим, что он является корнем кратности два. Это возможно только тогда, когда z — корень многочлена C_p'. Так как

$$C_p'(X) = 6(k-1)X^{6(k-1)-1}C_p\left(\frac{1}{X}\right) - X^{6(k-1)-2}C_p'\left(\frac{1}{X}\right)$$

и $C_p'(X) = -C_p'(-1-X)$, числа $1/z$ и $-1-z$ тоже являются двукратными корнями, откуда следует, что каждый элемент множества M_z является корнем кратности два.

Дифференцируя тождество $(X+1)^p - X^p - 1 = pX(X+1)(X^2+X+1)^eC_p(X)$, получим

$$\begin{aligned}(X+1)^{p-1} - X^{p-1} &= (X(X+1)(X^2+X+1)^e)'C_p(X) \\ &\quad + X(X+1)(X^2+X+1)^eC_p'(X).\end{aligned}$$

Отсюда следует, что $(z+1)^{p-1} = z^{p-1}$, а значит, $(1+1/z)^{p-1} = 1$, т. е. $1+1/z$ является корнем из 1 кратности $(p-1)$ и, таким образом, $|1+1/z| = 1$.

Рассматривая сначала двукратный корень $-z/(1+z)$ (вместо z), получим, что $1+(-(1+z)/z) = -1/z$ также является корнем из 1 кратности $(p-1)$ и $|1/z| = 1$. Таким образом, все стороны треугольника с вершинами в точках $0, 1, \xi = -1/z$ имеют длину 1, т. е. он равносторонний, поэтому ξ является первообразным корнем из 1 степени 6. Значит, $\xi^2 - \xi + 1 = 0$ и $\xi^3 = -1$. Тогда число $-(z+1)/z = -1 - 1/z = -1 + \xi$ удовлетворяет равенству

$$(-1+\xi)^3 = -1 + 3\xi - 3\xi^2 + \xi^3 = -1 + 3\xi - 3\xi + 3 - 1 = 1,$$

поэтому многочлен $X^2 + X + 1$ является для этого числа минимальным. Так как $-(z+1)/z$ тоже является корнем многочлена $C_p(X)$, многочлен $X^2 + X + 1$ делит $C_p(X)$, что противоречит утверждению (2A). □

В 1903 г. Мириманов предположил, что многочлен $C_p(X)$ является неприводимым. В 1970 г. Клёсген проверил, используя ЭВМ, что для всех $p \leqslant 31$ многочлен Коши $C_p(X)$ неприводим над $\mathbb{Z}[X]$. Так как максимальное значение коэффициентов $C_p(X)$ с ростом p растет очень быстро, дальнейшие проверки не проводились.

Мы приведем без доказательства следующие результаты, полученные в 1997 г. Алу.

Если $n \geqslant 3$ — нечетное число, то для любого простого числа p многочлен C_n по модулю p приводим над полем из p элементов. Кроме того, если n — нечетное простое число и существует простое число p, такое, что C_n по модулю p имеет не менее трех делителей, то C_n неприводим. Алу приписывал Филасете доказательство того факта, что многочлен C_{2p} неприводим для любого нечетного простого числа p. Это доказательство представлено Алу в его работе 1997 г. Многочисленные результаты исследования многочленов Коши можно найти в работе Тержаняна (1989).

В дальнейшем нам потребуется другое выражение для многочленов Коши. Обобщая предыдущие рассуждения, мы будем рассматривать $S_n(X,Y) = (X+Y)^n + (-1)^n(X^n + Y^n)$ как многочлен от переменных $U = X^2 + XY + Y^2$ и $V = XY(X+Y)$.

Привести $S_n(X,Y)$ к такому виду можно двумя способами.

Можно рассмотреть многочлен третьей степени от переменной T, коэффициенты которого принадлежат $\mathbb{Z}[X,Y]$, а корнями

являются $X+Y, -X, -Y$:

$$\begin{aligned} F(T) &= (T+X)(T+Y)(T-X-Y) \\ &= T^3 + a_1T^2 + a_2T + a_3, \end{aligned}$$

где

$$\begin{cases} a_1 = X+Y-(X+Y) = 0, \\ a_2 = XY - X(X+Y) - Y(X+Y) = -(X^2+XY+Y^2), \\ a_3 = -XY(X+Y). \end{cases}$$

Тогда $S_n(X,Y) = (X+Y)^n + (-1)^n(X^n+Y^n)$ является суммой n-х степеней корней многочлена $F(T)$. Мы будем использовать следующее классическое выражение для суммы

$$p_n = x_1^n + \ldots + x_k^n \qquad (n = 0, 1, \ldots)$$

корней многочлена

$$T^k + a_1T^{k-1} + \ldots + a_k = \prod_{i=1}^{k}(T - x_i),$$

принадлежащее Варингу (1782) (см. лемму 2.1).

Частные случаи для $n = 1, 2, 3, 4$ были рассмотрены Жераром (1629) (см. также Зальшутц (1906)). Доказательство можно найти у Серре (1885), Люка (1891) и Перрона (1951). Современное алгебраическое доказательство было дано Редеем (1952, 1959). Другое доказательство, использующее степенные ряды, получили Чезаро и Ковалевская (1904).

Лемма 2.1. *Во введенных обозначениях*

$$p_n = n\prod_{i=1}^{n}\frac{(-1)^i}{i}\{(a_1+\ldots+a_k)^i\}_n,$$

где $\{(a_1+\ldots+a_k)^i\}_n$ — *сумма всех одночленов* $(i!/(i_1!\ldots i_k!))\times$ $\times a_1^{i_1}\ldots a_k^{i_k}$ (*с показателями* $i_1+\ldots+i_k = i$, $0 \leqslant i_1, \ldots, i_k$), *имеющая вес, равный* n, *то есть* $i_1 + 2i_2 + \ldots + ki_k = n$.

Следующее утверждение было доказано для четных степеней Феррерсом и Джексоном (1852, см. ссылку в книге Диксона «История теории чисел», т. II, с. 747). Доказательство для произвольной степени появилось в книге Тодхантера (1861). Это утверждение заново доказал Муир (1879), используя сформулированную выше лемму. Капферер (1949) вновь получил такое же доказательство для случая, когда n — простое число. В 1969 г. Карлиц и Хантер получили доказательство с использованием метода степенных рядов.

(2E) *Пусть* $n \geqslant 2$, $U = X^2 + XY + Y^2$ *и* $V = XY(X+Y)$. *Тогда*

$$(X+Y)^n + (-X)^n + (-Y)^n = \sum_r \frac{n}{n-2-2r}\binom{r}{n-3-2r} U^{3r-n+3} V^{n-2r-2}$$

(*суммирование производится по всем индексам* r, *для которых* $\max\{0, (n-3)/3\} \leqslant r \leqslant (n-2)/2$, *причем если число* n *четно и* $r = (n-2)/2$, *то коэффициент при слагаемом равен* 2).

Доказательство. Первое доказательство (Муир). По предыдущей лемме

$$\begin{aligned}
(X+Y)^n + (-X)^n + (-Y)^n &= \sum_{i=1}^{n} \frac{(-1)^i n}{i} \{(a_2 + a_3)^i\}_n \\
&= n \sum_{i=1}^{n} \frac{(-1)^i}{i} \sum_{\substack{i_2+i_3=i \\ 2i_2+3i_3=n}} \frac{i!}{i_2!\, i_3!} a_2^{i_2} a_3^{i_3} \\
&= n \sum_{i=1}^{n} (-1)^i \sum_{\substack{i_2+i_3=i \\ 2i_2+3i_3=n}} \frac{(i_2+i_3-1)!}{i_2!\, i_3!} a_2^{i_2} a_3^{i_3} \\
&= n \sum \frac{(i_2+i_3-1)!}{i_2!\, i_3!} (-a_2)^{i_2} (-a_3)^{i_3}
\end{aligned}$$

(суммирование ведется по всем i_2, i_3, таким, что $0 \leqslant i_2, i_3$; $1 \leqslant i_2 + i_3$; $2i_2 + 3i_3 = n$). Но $-a_2 = U$, $-a_3 = V$ и

$$\frac{(i_2+i_3-1)!}{i_2!\, i_3!} = \frac{1}{i_3}\binom{i_2+i_3-1}{i_3-1}$$

(это верно при $i_2 \neq 0$ или $i_3 \neq 0$). Пусть $i_2 + i_3 - 1 = r$. Тогда $n - 2 - 2r = (2i_2 + 3i_3) - 2(i_2 + i_3 - 1) - 2 = i_3$. Следовательно, $i_2 = 3r - n + 3$ и

$$(X+Y)^n + (-X)^n + (-Y)^n = \sum_r \frac{n}{n-2-2r}\binom{r}{n-3-2r} U^{3r-n+3} V^{n-2r-2},$$

причем суммирование ведется по всем индексам r, для которых $\max\{0, (n-3)/3\} \leqslant r \leqslant (n-2)/2$. Кроме того, если число n четно и $r = (n-2)/2$, то соответствующее слагаемое имеет коэффициент 2 (так как $i_2 = n/2$, $i_3 = 0$). □

Второе доказательство (Карлиц и Хантер). В этом доказательстве не используется лемма Варинга. Рассмотрим тождество

$$\frac{Z}{1-ZW}+\frac{X}{1-XW}+\frac{Y}{1-YW}$$
$$=\frac{(X+Y+Z)-2(XY+YZ+ZX)W+3XYZW^2}{1-(X+Y+Z)W+(XY+YZ+ZX)W^2-XYZW^3}.$$

Пусть $Z=-(X+Y)$; обозначим также $XY+YZ+ZX=-U$, $XYZ=-V$ и подставим новые обозначения в тождество, меняя знаки:

$$\frac{(X+Y)}{1+(X+Y)W}-\frac{X}{1-XW}-\frac{Y}{1-YW}=\frac{-2UW+3VW^2}{1-UW^2+VW^3}. \qquad (2.3)$$

Формальный степенной ряд для $1/(1-UW^2+VW^3)$ имеет вид

$$\begin{aligned}\frac{1}{1-UW+VW^3} &= \frac{1}{1-W^2(U-VW)}\\ &=\sum_{r=0}^{\infty}W^{2r}(U-VW)^r\\ &=\sum_{r=0}^{\infty}W^{2r}\left[\sum_{s=0}^{r}(-1)^s\binom{r}{s}U^{r-s}V^sW^s\right]\\ &=\sum_{n=0}^{\infty}(-1)^nW^n\sum_{r=0}^{\infty}\binom{r}{n-2r}U^{3r-n}V^{n-2r}\end{aligned}$$

(последняя сумма имеет смысл только при $n/3\leqslant r\leqslant n/2$, так что договоримся считать остальные слагаемые равными нулю). Левая часть соотношения (2.3) равна

$$\sum_{n=0}^{\infty}[X^{n+1}+Y^{n+1}-(-1)^n(X+Y)^{n+1}]W^n,$$

а правая часть равна

$$\sum_{n=0}^{\infty}(-1)^{n+1}W^{n+1}\sum_{r=0}^{\infty}2\binom{r}{n-2r}U^{3r+1-n}V^{n-2r}$$
$$+\sum_{n=0}^{\infty}(-1)^{n+2}W^{n+2}\sum_{r=0}^{\infty}3\binom{r}{n-2r}U^{3r-n}V^{n+1-2r}$$

$$= \sum_{n=0}^{\infty}(-1)^{n+1}W^{n+1}\sum_{r=0}^{\infty}2\binom{r}{n-2r}U^{3r+1-n}V^{n-2r}$$

$$+\sum_{n=1}^{\infty}(-1)^{n+1}W^{n+1}\sum_{r=0}^{\infty}3\binom{r}{n-1-2r}U^{3r+1-n}V^{n-2r}$$

$$= -2UW+3VW^2-2U^2W^3$$

$$+\sum_{n=3}^{\infty}(-1)^{n+1}W^{n+1}\sum_{r=0}^{\infty}\frac{n+1}{n-2r}\binom{r}{n-1-2r}U^{3r+1-n}V^{n-2r}$$

$$= -2UW+3VW^2-2U^2W^3$$

$$+\sum_{n=4}^{\infty}(-1)^{n}W^{n}\sum_{r=0}^{\infty}\frac{n+1}{n-1-2r}\binom{r}{n-2-2r}U^{3r+2-n}V^{n-1-2r},$$

поскольку

$$2\binom{r}{n-2r}+3\binom{r}{n-1-2r}=\frac{n+2}{n-2r}\binom{r}{n-1-2r}$$

(при $n \geqslant 3$). С другой стороны, левая часть соотношения (2.3) равна

$$\sum_{n=0}^{\infty}[(-1)^n(X+Y)^{n+1}-X^{n+1}-Y^{n+1}]W^n$$

$$=\sum_{n=2}^{\infty}[(X+Y)^n+(-X)^n+(-Y)^n](-1)^{n-1}W^{n-1}.$$

Сравнив две части равенства (2.3), приведенные выше, получаем наше утверждение. □

Отметим следующие особые случаи. Если показатель степени нечетен, то равенство примет вид

$$(X+Y)^{2k+1}-X^{2k+1}-Y^{2k+1} \tag{2.4}$$

$$=\sum_{\frac{2}{3}(k-1)\leqslant r\leqslant k-1}\frac{2k+1}{2k-1-2r}\binom{r}{2k-2-2r}U^{3r-2k+2}V^{2k-2r-1}.$$

Каждое простое число $p \neq 2,3$ можно представить в виде $p = 6k+1$ или $p = 6k-1$. Если $p \equiv 1 \pmod 6$, мы имеем (см. Люка (1897) и Карферер (1949))

$$(X+Y)^p-X^p-Y^p = pXY(X+Y)(X^2+XY+Y^2)^2 \tag{2.5}$$

$$\times\sum_{i=0}^{(p-7)/6}\binom{\frac{p-3}{2}-i}{2i}\frac{1}{2i+1}U^{(p-7)/2-3i}V^{2i},$$

а если $p \equiv -1 \pmod 6$, то

$$(X+Y)^p - X^p - Y^p = pXY(X+Y)(X^2+XY+Y^2) \times \sum_{i=0}^{(p-5)/6} \binom{\frac{p-3}{2}-i}{2i} \frac{1}{2i+1} U^{(p-5)/2-3i} V^{2i}. \tag{2.6}$$

Если показатель степени — четное число, мы получаем

$$(X+Y)^{2k} + X^{2k} + Y^{2k} = \sum_{(2k-3)/3 \leqslant r \leqslant k-1} \frac{k}{k-1-r} \binom{r}{2k-3-2r} U^{3r-2k+3} V^{2k-2r-2}. \tag{2.7}$$

В 1879 г., изучая и развивая идеи предшествовавших работ Глейшера (1878, 1879), Муир нашел следующее рекуррентное соотношение и изучил свойства делимости многочленов $S_n(X,Y)$.

(2F)

(1) *При $n \geqslant 0$ справедливо соотношение*

$$VS_n(X,Y) + US_{n+1}(X,Y) = S_{n+3}(X,Y).$$

(2) *При $n \geqslant 3$ справедливо соотношение*

$$6S_n(X,Y) = 3S_2(X,Y)S_{n-2}(X,Y) + 2S_3(X,Y)S_{n-3}(X,Y).$$

(3) *Если $n \equiv 0 \pmod 6$, то $U, V \nmid S_n(X,Y)$.*
Если $n \equiv 1 \pmod 6$, то $U^2V \mid S_n(X,Y)$.
Если $n \equiv 2 \pmod 6$, то $U \mid S_n(X,Y)$.
Если $n \equiv 3 \pmod 6$, то $V \mid S_n(X,Y)$.
Если $n \equiv 4 \pmod 6$, то $U^2 \mid S_n(X,Y)$.
Если $n \equiv 5 \pmod 6$, то $UV \mid S_n(X,Y)$.

Доказательство. (1) Пусть $n = 2m$. Заметив, что

$$\frac{2m}{2m-2r}\binom{r-1}{2m-1-2r} + \frac{2m+1}{2m+1-2r}\binom{r-1}{2m-2r} = \frac{2m+3}{2m+1-2r}\binom{r}{2m-2r},$$

и используя равенства (2.4) и (2.7), получим

$$VS_{2m}(X,Y) + US_{2m+1}(X,Y) = S_{2m+3}(X,Y).$$

Аналогичные рассуждения для $n = 2m+1$ позволяют показать, что

$$VS_{2m+1}(X,Y) + US_{2m+2}(X,Y) = S_{2m+4}(X,Y),$$

и убедиться в справедливости утверждения (1).

(2) Делая замену $S_2(X,Y) = 2U$ и $S_3(X,Y) = 3V$ и используя (1), получим

$$3S_2(X,Y)S_{n-2}(X,Y) + 2S_3(X,Y)S_{n-3}(X,Y)$$
$$= 6\,[VS_{n-3}(X,Y) + US_{n-2}(S,Y)] = 6S_n(X,Y).$$

(3) Утверждение немедленно следует из соотношений (2.4) и (2.7). □

Используя обобщение формулы Варинга, МакМагон в 1884 г. получил несколько новых алгебраических тождеств такого же вида.

Список литературы

1629 Girard, A., *Invention nouvelle en l'algèbre*, Amsterdam, 1629; reprinted by B. de Haan, Leyden, 1884.

1782 Waring, E., *Meditationes Algebraicae* (3rd ed.), Cambridge University Press, Cambridge, 1782.

1839 Lamé, G., *Mémoire sur le dernier théorème de Fermat*, C. R. Acad. Sci. Paris, **9** (1839), 45–46.

1839 Cauchy, A. and Liouville, J., *Rapport sur un mémoire de M. Lamé relatif au dernier théorème de Fermat*, C. R. Acad. Sci. Paris, **9** (1839), 359–363; reprinted in J. Math. Pures Appl., **5** (1840), 211–215; also in *Oeuvres Complètes*, (1), Vol. IV, pp. 499–504, Gauthier-Villars, Paris, 1911.

1840 Lamé, G., *Mémoire d'analyse indéterminée démontrant que l'équation $x^7 + y^7 = z^7$ est impossible en nombres entiers*, J. Math. Pures Appl., **5** (1840), 195–211.

1841 Cauchy, A., *Exercices d'analyse et de physique mathématique*, **2** (1841), 137–144 (Notes sur quelques théorèmes d'algèbre); *Oeuvres Complètes*, (2), Vol. XII, pp. 157–166, Gauthier-Villars, Paris, 1916.

1848 Ferrers, N.M. and Jackson, J.S., *Solutions of the Cambridge Senate-House Problems for 1848–1851*, pp. 83–85.

1861 Todhunter, I., *Theory of Equations*, Macmillan, London, 1861, pp. 173–176.

1878 Cayley, A., *An algebraic identity*, Messenger Math., (2), **8** (1878), 45–46.

1878 Glaisher, J.W.L., *Note on the above paper of Cayley*, Messenger Math., (2), **8** (1878), 46–47.

1878 Glaisher, J.W.L., *On a class of algebraic identities*, Messenger Math., (2), **8** (1878), 53–56.

1878 Glaisher, J.W.L., *Note on Cayley's theorem*, Messenger Math., (2), **8** (1878), 121.

1878 Glaisher, J.W.L., *Note on Cauchy's theorem relating to the factors of* $(x+y)^n - x^n - y^n$, Quart. J. Pure Appl. Math., **15** (1878), 365–366.

1878 Muir, T., *Cauchy's theorem regarding the divisibility of* $(x+y)^n + (-x)^n + (-y)^n$, Messenger Math., (2), **8** (1878), 119–120.

1879 Glaisher, J.W.L., *On Cauchy's theorem relating to the factors of* $(x+y)^n - x^n - y^n$, Quart. J. Pure Appl. Math., **16** (1879), 89–98.

1879 Muir, T., *On an expansion of* $(x+y)^n + (-x)^n + (-y)^n$, Quart. J. Pure Appl. Math., **16** (1879), 9–14.

1884 Catalan, E., *Question 1489*, Nouv. Ann. Math., (3), **3** (1884), 351.

1884 MacMahon, P.A., *Algebraic identities arising out of an extension of Waring's formula*, Messenger Math., **14** (1884), 8–11.

1885 Catalan, E., *Solution de la question 1489*, Nouv. Ann. Math., (3), **4** (1885), 520–521.

1885 Gérono, G.C., *Note du rédacteur sur l'article de Catalan*, Nouv. Ann. Math., (3), **4** (1885), 523–524.

1885 Serret, J.A., *Algèbre Supérieure*, Vol. I, p. 449 (5^e édition), Gauthier-Villars, Paris, 1885.

1886 Catalan, E., *Sur le dernier théorème de Fermat*, Mém. Soc. Roy. Sci. Liège, (2), **13** (1886), 387–397.

1886 Matthews, G.B., *A note in connexion with Fermat's last theorem*, Messenger Math., **15** (1886), 68–74.

1888 Lucas, E., *Sur un théorème de Cauchy*, Assoc. Française Avanc. Sci., Oran, 1888, pp. 29–31.

1891 Lucas, E., *Théorie des Nombres*, reprinted by A. Blanchard, Paris, 1961.

1897 Lucas, F., *Note relative à la théorie des nombres*, Bull. Soc. Math. France, **25** (1897), 33–35.

1903 Mirimanoff, D., *Sur l'équation* $(x+1)^l - x^l - 1 = 0$, Nouv. Ann. Math., (4), **3** (1903), 385–397.

1904 Cesàro, E. and Kowalewski, S., *Elementares Lehrbuch der algebraischen Analysis und der Infinitesimalrechnung*, Teubner, Leipzig, 1904.

1906 Barisien, E.N., *Questions 3076 et 3077*, L'Interm. Math., **13** (1906), 142.

1906 Saalschütz, L., *Albert Girard und die Waringsche Formel*, Arch. Math. Phys., (3), **12** (1906), 205–207.

1907 Nester, *Question 3230*, L'Interm. Math., **14** (1907), 126.
1907 Candido, G., *Sur la question 3230* (*de Nester*), L'Interm. Math., **14** (1907), 2.
1907 Taupin and Retall, V., *Sur la question 3077* (*de Barisien*), L'Interm. Math., **14** (1907), 36–39.
1907 Ursus and Grigorieff, E., *Sur la question 3077* (*de Barisien*), L'Interm. Math., **14** (1907), 93–95.
1909 Welsch, *Solution de la question 3230* (*de Nester*), L'Interm. Math., **16** (1909), 14–15.
1910 Brocard, H., *Sur la question 3230* (*de Nester*), L'Interm. Math., **17** (1910), 278–279.
1949 Kapferer, H., *Über ein Kriterium zur Fermatschen Vermutung*, Comment. Math. Helv., **23** (1949), 64–75.
1951 Perron, O., *Algebra*, Vol. I, W. de Gruyter, Berlin, 1951.
1952 Brčić-Kostić, M., *L'extension de la congruence* $(a+b)^n - a^n - b^n \equiv 0 \pmod{n}$ (*n un nombre premier*) (in Croatian, French summary), Hrvatsko Prirodoslovno Društvo, Glas. Mat. Ser. II, **7** (1952), 7–11.
1952 Rédei, L., *Kurzer Beweis der Waringschen Formel*, Acta Math. Acad. Sci. Hungar., **3** (1952), 151–153.
1959 Rédei, L., *Algebra*, Vol. I, Akademie Verlag, Geest & Portig, Leipzig, 1959.
1969 Carlitz, L. and Hunter, J.A.H., *Sums of powers of Fibonacci and Lucas numbers*, Fibonacci Quart., **7** (1969), 467–473.
1970 Klösgen, W., *Untersuchungen über Fermatsche Kongruenzen*, Gesellschaft Math. Datenverarbeitung, Bonn, Nr. 36, 1970, 124 pp.
1989 Terjanian, G., *Sur le loi de réciprocité des puissances l-èmes*, Acta Arith., **54** (1989), 87–125.
1997 Helou, C., *Cauchy–Mirimanoff polynomials*, C. R. Math. Rep. Acad. Sci. Canada, **19** (1997), 51–57.

Глава VIII

Переформулировки, следствия и критерии

В этой главе мы приводим ряд результатов, показывающих, насколько многочисленными были попытки решения проблемы Ферма. Это и эквивалентные формулировки теоремы Ферма, и следствия из нее, а также утверждения, выведенные из предположения, что теорема Ферма не выполнена для некоторого показателя.

VIII.1. Переформулировки и следствия из последней теоремы Ферма

В этом разделе содержатся утверждения, которые можно доказать исходя из справедливости последней теоремы Ферма. И наоборот, из некоторых из них следует последняя теорема Ферма.

A. Диофантовы уравнения, связанные с уравнением Ферма

Многие математики пытались связать уравнение Ферма с некоторым диофантовым уравнением. Мы последовательно опишем результаты, полученные В. А. Лебегом, Кристиллем, Перреном, Гурвицем и Капферером. Также мы кратко обсудим уравнения Фрея, сыгравшие центральную роль в недавнем подходе Уайлса к решению проблемы Ферма.

A1. Лебег

Первый результат из этой серии, описанный в литературе, принадлежит В. А. Лебегу (1840). Заново он был получен Теркемом в 1846 г. и еще раз Поклингтоном в 1913 г.

(1A) *Если последняя теорема Ферма справедлива для показателя* $n \geqslant 3$, *то уравнение* $X^{2n} + Y^{2n} = Z^2$ *имеет лишь тривиальные решения.*

Доказательство. Предположим, что отличные от нуля натуральные числа x, y, z таковы, что $x^{2n} + y^{2n} = z^2$. Легко видеть, что мы без ограничения общности можем считать числа x, y, z попарно взаимно простыми. Более того, числа x, y не могут быть одновременно нечетными, так как иначе выполнялось бы сравнение $z^2 \equiv 2 \pmod 4$, а это неверно. Поэтому мы можем считать, например, что x четно, а y нечетно, и тогда z нечетно.

Пусть $x = 2^a x'$, причем $a \geqslant 1$, x' нечетно, $x' > 0$. Тогда $(z+y^n)\times$ $\times(z - y^n) = z^2 - y^{2n} = x^{2n} = 2^{2an} x'^{2n}$. Заметим, что НОД$(z + y^n, z - y^n) = 2$, следовательно,

$$\begin{cases} z \pm y^n = 2r^{2n}, \\ z \mp y^n = 2^{2an-1} s^{2n}, \end{cases}$$

причем числа r, s нечетны и положительны, НОД$(r, s) = 1$.

Складывая и вычитая эти соотношения, получим

$$\begin{cases} z = r^{2n} + 2^{2an-2} s^{2n}, \\ \pm y^n = r^{2n} - 2^{2an-2} s^{2n} = (r^n - 2^{an-1} s^n)(r^n + 2^{an-1} s^n). \end{cases}$$

Так как НОД$(r^n - 2^{an-1} s^n, r^n + 2^{an-1} s^n) = 1$, мы получаем

$$\begin{cases} r^n + 2^{an-1} s^n = t^n, & t > 0, \\ r^n - 2^{an-1} s^n = \pm u^n, & u \geqslant 0. \end{cases}$$

Таким образом,

$$t^n \mp u^n = 2^{an} s^n = (2^a s)^n.$$

По предположению должно выполняться равенство $u = 0$, а значит, число $r^n = 2^{an-1} s^n$ нечетно, так что $an = 1$, чего быть не может. □

Как следствие Лиувилль в 1840 г. (см. также Теркем (1846)) доказал такой результат.

(1B) *Если последняя теорема Ферма справедлива для показателя* $n \geqslant 3$, *то уравнение* $X^{2n} - Y^{2n} = 2Z^n$ *имеет лишь тривиальные решения.*

Доказательство. Предположим, что x, y, z — отличные от нуля целые числа, такие, что $x^{2n} - y^{2n} = 2z^n$. Пусть $t = y^{2n} + z^n$. Тогда $t - z^n = y^{2n}$ и $t + z^n = x^{2n}$. Следовательно, $t^2 - z^{2n} = (xy)^{2n}$, так что $z^{2n} + (xy)^{2n} = t^2$.

Согласно (1A) должно выполняться равенство $t = 0$, а тогда непременно $z = 0$, чего быть не может. □

A2. Кристилль

Следующий результат был доказан Кристиллем в 1967 г. Предварительно докажем такую лемму.

Лемма 1.1. *Уравнение $X^3 + Y^3 + Z^3 = 3XYZ$ имеет решение в целых числах x, y, z тогда и только тогда, когда $x + y + z = 0$ или $x = y = z$.*

Доказательство. Легко проверить, что справедливо тождество

$$X^3 + Y^3 + Z^3 - 3XYZ \tag{1.1}$$
$$= (X + Y + Z)(X^2 + Y^2 + Z^2 - XY - YZ - ZX).$$

Таким образом, $x^3 + y^3 + z^3 = 3xyz$ тогда и только тогда, когда $x + y + z = 0$ или $x^2 + y^2 + z^2 = xy + yz + zx$.

Однако для любых целых чисел x, y уравнение $Z^2 - (x + y)Z + (x^2 + y^2 - xy) = 0$ имеет лишь решения $z = ((x+y) \pm (x-y)\sqrt{-3})/2$, которые являются целыми в точности тогда, когда $x = y$, а в этом случае $x = y = z$. □

(1C) *Пусть $n \geqslant 3$. Тогда следующие утверждения равносильны:*

(1) *последняя теорема Ферма справедлива для показателя n;*

(2) *все отличные от нуля целочисленные решения (x, y, z) уравнения $X^{3n} + Y^{3n} + Z^{3n} = 3X^nY^nZ^n$ задаются соотношением $x = y = z$.*

Доказательство. (1) ⇒ (2) Предположим, что x, y, z — отличные от нуля целые числа, не все равные друг другу, такие, что $x^{3n} + y^{3n} + z^{3n} = 3x^ny^nz^n$. По лемме имеем $x^n + y^n + z^n = 0$.

(2) ⇒ (1) Предположим, что отличные от нуля целые числа x, y, z таковы, что $x^n + y^n + z^n = 0$. Тогда равенство $x = y = z$ невозможно, и по лемме мы получаем $x^{3n} + y^{3n} + z^{3n} = 3x^ny^nz^n$. □

В той же статье Кристилль указал следующее достаточное условие для теоремы Ферма.

(1D) *Пусть $n \geqslant 3$. Тогда если уравнение $X^{5n} + Y^{5n} + Z^{5n} = 5X^nY^nZ^n(Z^{2n} - X^nY^n)$ не имеет решений в отличных от нуля целых числах, то последняя теорема Ферма справедлива для показателя n.*

Доказательство. Предположим, что отличные от нуля целые числа x, y, z таковы, что $x^n + y^n + z^n = 0$. Тогда

$$-z^{5n} = (x^n+y^n)^5 = x^{5n}+y^{5n}+5x^ny^n(x^{3n}+y^{3n})+10x^{2n}y^{2n}(x^n+y^n).$$

Отсюда

$$x^{5n} + y^{5n} + z^{5n} = -5x^ny^n[x^{3n} + y^{3n} - 3x^ny^nz^n + x^ny^nz^n].$$

Согласно тождеству (1.1) и предположению мы получаем

$$x^{3n} + y^{3n} + z^{3n} = 3x^ny^nz^n,$$

следовательно,

$$x^{5n} + y^{5n} + z^{5n} = 5x^ny^nz^n[z^{2n} - x^ny^n],$$

причем $x, y, z \neq 0$, что и доказывает наше утверждение. □

A3. Перрен

В 1885 г. Перрен доказал такой факт, связанный с кубическим уравнением Ферма.

(1E) *Следующие утверждения справедливы и равносильны:*

(1) *последняя теорема Ферма выполнена для показателя* 3;

(2) *для всех натуральных чисел* n *уравнение*

$$X^3 + Y^3 + 3^{3n-1}Z^3 = 2 \times 3^n XYZ \tag{1.2}$$

не имеет решений в отличных от нуля целых числах x, y, z, *не кратных трем.*

Доказательство. (1) $\Rightarrow$ (2) Предположим, что существуют натуральное число n и отличные от нуля целые числа x, y, z, $3 \nmid xyz$, удовлетворяющие уравнению (1.2). Пусть

$$\begin{cases} a = x(3^nyz - x^2), \\ b = y(3^nxz - y^2), \\ c = 3^nz(xy - 3^{2n-1}z^2). \end{cases}$$

Из условий $x, y, z \neq 0$ и $3 \nmid xyz$ следует, что $abc \neq 0$. Возведя обе части уравнения (1.2) в квадрат и в куб, получим

$$x^6+y^6+3^{6n-2}z^6+2x^3y^3+2\times3^{3n-1}x^3z^3+2\times3^{3n-1}y^3z^3 = 4\times3^{2n}x^2y^2z^2$$

и

$$\begin{aligned} x^9 + y^9 + 3^{9n-3}z^9 + 3x^6y^3 + 3x^3y^6 + 3^{3n}x^6z^3 \\ +2 \times 3^{3n}x^3y^3z^3 + 3^{3n}y^6z^3 + 3^{6n-1}x^3z^6 + 3^{6n-1}y^3z^6 \\ = 8 \times 3^{3n}x^3y^3z^3. \end{aligned}$$

Далее, мы имеем

$$a^3 = x^3(3^{3n}y^3z^3 - 3^{2n+1}x^2y^2z^2 + 3^{n+1}x^4yz - x^6),$$
$$b^3 = y^3(3^{3n}x^3z^3 - 3^{2n+1}x^2y^2z^2 + 3^{n+1}xy^4z - y^6),$$
$$c^3 = 3^{3n}z^3(x^3y^3 - 3^{2n}x^2y^2z^2 + 3^{4n-1}xyz^4 - 3^{6n-3}z^6).$$

Сложив эти равенства, с учетом уравнения (1.2) и предыдущих соотношений получим

$$a^3 + b^3 + c^3 = 0.$$

(2) $\Rightarrow$ (1) Предположим, что существуют отличные от нуля целые числа a, b, c, такие, что $a^3 + b^3 + c^3 = 0$. Можно считать, что числа a, b, c попарно взаимно просты. Из тождества

$$(X + Y + Z)^3 = X^3 + Y^3 + Z^3 + 3(X + Y)(Y + Z)(Z + X)$$

следует, что

$$(a + b + c)^3 = 3(a + b)(b + c)(c + a).$$

Но числа $a + b$, $b + c$, $c + a$ также попарно взаимно просты: например, если простое число p делит $a + b$ и $b + c$, то, так как p делит $a + b + c$, оно делит и c, и a, что противоречит предположению.

Следовательно, ровно один из множителей, скажем, $a + b$, делится на 3 и непременно существуют целые числа $n \geqslant 1$, x, y, z, такие, что

$$\begin{cases} a + b = 3^{3n-1}z^3, \\ b + c = x^3 \end{cases}$$

и $3^n xyz = a + b + c$. Таким образом,

$$x^3 + y^3 + 3^{3n-1}z^3 = 2(a + b + c) = 2 \times 3^n xyz.$$

Наконец, $x, y, z \neq 0$ (если, например, $z = 0$, то $a = -b$, откуда следует, что $c = 0$) и $3 \nmid xyz$, поскольку числа $a + b$, $b + c$, $c + a$ попарно взаимно просты. □

A4. Гурвиц

В 1908 г. Гурвиц занимался изучением диофантова уравнения

$$X^mY^n + Y^mZ^n + Z^mX^n = 0, \tag{1.3}$$

где $m > n > 0$ и НОД$(m, n) = 1$, что не ограничивает общности. Он доказал следующий результат.

(1F) *Уравнение* (1.3) *имеет лишь тривиальные решения тогда и только тогда, когда теорема Ферма справедлива для показателя* $m^2 - mn + n^2$.

Доказательство. Пусть x, y, z — отличные от нуля целые числа, такие, что $x^m y^n + y^m z^n + z^m x^n = 0$. Можно считать, что НОД$(x, y, z) = 1$.

Пусть $u = $ НОД(y, z), $v = $ НОД(z, x), $w = $ НОД(x, y). Тогда числа u, v, w попарно взаимно просты. Следовательно, произведение vw делит x, так что $x = x_1 vw$, где x_1 — целое число. Аналогично $y = y_1 wu$, $z = z_1 uv$, причем y_1, z_1 — целые числа. Более того, числа x_1, y_1, z_1 попарно взаимно просты. Подставив эти выражения в уравнение и разделив на $u^n v^n w^n$, получим

$$x_1^m y_1^n v^{m-n} w^m + y_1^m z_1^n w^{m-n} u^m + z_1^m x_1^n u^{m-n} v^m = 0.$$

Таким образом, u^{m-n} делит $x_1^m y_1^n v^{m-n} w^m$. Но НОД$(u, v) = 1$, НОД$(u, w) = 1$ и НОД$(u, x) = 1$, следовательно, НОД$(u, x_1) = 1$. Значит, u^{m-n} делит y_1^n. С другой стороны, y_1^n делит $z_1^m x_1^n u^{m-n} v^m$. Число y_1 взаимно просто с x_1, z_1 и v, поэтому y_1^n делит u^{m-n}. Следовательно, $y_1^n = \pm u^{m-n}$.

Аналогичным образом, $x_1^n = \pm w^{m-n}$, $z_1^n = \pm v^{m-n}$. Из условия НОД$(m, n) = 1$ следует, что НОД$(n, m-n) = 1$, а значит, $x_1 = w_1^{m-n}$, $y_1 = u_1^{m-n}$, $z_1 = v_1^{m-n}$ для некоторых целых чисел u_1, v_1, w_1, таких, что $u = \pm u_1^n$, $v = \pm v_1^n$, $w = \pm w_1^n$. Отсюда мы получаем

$$w_1^{(m-n)m} u_1^{(m-n)n} v_1^{(m-n)n} w_1^{mn} \pm u_1^{(m-n)m} v_1^{(m-n)n} w_1^{(m-n)n} u_1^{mn} \pm v_1^{(m-n)m} w_1^{(m-n)n} u_1^{(m-n)n} v_1^{mn} = 0.$$

Умножив на $u_1^{n^2-mn} v_1^{n^2-mn} w_1^{n^2-mn}$ и заметив, что число $m^2 - mn + n^2$ нечетно, получим уравнение

$$w_1^{m^2-mn+n^2} + (\pm u_1)^{m^2-mn+n^2} + (\pm v_1)^{m^2-mn+n^2} = 0.$$

Обратно, если отличные от нуля целые числа u, v, w удовлетворяют соотношению

$$u^{m^2-mn+n^2} + v^{m^2-mn+n^2} + w^{m^2-mn+n^2} = 0,$$

то, умножив на $u^{mn} v^{mn} w^{mn}$, получим

$$u^{m^2+n^2} v^{mn} w^{mn} + v^{m^2+n^2} u^{mn} w^{mn} + w^{m^2+n^2} u^{mn} v^{mn} = 0.$$

Положив

$$\begin{cases} x = v^n w^m, \\ y = w^n u^m, \\ z = u^n v^m, \end{cases}$$

получим $x^m y^n + y^m z^n + x^m x^n = 0$. □

В частности, при $m = 3$, $n = 1$ отсюда следует, что уравнение

$$X^3Y + Y^3Z + Z^3Y = 0$$

имеет лишь тривиальные решения.

A5. Капферер

В 1933 г. Капферер опубликовал доказательство того факта, что последняя теорема Ферма справедлива для показателя $n \geqslant 3$ тогда и только тогда, когда уравнение

$$Z^3 - Y^2 = 3^3 \times 2^{2n-2} X^{2n} \tag{1.4}$$

не имеет решений в отличных от нуля попарно взаимно простых целых числах x, y, z.

Доказательство Капферера содержало ошибку, частично исправленную Рибенбоймом (о чем он сообщил Инкери). Инкери сформулировал и доказал (без ошибок) нижеследующие результаты. Комментарии на эту тему, сделанные Ганди и Стаффом (1975), были не точны.

Начнем с частного случая $n = 3$, рассмотренного Фюетером (1930).

(1G) *Уравнение*

$$Z^3 - Y^2 = 3^3 \times 2^4 X^6 \tag{1.5}$$

не имеет решений в отличных от нуля целых числах x, y, z, *для которых* $\text{НОД}(y, z) = 1$.

Доказательство. Предположим, что x, y, z — отличные от нуля целые числа, такие, что $\text{НОД}(y, z) = 1$ и

$$z^3 - y^2 = 3^3 \times 2^4 x^6.$$

Пусть

$$\begin{cases} u = 6^2 x^3 + y, \\ v = 6^2 x^3 - y, \\ w = 6xz. \end{cases}$$

Тогда $u, v, w \in \mathbb{Z}$, $w \neq 0$. Покажем, что $u \neq 0$, $v \neq 0$. Если $u = 0$, то $6^2 x^3 = -y$, следовательно, $y \neq \pm 1$. Если простое число p делит y, то $p \mid 6x$, а значит, $p \mid z$, что противоречит предположению о том, что $\text{НОД}(y, z) = 1$. Аналогично $v \neq 0$.

Наконец, $u^3 + v^3 = (6^2 x^3 + y)^3 + (6^2 x^3 - y)^3 = 2 \times 6^6 x^9 + 6^3 x^3 y^2 = = 6^3 x^3 (2 \times 6^3 x^6 + y^2) = 6^3 x^3 z^3 = w^3$, а это невозможно. Полученное противоречие завершает доказательство. □

Аналогичным образом можно показать, что не существует целых чисел $x, y, z \neq 0$, таких, что НОД$(y, z) = 1$ и $z^3 - 3y^2 = 2^4 x^6$.

Приведем теперь критерий Инкери, являющийся исправлением опубликованного ранее утверждения Капферера (1933). Он также основан на родственном уравнении

$$Z^3 - 3Y^2 = 2^{2n-2} X^{2n}. \tag{1.6}$$

(1H) *Пусть $n \geqslant 3$ — нечетное целое число. Тогда следующие утверждения равносильны:*

(1) *последняя теорема Ферма справедлива для показателя n;*

(2) *уравнения* (1.4) *и* (1.6) *не имеют решений в отличных от нуля целых числах x, y, z, для которых* НОД$(y, z) = 1$.

Доказательство. (1) $\Rightarrow$ (2) Предположим, что существуют отличные от нуля целые числа x, y, z, такие, что НОД$(y, z) = 1$ и $z^3 - y^2 = 3^3 \times 2^{2n-2} x^{2n}$. Пусть

$$\begin{cases} a = y, \\ b = 3 \times 2^{n-1} x^n, \\ c = z. \end{cases}$$

Тогда $a^2 + 3b^2 = c^3$. Следовательно, число c нечетно и НОД$(a, b) = 1$, потому что НОД$(a, c) =$ НОД$(y, z) = 1$.

В силу леммы 4.7 гл. I существуют целые числа $r, s \neq 0$, такие, что НОД$(r, 3s) = 1$, $r \not\equiv s \pmod 2$ и выполняются соотношения

$$\begin{cases} a = r(r^2 - 9s^2), \\ b = 3s(r^2 - s^2), \\ c = r^2 + 3s^2. \end{cases}$$

Тогда

$$2^{n-1} x^n = \frac{b}{3} = s(r^2 - s^2) = s(r - s)(r + s).$$

Так как $x \neq 0$, числа s, $r - s$, $r + s$ отличны от нуля. Более того, s четно, потому что $r \not\equiv s \pmod 2$. Поскольку НОД$(r, s) = 1$, числа s, $r - s$, $r + s$ попарно взаимно просты. Поэтому существуют отличные от нуля целые числа u, v, w, такие, что $2s = w^n$, $r - s = u^n$, $-r - s = v^n$. Тогда $u^n + v^n + w^n = 0$. Заметим, что $u, v, w \neq 0$ и НОД$(u, v, w) = 1$.

Теперь предположим, что существуют отличные от нуля целые числа x, y, z, такие, что $\text{НОД}(y, z) = 1$ и $z^3 - 3y^2 = 2^{2n-2}x^{2n}$. Пусть

$$\begin{cases} a = 2^{n-1}x^n, \\ b = y, \\ c = z. \end{cases}$$

Тогда $a^2 + 3b^2 = c^3$, причем число c снова нечетно и $\text{НОД}(a, b) = 1$.

В силу леммы 4.7 гл. I существуют отличные от нуля целые числа r, s, такие, что $\text{НОД}(r, 3s) = 1$, $r \not\equiv s \pmod 2$ и выполняются соотношения

$$\begin{cases} a = r(r^2 - 9s^2), \\ b = 3s(r^2 - s^2), \\ c = r^2 + 3s^2. \end{cases}$$

Тогда

$$2^{n-1}x^n = a = r(r - 3s)(r + 3s).$$

Заметим, что число r непременно четно, так как $r - 3s$, $r + 3s$ нечетны. Отсюда следует, что числа r, $r - 3s$, $r + 3s$ попарно взаимно просты. Таким образом, существуют отличные от нуля целые числа u, v, w, такие, что $2r = w^n$, $-r + 3s = u^n$, $-r - 3s = v^n$ и, следовательно, $u^n + v^n + w^n = 0$, причем $u, v, w \neq 0$, $\text{НОД}(u, v, w) = 1$.

(2) $\Rightarrow$ (1) Предположим, что отличные от нуля целые числа u, v, w таковы, что $u^n + v^n + w^n = 0$. Можно без ограничения общности предполагать, что u, v, w попарно взаимно просты, число w четно, а u и v нечетны. Пусть $s = w^n/2$ и $r = u^n + s$. Тогда $2s = w^n$, $r - s = u^n$, $-r - s = v^n$. Положим

$$\begin{cases} a = r(r^2 - 9s^2), \\ b = 3s(r^2 - s^2), \\ c = r^2 + 3s^2. \end{cases}$$

Тогда $a^2 + 3b^2 = c^3$ и $b = 3s(r^2 - s^2) = -3 \times 2^{n-1}\left(\frac{1}{2}uvw\right)^n$. Положив

$$\begin{cases} x = \frac{1}{2}uvw, \\ y = a, \\ z = c, \end{cases}$$

получим $z^3 - y^2 = 3^3 \times 2^{2n-2}x^{2n}$. Из условия $\text{НОД}(u, v) = 1$ по предположению мы получаем $\text{НОД}(r, s) = 1$ и $x \neq 0$. Итак, число w четно, откуда следует, что s четно, поэтому y нечетно, а значит, $y \neq$ $\neq 0$. Далее, $3 \nmid uvw$ тогда и только тогда, когда $3 \mid r$. Действительно,

если $3 \nmid uvw$, то $3 \nmid s(r^2-s^2)$, откуда следует, что непременно $3 \mid r$, и наоборот, если $3 \mid r$, учитывая то обстоятельство, что $\text{НОД}(r,s)=1$, получим $3 \nmid s(r^2-s^2)$, а значит, $3 \nmid uvw$.

Теперь покажем, что $\text{НОД}(y,z)=1$. Проведем доказательство в несколько этапов.

(a) Число s четно и $\text{НОД}(r,s)=1$, значит, число r нечетно. Тогда $\text{НОД}(r^2-s^2, r^2-9s^2)=1$. В самом деле, если $p \mid (r^2-s^2)$ и $p \mid (r^2-9s^2)$, то $p \neq 2$ и $p \mid 8r^2$, $p \mid 8s^2$, откуда следует, что $p \mid \text{НОД}(r,s)=1$, а это невозможно.

(b) Справедливы равенства $\text{НОД}(r, r^2-s^2) = \text{НОД}(s, r^2-9s^2)=1$, потому что $\text{НОД}(r,s)=1$.

(c) Таким образом, $\text{НОД}(a, b/3)=1$. Из условий $x \mid b/3$ и $y=a$ следует, что $\text{НОД}(x,y)=1$. Число y нечетно, значит, и $\text{НОД}(2x,y)=1$. Далее, $\text{НОД}(a,b)=1$ или 3. Говоря более точно, $\text{НОД}(a,b)=1$ при $3 \nmid r$ и $\text{НОД}(a,b)=3$ при $3 \mid r$. Заметим, что $3 \mid r$ тогда и только тогда, когда $3 \mid r(r^2-9s^2)=a$, а это равносильно условию $3 \nmid uvw$.

Аналогично $\text{НОД}(y,z)=\text{НОД}(a,c)=1$ или 3 в зависимости от того, делится ли число r на 3. Действительно, если p — простое число, $e \geqslant 1$ и $p^e \mid \text{НОД}(a,c)$, то, учитывая равенство $a^2+3b^2=c^3$, получим, что $p^2 \mid 3b^2$, откуда следует, что $p \mid b$, поэтому $p=3$, $\text{НОД}(a,b)=3$ и $3^2 \nmid c$, а это значит, что если $\text{НОД}(a,c) \neq 1$, то $\text{НОД}(a,c)=3$ и $3 \mid r$. Обратно, если $3 \mid r$, то $\text{НОД}(a,b)=3$, откуда следует, что $3^2 \nmid c$, а кроме того, как и выше, $\text{НОД}(a,c)=3$.

Если $\text{НОД}(y,z)=3$, то y делится на 9. Положим $x_1=x$, $y_1=y/9$, $z_1=z/3$. Тогда $z_1^3-3y_1^2=2^{2n-2}x_1^{2n}$, причем $x_1, y_1, z_1 \neq 0$, $\text{НОД}(y_1, z_1)=1$. Это завершает доказательство. □

Далее нам потребуется то обстоятельство, что (во введенных обозначениях) $\text{НОД}(2x,y)=1$.

Приведем еще один подобный результат.

(1I) *Пусть $n \geqslant 3$. Тогда следующие утверждения равносильны:*

(1) *последняя теорема Ферма справедлива для показателя n;*

(2) *уравнение (1.4) не имеет решений в отличных от нуля целых числах x, y, z, таких, что $\text{НОД}(2x,y)=1$.*

Доказательство. (1) $\Rightarrow$ (2) Предположим, что $x,y,z \neq 0$, $\text{НОД}(2x,y)=1$ и $z^3-y^2=3^3 \times 2^{2n-2}x^{2n}$. Если p — простое число и $p \mid \text{НОД}(y,z)$, то $p \nmid 2x$, следовательно, $p=3$, так что $3^3 \mid y^2$, а значит, $9 \mid y$. Пусть $x_1=x$, $y_1=y/9$, $z_1=z/3$. Тогда

$z_1^3 - 3y_1^2 = 2^{2n-2}x_1^{2n}$, причем $x_1, y_1, z_1 \neq 0$, НОД$(y_1, z_1) = 1$. Как следует из доказательства импликации (1) $\Rightarrow$ (2) утверждения (1H), существуют числа $u, v, w \neq 0$, такие, что $u^n + v^n + w^n = 0$.

(2) $\Rightarrow$ (1) Предположим, что $u, v, w \neq 0$, НОД$(u, v, w) = 1$ и $u^n + v^n + w^n = 0$. Как следует из доказательства импликации (2) $\Rightarrow$ (1) утверждения (1H) и сделанного после него замечания, найдутся такие числа $x, y, z \neq 0$, что НОД$(2x, y) = 1$ и $z^3 - y^2 = 3^3 \times 2^{2n-2}x^{2n}$. □

Изучим связь между уравнением (1.4) и уравнением Ферма более подробно.

(1J) *Предположим, что уравнение* (1.4) *не имеет решений в отличных от нуля взаимно простых целых числах. Если* $u, v, w \neq 0$, НОД$(u, v, w) = 1$ *и* $u^n + v^n = w^n$, *то*

(1) *показатель* n *нечетен,* $u \equiv v \equiv -w \pmod 3$, $3 \nmid uvw$;

(2) *если простое число* p *делит* n, *то* $p \equiv 1 \pmod 6$.

Доказательство. (1) Как следует из доказательства импликации (2) $\Rightarrow$ (1) утверждения (1H), существуют отличные от нуля целые числа x, y, z, такие, что $z^3 - y^2 = 3^3 \times 2^{2n-2}x^{2n}$, причем НОД$(y, z) = 3$ и $3 \nmid uvw$.

В силу утверждения (4L) гл. VI число n нечетно, а значит, $u^n + v^n + (-w)^n = 0$. Пусть $r = u^n$, $s = -v^n$. Тогда $r, s \neq 0$, $r \neq s$ (так как $w \neq 0$). Поскольку $3 \nmid w$, мы получаем $r \not\equiv s \pmod 3$. Следовательно, $u \equiv u^n = r \not\equiv s = -v^n \equiv -v \pmod 3$. Так как $3 \nmid uv$, должно выполняться сравнение $u \equiv v \pmod 3$. С учетом симметрии получаем $u \equiv v \equiv -w \pmod 3$.

(2) Пусть простое число p делит показатель n, $n = pt$, $u_1 = u^t$, $v_1 = v^t$, $w_1 = w^t$. Тогда $u_1^p + v_1^p + (-w_1)^p = 0$, причем НОД$(u_1, v_1, w_1) = 1$, $u_1 \equiv v_1 \equiv -w_1 \pmod 3$. В силу утверждения (2A) гл. VI имеем $p \equiv 1 \pmod 6$. □

Инкери с помощью неэлементарных методов (а именно методов теории полей классов) показал, что при сделанных допущениях справедливо сравнение $3^p \equiv 3 \pmod{p^2}$, которому простые числа удовлетворяют довольно редко.

Теперь уместно указать ряд фактов, касающихся уравнения

$$Z^3 - Y^2 = c. \tag{1.7}$$

(Подробности можно найти в книге Рибенбойма, 1994.) Эйлер в 1738 г. доказал, что если $c = \pm 1$, то единственным решением урав-

нения (1.7) в целых числах, больших 1, является $y = 3, z = 2$. В 1929 г. Зигель, используя глубокие аналитические методы, доказал, что для каждого числа c существует не более чем конечное число решений уравнения (1.7).

Следующий результат будет доказан с помощью утверждения (1H).

(1K) *Если* $c = 3^3 \times 2^{2n-2}x^{2n}$, *где* $n \geqslant 3$, $x = 1$, p *или* pq (*простые числа* p, q *различны*), *то уравнение* (1.7) *не имеет решений в отличных от нуля взаимно простых целых числах* y, z.

Доказательство. Предположим, что y, z — отличные от нуля взаимно простые целые числа, такие, что $z^3 - y^2 = 3^3 \times 2^{2n-2}x^{2n}$. Как следует из доказательства импликации (1) $\Rightarrow$ (2) утверждения (1H), справедливо соотношение $2^{n-1}x^n = s(r^2 - s^2)$, причем $r, s \not\equiv 0$, $r \not\equiv s \pmod 2$, НОД$(r, s) = 1$. Но тогда НОД$(r, r^2 - s^2) = 1$ и, очевидно, $r^2 - s^2 \neq 1$.

Если $x = 1$, то $r = \pm 1$, $r^2 - s^2 = \pm 2^{n-1}$, откуда следует, что $s^2 = 2^{n-1} + 1$, а это невозможно.

Если $x = p$, то $2^{n-1}p^n = r(r^2 - s^2)$. При $p = 2$ мы приходим к противоречию с помощью изложенного выше рассуждения. Если же $p \neq 2$, то или $r = 2^{n-1}$, $r^2 - s^2 = p^n$, или наоборот, $p^n = 2^{n-1}$, $r^2 - s^2 = r$. В первом случае $r - s = \pm 1$, $r + s = \pm p^n$ (или $r - s = \pm p^n$, $r + s = \pm 1$); в обоих случаях мы получим противоречивое равенство вида $2^n = \pm(p^n + 1)$ или аналогичное противоречивое равенство.

Если $x = pq$, причем одно из чисел p или q равно 2, то воспользуемся предыдущим рассуждением. Если оба числа p, q нечетны, то $2^{n-1}p^nq^n = r(r-s)(r+s)$. Если $r = \pm p^n$, то $r - s = \pm 2^{n-1}$, $r + s = \pm q^n$ (или $\mp q^n$) или наоборот, $r + s = \pm 2^{n-1}$, $r - s = \pm q^n$ (или $\mp q^n$), и $2p^n = \pm(2^{n-1} \pm q^n)$, что невозможно. Аналогично $r \neq \pm q^n$. Остается случай $r = \pm 2^{n-1}$, $r - s = \pm p^n$, $r + s = \pm q^n$ (с подходящими знаками), следовательно, $2^n = \pm p^n \pm q^n$. Но в силу утверждения (3B) гл. VI это невозможно. □

Статья Яхьи (1973), в которой он опубликовал доказательство последней теоремы Ферма, содержала ряд изъянов, одним из которых было использование неверного результата Капферера. Яхья также связал уравнение Ферма с другим диофантовым уравнением. Инкери изучил эту взаимосвязь и корректно доказал такое утверждение.

(1L) *Пусть $n \geqslant 3$. Тогда следующие утверждения равносильны:*

(1) *последняя теорема Ферма справедлива для показателя n;*

(2) *уравнение*

$$2^{2n-2}X^3 - Y^2X - Z^n = 0 \tag{1.8}$$

не имеет решений в отличных от нуля целых числах x, y, z, таких, что $\text{НОД}(z, y) = \text{НОД}(y, 2z) = 1$.

A6. Фрей

Эльгуарш (1972) связал гипотетическое решение уравнения Ферма с показателем $2p^n$ (где $n \geqslant 1$ и p — простое число) с эллиптической кривой. Целью было показать отсутствие на эллиптической кривой точек определенного порядка.

В 1986 г. Фрей независимо высказал ту же идею, состоящую в том, чтобы сопоставить каждому решению уравнения Ферма эллиптическую кривую. Если a, b — отличные от нуля взаимно простые целые числа, $n > 3$ и a четно, то ***кривая Фрея*** задается уравнением

$$Y^2 = X(X - a^n)(X + b^n). \tag{1.9}$$

Фрей изучил свойства этой эллиптической кривой. Рибет и Уайлс рассматривали эту кривую исходя из предположения, что существует отличное от нуля целое число c, такое, что $a^n + b^n = c^n$. Использование неэлементарных методов теории эллиптических кривых, модулярных форм и представлений Галуа привело к противоречию, означающему, таким образом, справедливость последней теоремы Ферма. Мы вернемся к этому разговору в эпилоге.

B. Переформулировки последней теоремы Ферма

Следующие утверждения, которые равносильны теореме Ферма, были сформулированы Пересом-Качо в 1946 г. Равносильность утверждений (1), (2), (3) и (4) была впервые доказана Бендцем в 1901 г. Впоследствии этот результат независимо доказали Краснер, опубликовавший свою статью в 1939 г. (см. также Ривуар (1968)), и Човла в 1978 г. (см. также Инкери (1984)). В 1909 г. Линд указал некоторые частные случаи.

(1M) *Пусть $m \geqslant 2$, $n = 2m - 1$. Тогда следующие утверждения равносильны.*

(1) *Уравнение $X^n + Y^n = Z^n$ имеет лишь тривиальные решения в целых числах.*

(2) *Уравнение* $X(1+X) = T^n$ *имеет лишь тривиальные решения в* $\mathbb{Q}$.

(3) *Уравнение* $X^2 = 4Y^n + 1$ *имеет лишь тривиальные решения в* $\mathbb{Q}$.

(4) *Уравнение* $X^2 = Y^{n+1} - 4Y$ *имеет лишь тривиальные решения в* $\mathbb{Q}$.

(5) *Для любого отличного от нуля рационального числа* a *многочлен* $Z^2 - a^m Z + a$ *неприводим над* $\mathbb{Q}$.

(6) *Уравнение* $(XY)^m = X + Y$ *имеет лишь тривиальные решения в* $\mathbb{Q}$.

(7) *Уравнение* $X^m = X/Y + Y$ *имеет лишь тривиальные решения в* $\mathbb{Q}$.

(8) *Если рациональные числа* u_1, r *отличны от нуля и числа* $u_1, u_2, \ldots$ *образуют геометрическую прогрессию со знаменателем* r, *то* $u_m^2 - u_1 + r \neq 0$.

(9) *Если в треугольнике* ABC *угол* A *прямой, длина стороны* AB *равна* 2 *и сумма длин сторон* $AB + BC$ *является* n*-й степенью рационального числа, то длина стороны* AC *иррациональна.*

***Более** того, из этих условий следует, что*

(10) ***касательные к параболе*** $Y^2 = 4X$ ***в каждой рациональной точке, отличной от вершины, пересекают кривую*** $Y = X^m$ ***в иррациональных точках.***

Доказательство. (1) $\Rightarrow$ (2) Пусть отличные от нуля целые числа a, b, c, d таковы, что $b > 0$, $d > 0$, $\text{НОД}(a, b) = \text{НОД}(c, d) = 1$ и $(a/b)(1 + a/b) = (c/d)^n$. Тогда $a(a+b)/b^2 = c^n/d^n$. Следовательно, $a(a + b) = c^n$, $b^2 = d^n$. Так как показатель n нечетен, $b = y^n$ для некоторого целого числа y. Так как $\text{НОД}(a, a + b) = 1$, найдутся такие ненулевые целые числа y, z, что $a = x^n$, $a + b = z^n$. Таким образом, $x^n + y^n = z^n$.

(2) $\Rightarrow$ (3) Пусть x, y — отличные от нуля рациональные числа, такие, что $x^2 = 4y^n + 1$. Тогда $x \neq \pm 1$ и $((x-1)/2)((x-1)/2+1) = y^n$.

(3) $\Rightarrow$ (4) Если x, y — отличные от нуля рациональные числа, такие, что $x^2 = y^{n+1} - 4y$, то, разделив на $y^{n+1} = y^{2m}$, получим равенство

$$\left(\frac{x}{y^m}\right)^2 = 1 + 4\left(\frac{-1}{y}\right)^n.$$

(4) $\Rightarrow$ (5) Дискриминант трехчлена $Z^2 - a^m Z + a$ равен $a^{n+1} - 4a \neq 0$ (так как n нечетно). По предположению число $a^{n+1} - 4a$

не является квадратом, следовательно, многочлен $Z^2 - a^m Z + a$ не имеет корней в $\mathbb{Q}$.

(5) $\Rightarrow$ (6) Пусть отличные от нуля рациональные числа x, y таковы, что $(xy)^m = x + y$. Положим $xy = a$. Тогда трехчлен $Z^2 - a^m Z + a$ имеет рациональный корень.

(6) $\Rightarrow$ (7) Пусть x, y — отличные от нуля рациональные числа, такие, что $x^m = x/y + y$. Положим $t = x/y$. Тогда $t + y = (ty)^m$.

(7) $\Rightarrow$ (1) Пусть отличные от нуля целые числа a, b, c таковы, что $a^n + b^n = c^n$. Положим $x = c^2/ab$ и $y = cb^{m-1}/a^m$. Тогда

$$\frac{x}{y} + y = \frac{ca^{m-1}}{b^m} + \frac{cb^{m-1}}{a^m} = \frac{c(a^n + b^n)}{a^m b^m} = \left(\frac{c^2}{ab}\right)^m = x^m.$$

(3) $\Rightarrow$ (8) Предположим, что $u_m^2 = u_1 - r$. Из равенства $u_m = u_1 r^{m-1}$ следует, что уравнение $r^{2(m-1)} Z^2 - Z + r$ имеет рациональный корень u_1 и, таким образом, его дискриминант является квадратом, т. е. $1 - 4r^{2m-1} = s^2$. Следовательно, пара $(s, -r)$ удовлетворяет уравнению $X^2 = 4Y^n + 1$.

(8) $\Rightarrow$ (3) Доказательство обратного утверждения аналогично. В самом деле, если отличные от нуля рациональные числа x, y таковы, что $4y^n + 1 = x^2$, то уравнение $y^{2(m-1)} Z^2 - Z - y = 0$ имеет рациональный корень u_1. Пусть $u_i = u_1(-y)^{i-1}$. Тогда $u_m^2 = u_1^2 y^{2(m-1)} = u_1 + (-y)$.

(5) $\Leftrightarrow$ (9) Условие (5) равносильно тому, что $a^{2m} - 4a$ не является квадратом в $\mathbb{Q}$, т. е. $a^{2n} - 4a^n$ не является квадратом в $\mathbb{Q}$, или, иначе говоря, уравнение $(a^{m-1} Z)^2 = a^{2n} - 4a^n$ не имеет рациональных решений для всех рациональных чисел $a \neq 0$. Прибавив к левой и правой частям равенства 4, получим, что это условие эквивалентно отсутствию рациональных решений уравнения

$$4 + (a^{m-1} Z)^2 = (a^n - 2)^2,$$

что, в свою очередь, равносильно утверждению (9).

(7) $\Rightarrow$ (10) Пусть $(x_1, y_1) \neq (0, 0)$ — рациональная точка параболы $Y^2 = 4X$. Касательная к параболе в этой точке задается уравнением

$$y_1 Y = 2(X + x_1),$$

то есть

$$y_1 Y = 2\left(X + \frac{y_1^2}{4}\right),$$

следовательно,

$$Y = \frac{2}{y_1} X + \frac{y_1}{2}.$$

Эта касательная пересекается с кривой $Y = X^m$ в точках (x, y), таких, что $y = (2/y_1)x + y_1/2$, $y = x^m$. Таким образом, $(x, y_1/2)$ является решением уравнения $X^m = X/Y + Y$. В силу утверждения (7) число x должно быть иррациональным. □

В 1958 г. Перес-Качо доказал такой факт.

(1N) *Пусть $n \geqslant 2$. Тогда между множествами F и F' существует биекция, где*

(F) *— множество таких решений (x, y, z) уравнения $X^n + Y^n = Z^n$, что отличные от нуля натуральные числа x, y, z попарно взаимно просты;*

(F′) *— множество таких решений (u, v, w, t) уравнения $U^n + V^{2n} = W^n + T^{2n}$, что u, v, w, t — отличные от нуля натуральные числа,* $\text{НОД}(u, v) = \text{НОД}(w, t) = \text{НОД}(v, t) = 1$, *причем $w = v \cdot \text{НОД}(u, w)$, $u = t \cdot \text{НОД}(u, w)$, $t \neq v$.*

Доказательство. Пусть $(x, y, z) \in F$. Положим $u = xz$, $v = y$, $w = yz$, $t = x$. Тогда $v \neq t$, так как $x \neq y$, потому что $2x^n$ не является n-й степенью. Далее, $u^n + v^{2n} = x^n z^n + y^{2n} = x^n(x^n + y^n) + y^{2n} = (x^n + y^n)y^n + x^{2n} = y^n z^n + x^{2n} = w^n + t^{2n}$.

Итак, $u, v, w, t \neq 0$, $\text{НОД}(u, v) = \text{НОД}(w, t) = \text{НОД}(v, t) = 1$, $z = \text{НОД}(u, w)$ и $u = t \cdot \text{НОД}(u, w)$, $w = v \cdot \text{НОД}(u, w)$. Следовательно, $(u, v, w, t) \in F'$.

Обратно, пусть $(u, v, w, t) \in F'$. Положим $x = t$, $y = v$, $z = \text{НОД}(u, w)$. Тогда $w = vz = yz$, $u = tz = xz$ и $x^{2n} - y^{2n} = t^{2n} - v^{2n} = u^n - w^n = (x^n - y^n)z^n$. Из условия $t \neq v$ следует, что $x^n + y^n = z^n$.

Ясно, что установленное соответствие между множествами (F) и (F′) является взаимно однозначным. □

В 1979 г. Врэнчеану указал чуть менее интересное утверждение, равносильное последней теореме Ферма для показателя n.

Приведем теперь эквивалентную комбинаторную (!) формулировку последней теоремы Ферма, появившуюся в короткой заметке Квайна (1989).

Рассмотрим множество, состоящее из $n \geqslant 3$ шаров, которые требуется распределить по z корзинам, окрашенным в белый, синий или красный цвет.

Пусть

$W =$ числу белых корзин,
$B =$ числу синих корзин,
$R =$ числу красных корзин.

Тогда $z = W + B + R$. Пусть, далее,

$(r'b) =$ числу таких размещений n шаров по корзинам, что красные корзины остаются пустыми, но не все синие корзины пусты;
$(rb') =$ числу таких размещений n шаров по корзинам, что синие корзины пусты, а хотя бы в одной красной что-то есть;
$(rb) =$ числу таких размещений n шаров по корзинам, что не все синие и красные корзины пусты;
$(w) =$ числу таких размещений n шаров по корзинам, что все шары сосредоточены в белых корзинах.

Докажем следующий критерий.

(1О) *Последняя теорема Ферма справедлива для показателя n тогда и только тогда, когда $(w) \neq (rb)$ для всех множеств из z корзин.*

Доказательство. Так как число всех размещений из n шаров по z корзинам равно z^n, мы получаем

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

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

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

Аналогично 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, $(rb) \neq (w)$.

С другой стороны, если последняя теорема Ферма не справедлива для показателя $n \geqslant 3$, обозначим через x, y, z такие натуральные числа, что $x^n + y^n = z^n$. Пусть числа W, B, R определяются из равенств

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

Согласно изложенному рассуждению $(w) = (rb)$. □

Список литературы

1738 Euler, L., *Theorematum quorundam arithmeticorum demonstrationes*, Comm. Acad. Sci. Petrop., **10** (1738), 125–146; reprinted in *Opera Omnia*, Commentationes Arithmeticae, Vol. I, pp. 38–58, Teubner, Leipzig, 1915.

1840 Lebesgue, V.A., *Sur un théorème de Fermat*, J. Math. Pures Appl., **5** (1840), 184–185.

1840 Liouville, J., *Sur l'équation* $Z^{2n} - Y^{2n} = 2X^n$, J. Math. Pures Appl., **5** (1840), 360.

1846 Terquem, O., *Théorèmes sur les puissances des nombres*, Nouv. Ann. Math., **5** (1846), 70–78.

1885 Perrin, R., *Sur l'équation indéterminée* $x^3 + y^3 = z^3$, Bull. Soc. Math. France, **13** (1885), 194–197.

1901 Bendz, T.R., *Öfver Diophantiska Ekvationen* $x^n + y^n = z^n$, Almqvist & Wiksells Boktryckeri, Uppsala, 1901, 35 pp.

1908 Hurwitz, A., *Über die diophantische Gleichung* $x^3y + y^3z + z^3x = 0$, Math. Ann., **65** (1908), 428–430; reprinted in *Math. Werke*, Vol. II, pp. 427–429, Birkhäuser, Basel, 1963.

1909 Lind, B., *Einige zahlentheoretische Sätze*, Arch. Math. Phys., (3), **15** (1909), 368–369.

1913 Pocklington, H.C., *Some diophantine impossibilities*, Proc. Cambridge Philos. Soc., **17** (1913), 108–121.

1929 Siegel, C.L., *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Berlin, Phys. Math. Kl., **1** (1929), 57 pp.

1930 Fueter, R., *Über kubische diophantische Gleichungen*, Comment. Math. Helv., **2** (1930), 69–89.

1933 Kapferer, H., *Über die diophantischen Gleichungen* $Z^3 - Y^2 = 3^3 \cdot 2^\lambda \cdot X^{\lambda+2}$ *und deren Abhängigkeit von der Fermatschen Vermutung*, Heidelberger Akad., Math. Naturwiss. Klasse, Abh., **2** (1933), 32–37.

1939 Krasner, M., *Sur le théorème de Fermat*, C. R. Acad. Sci. Paris, **208** (1939), 1468–1471.

1946 Pérez-Cacho, L., *El último teorema de Fermat y los números de Mersenne*, Rev. Real Acad. Cienc. Exact. Fiis. y Natur., Madrid, **40** (1946), 39–57.

1958 Pérez-Cacho, L., *Sobre algunas cuestiones de la teoria de números*, Rev. Mat. Hisp.-Amer., (4), **18** (1958), 10–27 and 113–124.

1967 Christilles, W.E., *A note concerning Fermat's conjecture*, Amer. Math. Monthly, **74** (1967), 292–294.

1968 Rivoire, P., *Dernier Théorème de Fermat et Groupes de Classes dans Certains Corps Quadratiques Imaginaires*, Thèse, Université Clermont-Ferrand, 1968, 59 pp.; reprinted in Ann. Sci. Univ. Clermont-Ferrand II, **68** (1979), 1–35.

1972 Hellegouarch, Y., *Courbes Elliptiques et Équation de Fermat*, Thesis, Univiversité Besançon, 1972.

1973 Yahya, Q.A.M.M., *On general proof of Fermat's last theorem*, Portugal. Math., **32** (1973), 157–170.

1975 Gandhi, J.M. and Stuff, M., *Comments on certain results about Fermat's last theorem*, Notices Amer. Math. Soc., **22** (1975), A-502.

1978 Chowla, S., L-series and elliptic curves, Part 4, On Fermat's last theorem. *Number Theory Day*, Springer Lecture Notes, No. 626, pp. 19–24, Springer-Verlag, New York, 1978.

1979 Vrănceanu, G., *Une interprétation géométrique du théorème de Fermat*, Rev. Roumaine Math. Pures Appl., **24** (1979), 1137–1140.

1984 Inkeri, K., *On certain equivalent statements for Fermat's last theorem – with requisite corrections*, Ann. Univ. Turkuenis, Ser. AI, **186** (1984) 12–22; reprinted in *Collected Papers* of Kustaa Inkeri (editor P. Ribenboim), Queen's Papers in Pure and Applied Mathematics, Vol. 91, Kingston, Ontario, 1992.

1986 Frey, G., *Elliptic curves and solutions of* $A - B = C$, in: Sém. Th. Nombres, Paris, 1985–1986 (editor C. Goldstein), Progress in Math., Birkhäuser, Boston, 1986, pp. 39–51.

1987 Frey, G., *Links between elliptic curves and solutions of* $A - B = C$, J. Indian Math. Soc., **51** (1987), 117–145.

1989 Quine, W.V., *Fermat's last theorem in combinatorial form*, Amer. Math. Monthly, **95** (1989), 626.

1994 Ribenboim, P., *Catalan's Conjecture*, Academic Press, Boston, 1994.

VIII.2. Различные утверждения, связанные с последней теоремой Ферма

В этом разделе собран ряд разнообразных результатов, доказанных элементарными методами. Для удобства читателя мы разбили излагаемый материал на подразделы.

A. Связь с функцией Эйлера.
B. Связь с функцией Мёбиуса.
C. Отсутствие нетривиальных решений в арифметической прогрессии.
D. Связь с символом Лежандра.
E. Связь с дискриминантом.
F. Связь с кубическим сравнением.
G. Связь с определителем.
H. Связь с бинарной квадратичной формой.
I. Отсутствие алгебраических соотношений между решениями уравнения Ферма.
J. Связь с линейными рекуррентными последовательностями второго порядка.
K. Возмущение показателя.
L. Условие делимости для пифагоровых троек.

A. Связь с функцией Эйлера

Первый результат в несколько более слабой форме был доказан Пересом-Качо в 1928 г.

(2A) *Пусть x, y — отличные от нуля взаимно простые целые числа, число $n \geqslant 2$ целое и простое число p делит n, $n = pm$. Пусть, далее, целое число $z \geqslant 3$ таково, что z делит $x^n \pm y^n$, но z не делит $x^m \pm y^m$. Тогда p делит $\varphi(z)$.*

Доказательство. Если $p = 2$, то утверждение справедливо, так как $z \geqslant 3$, а значит, $\varphi(z)$ четно.

Пусть теперь простое число p нечетно, $n = pm$ и $p \nmid \varphi(z)$. Тогда существуют целые числа r, s, такие, что $rp - s\varphi(z) = 1$. Число $\varphi(z)$ четно, значит, r нечетно.

Если предположить, что $x^{pm} \equiv -y^{pm} \pmod z$, но $x^m \not\equiv -y^m \pmod z$, то $x^{rpm} \equiv -y^{rpm} \pmod z$, следовательно, $x^{(s\varphi(z)+1)m} \equiv -y^{(s\varphi(z)+1)m} \pmod z$. Справедливы соотношения $\text{НОД}(z, x) = \text{НОД}(z, y) = 1$. Действительно, если простое число q делит, например, x и z, то оно делит и $x^n + y^n$, а значит, и y, что противоречит предположению. По теореме Эйлера $x^{\varphi(z)} \equiv y^{\varphi(z)} \equiv 1 \pmod z$, следовательно, $x^m \equiv -y^m \pmod z$, что также противоречит предположению.

Для случая $z \mid (x^n - y^n)$, $z \nmid (x^m - y^m)$ доказательство аналогично. □

В частности, если НОД $(x, y) = 1$ и $p \mid n$, то, положив $z = x^n \pm y^n$, получим, что $p \mid \varphi(x^n \pm y^n)$. Более того, как показал Перес-Качо, это утверждение справедливо и при НОД $(x, y) = d \neq 1$. Действительно, пусть $x = dx_1$, $y = dy_1$. Тогда НОД $(x_1, y_1) = 1$ и $p \mid \varphi(x_1^n \pm y_1^n)$, но $x^n \pm y^n = d^n(x_1^n \pm y_1^n)$, так что $p \mid \varphi(x^n \pm y^n)$.

Как следствие имеем результат Свистака (1969).

(2B) *Если простое число p нечетно и натуральные числа x, y, z, $x < y < z$, таковы, что $x^p + y^p = z^p$, то p делит $\varphi(x)$, $\varphi(y)$ и $\varphi(z)$.*

Доказательство. Без ограничения общности можно считать, что числа x, y, z попарно взаимно просты, потому что если, например, $x = dx_1$ и $p \mid \varphi(x_1)$, то $p \mid \varphi(x)$.

Справедливы условия $3 \leqslant z$, $z \mid (x^p + y^p)$ и $z \nmid (x + y)$. В самом деле, $z^p = x^p + y^p < (x+y)^p$, следовательно, $z < x+y < 2z$. Согласно утверждению (2A) мы получаем $p \mid \varphi(z)$.

Аналогично $x \mid (z^p - y^p)$, $x \nmid (z-y)$, поскольку $z - y < x$. Далее,

$$x^p = (z-y)\left(z^{p-1} + pz^{p-2}y + \binom{p}{2} z^{p-3}y^2 + \ldots + y^{p-1}\right)$$
$$> 2^{p-1}p > 2^p,$$

следовательно, $x \geqslant 3$. В соответствии с утверждением (2A) мы вновь заключаем, что $p \mid \varphi(x)$.

Наконец, $y \mid (z^p - x^p)$, $y \nmid (z - x)$, так как $z - x < y$ и $3 \leqslant x < y$, откуда также следует, что $p \mid \varphi(y)$. □

Бусси в 1943 г. отметил такое следствие.

(2C) *Пусть x, y, z — попарно взаимно простые натуральные числа и простое число p таково, что $p \nmid xyz$ и $x^p + y^p = z^p$. Тогда существуют простые числа q, r, s, такие, что $q \equiv r \equiv s \equiv 1 \pmod p$ и $q \mid x$, $r \mid y$, $s \mid z$.*

Доказательство. Согласно утверждению (2B) число p делит $\varphi(x)$, $\varphi(y)$, $\varphi(z)$. Из условия $p \nmid xyz$ следует, что существуют простые числа q, r, s, такие, что $p \mid (q-1)$, $p \mid (r-1)$, $p \mid (s-1)$ и $q \mid x$, $r \mid y$, $s \mid z$. □

Этот результат также является и следствием утверждения (1B) гл. III. В 1932 г. Бусси отметил еще одно утверждение.

(2D) *Пусть $n > 2$ и попарно взаимно простые натуральные числа x, y, z таковы, что $x^n + y^n = z^n$. Если целое число k таково, что $\varphi(k) = n$, то* НОД $(k, xyz) > 1$.

Доказательство. Если НОД$(k, xyz) = 1$, то $x^{\varphi(k)} \equiv y^{\varphi(k)} \equiv z^{\varphi(k)} \equiv 1 \pmod{k}$. Но $\varphi(k) = n$, а значит, $1 \equiv z^n = x^n + y^n \equiv 2 \pmod{k}$, чего быть не может. □

B. Связь с функцией Мёбиуса

В 1969 г. Рамесвар Рао доказал следующее утверждение.

(2E) *Если число $n \geqslant 3$ нечетно и натуральные числа x, y, z таковы, что $x^n + y^n = z^n$, то значение функции Мёбиуса μ[1] от суммы $x + y$ равно нулю.*

Доказательство. Число n нечетно, поэтому сумма $x + y$ делит $x^n + y^n = z^n$. Всякое простое число p, делящее $x + y$, делит и z^n, а значит, и z.

Если $\mu(x+y) \neq 0$, то $x+y$ не делится на квадрат простого числа, так что $x+y$ делит z, в частности, $x+y \leqslant z$. Это противоречит тому, что $z < x + y$. □

C. Отсутствие нетривиальных решений в арифметической прогрессии

Следующий результат принадлежит Боттари (1907). Позднее он был доказан Гольдзихером (1913), Михальинечем (1952) и Рамесваром Рао (1969). В 1908 г. Каттанео получил следующее изящное доказательство, которое в точности и повторил Рамесвар Рао.

(2F) *Если $n > 2$ и натуральные числа x, y, z таковы, что $x^n + y^n = z^n$, то x, y, z не могут быть последовательными членами арифметической прогрессии.*

Доказательство. Предположим противное. Пусть существует натуральное число a, такое, что $x = y - a$, $z = y + a$. Тогда

$$(y - a)^n + y^n = (y + a)^n. \tag{2.1}$$

При необходимости разделив на наибольший общий делитель чисел a и y, будем считать, что НОД$(a, y) = 1$. Ясно также, что y не может быть нечетным. Из соотношения (2.1) следует, что $y^n = am$,

[1] Функция натурального аргумента $\mu(n)$, определяемая равенствами

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } p^2 \mid n, \\ (-1)^r, & \text{если } n \text{ есть произведение } r \text{ различных простых чисел,} \end{cases}$$

называется функцией Мёбиуса (см. разд. II.2). — *Прим. ред.*

где m — некоторое целое число. Из условия НОД$(a, y) = 1$ следует, что $a = 1$, а значит, $(y-1)^n + y^n = (y+1)^n$.

Заметим, что число n не может быть нечетным, иначе выполнялось бы равенство

$$y^n = 2\left[\binom{n}{1}y^{n-1} + \binom{n}{3}y^{n-3} + \ldots + \binom{n}{n-2}y^2 + 1\right]$$

и, так как y четно, мы получили бы, что нечетное число в квадратных скобках делится на 2^{n-1}.

Так как n четно, разделив на y, получим[2]

$$y^{n-1} = 2\left[\binom{n}{1}y^{n-2} + \binom{n}{3}y^{n-4} + \ldots + \binom{n}{n-1}\right],$$

т. е. $y^{n-1} = 2l$, где l — целое число. Следовательно, $y/2$ делит l. Поскольку $y/2$ делит все слагаемые в скобках, кроме последнего, отсюда следует также, что $y/2$ делит и $\binom{n}{n-1} = n$, а значит, $y \leqslant 2n$.

Таким образом, $y^{n-1} > 2\binom{n}{1}y^{n-2} \geqslant y^{n-1}$. Полученное противоречие завершает доказательство. □

D. Связь с символом Лежандра

В 1958 г. Перес-Качо доказал следующий признак.

(2G) *Пусть p — нечетное простое число. Пусть, далее, для всяких отличных от нуля взаимно простых целых чисел x, y, z существует такое простое число q, что $q \neq p$, $q \mid \left(z^2 - pxy\right)$ и*

$$\left(\frac{p^{p+1} - 4p}{q}\right) = -1.$$

Тогда последняя теорема Ферма справедлива для показателя p.

Доказательство. Предположим, что существуют отличные от нуля взаимно простые целые числа x, y, z, такие, что $x^p + y^p = z^p$. По условию существует простое число q, $q \neq p$, такое, что q делит $z^2 - pxy$ и $\left((p^{p+1} - 4p)/q\right) = -1$.

Из равенства $z^{2p} = x^{2p} + 2x^p y^p + y^{2p}$ следует, что

$$z^{2(p+1)} - 4z^2x^py^p = z^2(x^{2p} - 2x^py^p + y^{2p}) = [z(x^p - y^p)]^2.$$

---

[2] При четном n в предыдущем равенстве последний член в квадратных скобках имеет вид $\binom{n}{n-1}y$. — *Прим. ред.*

Пусть число k определяется из равенства $z^2 = pxy + kq$. Тогда

$$\begin{aligned}(p^{p+1} - 4p)(xy)^{p+1} &= (z^2 - kq)^{p+1} - 4(xy)^p(z^2 - kq)\\ &\equiv z^{2(p+1)} - 4z^2x^py^p\\ &\equiv [z(x^p - y^p)]^2 \pmod q.\end{aligned}$$

Число $p+1$ четно, значит, $p^{p+1} - 4p$ является квадратом по модулю q, чего быть не может. □

E. Связь с дискриминантом

В 1949 г. Капферер указал признак, связанный с дискриминантом некоторого многочлена. Для доказательства этого результата нам потребуется ряд фактов, касающихся результанта и дискриминанта бинарных форм, которые приведены в разд. II.4.

Капферер воспользовался следующей леммой, которая содержится в его статье вместе с доказательством.

ЛЕММА 2.1. *Пусть $F(X,Y)$, $G(X,Y)$ — бинарные формы степеней n, m соответственно, а формы $L(X,Y)$, $M(X,Y)$ имеют степень k, и пусть*

$$\Phi(X,Y) = F(L(X,Y), M(X,Y))$$

(форма степени kn),

$$\Gamma(X,Y) = G(L(X,Y),\ M(X,Y))$$

(форма степени km). Тогда

$$R(\Phi,\Gamma) = [R(F,G)]^k\,[R(L,M)]^{mn}.$$

ДОКАЗАТЕЛЬСТВО. Если $n = 0$ или $m = 0$, то утверждение очевидно, поэтому будем считать, что $n \geqslant 1$, $m \geqslant 1$.

Пусть $F(X,Y) = \prod_{i=1}^n(\alpha_i'X - \alpha_iY)$, где коэффициенты α_i, α_i' не равны одновременно нулю для всех $i = 1,\dots,n$. Таким образом, $\Phi(X,Y) = F(L,M) = \prod_{i=1}^n(\alpha_i'L - \alpha_iM)$. Аналогично, если $G(X,Y) = \prod_{j=1}^m(\beta_j'X - \beta_jY)$, то $\Gamma(X,Y) = \prod_{j=1}^m(\beta_j'L - \beta_jM)$.

Тогда в силу утверждения (4A) гл. II мы получаем

$$R(\Phi,\Gamma) = \prod_{i=1}^n\prod_{j=1}^m R(\alpha_i'L - \alpha_iM,\ \beta_j'L - \beta_jM).$$

Пусть, например, $\beta_j \neq 0$. Тогда

$$\begin{aligned} R(\alpha_i' L - \alpha_i M,\, \beta_j' L - \beta_j M) \\ &= \frac{1}{\beta_j^k} R(\beta_j \alpha_i' L - \beta_j \alpha_i M,\, \beta_j' L - \beta_j M) \\ &= \frac{1}{\beta_j^k} R\left((\beta_j \alpha_i' - \alpha_i \beta_j') L,\, \beta_j' L - \beta_j M\right) \\ &= \frac{(\beta_j \alpha_i' - \alpha_i \beta_j')^k}{\beta_j^k} R(L,\, \beta_j' L - \beta_j M) \\ &= \frac{(-1)^k (\beta_j' \alpha_i - \beta_j \alpha_i')^k}{\beta_j^k} R(L,\, -\beta_j M) \\ &= (\beta_j' \alpha_i - \beta_j \alpha_i')^k R(L, M). \end{aligned}$$

Следовательно,

$$\begin{aligned} R(\Phi, \Gamma) &= \prod_{i=1}^{n} \prod_{j=1}^{m} (\beta_j' \alpha_i - \beta_j \alpha_i')^k R(L, M) \\ &= [R(F, G)]^k \, [R(L, M)]^{mn}. \quad \square \end{aligned}$$

Теперь мы приведем признак Капферера.

(2H) *Пусть $p > 7$ — простое число. Если существуют отличные от нуля целые числа x, y, z, такие, что*

$$p \nmid xyz(x-y)(y-z)(z-x)(x^2+y^2+z^2)$$

и $x^p + y^p + z^p \equiv 0 \pmod{p^2}$, то p делит дискриминант однородного многочлена

$$K_p(X, Y) = \sum_{i=0}^{(p-7)/6} \binom{\frac{p-3}{2} - i}{2i} \frac{1}{2i+1} X^{(p-7)/6-i} Y^i$$

при $p \equiv 1 \pmod 6$ или

$$K_p(X, Y) = \sum_{i=0}^{(p-5)/6} \binom{\frac{p-3}{2} - i}{2i} \frac{1}{2i+1} X^{(p-5)/6-i} Y^i$$

при $p \equiv -1 \pmod 6$.

Доказательство. Действительно,

$$x^p \equiv x \pmod p, \qquad y^p \equiv y \pmod p, \qquad z^p \equiv z \pmod p,$$

следовательно, $x+y+z \equiv 0 \pmod p$, а значит, $z^p \equiv -(x+y)^p \pmod{p^2}$. Таким образом, $(x+y)^p - x^p - y^p \equiv 0 \pmod{p^2}$.

Заметим, что $y-z \equiv x+2y \pmod p$, $z-x \equiv -(2x+y) \pmod p$, $x^2+y^2+z^2 \equiv 2(x^2+xy+y^2) \pmod p$, следовательно, выполнено условие $p \nmid xy(x+y)(x-y)(2x+y)(2y+x)(x^2+xy+y^2)$.

Как следует из соотношения (2.2) гл. VII,

$$(X+Y)^p - X^p - Y^p = pXY(X+Y)(X^2+XY+Y^2)^e C_p(X,Y),$$

где $C_p(X,Y) \in \mathbb{Z}[X,Y]$ — однородный многочлен Коши, причем $e=1$ или 2 в зависимости от того, сравнимо ли число p с -1 или с 1 $\pmod 6$. Таким образом, p делит $C_p(x,y)$.

Покажем, что p делит дискриминант многочлена $C_p(X,Y)$. Действительно, пусть $Q(X,Y) = XY(X+Y)(X^2+XY+Y^2)^e$. Тогда

$$\frac{1}{p}\left[(X+Y)^p - X^p - Y^p\right] = Q(X,Y)C_p(X,Y).$$

Выпишем частные производные:

$$(X+Y)^{p-1} - X^{p-1} = Q(X,Y)\frac{\partial C_p}{\partial X}(X,Y) + \frac{\partial Q}{\partial X}(X,Y)C_p(X,Y),$$

$$(X+Y)^{p-1} - Y^{p-1} = Q(X,Y)\frac{\partial C_p}{\partial Y}(X,Y) + \frac{\partial Q}{\partial Y}(X,Y)C_p(X,Y).$$

Из условия $p \nmid xy(x+y)$ следует, что $x^{p-1} \equiv y^{p-1} \equiv (x+y)^{p-1} \equiv 1 \pmod p$; с другой стороны, $p \nmid Q(x,y)$. Таким образом, поскольку p делит $C_p(x,y)$, мы заключаем также, что $p \mid (\partial C_p/\partial X)(x,y)$ и $p \mid (\partial C_p/\partial Y)(x,y)$. Отсюда получим

$$\operatorname{Discr}(C_p(X,Y)) = R\left(\frac{\partial C_p}{\partial X}(X,Y),\ \frac{\partial C_p}{\partial Y}(X,Y)\right) \equiv 0 \pmod p.$$

Теперь воспользуемся записью $C_p(X,Y)$ в виде однородного многочлена от выражений

$$L(X,Y) = (X^2+XY+Y^2)^3 = U^3,$$
$$M(X,Y) = X^2Y^2(X+Y)^2 = V^2,$$

которая была получена в гл. VII (см. соотношения (2.5) и (2.6)): $C_p(X,Y) = K_p(L,M)$, где

$$K_p(L,M) = \sum_{i=0}^{(p-7)/6} \binom{\frac{p-3}{2}-i}{2i} \frac{1}{2i+1} L^{(p-7)/6-i} M^i$$

при $p \equiv 1 \pmod 6$ и

$$K_p(L,M) = \sum_{i=0}^{(p-5)/6} \binom{\frac{p-3}{2} - i}{2i} \frac{1}{2i+1} L^{(p-5)/6-i} M^i$$

при $p \equiv -1 \pmod 6$. По формулам вычисления частных производных сложной функции имеем

$$\frac{\partial C_p}{\partial X} = \frac{\partial K_p}{\partial L} \cdot \frac{\partial L}{\partial X} + \frac{\partial K_p}{\partial M} \cdot \frac{\partial M}{\partial X},$$
$$\frac{\partial C_p}{\partial Y} = \frac{\partial K_p}{\partial L} \cdot \frac{\partial L}{\partial Y} + \frac{\partial K_p}{\partial M} \cdot \frac{\partial M}{\partial Y},$$

где

$$\frac{\partial L}{\partial X} = 3(X^2+XY+Y^2)^2(2X+Y),$$
$$\frac{\partial M}{\partial X} = 2XY^2(X+Y)(2X+Y),$$
$$\frac{\partial L}{\partial Y} = 3(X^2+XY+Y^2)^2(X+2Y),$$
$$\frac{\partial M}{\partial Y} = 2X^2Y(X+Y)(X+2Y).$$

Положив $L(x,y) = r$, $M(r,s) = s$, получим, что $p \nmid rs$, и, поскольку

$$\frac{\partial C_p}{\partial X}(x,y) \equiv \frac{\partial C_p}{\partial Y}(x,y) \equiv 0 \pmod p,$$

можно заключить, что либо

$$\frac{\partial K_p}{\partial L}(r,s) \equiv \frac{\partial K_p}{\partial M}(r,s) \equiv 0 \pmod p,$$

либо

$$\det \begin{pmatrix} \frac{\partial L}{\partial X}(x,y) & \frac{\partial M}{\partial X}(x,y) \\ \frac{\partial L}{\partial Y}(x,y) & \frac{\partial M}{\partial Y}(x,y) \end{pmatrix} \equiv 0 \pmod p.$$

Вычислив этот определитель, получим сравнение

$$6(x^2+xy+y^2)^2(2x+y)(x+2y)xy(x+y)(x-y) \equiv 0 \pmod p.$$

Однако по предположению этот определитель не делится на p. Таким образом,

$$\frac{\partial K_p}{\partial L}(r,s) \equiv \frac{\partial K_p}{\partial M}(r,s) \equiv 0 \pmod p,$$

т. е. p делит результант бинарных форм $(\partial K_p/\partial L)(X,Y)$ и $(\partial K_p/\partial M)(X,Y)$ степени $m-1$, где

$$m = \begin{cases} \frac{p-7}{6} & \text{при} \quad p \equiv 1 \pmod 6, \\ \frac{p-5}{6} & \text{при} \quad p \equiv -1 \pmod 6. \end{cases}$$

Так как бинарные формы $L(X,Y)$, $M(X,Y)$ имеют степень 6, из утверждения (1A) гл. V следует, что

$$R\left(\frac{\partial K_p}{\partial L}(X,Y), \frac{\partial K_p}{\partial M}(X,Y)\right)$$
$$= \left[R\left(\frac{\partial K_p}{\partial L}(L,M), \frac{\partial K_p}{\partial M}(L,M)\right)\right]^6 R(L(X,Y), M(X,Y))^{(m-1)^2}$$

Но

$$R(L(X,Y), M(X,Y)) = R((X^2+XY+Y^2)^3, X^2Y^2(X+Y)^2)$$
$$= \left[R(X^2+XY+Y^2, XY(X+Y))\right]^6 = 1.$$

Следовательно, p делит результант

$$R\left(\frac{\partial K_p}{\partial L}(L,M), \frac{\partial K_p}{\partial M}(L,M)\right) = \mathrm{Discr}(K_p(L,M)). \quad \square$$

Заметим, что мы на самом деле показали, что если $r = (x^2+xy+y^2)^3 \not\equiv 0 \pmod p$ и $s = x^2y^2(x+y)^2 \not\equiv 0 \pmod p$, то пара (r,s) является кратным корнем сравнения $K_p(L,M) \equiv 0 \pmod p$.

Из утверждения (2G) получим такой признак.

(2I) *Пусть p — простое число. Если существуют такие отличные от нуля взаимно простые целые числа x, y, z, что $x^p+y^p+z^p = 0$, то или*

$$p \mid xyz(x-y)(y-z)(z-x)(x^2+y^2+z^2),$$

или p делит дискриминант многочлена

$$F_p(T) = F(T) = \sum_i \binom{m-i}{2i} \frac{1}{2i+1} T^i,$$

где $m = (p-3)/2$ и суммирование ведется от $i = 0$ до

$$i = \begin{cases} \frac{p-7}{6} & \textit{при} \quad p \equiv 1 \pmod 6, \\ \frac{p-5}{6} & \textit{при} \quad p \equiv -1 \pmod 6. \end{cases}$$

Доказательство. Предположим, что отличные от нуля взаимно простые целые числа x, y, z таковы, что $p \nmid xyz(x-y)(y-z)(z-x) \times (x^2+y^2+z^2)$ и $x^p+y^p+z^p=0$, так что $p>7$.

Тогда $x^p+y^p+z^p \equiv 0 \pmod{p^2}$, следовательно, согласно утверждению (2G) число p делит дискриминант формы $K_p(X,Y)$, точнее говоря, пара (r,s), где

$$r=(x^2+xy+y^2)^3 \not\equiv 0 \pmod{p},$$
$$s=x^2y^2(x+y)^2 \not\equiv 0 \pmod{p},$$

является кратным корнем сравнения $K_p(X,Y) \equiv 0 \pmod{p}$.

Положим $T=Y/X$. Тогда

$$K_p(1, Y/X)=F(T), \qquad K_p(X,Y)=X^mF(T),$$

где

$$m=\begin{cases} \frac{p-7}{6} & \text{при} \quad p \equiv 1 \pmod 6, \\ \frac{p-5}{6} & \text{при} \quad p \equiv -1 \pmod 6. \end{cases}$$

Но

$$\frac{\partial K_p}{\partial X} = mX^{m-1}F(T) - X^{m-2}YF'(T),$$
$$\frac{\partial K_p}{\partial Y} = X^{m-1}F'(T),$$

и, так как (r,s) — простой корень сравнений

$$\frac{\partial K_p}{\partial X}(r,s) \equiv 0 \pmod{p},$$
$$\frac{\partial K_p}{\partial Y}(r,s) \equiv 0 \pmod{p},$$

выбрав такое число $t \in \mathbb{Z}$, что $tr \equiv s \pmod{p}$, мы получим

$$\begin{cases} 0 \equiv mr^{m-1}F(t) - r^{m-2}sF'(t) \pmod{p}, \\ 0 \equiv r^{m-1}F'(t) \pmod{p}, \end{cases}$$

следовательно, $F(t) \equiv F'(t) \equiv 0 \pmod{p}$. Это означает, что p делит дискриминант формы $F(T)$. □

F. Связь с кубическим сравнением

В 1944 г. Пьер свел уравнение Ферма к двум системам сравнений. воспользовавшись методом, подобным методу Капферера.

Для начала нам потребуется одна лемма. Часть утверждений этой леммы была доказана Мириманновым в 1907 г. и Сколемом в 1937 г. (см. также Сколем (1941)).

ЛЕММА 2.2. *Пусть p — простое число, $p = 6k \pm 1$, целые числа a, b таковы, что $p \nmid b$, и число $t \in \mathbb{Z}$ таково, что $tb^2 \equiv a^3 \pmod{p}$. Положим*

$$\Psi_p(T) = T^{k-1} - 3\frac{(p-5)(p-7)}{2^2 \times 3!}T^{k-2} + \dots$$
$$+ (-1)^{s-1}(2s-1)\frac{[p-(2s+1)][p-(2s+3)]\dots[p-(4s-1)]}{2^{2(s-1)}(2s-1)!}T^{k-s}$$
$$+ \dots$$
$$+ (-1)^{k-1}(2k-1)\frac{[p-(2k+1)][p-(2k+3)]\dots[p-(4k-1)]}{2^{2(k-1)}(2k-1)!}.$$

Рассмотрим сравнение

$$X^3 + aX + b \equiv 0 \pmod{p}.$$

Тогда

(1) *если $-(4t+27)$ не является квадратичным вычетом по модулю p, то это сравнение имеет единственное решение x, $0 < x < p$;*

(2) *если $4t + 27 \equiv 0 \pmod{p}$, то это сравнение имеет два различных решения x_1, x_2, $0 < x_1, x_2 < p$;*

(3) *если $-(4t+27)$ является квадратичным вычетом по модулю p и $\Psi_p(t) \equiv 0 \pmod{p}$, то это сравнение имеет три различных решения x_1, x_2, x_3, $0 < x_1, x_2, x_3 < p$;*

(4) *если $-(4t+27)$ является квадратичным вычетом по модулю p, но $\Psi_p(t) \not\equiv 0 \pmod{p}$, то это сравнение не имеет решений;*

(5) *существует в точности k значений числа t, для которых это сравнение имеет несколько различных решений, и ровно $2k$ значений числа t, для которых это сравнение не имеет решений.*

В связи с этим Келле (1908) указал связь между разрешимостью сравнения третьей степени и линейными рекуррентными последовательностями второго порядка (см. также Мириманов (1909)).

Пусть $F_p(T)$ — многочлен, определенный в утверждении (2H). Применив лемму 2.2, Пьер доказал такой факт.

(2J) *Пусть взаимно простые целые числа* x, y, z *таковы, что* $p \nmid xyz(x-y)(y-z)(z-x)(x^2+y^2+z^2)$ *и* $x^p+y^p+z^p=0$. *Пусть, далее,* $r=(x^2+xy+y^2)^3$, $s=x^2y^2(x+y)^2$. *Тогда*

(1) *если число* t *удовлетворяет сравнению* $rt \equiv s \pmod{p^3}$, *то* $F_p(t) \equiv 0 \pmod{p^3}$;

(2) *если число* t *удовлетворяет сравнению* $r+ts \equiv 0 \pmod{p}$, *то*

$$\left(\frac{-4t-27}{p}\right)=1, \qquad \Psi_p(t) \equiv 0 \pmod{p}.$$

Доказательство. (1) Согласно результату (1C) гл. VI справедливо сравнение $x+y+z \equiv 0 \pmod{p^3}$. Следовательно, $x^p+y^p = -z^p \equiv (x+y)^p \pmod{p^4}$. Таким образом, p^4 делит $(x+y)^p - x^p - y^p = pxy(x+y)(x^2+xy+y^2)^e C_p(x,y)$, причем $e=2$ при $p \equiv 1 \pmod 6$ и $e=1$ при $p \equiv -1 \pmod 6$. Поскольку $p \nmid z$, мы также делаем вывод, что $p \nmid (x+y)$.

Аналогично из условия $p \nmid (x^2+y^2+z^2)$ следует, что $p \nmid (x^2+xy+y^2)$. Таким образом, p^3 делит $C_p(x,y)$. Во введенных обозначениях $C_p(x,y) = K_p(r,s) \equiv r^m F_p(t) \pmod{p^3}$, причем $m=(p-7)/6$ при $p \equiv 1 \pmod 6$ и $m=(p-5)/6$ при $p \equiv -1 \pmod 6$. Поскольку $p \nmid r$, мы получаем, что $F_p(t) \equiv 0 \pmod{p^3}$.

(2) Заметим, что сравнение

$$(x^2+xy+y^2)^3 + Tx^2y^2(x+y)^2 \equiv 0 \pmod{p}$$

имеет решение t тогда и только тогда, когда

$$\begin{cases} d^3x^3+tdx+t \equiv 0 \pmod{p}, \\ d^3y^3+tdy+t \equiv 0 \pmod{p} \end{cases}$$

для некоторого числа d, не кратного p.

Действительно, если числа dx, dy являются решениями сравнения $X^3+tX+t \equiv 0 \pmod{p}$, то другое решение сравнимо с $-d(x+y)$ по модулю p. Следовательно,

$$\begin{cases} d^2[xy-x(x+y)-y(x+y)] \equiv t \pmod{p}, \\ -d^3xy(x+y) \equiv -t \pmod{p}. \end{cases}$$

Таким образом,

$$\begin{cases} d^2(x^2+xy+y^2) \equiv -t \pmod{p}, \\ d^3xy(x+y) \equiv t \pmod{p}, \end{cases}$$

а значит, $(x^2+xy+y^2)^3 + tx^2y^2(x+y)^2 \equiv 0 \pmod{p}$.

Обратно, пусть число d таково, что $dxy(x+y) \equiv -(x^2+xy+y^2) \pmod{p}$. Рассмотрим сравнение $X^3+aX+b \equiv 0 \pmod{p}$ с корнями $dx, dy, -d(x+y)$. Тогда

$$\begin{cases} d^2[xy-x(x+y)-y(x+y)] \equiv a \pmod{p}, \\ -d^3xy(x+y) \equiv -b \pmod{p}. \end{cases}$$

Таким образом,

$$\begin{cases} d^2(x^2+xy+y^2) \equiv -a \pmod{p}, \\ d^3xy(x+y) \equiv b \pmod{p}. \end{cases}$$

Отсюда $b \equiv a \equiv t \pmod{p}$, так что

$$\begin{cases} d^3x^3+tdx+t \equiv 0 \pmod{p}, \\ d^3y^3+tdy+t \equiv 0 \pmod{p}. \end{cases}$$

Из проведенных рассуждений следует, что сравнение $X^3+tX+t \equiv 0 \pmod{p}$ имеет три попарно несравнимых решения dx, dy и $-d(x+y)$. Действительно, если, например, $dx \equiv -d(x+y) \pmod{p}$, то $x \equiv -x(x+y) \equiv z \pmod{p}$, что противоречит предположению. Согласно предыдущей лемме $-(4t+27)$ является квадратичным вычетом по модулю p и $\Psi_p(t) \equiv 0 \pmod{p}$.

Это завершает доказательство. □

Будет уместным напомнить, что если $p \equiv -1 \pmod{6}$, то $p \nmid (x^2+xy+y^2)$, а значит, $p \nmid (x^2+y^2+z^2)$ (см. лемму 1.2 гл. VI).

Но Поллачек в 1917 г. также показал (см. утверждение (2J) гл. VI), что даже если $p \equiv 1 \pmod{6}$, то из условий $x^p+y^p+z^p = 0$, $p \nmid xyz$ следует, что $p \nmid (x^2+xy+y^2)$, или, что равносильно, $p \nmid (x^2+y^2+z^2)$.

Аналогично, если $x \equiv y \pmod{p}$, то $x^p \equiv y^p \pmod{p^2}$, $z \equiv -2x \pmod{p}$, $z^p \equiv -2^p x^p \pmod{p^2}$, а значит, $2x^p \equiv 2^p x^p \pmod{p^2}$. Таким образом, если $p \nmid x$, то $2^p \equiv 2 \pmod{p^2}$. На самом деле в своей статье 1946 г. Инкери показал, что $2^p \equiv 2 \pmod{p^4}$. Следовательно, если простое число p таково, что $2^p \not\equiv 2 \pmod{p^4}$, то непременно $p \nmid (x-y)(y-z)(z-x)$.

Виферих в 1909 г. доказал, что из предположения о том, что первый случай последней теоремы Ферма не выполнен для показателя p, следует сравнение $2^p \equiv 2 \pmod{p^2}$. Это был первый из серии подобных результатов, полученных Миримановым, Вандивером, Поллачеком, Россером и Грэнвиллем. Их доказательства до-

статочно объемны и неэлементарны. Более полное изложение можно найти в моей книге «13 лекций о последней теореме Ферма»[3].

G. Связь с определителем

В 1907 г. Бини воспользовался классическим рекуррентным соотношением и получил выражение суммы $x^n + y^n + z^n$ через определитель.

(2K) *Пусть x, y, z — произвольные целые числа. Положим*

$$\begin{cases} a = x + y + z, \\ b = xy + yz + zx, \\ c = xyz \end{cases}$$

и для всех $n \geqslant 1$ обозначим

$$S_n = x^n + y^n + z^n.$$

Тогда

(1) $S_n - aS_{n-1} + bS_{n-2} + cS_{n-3} = 0$;

(2)

$$S_n = \det \begin{pmatrix} 0 & -a & b & -c & 0 & \dots & 0 & 0 \\ 0 & 1 & -a & b & -c & \dots & 0 & 0 \\ 0 & 0 & 1 & -a & b & \dots & 0 & 0 \\ 0 & 0 & 0 & 1 & -a & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & b & -c \\ 3c & 0 & 0 & 0 & 0 & \dots & -a & b \\ -2b & 0 & 0 & 0 & 0 & \dots & 1 & -a \\ a & 0 & 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

Доказательство. (1) Числа x, y, z удовлетворяют уравнению

$$X^3 - aX^2 + bX - c = 0.$$

Умножив на X^{n-3}, получим

$$X^n - aX^{n-1} + bX^{n-2} - cX^{n-3} = 0.$$

Заменяя X последовательно на x, y, z и складывая получающиеся соотношения, приходим к уравнению

$$S_n - aS_{n-1} + bS_{n-2} - cS_{n-3} = 0.$$

---

[3] 13 *Lectures on Fermat's Last Theorem.* — *Прим. перев.*

(2) Выпишем полученные соотношения для $k = 1, 2, \ldots, n$. Итак, числа $S_1, S_2, \ldots, S_n$ удовлетворяют системе n линейных уравнений

$$\begin{cases} S_n - aS_{n-1} + bS_{n-2} - cS_{n-3} = 0, \\ \qquad\qquad\qquad\qquad\qquad\quad \vdots \\ S_4 - aS_3 + bS_2 - cS_1 = 0, \\ S_3 - aS_2 + bS_1 = 3c, \\ S_2 - aS_1 = -2b, \\ S_1 = a. \end{cases}$$

Определитель, составленный из коэффициентов этой системы, равен 1. Поэтому согласно правилу Крамера S_n равняется определителю, указанному в условии утверждения. □

Отметим, что Бини вывел отсюда такое следствие: если p — нечетное простое число и $x+y+z=0$, то xyz делит $x^p+y^p+z^p$. Но, кстати говоря, это утверждение непосредственно следует из замечания перед утверждением (2A) гл. VII, если заметить, что $-z = x+y$.

H. Связь с бинарной квадратичной формой

В 1963 г. Пиньятаро связал уравнение Ферма с представлением p-й степени в виде бинарной квадратичной формы.

Сначала напомним следующий широко известный факт. Ферма в 1657 г. рассмотрел уравнение $X^2 - dY^2 = 1$, где натуральное число d не является квадратом (это уравнение ошибочно носит имя Пелля). Ферма заявил, что он методом спуска доказал существование бесконечного числа решений в целых числах. Однако первое опубликованное доказательство принадлежит Лагранжу (около 1766 г.). Вот этот результат.

ЛЕММА 2.3. *Пусть натуральное число d не является квадратом. Тогда существует решение уравнения $X^2 - dY^2 = 1$ в натуральных числах (x_1, y_1), обладающее следующим свойством: пара (x, y) также является решением в натуральных числах тогда и только тогда, когда существует целое число m, такое, что $x + y\sqrt{d} = (x_1 + y_1\sqrt{d})^m$. В частности, различным значениям m соответствуют различные решения, и, таким образом, уравнение $X^2 - dY^2 = 1$ имеет бесконечно много решений в натуральных числах.*

Доказательство Лагранжа опиралось на непрерывные дроби. Другое доказательство можно найти, например, в книге Рибенбойма (1999).

Введем следующее обозначение. Если b, c — отличные от нуля целые числа, положим $\langle b, c\rangle = bX^2 + cY^2$.

(2L) *Пусть p — нечетное простое число и тройка натуральных чисел (x, y, z) удовлетворяет уравнению $x^p + y^p = z^p$, причем число x нечетно и является наименьшим из возможных. Тогда*

(1) *yz является квадратичным вычетом по модулю x;*

(2) *существует бесконечно много способов представления x^p в виде квадратичной формы $\langle z, -y\rangle$.*

Доказательство. (1) Сначала заметим, что, так как $x^p + y^p = z^p$ и x минимально, числа x, y, z попарно взаимно просты. Справедливы равенства

$$x^p = z^p - y^p = z\left(z^{(p-1)/2}\right)^2 - y\left(y^{(p-1)/2}\right)^2,$$

т. е. x^p представимо в виде $\langle z, -y\rangle$. Далее, поскольку $z\left(z^{(p-1)/2}\right)^2 \equiv y\left(y^{(p-1)/2}\right)^2 \pmod{x}$, мы заключаем, что $yz\left(z^{(p-1)/2}\right)^2 \equiv y^{p+1} \pmod{x}$, а значит, yz является квадратичным вычетом по модулю x.

(2) Теперь покажем, что числа y, z не могут быть квадратами одновременно. Действительно, предположим, что $y = y_1^2$, $z = z_1^2$, причем $y_1, z_1 > 0$. Тогда

$$x^p = z_1^{2p} - y_1^{2p} = (z_1^p - y_1^p)(z_1^p + y_1^p).$$

Число x нечетно и НОД$(y, z) = 1$, значит, НОД$(z_1^p - y_1^p,\ z_1^p + y_1^p) = 1$ и, очевидно, $z_1^p + y_1^p > 1$. Следовательно, $z_1^p - y_1^p$ есть p-я степень нечетного натурального числа x', $0 < x' < x$, что противоречит минимальности x.

Как мы видели, $x^p = za^2 - yb^2$, где $a = z^{(p-1)/2}$, $b = y^{(p-1)/2}$. Рассмотрим уравнение $X^2 - yzY^2 = 1$. Так как НОД$(y, z) = 1$ и числа y, z не являются квадратами одновременно, мы делаем вывод, что yz не является квадратом.

Согласно лемме 2.3 существуют натуральные числа u_1, v_1, такие, что $1 = u_1^2 - yzv_1^2$ и, более того, для всех целых чисел m из соотношения $u_m + v_m\sqrt{yz} = (u_1 + v_1\sqrt{yz})^m$ следует, что $1 = u_m^2 - yzv_m^2$. Заметим, что если $1 \leqslant m$, то $u_m < u_{m+1}$ и $v_m < v_{m+1}$. Тогда

$$\begin{aligned} x^p &= (za^2 - yb^2)(u_m^2 - yzv_m^2) \\ &= z\left(a^2 - \frac{y}{z}b^2\right)\left(u_m^2 - \frac{y}{z}z^2v_m^2\right) \\ &= z\left(a - b\sqrt{\frac{y}{z}}\right)\left(u_m - v_m z\sqrt{\frac{y}{z}}\right)\left(a + b\sqrt{\frac{y}{z}}\right)\left(u_m + v_m z\sqrt{\frac{y}{z}}\right) \end{aligned}$$

$$= z\left[(au_m + bv_m y) - (av_m z + bu_m)\sqrt{\frac{y}{z}}\right]$$
$$\cdot\left[(au_m + bv_m y) + (av_m z + bu_m)\sqrt{\frac{y}{z}}\right]$$
$$= z(au_m + bv_m y)^2 - y(av_m z + bu_m)^2.$$

Это означает, что существует бесконечно много способов представления x^p в виде квадратичной формы $\langle z, -y\rangle$. □

I. Отсутствие алгебраических соотношений между решениями уравнения Ферма

В 1895 г. Жонкюре изучил возможность существования алгебраических соотношений между гипотетическими решениями уравнения Ферма.

Для $n = 2$ существует алгебраическое соотношение

$$(X^2 + Y^2)^2 - (X^2 - Y^2)^2 = (2XY)^2,$$

которому, как было показано в утверждении (1A) гл. I, удовлетворяют все примитивные решения уравнения Пифагора.

Оказывается, при $n > 2$ ничего подобного быть не может.

Лемма 2.4. *Пусть $F = F_0 + F_1 + F_2 + \ldots \in \mathbb{Z}[X, Y]$, где F_i — однородные части степени i многочлена F. Если $n \geqslant 1$, то существуют однородные многочлены $P_2 \in \mathbb{Z}[X_0, X_1]$, $P_3 \in \mathbb{Z}[X_0, X_1, X_2], \ldots$ степени n (зависящие только от n), такие, что однородными частями многочлена F^n являются*

$$\begin{aligned}
(F^n)_0 &= (F_0)^n,\\
(F^n)_1 &= n(F_0)^{n-1}F_1,\\
(F^n)_2 &= n(F_0)^{n-1}F_2 + P_2(F_0, F_1),\\
(F^n)_3 &= n(F_0)^{n-1}F_3 + P_3(F_0, F_1, F_2),\\
&\vdots\\
(F^n)_k &= n(F_0)^{n-1}F_k + P_k(F_0, F_1, \ldots, F_{k-1}).
\end{aligned}$$

Доказательство. Возводя F в степень n, заметим, что однородная часть многочлена $(F^n)_k$ состоит из члена $n(F_0)^{n-1}F_k$ и слагаемых, получаемых за счет вклада однородных частей, степени которых меньше чем k. Это выражение является многочленом с мультиномиальными коэффициентами, зависящими не от F, а только от n. □

(2M) *При $n > 2$ не существует многочленов $F, G \in \mathbb{Z}[X, Y]$, таких, что $X^nY^n = F^n - G^n$.*

Доказательство. Пусть $F = F_0 + F_1 + F_2 + \ldots$, $G = G_0 + G_1 + G_2 + \ldots$, где F_k, G_k — однородные части степени k многочленов F, G соответственно. Если $F^n - G^n = X^nY^n$, то $(F^n)_k = (G^n)_k$ для $k = 0, 1, \ldots, 2n-1$, $(F^n)_{2n} - (G^n)_{2n} = X^nY^n$. Как следует из леммы 2.4, $F_0 = G_0, \ldots, F_{2n-1} = G_{2n-1}$, а значит,

$$\begin{aligned} n(F_0)^{n-1}F_{2n} &= (F^n)_{2n} - P_{2n}(F_0, F_1, \ldots, F_{2n-1}) \\ &= (G^n)_{2n} + X^nY^n - P_{2n}(G_0, G_1, \ldots, G_{2n-1}) \\ &= n(G_0)^{n-1}G_{2n} + X^nY^n, \end{aligned}$$

и потому $n(F_0)^{n-1}(F_{2n} - G_{2n}) = X^nY^n$. Это означает, что $n = 1$, чего быть не может. □

Напомним, что в силу утверждения (3C) гл. VI, если $n > 2$ и натуральные числа x, y, z, $x < y < z$, таковы, что $x^n + y^n = z^n$, то y не является степенью простого числа. Отсюда следует, что $y = ab$, причем $a, b > 1$, НОД$(a, b) = 1$. Приведенный результат означает, что невозможно найти многочлены $F, G \in \mathbb{Z}[X, Y]$, такие, чтобы для всех $a, b \in \mathbb{Z}$ выполнялось равенство $a^nb^n = [F(a, b)]^n - [G(a, b)]^n$.

J. Связь с линейными рекуррентными последовательностями второго порядка

Переформулируем результаты (1A), (1B), (1C) гл. III в терминах линейных рекуррентных последовательностей (см. Кисс (1980)). Напомним, что если $m > 1$ и $(R_k)_{k \geqslant 0}$ — целочисленная последовательность, то $r(m)$ обозначает наименьший индекс r, для которого m делит R_r.

(2N) *Пусть нечетное простое число p и взаимно простые целые числа x, y, z таковы, что $x^p + y^p + z^p = 0$. Пусть, далее, $A = x - y$, $B = -xy$, $R_0 = 0$, $R_1 = 1$. Для всех $k \geqslant 2$ положим $R_k = AR_{k-1} - BR_{k-2}$ и $D = A^2 - 4B = (x + y)^2$. Тогда*

(1) *если $p \nmid z$, то $R_p = d^p$, где число d целое, $R_p \equiv D^{(p-1)/2} \equiv 1 \pmod{p^2}$ и $d \equiv 1 \pmod{p}$, $r(d) = r(d^2) = \ldots = r(d^p) = p$ (в обозначениях, введенных перед леммой 2.2 гл. V);*

(2) *если $p \mid z$, то $R_p/p = d^p$, где число d целое, $R_p \equiv p \pmod{p^4}$, $D \equiv 0 \pmod{p^{4p-2}}$ и $r(d) = r(d^2) = \ldots = r(d^p) = p$, $r(d^{p+1}) \neq p$.*

ДОКАЗАТЕЛЬСТВО. (1) Корнями трехчлена $X^2 - AX + B$ являются числа $x, -y$. Как следует из леммы 2.1 гл. V и утверждений (1A) и (1B) гл. III, $R_p = (x^p + y^p)/(x+y) = d^p$ (причем $d > 1$), $x + y = c^p$, где $c = t$, $d = t_1 \equiv 1 \pmod{p}$ (мы используем те же обозначения, что и выше). Тогда $R_p = d^p \equiv 1 \pmod{p^2}$. Поскольку $p \nmid z$ и $x + y + z \equiv 0 \pmod{p}$, мы можем заключить, что $p \nmid (x + y)$, а значит, $p \nmid c$. Следовательно, $D^{(p-1)/2} = (x + y)^{p-1} = c^{p(p-1)} \equiv 1 \pmod{p^2}$.

Наконец, так как $d^p \mid R_p$, по лемме 2.2 гл.V числа $r(d), r(d^2), \ldots, r(d^p)$ делят p. Поскольку $d > 1$, мы получаем, что $r(d^i) \neq 1$, а значит, $r(d) = r(d^2) = \ldots = r(d^p) = p$.

(2) Предположив, что $p \mid z$, из утверждений (1B) и (2C) гл. III получим, что $R_p = (x^p + y^p)/(x + y) = pd^p$, где $d = t_1 \equiv 1 \pmod{p^2}$, $x + y = p^{np-1}c^p$, где $n \geqslant 2$, $c = t$. Тогда $R_p/p = d^p \equiv 1 \pmod{p^3}$, так что $R_p \equiv p \pmod{p^4}$. Далее, $D = (x + y)^2 \equiv 0 \pmod{p^{4p-2}}$.

Наконец, так как $d^p \mid R_p$, но $d^{p+1} \nmid R_p$, мы получаем, что $r(d) = \ldots = r(d^p) = p$, $r(d^{p+1}) \neq p$. □

Теперь пришло время указать результат Кисса и Фонга (1979), содержащий интерпретацию сравнения $q^{p-1} \equiv 1 \pmod{p^2}$ в терминах соответствующей рекуррентной последовательности.

(2O) *Пусть различные простые числа p, q таковы, что $p \neq 2$ и $p \nmid (q-1)$. Положим $A = q + 1$, $B = q$, $R_0 = 0$, $R_1 = 1$ и $R_k = AR_{k-1} - BR_{k-2}$ для всех $k \geqslant 2$. Пусть, далее, $D = A^2 - 4B = (q-1)^2$. Тогда следующие условия равносильны:*

(a) $q^{p-1} \equiv 1 \pmod{p^2}$;

(b) $p^2 \mid R_{p-1}$;

(c) $r(p) = r(p^2)$.

ДОКАЗАТЕЛЬСТВО. $(a) \Leftrightarrow (b)$ Трехчлен $X^2 - AX + B = X^2 - (q+1)X + q$ имеет корни $\alpha = q$, $\beta = 1$. Как следует из леммы 2.1(1) гл. V, $R_{p-1} = (q^{p-1} - 1)/(q-1)$. Так как $p \nmid (q-1)$, условие $p^2 \mid R_{p-1}$ выполнено тогда и только тогда, когда $p^2 \mid \left(q^{p-1} - 1\right)$.

$(b) \Leftrightarrow (c)$ По лемме 2.2(5) гл. V число $r(p)$ делит $p - (D/p) = p - 1$, поскольку D является квадратом целого числа. Пусть $p - 1 = sr(p)$. В силу леммы 2.2(8) гл. V имеем $R_{p-1} = R_{sr(p)} \equiv sR_{r(p)}R_{r(p)+1}^{s-1} \pmod{R_{r(p)}^2}$.

Из условия $p \mid R_{r(p)}$ следует, что $p^2 \mid R_{r(p)}^2$, и, вновь используя лемму 2.2(2) гл. V, мы получаем, что $p \mid R_{sr(p)}$, $p \nmid R_{r(p)+1}$ и $p \nmid s$

(поскольку $s \leqslant p-1$). Следовательно, $p^2 \mid R_{p-1}$ тогда и только тогда, когда $p^2 \mid R_{r(p)}$. Пусть $v_p(R_{r(p)}) = k \geqslant 2$.

Согласно части (6) леммы 2.2 гл. V мы имеем $r(p^k) = r(p)$. Но $r(p) \mid r(p^2)$, поскольку $p \mid R_{r(p^2)}$. С другой стороны, $2 \leqslant k$, так что $p^2 \mid R_{r(p^k)} = R_{r(p)}$, а значит, $r(p^2) \mid r(p)$, что доказывает равенство (c). И наоборот, если $r(p) = r(p^2)$, то $p^2 \mid R_{r(p)}$. □

K. Возмущение показателя

Следующий результат (см. Шаумбергер (1973), Кламкин (1974)) достаточно любопытен: оказывается, если хотя бы немного «пошевелить» один из показателей в уравнении Ферма, то новое уравнение будет иметь бесконечно много решений в целых числах.

Сначала докажем такой факт.

(2P) *Если натуральные числа a, b, c таковы, что* НОД$(ab, c) = 1$, *то уравнение $X^a + Y^b = Z^c$ имеет бесконечно много решений в целых числах.*

Доказательство. Для $c = 1$ утверждение очевидно. Пусть $c \neq 1$. Заметим, что существуют целые числа d, e, такие, что $abd + 1 = ce$. Тогда $d \neq 0$, так как в противном случае $ce = 1$, $c \geqslant 1$, а значит, $c = 1$, что противоречит предположению. Далее, существует целое число t, такое, что $d + tc \geqslant 1$ и $ab(d + tc) + 1 = c(e + abt)$, причем $e + abt \geqslant 1$, так как $c \geqslant 1$. Таким образом, можно без ограничения общности считать, что $d \geqslant 1$, $e \geqslant 1$ и $abd + 1 = ce$.

Пусть число $u \geqslant 1$ произвольно. Положим

$$\begin{cases} x = 2^{bd} u^{bc}, \\ y = 2^{ad} u^{ac}, \\ z = 2^{e} u^{ab}. \end{cases}$$

Тогда $x^a + y^b = 2^{abd} u^{abc} + 2^{abd} u^{abc} = 2^{abd+1} u^{abc} = 2^{ce} u^{abc} = z^c$. Ввиду произвольности выбора параметра u данное уравнение имеет бесконечно много решений в целых числах. □

Отсюда получаем такое следствие.

(2Q) *Уравнение $X^n + Y^n = Z^{n+1/k}$ имеет бесконечно много решений в целых числах при любых натуральных числах n, k.*

Доказательство. Сначала заметим, что тройка (x, y, z) является решением уравнения $X^n + Y^n = Z^{kn+1}$ тогда и только тогда, когда (x, y, z^k) есть решение уравнения $X^n + Y^n = Z^{n+1/k}$. Положив

в условии утверждения (2P) $a = n$, $b = n$, $c = kn + 1$, получим, что данное уравнение действительно имеет бесконечно много решений в целых числах. □

L. Условие делимости для пифагоровых троек

В 1913 г. Невядомский рассматривал многочлены от трех переменных

$$D_0 = D_0(X, Y, Z) = -1$$

и

$$D_n = D_n(X, Y, Z) = Z^n - X^n - Y^n, \quad n \geqslant 1.$$

Для $n \geqslant 1$ он вывел тождество

$$D_{n+1} - (X + Y)D_n + XYD_{n-1} = Z^{n-1}(Z - X)(Z - Y), \qquad (2.2)$$

справедливость которого легко проверяется.

С помощью этого тождества Невядомский и Метро доказали (1913) такой факт.

(2R) *Пусть натуральные числа x, y, z таковы, что $x^2 + y^2 = z^2$ и $d_n = D_n(x, y, z)$ для всех $n \geqslant 1$. Тогда $2d_n$ делится на d_1^2 при $n \geqslant 2$.*

Доказательство. Без ограничения общности можно считать числа x, y, z взаимно простыми. Действительно, пусть $e = \text{НОД}(x, y, z)$, $x' = x/e$, $y' = y/e$, $z' = z/e$. Тогда $x'^2 + y'^2 = z'^2$, и мы можем полагать, что число x' четно, а y', z' нечетны. Пусть $d'_n = D_n(x', y', z')$. Тогда $d_n = e^n d'_n$, в частности $d_1 = ed'_1$. Заметим, что $d_1 \neq 0$. Следовательно, $2d_n/d_1^2 = e^{n-2} 2d'_n/d_1'^2$. Поскольку $n \geqslant 2$, достаточно показать, что число $2d'_n/d_1'^2$ целое.

Из предположения, что $e = 1$, и результата (1A) гл. I следует, что существуют такие натуральные числа a, b, $b < a$, что $\text{НОД}(a, b) = 1$ и

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

Если $n = 2$, то $d_2 = 0$ делится на d_1^2. Аналогично согласно соотношению (2.2) мы получаем

$$d_3 = (x + y)d_2 - xyd_1 + z(z - x)(z - y).$$

Следовательно, заметив, что $d_1 = 2b(b - a)$, имеем

$$\begin{aligned} 2d_3 &= -4ab(a^2 - b^2)d_1 + (a^2 + b^2)(a - b)^2 4b^2 \\ &= [2a(a + b) + a^2 + b^2]d_1^2 = [(a + b)^2 + 2a^2]d_1^2. \end{aligned}$$

Предположив, что $2d_{n-1}$ и $2d_n$ кратны d_1^2, с учетом (2.2) получим, что число

$$2d_{n+1} = (x+y)2d_n - xy \cdot 2d_{n-1} + 2z^{n-1}(z-x)(z-y)$$

также делится на d_1^2, поскольку

$$2z^{n-1}(z-x)(z-y) = (a^2+b^2)^{n-1}(a-b)^2 4b^2 = (a^2+b^2)^{n-1}d_1^2. \quad \square$$

Список литературы

1657 Fermat, P. de, Lettre à Frénicle (Février 1657) et Second Défi aux Mathématiciens, *Oeuvres*, Vol. II, pp. 333–335, Gauthier-Villars, Paris, 1894.

1766 Lagrange, J.L., *Solution d'un problème d'arithmétique*, Miscellanea Taurinensia, **4** (1766–1769); reprinted in *Oeuvres*, Vol. I, pp. 671–731, Gauthier-Villars, Paris, 1867.

1895 Jonquières, E. de, *Sur une question d'algèbre qui a des liens avec le dernier théorème de Fermat*, C. R. Acad. Sci. Paris, **120** (1895), 1139–1143.

1907 Bini, U., *Sopra alcune congruenze*, Period. Mat., (3), **22** (1907), 180–183.

1907 Bôcher, M., *Introduction to Higher Algebra*, Macmillan, New York, 1907.

1907 Bottari, A., *Soluzioni intere in progressione aritmetica appartinenti a equazione indeterminate del tipo* $\sum_{v=1}^{r} x_v^n = x_{r+1}^n$, Period. Mat., (3), **22** (1907), 156–158.

1907 Mirimanoff, D., *Sur les congruences du troisième degré*, Enseign. Math., **9** (1907), 381–384.

1908 Cailler, R., *Sur les congruences du troisième degré*, Enseign. Math., **10** (1908), 474–487.

1908 Cattaneo, P., *Osservazioni sopra due articoli del Signor Amerigo Bottari*, Period. Mat., (3), **23** (1908), 218–220.

1909 Mirimanoff, D., *Sur le dernier théorème de Fermat*, Enseign. Math., **11** (1909), 49–51.

1913 Goldziher, H., *Hatványszamok Telbontása hatványszamok összegere*, Középiskolai Math. Lapok, **21** (1913), 177–184.

1913 Niewiadomski, R., *Question 4205*, L'Interm. Math., **20** (1913), 98–100.

1913 Métrod, G., *Sur la question 4205 de Niewiadomski*, L'Interm. Math., **20** (1913), 215–216.

1917 Pollaczek, F., *Über den großen Fermat'schen Satz*, Sitzungsber. Akad. Wiss., Wien, Abt. IIa, **126** (1917), 45–59.

1928 Pérez-Cacho, L., *Una proposición sobre el indicador*, Rev. Mat. Hisp.-Amer., (2), **3** (1928), 273–275

1932 Bussi, C., *Sull'ultimo teorema di Fermat*, Boll. Un. Mat. Ital., **11** (1932), 267–269.

1937 Skolem, T., *Zwei Sätze über kubische Kongruenzen*, Det Kongel. Norske Vidensk. Selskab Forhandlinger, Trondheim, **10** (1937), no. 24, 89–92.

1941 Skolem, T., *Die Anzahl der Wurzeln der Kongruenz* $x^3+ax+b \equiv 0 \pmod{p}$ *für die verschiedenen Paare* a, b, Det Kongel. Norske Vidensk. Selskab Forhandlinger, Trondheim, **14** (1941), no. 43, 161–164.

1943 Bussi, C., *Osservazione sull'ultimo teorema di Fermat*, Boll. Un. Mat. Ital., (2), **5** (1943), 42–43.

1944 Pierre, C., *Remarques arithmétiques en connexion avec le dernier théorème de Fermat*, C. R. Acad. Sci. Paris, **218** (1944), 23–25.

1946 Inkeri, K., *Untersuchungen über die Fermatsche Vermutung*, Ann. Acad. Sci. Fenn., Ser. A1, Nr. 33, 1946, 60 pp.

1949 Kapferer, H., *Über ein Kriterium zur Fermatschen Vermutung*, Comment. Math. Helv., **23** (1949), 64–75.

1952 Mihaljinec, M., *Prilog Fermatovu problemu* (Une contribution au problème de Fermat), Hrvatsko Prirodoslovno Društvo, Glas. Mat. Fiz. Astr. Ser. II, **7** (1952), 12–18.

1958 Pérez-Cacho, L., *Sobre algunas cuestiones de la teoria de números*, Rev. Mat. Hisp.-Amer., (4), **18** (1958), 10–27 and 113–124.

1963 Pignataro, S., *Una osservazione sull'ultimo teorema di Fermat*, Rend. Accad. Sci. Fis. Mat. Napoli, (4), **30** (1963), 281–286.

1969 Rameswar Rao, D., *Some theorems on Fermat's last theorem*, Math. Student, **37** (1969), 208–210.

1969 Swistak, J.M., *A note on Fermat's last theorem*, Amer. Math. Monthly, **76** (1969), 173–174.

1972 Ribenboim, P., *Algebraic Numbers*, Wiley-Interscience, New York, 1972.

1973 Schaumberger, N., *Question 572*, Math. Mag., **46** (1973), 168.

1974 Klamkin, M.S., *Solution of the question 572*, Math. Mag., **47** (1974), 177–178.

1979 Kiss, P. and Phong, Bui Minh, *Divisibility properties in second order recurrences*, Publ. Math. Debrecen, **26** (1979), 187–197.

1979 Ribenboim, P., *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.
1980 Kiss, P., *Connection between second-order recurrences and Fermat's last theorem*, Period. Math. Hungar., **11** (1980), 151–157.
1999 Ribenboim, P., *The Classical Theory of Algebraic Numbers*, Springer-Verlag, New York, 1999.

Глава IX

Эпизоды 9 и 10

Для изучения сравнения Ферма нам понадобятся периоды Гаусса и **резольвенты** Лагранжа.

IX.1. Периоды Гаусса

Пусть q — нечетное простое число, ρ — первообразный корень **степени** q из единицы, h — первообразный корень по модулю q, $L = \mathbb{Q}(\rho)$, $B = \mathbb{Z}[\rho]$, и пусть τ — образующая группы Галуа расширения $L \mid \mathbb{Q}$, определяемая равенством $\tau(\rho) = \rho^h$.

Каждый элемент $\alpha \in L$ может быть единственным образом **представлен** в виде

$$\alpha = \sum_{i=0}^{q-2} a_i \rho^i \qquad \text{или} \qquad \alpha = \sum_{j=0}^{q-2} a'_j \rho^{h^j},$$

где $a_i, a'_j \in \mathbb{Q}$. Более того, $\alpha \in B$ тогда и только тогда, когда a_i, a'_j — **целые** числа.

Сравнив эти два представления, с учетом равенства

$$\rho^{h^{(q-1)/2}} = \rho^{q-1} = -(1 + \rho + \ldots + \rho^{q-2})$$

получим, что $a_0 = -a'_{(q-1)/2}$ и $a_i = a'_j - a'_{(q-1)/2}$, где $i \equiv h^j \pmod q$ **(для** $i = 1, \ldots, q-2$).

Если $q - 1 = fr$, то определим r периодов из f членов (относительно ρ и τ или h) следующим образом:

$$\begin{cases} \mu_0 &= \rho + \rho^{h^r} + \rho^{h^{2r}} + \ldots + \rho^{h^{(f-1)r}}, \\ \mu_1 &= \rho^h + \rho^{h^{r+1}} + \rho^{h^{2r+1}} + \ldots + \rho^{h^{(f-1)r+1}}, \\ &\vdots \\ \mu_{r-1} &= \rho^{h^{r-1}} + \rho^{h^{2r-1}} + \rho^{h^{3r-1}} + \ldots + \rho^{h^{q-2}}. \end{cases} \tag{1.1}$$

Нетрудно видеть, что $\sum_{j=0}^{r-1}\mu_j = -1$. Для каждого числа j положим $\mu_j = \mu_{j_0}$ при $0 \leqslant j_0 \leqslant r-1$ и $j \equiv j_0 \pmod r$. Периоды μ_j сопряжены друг с другом, т. е. $\tau^i(\mu_j) = \mu_{i+j}$ (при $i = 0, 1, \ldots, q-2$ и для любого числа j). В частности, $\tau^r(\mu_j) = \mu_j$ при $j = 0, 1, \ldots, r-1$.

Обозначим через L' подполе поля L, состоящее из элементов, неподвижных относительно автоморфизма τ^r. Тогда $[L : L'] = f$, $[L' : \mathbb{Q}] = r$. Группа Галуа расширения $L \mid L'$ порождается элементом τ^r, а группа Галуа расширения $L' \mid \mathbb{Q}$ порождается элементом τ', являющимся ограничением автоморфизма τ на подполе L'. Через B' обозначим кольцо целых в L'.

(1A)

(1) *Элементы* $\{\mu_0, \mu_1, \ldots, \mu_{r-1}\}$ *образуют базис* $\mathbb{Z}$*-модуля* B'.

(2) *Справедливы равенства*

$$L' = \mathbb{Q}(\mu_0, \ldots, \mu_{r-1}),\ B' = \mathbb{Z}[\mu_0, \ldots, \mu_{r-1}].$$

(3) *Элементы* $\{1, \rho, \rho^2, \ldots, \rho^{f-1}\}$ *образуют базис* B'*-модуля* B.

(4) *Многочлен периодов*

$$F_{\mu_0}(X) = \prod_{i=0}^{r-1}(X - \mu_i) \tag{1.2}$$

есть многочлен с целыми коэффициентами и является неприводимым.

Доказательство. (1) Элементы $\mu_0, \mu_1, \ldots, \mu_{r-1}$ линейно независимы над $\mathbb{Z}$. Действительно, если $\sum_{i=0}^{r-1} a_i\mu_i = 0$ (где $a_i \in \mathbb{Z}$), то, подставляя вместо каждого элемента μ_i его выражение из (1.1), получим, что линейная комбинация элементов $\rho, \rho^2, \ldots, \rho^q$ равна нулю, а значит, имеет нулевые коэффициенты. Следовательно, все $a_i = 0$.

С другой стороны, если $\alpha \in B' \subseteq B$, то мы можем записать $\alpha = \sum_{i=0}^{q-2} a_i\rho^{h^i}$, где $a_i \in \mathbb{Z}$. Так как $\tau^r(\alpha) = \alpha$, справедливо соотношение

$$\sum_{i=0}^{q-2} a_i\rho^{h^{i+r}} = \sum_{i=0}^{q-2} a_i\rho^{h^i},$$

и из единственности разложения мы получаем

$$\begin{cases} a_0 = a_r = \ldots = a_{(f-1)r}, \\ a_1 = a_{r+1} = \ldots = a_{(f-1)r+1}, \\ \vdots \\ a_{r-1} = a_{2r-1} = \ldots = a_{q-2}. \end{cases}$$

Поэтому

$$a = \sum_{j=0}^{r-1} a_j \mu_j.$$

(2) Легко видеть, что

$$L' \supseteq \mathbb{Q}(\mu_0, \ldots, \mu_{r-1}) \quad \text{и} \quad B' \supseteq \mathbb{Z}[\mu_0, \ldots, \mu_{r-1}].$$

А обратное утверждение следует из системы (1.1).

(3) Пусть $G(X) = \prod_{i=0}^{f-1}(X - \rho^{h^{ir}})$ — многочлен, корни которого являются слагаемыми периода μ_0. Тогда все коэффициенты многочлена $G(X)$ неподвижны относительно автоморфизма τ^r, а значит, лежат в $B \cap L' = B'$.

Таким образом, $G(X) = X^f + \alpha_1 X^{f-1} + \ldots + \alpha_f$, и, поскольку ρ — корень многочлена $G(X)$, $\rho^f = -(\alpha_1 \rho^{f-1} + \ldots + \alpha_f)$. Значит, ρ^f есть линейная комбинация элементов $1, \rho, \ldots, \rho^{f-1}$ с коэффициентами из B'. Умножая приведенное выше соотношение последовательно на $\rho, \rho^2, \ldots$, мы получим, что $\rho^{f+1}, \rho^{f+2}, \ldots, \rho^{q-1}$ также являются линейными комбинациями элементов $1, \rho, \rho^2, \ldots, \rho^{f-1}$ с коэффициентами из B'. Следовательно, каждый элемент из $B = \mathbb{Z}[\rho]$ есть линейная комбинация элементов $1, \rho, \ldots$ с коэффициентами из B'.

Итак, $\{1, \rho, \ldots, \rho^{f-1}\}$ есть система образующих L'-векторного пространства L. Поскольку $[L : L'] = f$, система $\{1, \rho, \ldots, \rho^{f-1}\}$ линейно независима над L', а значит, и над B'.

(4) Коэффициенты многочлена $F_{\mu_0}(X)$ принадлежат $\mathbb{Q}$, поскольку они неподвижны относительно автоморфизма τ. Значит, они принадлежат $B' \cap \mathbb{Q} = \mathbb{Z}$.

Так как $F_{\mu_0}(\mu_0) = 0$, минимальный многочлен для μ_0 делит многочлен $F_{\mu_0}(X)$ и его корни сопряжены с μ_0. Отсюда следует, что он совпадает с многочленом $F_{\mu_0}(X)$, который, таким образом, является неприводимым. □

Вообще говоря, неверно, что

$$\mathbb{Z}[\mu_0, \ldots, \mu_{r-1}] = \mathbb{Z}[\mu_0] = \ldots = \mathbb{Z}[\mu_{r-1}].$$

Например, при $q = 13$, $f = 3$, $r = 4$ и $k = 2$ периоды выражаются формулами

$$\begin{aligned}
\mu_0 &= \rho + \rho^3 + \rho^{-4}, \\
\mu_1 &= \rho^2 + \rho^6 + \rho^5, \\
\mu_2 &= \rho^4 + \rho^{-1} + \rho^{-3}, \\
\mu_3 &= \rho^{-5} + \rho^{-2} + \rho^{-6}.
\end{aligned}$$

Покажем, что из единственности представлений μ_1, μ_2, μ_3 в виде многочленов от μ_0 с рациональными коэффициентами следует, что некоторые из этих коэффициентов не будут целыми числами. В самом деле,

$$\mu_0^2 = \mu_1 + 2\mu_2,$$
$$\mu_0\mu_1 = \mu_0 + \mu_1 + \mu_3,$$
$$\mu_0\mu_2 = 3 + \mu_1 + \mu_3$$

и

$$\begin{aligned}\mu_0^3 &= \mu_0\mu_1 + 2\mu_0\mu_2 = 6 + \mu_0 + 3\mu_1 + 3\mu_3 \\ &= 6 + \mu_0 + 3(-1 - \mu_0 - \mu_2),\end{aligned}$$

так что

$$\mu_2 = \frac{1}{3}(-\mu_0^3 - 2\mu_0 + 3).$$

Отсюда имеем

$$\begin{aligned}\mu_1 &= \mu_0^2 - 2\mu_2 = \frac{1}{3}(2\mu_0^3 + 3\mu_0^2 + 4\mu_0 - 6), \\ \mu_3 &= -1 - \mu_0 - \mu_1 - \mu_2 = \frac{1}{3}(-\mu_0^3 - 3\mu_0^2 - 5\mu_0).\end{aligned}$$

Из утверждения (1A) следует, что для заданных номеров i, j, $0 \leqslant i, j \leqslant r-1$, существуют, причем единственные, целые числа $n_{ijk} \in \mathbb{Z}$ $(0 \leqslant k \leqslant r-1)$, такие, что $\mu_i\mu_j = \sum_{k=0}^{r-1} n_{ijk}\mu_k$. Точнее, справедливо следующее утверждение.

(1B) *Если* $0 \leqslant k \leqslant r-1$, *то*

$$\sum_{i=0}^{r-1} \mu_i\mu_{i+k} = n_k q - f,$$

где

$$n_k = \begin{cases} 1, & \text{если } f \text{ четно и } k = 0, \\ 1, & \text{если } f \text{ нечетно и } k = 0 \text{ или } r/2, \\ 0 & \text{в противном случае.} \end{cases}$$

Доказательство. Вначале вычислим произведение

$$\mu_0\mu_k = \left(\sum_{l=0}^{f-1} \rho^{h^{lr}}\right)\left(\sum_{j=0}^{f-1} \rho^{h^{k+jr}}\right).$$

Записав $j \equiv i + l \pmod{q-1}$, получим

$$\mu_0 \mu_k = \sum_{l=0}^{f-1} \sum_{i=0}^{f-1} \rho^{h^{lr}(1+h^{k+ir})}.$$

Положим

$$\mu_i' = \sum_{l=0}^{f-1} \rho^{h^{lr}(1+h^{k+ir})}.$$

Если $1+h^{k+ir} \not\equiv 0 \pmod{q}$, то существует единственное целое число t, $0 \leqslant t \leqslant q-2$, такое, что $1 + h^{k+ir} \equiv h^t \pmod{q}$, поэтому μ_i' равно периоду μ_t. А если $1+h^{k+ir} \equiv 0 \pmod{q}$, то $\mu_i' = f$. Таким образом, мы можем записать

$$\mu_0 \mu_k = n_k f + m_{k,0}\mu_0 + m_{k,1}\mu_1 + \ldots + m_{k,r-1}\mu_{n-1}, \qquad (1.3)$$

где $n_k \geqslant 0$, $m_{k,0} \geqslant 0, \ldots, m_{k,r-1} \geqslant 0$ — целые числа. Определим теперь n_k.

(I) Если число f четно и $k = 0$, положим $f = 2f'$. Тогда $1 + h^{f'r} \equiv 0 \pmod{q}$, так как $fr = q-1$. Значит, $\mu_{f/2}' = f$. С другой стороны, если $0 \leqslant i < f$ и $\mu_i' = f$, то $1 + h^{ir} \equiv 0 \pmod{q}$, поэтому $2ir \equiv 0 \pmod{q-1}$, т. е. $2ir = mrf$, но $mf = 2i < 2f$, а значит, $m = 0$ или 1. При $m = 0$ получим, что $i = 0$, а это противоречит предположению о том, что q нечетно. Следовательно, $m = 1$ и $i = f/2$. Таким образом, в этом случае $n_k = 1$.

(II) Если число f нечетно (значит, r четно) и $k = r/2$, положим $i = (f-1)/2$. Тогда $1 + h^{r/2+((f-1)/2)r} \equiv 0 \pmod{q}$, поэтому $\mu_{(f-1)/2}' = f$. С другой стороны, если $0 \leqslant i < f$ и $\mu_i' = f$, то $1 + h^{r/2+ir} \equiv 0 \pmod{q}$, так что $r + 2ir = mrf$, и, таким образом, $mf = 1 + 2i < 1 + 2f$. Отсюда следует, что m — нечетное число, а значит, $m = 1$ и $i = (f-1)/2$.

(III) Рассмотрим оставшиеся случаи. Если $1+h^{k+ir} \equiv 0 \pmod{q}$, то $2k + 2ir = mrf$ и $0 \leqslant r(mf - 2i) = 2k < 2r$, а следовательно, $mf - 2i = 0$ или 1.

Если $mf = 2i < 2f$, то $m = 0$ или 1 и $k = 0$. Если $m = 0$, то $i = 0$ и $k = 0$, что противоречит предположению о том, что q — нечетное число. Поэтому $m = 1$ и f четно.

Если $mf = 2i + 1 < 2f + 1$, то число m нечетно, $m \leqslant 2$, а следовательно, $m = 1$, число f нечетно, $i = (f-1)/2$ и $k = r/2$, т. е. мы пришли к случаю (II), рассмотренному выше. Таким образом, в случае (III) мы получаем $n_k = 0$.

Так как $\mu_0\mu_k$ — сумма f^2 членов вида ρ^i и каждый период содержит f таких членов с разными показателями i, $0 \leqslant i \leqslant q-1$, справедливо соотношение

$$n_k + m_{k,0} + m_{k,1} + \ldots + m_{k,n-1} = f.$$

Применяя автоморфизмы τ^i, из равенства (1.3) получим

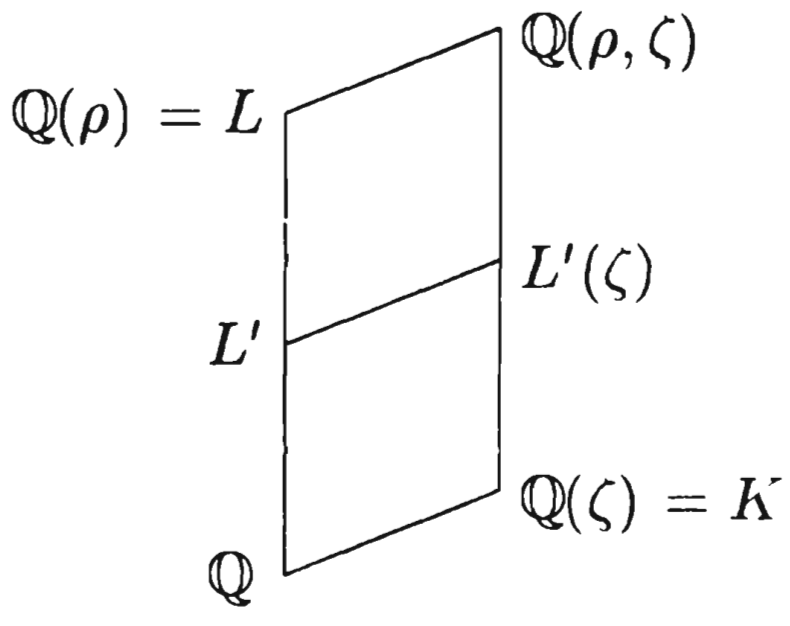
$$\mu_i\mu_{k+i} = n_k f + m_{k,0}\mu_i + m_{k,1}\mu_{i+1} + \ldots + m_{k,n-1}\mu_{r-1}.$$

Следовательно, поскольку $\sum_{i=0}^{r-1}\mu_i = -1$, мы заключаем, что $\sum_{i=0}^{r-1}\mu_i\mu_{i+k} = n_k(q-1) - (m_{k,0} + m_{k,1} + \ldots + m_{k,r-1}) = n_k q - f$. □

IX.2. Резольвенты Лагранжа

Мы будем использовать следующие обозначения:

- p, q — простые числа, такие, что $q - 1 = 2kp$;
- ζ — первообразный корень степени k из единицы;
- g — первообразный корень по модулю p;
- h — первообразный корень по модулю q;
- $K = \mathbb{Q}(\zeta)$;
- $A = \mathbb{Z}[\zeta]$;
- σ — образующая группы Галуа расширения $K \mid \mathbb{Q}$, определяемая равенством $\sigma(\zeta) = \zeta^g$;
- ρ — первообразный корень степени q из единицы;
- $L = \mathbb{Q}(\rho)$, $B = \mathbb{Z}[\rho]$;
- τ — образующая группы Галуа расширения $L \mid \mathbb{Q}$, определяемая равенством $\tau(\rho) = \rho^h$;
- $\mu_0, \ldots, \mu_{p-1}$ — p периодов из $2k$ членов (относительно ρ и τ);
- $L' = \mathbb{Q}(\mu_0, \ldots, \mu_{p-1}) = \mathbb{Q}(\mu_0) = \ldots = \mathbb{Q}(\mu_{p-1})$;
- $B' = \mathbb{Z}[\mu_0, \ldots, \mu_{p-1}]$;
- τ' — ограничение автоморфизма τ на L'.



Заметим, что $L \cap K = \mathbb{Q}$. Действительно, простое число q полностью разветвляется в L и не разветвляется в K, следовательно, оно одновременно разветвляется и не разветвляется в $L \cap K$, значит, $L \cap K = \mathbb{Q}$.

Таким образом, $\mathbb{Q}(\rho, \zeta)$ — расширение Галуа поля K с группой Галуа, изоморфной группе Галуа расширения $L \mid \mathbb{Q}$ и порожденной автоморфизмом $\tilde{\tau}$, который определяется равенствами

$$\begin{cases} \tilde{\tau}(\rho) = \rho^h, \\ \tilde{\tau}(\zeta) = \zeta. \end{cases}$$

Аналогично получаем, что $\mathbb{Q}(\rho, \zeta)$ — расширение Галуа поля L с группой Галуа, изоморфной группе Галуа расширения $K \mid \mathbb{Q}$ и порожденной автоморфизмом $\tilde{\sigma}$, который определяется равенствами

$$\begin{cases} \tilde{\sigma}(\rho) = \rho, \\ \tilde{\sigma}(\zeta) = \zeta^g. \end{cases}$$

Для удобства введем следующие обозначения.

Если t — целое число, не делящееся на q, то существует единственное целое число s, $0 \leqslant s \leqslant q-2$, такое, что $t \equiv h^s \pmod{q}$. Число s называется *индексом* числа t (относительно h и q) и обозначается $s = \operatorname{ind}_h(t)$ или просто $s = \operatorname{ind}(t)$, если первообразный корень h выбран однозначно.

Например, $\operatorname{ind}(1) = 0$ и $\operatorname{ind}(-1) = (q-1)/2$. Если $t \equiv t' \pmod{q}$, то $\operatorname{ind}(t) = \operatorname{ind}(t')$, и если числа t и t' не делятся на q, то $\operatorname{ind}(tt') \equiv \equiv \operatorname{ind}(t) + \operatorname{ind}(t') \pmod{q-1}$. Также ясно, что каждое целое число s, $0 \leqslant s \leqslant q-2$, является индексом, а именно $s = \operatorname{ind}(h^s)$.

Определим *резольвенты Лагранжа* $\langle \alpha, \beta \rangle_\tau$, где $\alpha \in K$, $\beta \in L$ и τ — автоморфизм, определенный выше:

$$\langle \alpha, \beta \rangle_\tau = \beta + \alpha\tau(\beta) + \alpha^2\tau^2(\beta) + \ldots + \alpha^{p-1}\tau^{p-1}(\beta). \tag{2.1}$$

Будем вместо $\langle \alpha, \beta \rangle_\tau$ писать просто $\langle \alpha, \beta \rangle$. Элемент $\langle \alpha, \beta \rangle$ принадлежит полю $\mathbb{Q}(\zeta, \rho)$. Справедливо следующее утверждение.

(2A) *Для любого целого числа n и любого элемента $\beta \in \mathbb{Q}(\rho)$ резольвенты Лагранжа удовлетворяют условиям*

$$\zeta^n \tilde{\tau}\left(\langle \zeta^n, \beta \rangle\right) = \langle \zeta^n, \beta \rangle \qquad \text{и} \qquad \langle \zeta^n, \beta \rangle^p \in \mathbb{Q}(\zeta).$$

Доказательство. Так как $\zeta^p = 1$, мы имеем

$$\begin{aligned} \zeta^n \tilde{\tau}\left(\langle \zeta^n, \beta \rangle\right) &= \zeta^n \tilde{\tau}(\beta + \zeta^n\tau(\beta) + \zeta^{2n}\tau^2(\beta) + \ldots + \zeta^{(p-1)n}\tau^{p-1}(\beta)) \\ &= \langle \zeta^n, \beta \rangle. \end{aligned}$$

Значит, $\tilde{\tau}(\langle\zeta^n,\beta\rangle^p) = (\tilde{\tau}\langle\zeta^n,\beta\rangle)^p = \zeta^{-np}\cdot\langle\zeta^n,\beta\rangle^p = \langle\zeta^n,\beta\rangle^p$. Поскольку элемент $\langle\zeta^n,\beta\rangle^p$ неподвижен относительно автоморфизма $\tilde{\tau}$, мы получаем, что $\langle\zeta^n,\beta\rangle^p \in \mathbb{Q}(\zeta)$. □

Рассмотрим резольвенты $\langle\zeta^n,\rho^m\rangle$. Используя индексы, введенные выше, мы можем записать

$$\langle\zeta^n,\rho^m\rangle_\tau = \sum_{u=0}^{q-2}\zeta^{nu}\rho^{mh^u} = \sum_{t=1}^{q-1}\zeta^{n\operatorname{ind}_h(t)}\rho^{mt}. \tag{2.2}$$

Комплексное число, сопряженное с $\langle\zeta^n,\rho^m\rangle_\tau$, есть $\overline{\langle\zeta^n,\rho^m\rangle_\tau} = \langle\zeta^{-n},\rho^{-m}\rangle_\tau$. Отметим следующий результат.

(2B) *Во введенных выше обозначениях при* $n = 1,2,\ldots,p-1$ *справедливо неравенство*

$$\langle\zeta^n,\rho\rangle_\tau = \langle\zeta^n,\mu_0\rangle_{\tau'} \neq 0$$

и $\langle\zeta^n,\rho\rangle_\tau \in L'$.

Доказательство. Используя соотношение (2.2), получим

$$\begin{aligned}\langle\zeta^n,\rho\rangle_\tau &= \rho+\zeta^n\rho^h+\zeta^{2n}\rho^{h^2}+\ldots+\zeta^{(q-2)n}\rho^{h^{q-2}} \qquad (2.3)\\ &= \rho+\zeta^n\rho^h+\ldots+\zeta^{(p-1)n}\rho^{h^{p-1}}\\ &\quad+\rho^{h^p}+\zeta^n\rho^{h^{p+1}}+\ldots+\zeta^{(p-1)n}\rho^{h^{2p-1}}\\ &\quad+\ldots\\ &\quad+\rho^{h^{(2k+1)p}}+\zeta^n\rho^{h^{(2k-1)p+1}}+\ldots+\zeta^{(p-1)n}\rho^{h^{q-1}}\\ &= \mu_0+\zeta^n\mu_1+\ldots+\zeta^{(p-1)n}\mu_{p-1}\\ &= \langle\zeta^n,\mu_0\rangle_{\tau'}\in L'.\end{aligned}$$

Кроме того, $\langle\zeta^n,\mu_0\rangle_{\tau'} \neq 0$. Действительно, периоды $\mu_0,\mu_1,\ldots,\mu_{p-1}$, являющиеся базисом в $L' \mid \mathbb{Q}$, будут базисом и в $L'(\zeta) \mid \mathbb{Q}$, поскольку это расширение имеет степень p. □

Теории периодов Гаусса, резольвент Лагранжа и более общих сумм корней из единицы очень богаты и имеют важное значение. Отметим результаты, которые понадобятся нам в дальнейшем.

(2C) *Если* $p \nmid n$ *и* $q \nmid m$, *то* $\langle\zeta^n,\rho^m\rangle = \langle\zeta^n,\rho\rangle\zeta^{-n\operatorname{ind}(m)}$. *В частности,* $\langle\zeta^n,\rho^{n^i}\rangle = \langle\zeta^n,\rho\rangle\zeta^{-ni}$.

Доказательство. Воспользуемся соотношением

$$\langle\zeta^n,\rho^m\rangle = \sum_{t=1}^{q-1}\zeta^{n\operatorname{ind}(t)}\rho^{mt}.$$

Поскольку $\operatorname{ind}(tm) \equiv \operatorname{ind}(t) + \operatorname{ind}(m) \pmod{q-1}$, мы получаем

$$\begin{aligned}\langle \zeta^n, \rho^m \rangle &= \zeta^{-n \operatorname{ind}(m)} \sum_{t=1}^{q-1} \zeta^{n \operatorname{ind}(tm)} \rho^{tm} \\ &= \zeta^{-n \operatorname{ind}(m)} \sum_{s=1}^{q-1} \zeta^{n \operatorname{ind}(s)} \rho^{s} \\ &= \zeta^{-n \operatorname{ind}(m)} \langle \zeta^n, \rho \rangle. \quad \square\end{aligned}$$

(2D) *Если $p \nmid n$, то $\langle \zeta^n, \rho \rangle \langle \zeta^{-n}, \rho \rangle = q$.*

Доказательство. Нетрудно видеть, что

$$\begin{aligned}\langle \zeta^n, \rho \rangle \langle \zeta^{-n}, \rho \rangle &= \left(\sum_{t=1}^{q-1} \zeta^{n \operatorname{ind}(t)} \rho^{t} \right) \left(\sum_{s=1}^{q-1} \zeta^{-n \operatorname{ind}(s)} \rho^{s} \right) \\ &= \sum_{s=1}^{q-1} \sum_{t=1}^{q-1} \zeta^{n[\operatorname{ind}(t) - \operatorname{ind}(s)]} \rho^{t+s}.\end{aligned}$$

Пусть r определяется из сравнения $t \equiv rs \pmod{q}$ для каждого s. Так как $p \mid (q-1)$, мы получаем, что $\zeta^{q-1} = 1$, а следовательно, приведенная выше сумма равна

$$\sum_{s=1}^{q-1} \sum_{r=1}^{q-1} \zeta^{n \operatorname{ind}(r)} \rho^{(r+1)s}.$$

Используя равенство $q - 1 = 2kp$, получим

$$\sum_{r=1}^{q-1} \zeta^{n \operatorname{ind}(r)} = \sum_{m=1}^{q-1} \zeta^{m} = 2k \sum_{m=1}^{p} \zeta^{m} = 0,$$

таким образом, добавив сумму $\sum_{r=1}^{q-1} \zeta^{n \operatorname{ind}(r)} = 0$, мы можем записать

$$\begin{aligned}\langle \zeta^n, \rho \rangle \langle \zeta^{-n}, \rho \rangle &= \sum_{s=0}^{q-1} \sum_{r=1}^{q-1} \zeta^{n \operatorname{ind}(n)} \rho^{(r+1)s} \\ &= \sum_{r=1}^{q-1} \zeta^{n \operatorname{ind}(r)} \left(\sum_{s=0}^{q-1} \rho^{(r+1)s} \right).\end{aligned}$$

Но

$$\sum_{s=0}^{q-1} \rho^{(r+1)s} = \begin{cases} q, & \text{если } r = q-1, \\ 0, & \text{если } 1 \leqslant r \leqslant q-2, \end{cases}$$

а следовательно,

$$\langle \zeta^n, \rho\rangle\langle \zeta^{-n}, \rho\rangle = q\zeta^{n\,\mathrm{ind}(q-1)} = q\zeta^{n\,\mathrm{ind}(-1)} = q\zeta^{n(q-1)/2} = q\zeta^{nkp} = q.$$

□

(2E) *Если $p \nmid m$, то $|\langle \zeta^m, \rho\rangle| = \sqrt{q}$.*

Доказательство. Как следует из результатов (2D) и (2C), квадрат абсолютного значения величины $\lambda_m = \langle \zeta^m, \rho\rangle$ есть

$$\begin{aligned} |\lambda_m|^2 &= \lambda_m\overline{\lambda_m} = \langle \zeta^m, \rho\rangle\langle \zeta^{-m}, \rho^{-1}\rangle \\ &= \langle \zeta^m, \rho\rangle\langle \zeta^{-m}, \rho\rangle\zeta^{-m\,\mathrm{ind}(-1)} = q\zeta^{m(q-1)/2} \\ &= q\zeta^{mkp} = q. \ \square \end{aligned}$$

Выразим периоды Гаусса через резольвенты Лагранжа.

(2F) *Если $p \nmid n$, то*

$$\mu_n = \frac{1}{p}\sum_{j=0}^{p-1} \zeta^{-jn}\langle \zeta^j, \rho\rangle.$$

Доказательство. Вычислим правую часть этого равенства:

$$\begin{aligned} \sum_{j=0}^{p-1} \zeta^{-jn}\langle \zeta^j, \rho\rangle &= \sum_{j=0}^{p-1} \zeta^{-jn}\left(\sum_{u=0}^{q-2} \zeta^{ju}\rho^{h^u}\right) \\ &= \sum_{j=0}^{p-1}\sum_{u=0}^{q-2} \zeta^{j(u-n)}\rho^{h^u} \\ &= \sum_{j=0}^{p-1}\sum_{t=-n}^{q-2-n} \zeta^{jt}\rho^{h^{t+n}} \\ &= \sum_{t=-n}^{q-2-n} \rho^{h^{t+n}}\left(\sum_{j=0}^{p-1} \zeta^{jt}\right). \end{aligned}$$

Но $\sum_{j=0}^{p-1}\zeta^{jt} = p$ при $p \mid t$ и $\sum_{j=0}^{p-1}\zeta^{jt} = 0$ в противном случае. Таким образом, приведенная выше сумма равна

$$p\left(\sum_{i=-n,\,p|t}^{q-2-n} \rho^{h^{t+n}}\right) = p\mu_n. \ \square$$

Глава X

Локальная и модулярная проблемы Ферма

В этой главе рассматриваются некоторые естественные видоизменения проблемы Ферма. В первом разделе изучаются решения в целых q-адических числах, а далее рассматривается сравнение Ферма.

X.1. Локальная проблема Ферма

Наша цель — показать, что для каждого простого числа q уравнение Ферма имеет ненулевые решения в целых q-адических числах. Для этого мы воспользуемся леммой Гензеля.

(1A) ***Для любых простых чисел q и p уравнение $X^p + Y^p = Z^p$ имеет нетривиальное решение в целых q-адических числах.***

Доказательство. При $p = 2$ утверждение тривиально (см. гл. I, утверждение (1A)). Будем считать, что $p \neq 2$, и для удобства рассмотрим уравнение $X^p + Y^p + Z^p = 0$.

Случай 1: $q \neq p$.

Пусть $F(X) = X^p + q^p - 1$. Тогда $X^p + q^p - 1 \equiv X^p - 1 \equiv$ $\equiv (X-1)(X^{p-1}+X^{p-2}+\ldots+X+1) \pmod{q}$. Поскольку $1 \pmod{q}$ не является корнем многочлена $X^{p-1}+X^{p-2}+\ldots+X+1$ по модулю q, по лемме Гензеля (см. гл. V, утверждения (1T) и (1U)) существует целое q-адическое число α, такое, что $\alpha \equiv 1 \pmod{q}$ и $\alpha^q + q^p + (-1)^p = 0$.

Случай 2: $q = p$.

Пусть $F(X) = X^p + p^p - 1$ и $G_0(X) = X - 1$, $H_0(X) = X^{p-1} + X^{p-2}+\ldots+X+1$. Из утверждения (4B) гл. II следует, что результант многочленов G_0 и H_0 равен $R = H_0(1) = p$, т. е. $v_p(R) = 1$. Так как $G_0(X)H_0(X) = X^p - 1$, мы получаем, что $F(X) \equiv G_0(X)H_0(X) \pmod{p^p}$. Но $p \geqslant 3 > 2v_p(R)$, поэтому мы можем применить лем-

му Гензеля (см. гл. V, утверждения (1T) и (1U)). Следовательно, существуют приведенные многочлены $G(X)$ и $H(X)$ из $\hat{\mathbb{Z}}_p[X]$, такие, что $G(X) \equiv G_0(X) \pmod{p^{p-1}}$, $H(X) \equiv H_0(X) \pmod{p^{p-1}}$ и $F(X) = G(X) \cdot H(X)$. Поэтому $G(X) = X - \alpha$, где α — целое p-адическое число, $\alpha \equiv 1 \pmod{p^{p-1}}$, $\alpha \neq 0$ и $F(\alpha) = 0$, т. е. $\alpha^p + p^p + (-1)^p = 0$. □

В процессе доказательства мы получили решения, одно из которых не является единицей в поле q-адических чисел. Поэтому возникает естественный вопрос: всегда ли существуют решения в q-адических единицах? В дальнейшем мы получим результаты, которые можно найти в работе Клёсгена 1970 г.

(1B) *Пусть $n \geqslant 1$, и пусть p — нечетное простое число. Тогда следующие условия равносильны.*

(a) *Существуют целые числа x, y, z, не делящиеся на p, такие, что $x^{p^n} + y^{p^n} + z^{p^n} \equiv 0 \pmod{p^{n+1}}$.*

(b) *Для каждого $m \geqslant 0$ существуют целые числа x_m, y_m, z_m, не делящиеся на p, такие, что $x_m^{p^n} + y_m^{p^n} + z_m^{p^n} \equiv 0 \pmod{p^{n+1+m}}$ и $x_{m+1} \equiv x_m \pmod{p^{m+1}}$, $y_{m+1} \equiv y_m \pmod{p^{m+1}}$, $z_{m+1} \equiv z_m \pmod{p^{m+1}}$.*

Доказательство. Достаточно показать, что из условия (a) следует условие (b). Воспользуемся индукцией по m. Если справедливо сравнение $x_m^{p^n} + y_m^{p^n} + z_m^{p^n} \equiv 0 \pmod{p^{n+1+m}}$, где x_m, y_m, z_m — целые числа, не кратные p, мы можем записать, что $x_m^{p^n} + y_m^{p^n} + z_m^{p^n} = r' p^{n+1+m}$, где $r' \in \mathbb{Z}$. Так как $p \nmid z_m$, существует целое число r, удовлетворяющее условию $r z_m^{p^n - 1} \equiv r' \pmod{p}$. Положим $x_{m+1} = x_m$, $y_{m+1} = y_m$ и $z_{m+1} = z_m - r p^{m+1}$. Тогда

$$\begin{aligned} z_{m+1}^{p^n} &= z_m^{p^n} - z_m^{p^n - 1} r p^{n+1+m} + \binom{p^n}{2} z_m^{p^n - 2} r^2 p^{2(1+m)} \\ &\quad - \binom{p^n}{3} z_m^{p^n - 3} r^3 p^{3(1+m)} + \dots \\ &\equiv z_m^{p^n} - z_m^{p^n - 1} r p^{n+1+m} \pmod{p^{n+2+m}}, \end{aligned}$$

и, поскольку $m \geqslant 0$, $p \neq 2$, число p^{n+2+m} делит все слагаемые, за исключением двух первых. Итак, мы получаем

$$x_{m+1}^{p^n} + y_{m+1}^{p^n} + z_{m+1}^{p^{n+1}} \equiv x_m^{p^n} + y_m^{p^n} + z_m^{p^n} - z_m^{p^n - 1} r p^{n+1+m}$$

$$\equiv (r' - z_m^{p^n-1} r) p^{n+1+m}$$
$$\equiv 0 \pmod{p^{n+2+m}}. \quad \square$$

Заметим, что фактически мы можем положить $x_m = x_0$, $y_m = y_0$ для каждого $m \geqslant 0$. В дополнение получим аналогичный результат при $p = 2$.

(1C) *Пусть $n \geqslant 1$. Тогда следующие условия равносильны.*

(a) *Существуют нечетные числа x, y, z, такие, что*

$$x^{2^n} + y^{2^n} + z^{2^n} \equiv 0 \pmod{2^{n+2}}.$$

(b) *Для каждого целого числа $m \geqslant 1$ существуют нечетные числа x_m, y_m, z_m, такие, что $x_m^{2^n} + y_m^{2^n} + z_m^{2^n} \equiv 0 \pmod{2^{n+2+m}}$ и $x_{m+1} \equiv x_m \pmod{2^{m+1}}$, $y_{m+1} \equiv y_m \pmod{2^{m+1}}$, $z_{m+1} \equiv z_m \pmod{2^{m+1}}$.*

Доказательство совершенно аналогично. Достаточно заметить, что если $z_{m+1} = z_m - r2^{m+1}$, то

$$z_{m+1}^{2^n} = z_m^{2^n} - z_m^{2^n-1} r 2^{n+1+m} + \binom{2^n}{2} z_m^{2^n-2} r^2 2^{2(1+m)}$$
$$- \binom{2^n}{3} z_m^{2^n-3} r^3 2^{3(1+m)} + \ldots$$
$$\equiv z_m^{2^n} - z_m^{2^n-1} r 2^{n+1+m} \pmod{2^{n+2+m}},$$

так как $2^{n-1+2(1+m)}$ делит все слагаемые, кроме двух первых, и $n + 2 + m \leqslant n - 1 + 2(1 + m)$, поскольку $m \geqslant 1$. $\square$

Для решений уравнения Ферма в p-адических единицах справедлив такой результат.

(1D) *Пусть p — нечетное простое число. Тогда следующие условия равносильны.*

(a) *Существуют единицы $\alpha, \beta, \gamma \in \hat{\mathbb{Z}}_p$, такие, что $\alpha^p + \beta^p + \gamma^p = 0$.*

(b) *Существуют целые числа x_0, y_0, z_0, не делящиеся на p, такие, что $x_0^p + y_0^p + z_0^p \equiv 0 \pmod{p^2}$.*

(c) *Для каждого $n \geqslant 0$ существуют целые числа x_n, y_n, z_n, не делящиеся на p, такие, что $x_n^p + y_n^p + z_n^p \equiv 0 \pmod{p^{n+2}}$ и $x_{n+1} \equiv x_n \pmod{p^{n+1}}$, $y_{n+1} \equiv y_n \pmod{p^{n+1}}$, $z_{n+1} \equiv z_n \pmod{p^{n+1}}$.*

Доказательство. (a) $\Rightarrow$ (b) Представим числа α, β, γ в виде $\alpha = x_0 + \alpha' p$, $\beta = y_0 + \beta' p$, $\gamma = z_0 + \gamma' p$, где x_0, y_0, z_0 — целые числа,

$0 \leqslant x_0, y_0, z_0 \leqslant p-1$, и $\alpha', \beta', \gamma' \in \hat{\mathbb{Z}}_p$. Так как α, β, γ являются единицами, $p \nmid x_0 y_0 z_0$. Из равенства $\alpha^p + \beta^p + \gamma^p = 0$ следует, что $x_0^p + y_0^p + z_0^p \equiv 0 \pmod{p^2}$.

(b) $\Rightarrow$ (c) Это было доказано в утверждении (1B).

(c) $\Rightarrow$ (a) Последовательности целых чисел $(x_n)_{n\geqslant 0}$, $(y_n)_{n\geqslant 0}$, $(z_n)_{n\geqslant 0}$ p-адически сходятся, поскольку $x_{n+1} \equiv x_n \pmod{p^{n+1}}$, $y_{n+1} \equiv y_n \pmod{p^{n+1}}$, $z_{n+1} \equiv z_n \pmod{p^{n+1}}$ для каждого $n \geqslant 0$. Пусть $\alpha = \lim x_n$, $\beta = \lim y_n$, $\gamma = \lim z_n$. Так как $x_n^p + y_n^p + z_n^p \equiv 0 \pmod{p^{n+2}}$, в пределе получим $\alpha^p + \beta^p + \gamma^p = 0$. $\square$

Из доказанного следует, что условия утверждения (1D) эквивалентны следующему.

(a′) Существуют целые числа x, y, не делящиеся на p, и единица $\gamma \in \hat{\mathbb{Z}}_p$, такие, что $x^p + y^p + \gamma^p = 0$.

Аналогичным образом доказывается и такой факт.

(1E) *Пусть q, p — различные простые числа. Тогда следующие условия равносильны.*

(a) *Существуют единицы $\alpha, \beta, \gamma \in \hat{\mathbb{Z}}_q$, такие, что $\alpha^p + \beta^p + \gamma^p = 0$.*

(b) *Существуют целые числа x_0, y_0, z_0, не делящиеся на q, такие, что $x_0^p + y_0^p + z_0^p \equiv 0 \pmod{q}$.*

(c) *Для любого $n \geqslant 0$ существуют целые числа x_n, y_n, z_n, не делящиеся на q, такие, что $x_n^p + y_n^p + z_n^p \equiv 0 \pmod{q^{n+1}}$ и $x_{n+1} \equiv x_n \pmod{q^{n+1}}$, $y_{n+1} \equiv y_n \pmod{q^{n+1}}$, $z_{n+1} \equiv z_n \pmod{q^{n+1}}$.*

Доказательство. (a) $\Rightarrow$ (b) Представим числа α, β, γ в виде $\alpha = x_0 + \alpha' q$, $\beta = y_0 + \beta' q$, $\gamma = z_0 + \gamma' q$, где x_0, y_0, z_0 — целые числа, $0 \leqslant x_0, y_0, z_0 \leqslant q-1$ и $\alpha', \beta', \gamma' \in \mathbb{Z}_q$. Поскольку α, β, γ — единицы, $q \nmid x_0 y_0 z_0$. Из равенства $\alpha^p + \beta^p + \gamma^p = 0$ следует, что $x_0^p + y_0^p + z_0^p \equiv 0 \pmod{q}$.

(b) $\Rightarrow$ (c) Докажем это утверждение индукцией по n. Для $n = 0$ утверждение верно. Предположим, что оно справедливо для некоторого $m \geqslant 0$. Пусть x_m, y_m, z_m — целые числа, не делящиеся на q, такие, что $x_m^p + y_m^p + z_m^p \equiv 0 \pmod{q^{m+1}}$. Тогда $x_m^p + y_m^p + z_m^p = r' q^{m+1}$, где r' — целое число. Так как $q \nmid z_m$, существует целое число r, удовлетворяющее сравнению $r p z_m^{p-1} \equiv r' \pmod{q}$. Положим $x_{m+1} = x_m$, $y_{m+1} = y_m$ и $z_{m+1} = z_m - r q^{m+1}$. Следовательно, $z_{m+1}^p = (z_m - r q^{m+1})^p \equiv z_m^p - p z_m^{p-1} r q^{m+1} \pmod{q^{m+2}}$ и $x_{m+1}^p + y_{m+1}^p + z_{m+1}^p \equiv x_m^p + y_m^p + z_m^p - p z_m^{p-1} r q^{m+1} \equiv (r' - p z_m^{p-1} r) q^{m+1} \equiv 0 \pmod{q^{m+2}}$.

(c) $\Rightarrow$ (a) Последовательности целых чисел $(x_n)_{n\geqslant 0}$, $(y_n)_{n\geqslant 0}$, $(z_n)_{n\geqslant 0}$ q-адически сходятся, поскольку $x_{n+1} \equiv x_n \pmod{q^{n+1}}$, $y_{n+1} \equiv y_n \pmod{q^{n+1}}$, $z_{n+1} \equiv z_n \pmod{q^{n+1}}$ при всех $n \geqslant 0$. Пусть $\alpha = \lim x_n$, $\beta = \lim y_n$, $\gamma = \lim z_n$. Так как $x_n^p + y_n^p + z_n^p \equiv 0 \pmod{q^{n+1}}$, в пределе получим $\alpha^p + \beta^p + \gamma^p = 0$. □

Так же как и для утверждении (1D), условия утверждения (1E) эквивалентны следующему.

(a″) Существуют целые числа x, y, не делящиеся на q, и единица $\gamma \in \hat{\mathbb{Z}}_q$, такие, что $x^p + y^p + \gamma^p = 0$.

Отметим, что уравнение Ферма (при $n \geqslant 3$) представляет собой интересный пример уравнения, у которого существуют нетривиальные решения в любом q-адическом поле (см. утверждение (1A)) и лишь тривиальные решения в целых числах, что было доказано Уайлсом.

Список литературы

1970 Klösgen, W., *Untersuchungen über Fermatsche Kongruenzen*, Gesellschaft Math. Datenverarbeitung, No. 36, 1970, 124 pp., Bonn.

X.2. Сравнение Ферма

Мы будем изучать следующие сравнения:

$$X^n + Y^n + Z^n \equiv 0 \pmod{q}, \tag{2.1}$$

$$X^n + Y^n \equiv Z^n \pmod{q}, \tag{2.2}$$

где q — нечетное простое число, $n \geqslant 0$ и q не делит n.

Пусть

$$N(n,q) = \#\{(x,y,z) \mid 1 \leqslant x,y,z < q,\ x^n + y^n + z^n \equiv 0 \pmod{q}\}$$

и

$$N'(n,q) = \#\{(x,y,z) \mid 1 \leqslant x,y,z < q,\ x^n + y^n \equiv z^n \pmod{q}\}.$$

Ясно, что если n — нечетное число, то $N(n,q) = N'(n,q)$. В этой связи рассмотрим следующие задачи.

(1) Определить, когда величины $N(n,q)$ и $N'(n,q)$ больше нуля.
(2) Найти верхние и нижние границы для $N(n,q)$ и $N'(n,q)$.
(3) Вычислить, если это возможно, значения $N(n,q)$ и $N'(n,q)$.

Напомним (см. гл. IV, утверждение (2A)), что если НОД$(n, q-1) = 1$ (значит, n — нечетное число), то $N(n,q) = N'(n,q) > 0$. В утверждении (2D) гл. IV мы также показали, что если числа p и $q = 6kp + 1$ простые, то $N(p,q) > 0$.

Следующее утверждение доказано Либри (1832, с. 275), Пепеном (1880), Пелле (1887) и Мэтьюсом (1895).

(2A) *Пусть p — простое число. Если существует бесконечное количество простых чисел q, таких, что $N(p,q) = 0$, то последняя теорема Ферма верна для показателя p.*

Доказательство. Предположим, что существуют ненулевые целые числа x, y, z, такие, что $x^p + y^p + z^p = 0$. Пусть q — любое простое число, удовлетворяющее условию $q > \max\{|x|, |y|, |z|\}$. Тогда $x^p + y^p + z^p \equiv 0 \pmod q$ и $N(p,q) > 0$. Таким образом, $N(p,q) = 0$ только для конечного количества простых чисел q, что и доказывает утверждение. □

Этот результат позволяет свести доказательство последней теоремы Ферма к доказательству того, что $N(p,q) = 0$ для бесконечного количества чисел q. На самом деле мы докажем обратное, а именно, что для каждого p существует простое число $q_0(p)$, такое, что если $q \geqslant q_0(p)$, то $N(p,q) > 0$.

Прежде чем приступить к доказательству этого утверждения, приведем некоторые из многочисленных результатов, связанных со сравнениями (2.1), (2.2).

Лежандр (1830) показал, что $N(3,7) = N(3,13) = 0$ и $N(5,q) = 0$ для $q = 11, 41, 71, 101$.

Либри написал ряд статей (1824, 1832), в которых был приведен метод вычисления количества решений для весьма общего вида сравнений. Либри вычислил $N(3,q)$ для многих простых чисел $q \equiv 1 \pmod 3$ и показал, что существует число $q_0(3)$, такое, что если $q \geqslant q_0(3)$, то $N(3,q) > 0$. Стоит отметить, что некоторые из вычисленных им значений оказались неверными. Такие же результаты были опубликованы Пепеном в 1880 г. (см. также его статью 1876 г.).

Так как $q \equiv 1 \pmod 3$, число -3 является квадратом по модулю q и существуют целые числа l, m одинаковой четности, такие, что $4q = l^2 + 3m^2$. Это следует из разложения числа q на множители в поле $\mathbb{Q}(\sqrt{-3})$. Поскольку число -3 является квадратом по модулю q, мы можем записать $q = \alpha\alpha'$, где $\alpha = (l + m\sqrt{-3})/2$, $\alpha' =$

$= (l - m\sqrt{-3})/2$ и l, m — целые числа одинаковой четности. Таким образом, $4q = l^2 + 3m^2$. Выберем представление с минимальным значением $|l|$. Заметим, что число l не делится на 3 и мы можем предполагать, что $l \equiv 1 \pmod 3$ (если это не так, то сделаем замену l на $-l$), следовательно, l однозначно определяется из введенных выше условий. Пепен показал, что

$$N(3, q) = (q - 1)(q - 8 + l). \tag{2.3}$$

Приведем несколько примеров:

$$\begin{aligned}
28 &= 1 + 3 \times 3^2 \quad \Rightarrow \quad N(3, 7) = 6(7 - 8 + 1) = 0;\\
52 &= 5^2 + 3 \times 3^2 \quad \Rightarrow \quad N(3, 13) = 12(13 - 8 - 5) = 0;\\
76 &= 1^2 + 3 \times 5^2 \quad \Rightarrow \quad N(3, 19) = 18(19 - 8 + 1) = 216;\\
124 &= 4^2 + 3 \times 6^2 \quad \Rightarrow \quad N(3, 31) = 30(31 - 8 + 4) = 810.
\end{aligned}$$

Пепен доказал, что если $l > -2\sqrt{q}$, то $N(3, q) > \sqrt{q}(\sqrt{q} - 2) - 8$. Отсюда следует, что если $q \geqslant 19$, то $N(3, q) > 0$.

Либри установил, что для любого простого числа p существует число $q_0(p)$, такое, что если $q \geqslant q_0(p)$, то $N(p, q) > 0$, однако он не нашел границы для $N(p, q)$ и способа вычисления $q_0(p)$. Пелле в 1887 г. использовал другой метод для получения такого же результата, и позднее (в 1911 г.) он установил границы для $N(p, q)$, но они оказались ошибочными.

В 1837 г. Лебег рассмотрел произвольные сравнения для многочленов

$$F(X_1, \ldots, X_s) \equiv 0 \pmod q, \tag{2.4}$$

где $s \geqslant 2$, q — нечетное простое число, $F \in \mathbb{Z}[X_1, \ldots, X_s]$. Пусть

$$\begin{aligned}
N = \#\{(x_1, \ldots, x_s) \mid\ & 1 \leqslant x_i \leqslant q - 1 \text{ для всех } i = 1, \ldots, s,\\
& \text{таких, что } F(x_1, \ldots, x_s) \equiv 0 \pmod q\},\\
N_0 = \#\{(x_1, \ldots, x_s) \mid\ & 0 \leqslant x_i \leqslant q - 1 \text{ для всех } i = 1, \ldots, s,\\
& \text{таких, что } F(x_1, \ldots, x_s) \equiv 0 \pmod q\}.
\end{aligned}$$

В многочлене F^{q-1} через A обозначим сумму коэффициентов всех одночленов $eX_1^{e_1} \ldots X_s^{e_s}$, таких, что $q - 1$ делит все e_i, а через A_0 — такую же сумму, но с дополнительным условием, что все e_i больше нуля.

Лебег показал, что N и N_0 удовлетворяют условиям

$$\begin{aligned}
N_0 &\equiv (-1)^{s+1} A_0 \pmod q,\\
N &\equiv (-1)^s (1 - A) \pmod q
\end{aligned}$$

Он применял свой метод к сравнениям вида

$$A_1 X_1^n + \ldots + A_s X_s^n \equiv 0 \pmod{q}, \tag{2.5}$$

где $n \geqslant 2$, $s \geqslant 2$, каждое A_i — ненулевое целое число, q — нечетное простое число, $q \equiv 1 \pmod{n}$. Лебег выразил количество решений N в терминах периодов кругового уравнения. Он подробно изучил следующие частные случаи сравнения (2.5): $s = 2, n = 2$; $s = 3$, $n = 3$; $s = 3$, $n = 4$. Для сравнения (2.1) при $n = 3$ Лебег повторил некоторые из результатов Либри.

Дальнейшие результаты, посвященные числу решений сравнения (2.5), опубликованы в работе Лебега 1838 г. В 1909 г. были опубликованы две статьи Диксона, а также статьи Корнаккьи и Гурвица, в которых они рассматривали это сравнение.

Корнаккья тщательно исследовал различные частные случаи сравнений (2.1) и (2.5) и получил много точных результатов, некоторые из которых были прежде указаны Лебегом, Пепеном и Пелле.

(a) Корнаккья доказал, что при $n = 2$ и $q \equiv 1 \pmod 4$ справедливо равенство

$$N'(2,q) = \begin{cases} \dfrac{q-9}{8}, & \text{если 2 есть квадрат по модулю } q, \\ \dfrac{q-5}{8} & \text{в противном случае,} \end{cases}$$

а при $n = 2$ и $q \equiv -1 \pmod 4$ имеет место равенство

$$N'(2,q) = \begin{cases} \dfrac{q-7}{8}, & \text{если 2 есть квадрат по модулю } q, \\ \dfrac{q-3}{8} & \text{в противном случае.} \end{cases}$$

(b) При $n = 3$ и $q \equiv 1 \pmod 3$ Корнаккья заново получил результат Пепена и показал, что если $N(3,q) = 0$, то $q = 7$ или 13.

(c) При $n = 4$ и $q \equiv 1 \pmod 4$ Корнаккья вычислил $N(4,q)$. Кроме того, он показал, что $N'(4,q) = 0$ в точности тогда, когда $q = 11, 17, 29, 41$.

(d) Значение $N'(6,q)$ при $n = 6$ и $q \equiv 1 \pmod 6$ также было определено в статье Корнаккьи. Кроме того, он доказал, что $N'(6,q) = 0$ только при $q = 7, 13, 19, 43, 61, 97, 157, 277$ и, с другой стороны, для сравнения $X^6 + Y^6 + Z^6 \equiv 0 \pmod q$ равенство $N(6,q) = 0$ выполняется лишь при $q = 7, 13, 31, 61, 67, 79, 97, 139, 157, 223, 277$.

(e) При $n = 8$ и $q \equiv 1 \pmod 8$ Корнаккья получил верхнюю и нижнюю оценки для $N'(8, q)$. Кроме того, он доказал, что $N'(8, q) = 0$ лишь при $q = 17, 41, 113$, и для сравнения $X^8 + Y^8 + Z^8 \equiv 0 \pmod q$ установил, что $N(8, q) = 0$ только в случае $q = 17, 41, 113, 137, 233, 761$.

Диксон в своих статьях (1909) рассмотрел сравнение (2.1). Его метод, использующий периоды круговых уравнений, позволил найти верхнюю и нижнюю границы для $N(p, q)$, а также верхнюю границу для $q_0(p)$, а именно

$$q_0(p) \leqslant (p-1)^2(p-2)^2 + 6p - 2.$$

В частности, Диксон показал, что $N(5, q) = 0$ в точности тогда, когда $q = 11, 41, 71, 101$, а $N(7, q) = 0$ лишь при $q = 29, 71, 113, 491$. Используя вычисления Кэри (1893) для квадратов и произведений периодов, Диксон применил свой метод к сравнению $X^4 + Y^4 \equiv Z^4 \pmod q$.

В работе Гурвица (1909) изучается сравнение более общего вида (2.5) при $n = p$, где p — простое число. Он рассмотрел семейство таких сравнений для всевозможных значений коэффициентов и указал соотношения, которым должны удовлетворять количества решений разнообразных сравнений из этого семейства. С помощью этих соотношений Гурвиц нашел верхнюю и нижнюю границы для числа решений сравнения

$$AX^p + BY^p + CZ^p \equiv 0 \pmod q, \tag{2.6}$$

где A, B, C — ненулевые целые числа. Он также определил положительное число $q_0(p)$ (зависящее от уравнения (2.6)), такое, что если $q \geqslant q_0(p)$, то уравнение (2.6) имеет решение (x, y, z), удовлетворяющее условию $1 \leqslant x, y, z \leqslant q - 1$.

В 1917 г. Шур доказал, что для любого $n \geqslant 2$ при $q \geqslant (n!)e + 1$ сравнение $X^n + Y^n + Z^n \equiv 0 \pmod q$ имеет такое решение (x, y, z), что $1 \leqslant x, y, z \leqslant q-1$. Доказательство Шура основано на следующей интересной комбинаторной лемме.

Лемма 2.1. *Пусть $n \geqslant 1$ и $N \geqslant (n!)e + 1$. Пусть, далее, множество чисел $\{1, 2, \ldots, N\}$ разбито на n непересекающихся подмножеств $L_1, \ldots, L_n$. Тогда существует по крайней мере одно подмножество L_i, такое, что если m и $m' \in L_i$, $m < m'$, то $m' - m \in L_i$.*

В дальнейшем уравнения

$$AX^e + BY^f + CZ^g = 0$$

и

$$A_1 X_1^{n_1} + A_2 X_2^{n_2} + \ldots + A_s X_s^{n_s} = 0,$$

с коэффициентами из конечного поля с q^d элементами ($d \geqslant 1$) и, возможно, различными показателями были объектом многочисленных исследований (см. работы Митчелла (1917), Вандивера (1944, 1945, 1946, 1947, 1948, 1949, 1954, 1955, 1956, 1959), Хуа и Вандивера (1948, 1949), Э. Лемера и Вандивера (1957)). Полный список литературы, включающий сравнительно недавние работы, читатель может найти в соответствующем разделе журнала «Mathematical Reviews».

В своей работе 1949 г. А. Вейль развернул историческую панораму развития первоначального метода Гаусса для сравнения $AX^3 - BY^3 \equiv 1 \pmod q$, где q — простое число, $q \equiv 1 \pmod 3$, основанного на суммах Гаусса. Эти идеи впоследствии были применены к широкому классу сравнений. Они использовались Харди и Литлвудом в связи с проблемой Варинга, Хассе выразил связь между гипотезой Римана для полей функций и различными типами тригонометрических сумм, А. Вейль опубликовал блестящие окончательные результаты по этому вопросу (1928).

Здесь мы отметим следующий результат (см. Вандивер (1946, с. 47–52); Хуа и Вандивер (1948, с. 258–263)), который непосредственно связан с предметом нашего исследования.

Пусть $s \geqslant 1$, $A_1, \ldots, A_s$ — ненулевые целые числа, $n_1, \ldots, n_s$ — целые числа, q — нечетное простое число, и пусть $d_i = \text{НОД}\,(q-1, |n_i|) > 1$ для $i = 1, \ldots, s$. Обозначим через N количество решений сравнения

$$A_1 X_1^{n_1} + \ldots + A_s X_s^{n_s} \equiv 0 \pmod q \qquad (2.7)$$

в целых числах $(x_1, \ldots, x_s)$, $1 \leqslant x_i \leqslant q-1$ (при $i = 1, \ldots, s$). Тогда

$$\frac{(q-1)^s}{q} - d_1 \ldots d_s q^{s/2} < N < \frac{(q-1)^s}{q} + d_1 \ldots d_s q^{s/2}.$$

В частности, существует положительное число q_0, такое, что при $q \geqslant q_0$ справедливо неравенство $N > 0$. Другое доказательство этой теоремы с использованием теории групповых характеров дано Фейтом (1967).

Теперь, после этого обзора результатов, которые связаны со сравнением Ферма, мы докажем теорему Диксона. Для этой цели напомним следующие обозначения и факты из гл. IX.

Предположим, что $p \geqslant 3$ и $q = 2kp + 1$ — простые числа.

Пусть

g — первообразный корень по модулю p,
ζ — первообразный корень степени p из единицы,
h — первообразный корень по модулю q,
ρ — первообразный корень степени q из единицы.

Запишем p периодов, состоящих из $2k$ членов в поле $\mathbb{Q}(\rho)$:

$$\begin{cases} \mu_0 = \rho + \rho^{h^p} + \rho^{h^{2p}} + \ldots + \rho^{h^{(2k-1)p}}, \\ \mu_1 = \rho^h + \rho^{h^{p+1}} + \rho^{h^{2p+1}} + \ldots + \rho^{h^{(2k-1)p+1}}, \\ \vdots \quad \vdots \\ \mu_i = \rho^{h^i} + \rho^{h^{p+i}} + \rho^{h^{2p+i}} + \ldots + \rho^{h^{(2k-1)p+i}}, \\ \vdots \quad \vdots \\ \mu_{p-1} = \rho^{h^{p-1}} + \rho^{h^{2p-1}} + \rho^{h^{3p-1}} + \ldots + \rho^{h^{q-2}}. \end{cases} \tag{2.8}$$

В гл. IX мы для каждого номера $j = 0, 1, \ldots, p-1$ определили резольвенты Лагранжа:

$$\lambda_j = \langle \zeta^j, \rho \rangle = \sum_{t=1}^{q-1} \zeta^{j \operatorname{ind}_h(t)} \rho^t, \tag{2.9}$$

где $\operatorname{ind}_h(t) = s$, $0 \leqslant s \leqslant q-2$, определяется из соотношения $t \equiv h^s \pmod q$. В частности, $\lambda_0 = \langle 1, \rho \rangle = \sum_{t=1}^{q-1} \rho^t = -1$.

Для удобства напомним также следующие результаты (см. утверждения (2D), (2E), (2F) гл. IX).

При $j = 1, \ldots, p-1$ мы имеем

$$\lambda_j \lambda_{p-j} = q, \tag{2.10}$$

$$|\lambda_j|^2 = \lambda_j \overline{\lambda_j} = q \tag{2.11}$$

($\overline{\lambda_j}$ — комплексное число, сопряженное с λ_j),

$$\mu_i = \frac{1}{p} \sum_{j=0}^{p-1} \zeta^{-ji} \lambda_j. \tag{2.12}$$

Дадим упрощенное доказательство теоремы Диксона, предложенное Клёсгеном (1970). Во-первых, выразим величину $N(p, q)$ через периоды μ_i.

(2B) *Справедливо равенство*

$$N(p,q) = \frac{1}{q} \left[(q-1)^3 + (q-1)p^2 \sum_{i=0}^{p-1} \mu_i^3 \right].$$

Доказательство. Для начала заметим, что для целых чисел x, y, z, удовлетворяющих условию $1 \leqslant x, y, z \leqslant q-1$, выполняется равенство

$$\sum_{t=0}^{q-1} \rho^{t(x^p+y^p+z^p)} = \begin{cases} 0, & \text{если } x^p+y^p+z^p \not\equiv 0 \pmod q, \\ q, & \text{если } x^p+y^p+z^p \equiv 0 \pmod q. \end{cases}$$

Таким образом,

$$\begin{aligned} qN(p,q) &= \sum_{x,y,z=1}^{q-1} \left(\sum_{t=0}^{q-1} \rho^{t(x^p+y^p+z^p)} \right) \\ &= \sum_{t=0}^{q-1} \left(\sum_{x,y,z=1}^{q-1} \rho^{tx^p} \rho^{ty^p} \rho^{tz^p} \right) \\ &= \sum_{t=0}^{q-1} \left(\sum_{x=1}^{q-1} \rho^{tx^p} \right)^3 \\ &= (q-1)^3 + \sum_{t=1}^{q-1} \left(\sum_{x=1}^{q-1} \rho^{tx^p} \right)^3. \end{aligned}$$

Если $t \equiv h^i \pmod q$ и $x \equiv h^j \pmod q$ (где $0 \leqslant i, j \leqslant q-2$), то $\sum_{x=1}^{q-1} \rho^{tx^p} = \sum_{j=0}^{q-2} \rho^{h^{i+pj}} = p\mu_i$. Так как $\mu_j = \mu_i$ при $j \equiv i \pmod p$, а $q = 2kp+1$, мы получаем

$$qN(p,q) = (q-1)^3 + 2k \sum_{i=0}^{p-1} p^3 \mu_i^3,$$

Поэтому

$$N(p,q) = \frac{1}{q} \left[(q-1)^3 + (q-1)p^2 \sum_{i=0}^{p-1} \mu_i^3 \right]. \quad \square$$

А теперь докажем теорему Диксона.

(2C) *Справедливы следующие утверждения:*

(1) $(q-1)[q+1-3p-(p-1)(p-2)\sqrt{q}] < N(p,q) < (q-1)[q+1-3p+(p-1)(p-2)\sqrt{q}]$;

(2) *при* $q \geqslant (p-1)^2(p-2)^2+6p-2$ *сравнение* (2.1) *имеет нетривиальное решение.*

ДОКАЗАТЕЛЬСТВО. (1) Из утверждения (2B) и равенства (2.11) следует, что

$$N(p,q) = \frac{1}{q}\left[(q-1)^3 + (q-1)p^2\frac{1}{p^3}\sum_{i=0}^{p-1}\left\{\sum_{j=0}^{p-1}\zeta^{-ji}\lambda_j\right\}^3\right]$$

$$= \frac{1}{q}\left[(q-1)^3 + \frac{q-1}{p}\sum_{i=0}^{p-1}\sum_{j_1,j_2,j_3=0}^{p-1}\zeta^{-i(j_1+j_2+j_3)}\lambda_{j_1}\lambda_{j_2}\lambda_{j_3}\right]$$

$$= \frac{1}{q}\left[(q-1)^3 + \frac{q-1}{p}\sum_{j_1,j_2,j_3=0}^{p-1}\lambda_{j_1}\lambda_{j_2}\lambda_{j_3}\left(\sum_{i=0}^{p-1}\zeta^{-i(j_1+j_2+j_3)}\right)\right].$$

Но

$$\sum_{i=0}^{p-1}\zeta^{-i(j_1+j_2+j_3)} = \begin{cases} 0, & \text{если } j_1+j_2+j_3 \not\equiv 0 \pmod p, \\ p, & \text{если } j_1+j_2+j_3 \equiv 0 \pmod p. \end{cases}$$

Поэтому

$$N(p,q) = \frac{1}{q}\left[(q-1)^3 + (q-1)\sum_{\substack{j_1,j_2,j_3=0 \\ j_1+j_2+j_3\equiv 0 \pmod p}}^{p-1}\lambda_{j_1}\lambda_{j_2}\lambda_{j_3}\right].$$

Так как $\lambda_0 = -1$, из соотношения (2.9) следует, что последняя сумма произведений $\lambda_{j_1}\lambda_{j_2}\lambda_{j_3}$ равна

$$\lambda_0^3 + 3\lambda_0\sum_{j=1}^{p-1}\lambda_j\lambda_{p-j} + S = -1 - 3q(p-1) + S,$$

где $S = \sum_{j_1,j_2,j_3=1}^{p-1}\lambda_{j_1}\lambda_{j_2}\lambda_{j_3}$. Следовательно,

$$N(p,q) = \frac{q-1}{q}[(q-1)^2 - 1 - 3q(p-1) + S],$$

а значит,

$$\frac{N(p,q)}{q-1} = \frac{1}{q}\left(q^2 - 3qp + q + S\right) = q - 3p + 1 + \frac{1}{q}S$$

и

$$\left|\frac{N(p,q)}{q-1} - (q+1-3p)\right| = \frac{1}{q}|S|.$$

Из равенства (2.10) имеем $|\lambda_j| = \sqrt{q}$. Заметим также, что для каждого j_1, $1 \leqslant j_1 \leqslant p-1$, существуют в точности $p-2$ пары (j_2, j_3), $1 \leqslant j_2, j_3 \leqslant p-1$, такие, что $j_1 + j_2 + j_3 = p$ или $2p$, а именно $(1, p-j_1-1)$, $(2, p-j_1-2), \ldots, (p-j_1-1, 1)$ и $(p-1, p-j_1+1)$, $(p-2, p-j_1+2), \ldots, (p-j_1+1, p-1)$. Следовательно, $|S| \leqslant (p-1)(p-2)q^{3/2}$, поэтому

$$\left|\frac{N(p,q)}{q-1} - (q+1-3p)\right| \leqslant (p-1)(p-2)\sqrt{q},$$

и мы можем заключить, что

$$\begin{aligned}(q-1)[q+1-3p-(p-1)(p-2)\sqrt{q}] &< N(p,q)\\ &< (q-1)[q+1-3p+(p-1)(p-2)\sqrt{q}].\end{aligned}$$

(2) Докажем следующее более общее утверждение, которое понадобится нам в дальнейшем: если ν — целое число, $\nu \geqslant 0$ и $q \geqslant (p-1)^2(p-2)^2 + 2(p\nu - 1)$, то $q+1-(p-1)(p-2)\sqrt{q} - p\nu \geqslant 0$. Если в этом утверждении положить $\nu = 3$ и воспользоваться неравенством (1), мы получим справедливость утверждения (2).

Как легко проверить, из неравенства

$$\alpha^2 + 2\beta \geqslant \alpha\sqrt{\alpha^2 + 4\beta}$$

(α и β — вещественные числа, такие, что $\alpha^2 + 2\beta \geqslant 0$) следует, что при $\alpha = (p-1)(p-2)$, $\beta = p\nu - 1$ справедливо неравенство

$$\begin{aligned}&(p-1)^2(p-2)^2 + 2(p\nu-1)\\ &\qquad \geqslant (p-1)(p-2)\sqrt{(p-1)^2(p-2)^2 + 4(p\nu-1)}.\end{aligned}$$

Положим $\delta = (p-1)^2(p-2)^2 + 4(p\nu-1) > 0$ и рассмотрим многочлены

$$f(T) = T^2 - (p-1)(p-2)T - (p\nu - 1)$$

с дискриминантом δ.

Достаточно показать, что

$$\sqrt{q} \geqslant \frac{(p-1)(p-2) + \sqrt{\delta}}{2}.$$

Действительно, из этого неравенства следует, что $f(\sqrt{q}) \geqslant 0$, т. е. $q + 1 - (p-1)(p-2)\sqrt{q} - p\nu \geqslant 0$. Но, как легко видеть,

$$\begin{aligned}4q &\geqslant 4[(p-1)^2(p-2)^2 + 2(p\nu-1)]\\ &\geqslant 2[(p-1)^2(p-2)^2 + 2(p\nu-1) + (p-1)(p-2)\sqrt{\delta}]\\ &= (p-1)^2(p-2)^2 + \delta + 2(p-1)(p-2)\sqrt{\delta}\\ &= [(p-1)(p-2) + \sqrt{\delta}]^2,\end{aligned}$$

а значит, выполняется неравенство $\sqrt{q} \geqslant ((p-1)(p-2)+\sqrt{\delta})/2$, что и требовалось доказать.

Из утверждения (1), подставляя $\nu = 3$, найдем

$$N(p,q) > (q-1)[(q+1) - 3p - (p-1)(p-2)\sqrt{q}] \geqslant 0. \quad \square$$

Верхние границы для числа $q_0(p)$, предложенные Диксоном, не являются точными, как это видно из следующих вычислений:

оценка Диксона	фактическое значение
$q_0(3) \leqslant 20$	$q_0(3) = 13$
$q_0(5) \leqslant 172$	$q_0(5) = 101$
$q_0(7) \leqslant 940$	$q_0(7) = 491$

Добавим, что в 1916 г. Мантель показал, что если $N(p,q) = 0$, то число q должно иметь вид $q = 6mp/(p-3) - 1$ (где m — некоторое целое число).

Принимая во внимание утверждение (2C) и результат (2B) гл. IV, получим, что если $k \geqslant 1$, $q = 2kp + 1$ — простое число и $q \geqslant (p-1)^2(p-2)^2 + 6p - 2$, то q делит определитель Вендта W_{2k}. Таким образом, для любого простого числа p существует не более чем конечное количество натуральных чисел k, таких, что число $q = 2kp + 1$ является простым и не делит W_{2k}. Неизвестно, существует ли в действительности *ровно* одно простое число q с вышеуказанным свойством для любого простого числа p (см. Фли Сен-Мари (1890) и Ландау (1913)).

Список литературы

1824 Libri, G., *Mémoires sur divers points d'analyse* (*art. cinquième*), Mém. Acad. Roy. Turin, **28** (1824), 152–280.

1830 Legendre, A.M., *Théorie des Nombres* (3^e édition), Firmin Didot Frères, Paris, 1830; reprinted by A. Blanchard, Paris, 1955.

1832 Libri, G., *Mémoires sur la théorie des nombres*, J. Reine Angew. Math., **9** (1832), 54–80, 169–188, 261–276.

1832 Libri, G., *Mémoire sur la résolution de quelques équations indéterminées*, J. Reine Angew. Math., **9** (1832), 277–294.

1837 Lebesgue, V.A., *Recherches sur les nombres*, J. Math. Pures Appl., **2** (1837), 255–292; **3** (1838), 113–144.

1876 Pepin, T., *Etude sur la théorie des résidues cubiques*, J. Math. Pures Appl., (3), **2** (1876), 313–324.

1880 Pepin, T., *Sur diverses tentatives de démonstration du théorème de Fermat*, C. R. Acad. Sci. Paris, **91** (1880), 366–367.

1887 Pellet, A.E., *Mémoire sur la théorie algébrique des équations*. Bull. Soc. Math. France, **15** (1887), 61–102.

1890 Flye Sainte-Marie, C., *Question 1339*, L'Interm. Math., **5** (1890), 195.

1893 Carey, F.S., *Notes on the division of the circle*, Quart. J. Pure Appl. Math., **26** (1893), 322–371.

1895 Matthews, G.B., *Note in connexion with Fermat's last theorem*, Messenger Math., **24** (1895), 97–99.

1909 Cornacchia, G., *Sulla congruenza* $x^n + y^n \equiv z^n \pmod{p}$, Giorn. Mat., **47** (1909), 219–268.

1909 Dickson, L.E., *On the congruence* $x^n + y^n + z^n \equiv 0 \pmod{p}$, J. Reine Angew. Math., **135** (1909), 134–141.

1909 Dickson, L.E., *Lower limit for the number of sets of solutions of* $x^e + y^e + z^e \equiv 0 \pmod{p}$, J. Reine Angew. Math., **135** (1909), 181–188.

1909 Hurwitz, A., *Über die Kongruenz* $ax^e + by^e + cz^e \equiv 0 \pmod{p}$, J. Reine Angew. Math., **136** (1909), 272–292.

1910 Dubouis, E., *Réponse à la question 1339 de C. Flye Sainte-Marie*, L'Interm. Math., **17** (1910), 103–104.

1910 Dubouis, E., *Problème 3771*, L'Interm. Math., **17** (1910), 241–242.

1911 Pellet, A.E., *Réponse à une question de M.E. Dubouis*, L'Interm. Math., **18** (1911), 81–82.

1913 Landau, E., *Réponse à la question 1339 de C. Flye Sainte-Marie*, L'Interm. Math., **20** (1913), 154.

1916 Mantel, W., *Vraagstuk XCI* (*Problem 91*), Wiskundige Opgaven, **12** (1916), 213–214.

1917 Schur, I., *Über die Kongruenz* $x^m + y^m \equiv z^m \pmod{p}$, Jahresber. Deutsch. Math.-Verein., **25** (1917), 114–117; reprinted in Gesammelte Abhandlungen, Vol. II, Springer-Verlag, Berlin, 1973.

1917 Mitchell, H.H., *On the congruence* $cx^\lambda + 1 \equiv dy^\lambda$ *in a Galois field*, Ann. of Math., (2), **18** (1917), 120–131.

1919 Bachmann, P., *Das Fermatproblem in seiner bisherigen Entwicklung*, W. de Gruyter, Berlin, 1919; reprinted by Springer-Verlag. Berlin, 1976.

1928 Weil, A., *L'arithmétique sur les courbes algébriques*, Acta Math., **52** (1928), 281–315; reprinted in *Oeuvres Scientifiques*, Vol. I, pp. 11–35, Springer-Verlag, New York, 1980.

1944 Vandiver, H.S., *Some theorems in finite fields with applications to Fermat's last theorem*, Proc. Nat. Acad. Sci. U.S.A., **30** (1944), 362–367.

1944 Vandiver, H.S., *On trinomial congruences and Fermat's last theorem*, Proc. Nat. Acad. Sci. U.S.A., **30** (1944), 368–370.

1945 Vandiver, H.S., *On the number of solutions of certain non-homogeneous trinomial equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A., **31** (1945), 170–175.

1946 Vandiver, H.S., *On the number of solutions of some general types of equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A., **32** (1946), 47–52.

1946 Vandiver, H.S., *Cyclotomy and trinomial equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A., **32** (1946), 317–319.

1946 Vandiver, H.S., *On some special trinomial equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A., **32** (1946), 320–326.

1947 Vandiver, H.S., *Limits for the number of solutions of certain general types of equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A., **33** (1947), 236–242.

1948 Hua, L.K. and Vandiver, H.S., *On the existence of solutions of certain equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A., **34** (1948), 258–263.

1948 Vandiver, H.S., *Applications of cyclotomy to the theory of non-homogeneous equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A., **34** (1948), 62–66.

1948 Vandiver, H.S., *Cyclotomic power characters and trinomial equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A., **34** (1948), 196–203.

1949 Hua, L.K. and Vandiver, H.S., *Characters over certain types of rings with applications to the theory of equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A., **35** (1949), 89–95.

1949 Hua, L.K. and Vandiver, H.S., *On the nature of the solutions of certain equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A., **35** (1949), 481–487.

1949 Hua, L.K. and Vandiver, H.S., *On the number of solutions of some trinomial equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A., **35** (1949), 477–481.

1949 Vandiver, H.S., *Quadratic relations involving the number of solutions of certain types of equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A., **35** (1949), 681–685.

1949 Weil, A., *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc., **55** (1949), 497–508; reprinted in *Oeuvres Scientifiques*, Vol. I, pp. 399–410, Springer-Verlag, New York, 1980.

1954 Vandiver, H.S., *On trinomial equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A., **40** (1954), 1008–1010.

1955 Vandiver, H.S., *On the properties of certain trinomial equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A., **41** (1955), 651–653.

1955 Vandiver, H.S., *On cyclotomic relations and trinomial equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A., **41** (1955), 775-780.

1956 Leveque, W.J., *Topics in Number Theory*, Vol. 2, Addison-Wesley, Reading, MA, 1956.

1956 Vandiver, H.S., *Diophantine equations in certain rings*, Proc. Nat. Acad. Sci. U.S.A., **42** (1956), 656–665.

1957 Lehmer, E. and Vandiver, H.S., *On the computation of the number of solutions of certain trinomial congruences*, J. Assoc. Comput. Mach., 4 (1957), 505–510.

1959 Vandiver, H.S., *On distribution problems involving the numbers of solutions of certain trinomial congruences*, Proc. Nat. Acad. Sci. U.S.A., **45** (1959), 1635–1641.

1967 Feit, W., *Characters of Finite Groups*, Benjamin, New York, 1967.

1970 Klösgen, W., *Untersuchungen über Fermatsche Kongruenzen*, Gesellschaft Math. Datenverarbeitung, No. 36, 1970, 124 pp., Bonn.

X.3. Сравнение Гурвица

Здесь мы докажем теорему Гурвица для сравнения

$$A_1 X_1^p + \ldots + A_s X_s^p \equiv 0 \pmod q, \tag{3.1}$$

где $p \geqslant 3$ и $q = 2kp + 1$ — простые числа и $A_1, \ldots, A_s$ — ненулевые целые числа. Пусть $N = N(A_1, \ldots, A_s, p, q)$ обозначает количество нетривиальных решений сравнения (3.1), т. е. количество наборов $(x_1, \ldots, x_s)$, $1 \leqslant x_i \leqslant q-1$, таких, что $\sum_{i=1}^s A_i x_i^p \equiv 0 \pmod q$. Пусть h — первообразный корень по модулю q, $a_i = \operatorname{ind}_h(A_i)$ (где $0 \leqslant a_i \leqslant q-2$). Тогда $A_i \equiv h^{a_i} \pmod q$ при $i = 1, \ldots, s$.

Таким образом, число N равно количеству наборов $(t_1, \ldots, t_s)$, $0 \leqslant t_i \leqslant q-2$, таких, что $\sum_{i=1}^s h^{pt_i + a_i} \equiv 0 \pmod q$.

Рассмотрим функцию $\chi\colon \mathbb{Z} \to \{0,1\}$, определенную соотношением

$$\chi(z) = \begin{cases} 1, & \text{если } q \mid z, \\ 0, & \text{если } q \nmid z. \end{cases}$$

Тогда

$$N = \sum_{t_1,\ldots,t_s=0}^{q-2} \chi\left(\sum_{i=1}^{s} h^{pt_i+a_i}\right). \tag{3.2}$$

Заметив, что $h^{pt_i+a_i} \equiv h^{pt_i'+a_i} \pmod q$ при $t_i \equiv t_i' \pmod{2k}$, мы можем переписать равенство (3.2) в виде

$$N = p^s \sum_{t_1,\ldots,t_s=0}^{2k-1} \chi\left(\sum_{i=1}^{s} h^{pt_i+a_i}\right). \tag{3.3}$$

Для удобства введем следующий символ:

$$[a_1,\ldots,a_s] = \frac{1}{2k} \sum_{t_1,\ldots,t_s=0}^{2k-1} \chi\left(\sum_{i=1}^{s} h^{pt_i+a_i}\right), \tag{3.4}$$

который является неотрицательным рациональным числом. Тогда равенство (3.3) принимает вид

$$N = 2kp^s[a_1,\ldots,a_s] = (q-1)p^{s-1}[a_1,\ldots,a_s], \tag{3.5}$$

поэтому, чтобы определить N, нам необходимо изучить свойства символа $[a_1,\ldots,a_s]$.

Во-первых, заметим, что $[a_1] = 0$, так как $q \nmid h^{pt_1+a_1}$ для любого t_1, $0 \leqslant t_1 \leqslant q-2$.

Лемма 3.1. *Справедливы равенства*

$$[a_1,a_2] = \begin{cases} 1, & \textit{если} \quad a_1 \equiv a_2 \pmod p, \\ 0, & \textit{если} \quad a_1 \not\equiv a_2 \pmod p. \end{cases}$$

Доказательство. Число q делит $h^{pt_1+a_1} + h^{pt_2+a_2}$ тогда и только тогда, когда $h^{pt_1+a_1} \equiv -h^{pt_2+a_2} \equiv h^{(q-1)/2+pt_2+a_2} \pmod q$, что эквивалентно сравнению $pt_1 + a_1 \equiv (q-1)/2 + pt_2 + a_2 \pmod{(q-1)}$. Пусть $a_1 \equiv a_2 \pmod p$, т. е. $a_2 = mp + a_1$ для некоторого целого числа m. Для каждого t_2, $0 \leqslant t_2 \leqslant 2k-1$, обозначим через t_1, $0 \leqslant t_1 \leqslant 2k-1$, единственное такое целое число, что $t_1 \equiv k + m + t_2 \pmod{2k}$. Тогда $(q-1)/2 + pt_2 + a_2 = p(k + t_2 + m) + a_1 \equiv pt_1 + a_1$

$(\mathrm{mod}\ 2kp)$. Следовательно,

$$[a_1, a_2] = \frac{1}{2k} \sum_{t_1, t_2 = 0}^{2k-1} \chi(h^{pt_1 + a_1} + h^{pt_2 + a_2}) = 1.$$

Обратно, если для некоторого числа t_2, $0 \leqslant t_2 \leqslant 2k-1$, существует единственное число t_1, такое, что $0 \leqslant t_1 \leqslant 2k-1$ и $pt_1 + a_1 \equiv pt_2 + a_2 + kp \pmod{q-1}$, то $p(t_1 - t_2 - k) \equiv a_2 - a_1 \pmod{2kp}$, поэтому $p \mid (a_2 - a_1)$. Если же $a_1 \not\equiv a_2 \pmod{p}$, то $\chi(h^{pt_1 + a_1} + h^{pt_2 + a_2}) = 0$ при любых t_1, t_2, значит, $[a_1, a_2] = 0$. $\square$

Приведем некоторые простые свойства символа $[a_1, \ldots, a_s]$.

Лемма 3.2.

(1) *Значение величины* $[a_1, \ldots, a_s]$ *не меняется при любых перестановках чисел* $a_1, \ldots, a_s$;

(2) $[a_1, \ldots, a_s] = [a'_1, \ldots, a'_s]$ *при* $a_1 \equiv a'_1 \pmod{p}, \ldots, a_s \equiv a'_s \pmod{p}$;

(3) $[a_1 + u, \ldots, a_s + u] = [a_1, \ldots, a_s]$ *при любом целом* u.

Доказательство. (1) Это следует непосредственно из определения символа $[a_1, \ldots, a_s]$.

(2) Действительно, пусть $a_i = pr_i + a'_i$ и $t_i + r_i \equiv t'_i \pmod{2k}$, где $0 \leqslant t'_i \leqslant 2k-1$. Тогда $h^{p(t_i + r_i)} \equiv h^{pt'_i} \pmod{q}$ и

$$[a_1, \ldots, a_n] = \frac{1}{2k} \sum_{t_1, \ldots, t_s = 0}^{2k-1} \chi\left(\sum_{i=1}^{s} h^{pt_i + a_i}\right)$$

$$= \frac{1}{2k} \sum_{t_1, \ldots, t_s = 0}^{2k-1} \chi\left(\sum_{i=1}^{s} h^{p(t_i + r - i) + a'_i}\right)$$

$$= \frac{1}{2k} \sum_{t'_1, \ldots, t'_s = 0}^{2k-1} \chi\left(\sum_{i=1}^{s} h^{pt'_i + a'_i}\right) = [a'_1, \ldots, a'_s].$$

(3) Так как $h^u \not\equiv 0 \pmod{q}$, для каждого $t_i = 0, 1, \ldots, q-2$ справедливо равенство

$$\chi\left(\sum_{i=1}^{s} h^{pt_i + a_i + u}\right) = \chi\left(\sum_{i=1}^{s} h^{pt_i + a_i}\right),$$

поэтому $[a_1 + u, \ldots, a_s + u] = [a_1, \ldots, a_s]$ для любого целого числа u. $\square$

ЛЕММА 3.3. *Символ* $[a_1, \ldots, a_s]$ *есть неотрицательное целое число, и оно представляется в виде*

$$[a_1, \ldots, a_s] = \sum_{t'_1, \ldots, t'_{s-1}=0}^{2k-1} \chi(h^{pt'_1+a_1} + \ldots + h^{pt'_{s-1}+a_{s-1}} + h^{a_s})$$

$$= \sum_{t'_1, \ldots, t'_{s-1}=0}^{2k-1} \chi(h^{pt'_1+a_1} + \ldots + h^{pt'_{s-1}+a_{s-1}} - h^{a_s}).$$

ДОКАЗАТЕЛЬСТВО. При заданных $t_1, \ldots, t_{s-1}$, $0 \leqslant t_i \leqslant 2k-1$, для каждого t_s определим $t'_1, \ldots, t'_{s-1}$ из условий $0 \leqslant t'_i \leqslant 2k-1$ и $t'_i \equiv t_i - t_s \pmod{2k}$. Заметив, что $h^{pt_s} \not\equiv 0 \pmod{q}$, получим

$$[a_1, \ldots, a_s]$$

$$= \frac{1}{2k} \sum_{t_1, \ldots, t_{s-1}=0}^{2k-1} \sum_{t_s=0}^{2k-1} \chi\left(\sum_{i=1}^{s} h^{pt_i+a_i}\right)$$

$$= \frac{1}{2k} \sum_{t'_1, \ldots, t'_{s-1}=0}^{2k-1} \sum_{t_s=0}^{2k-1} \chi(h^{pt_s}(h^{pt'_1+a_1} + \ldots + h^{pt'_{s-1}+a_{s-1}} + h^{a_s}))$$

$$= \frac{1}{2k} 2k \sum_{t'_1, \ldots, t'_{s-1}=0}^{2k-1} \chi(h^{pt'_1+a_1} + h^{pt'_2+a_2} + \ldots + h^{pt'_{s-1}+a_{s-1}} + h^{a_s}).$$

Следовательно, $[a_1, \ldots, a_s]$ — неотрицательное целое число. Для доказательства второго равенства заметим, что $a_s \equiv a_s + (q-1)/2 \pmod{p}$ и $h^{(q-1)/2} \equiv -1 \pmod{q}$, и, используя лемму 3.2, найдем

$$[a_1, \ldots, a_s] = \left[a_1, \ldots, a_{s-1}, a_s + \frac{q-1}{2}\right]$$

$$= \sum_{t'_1, \ldots, t'_{s-1}=0}^{2k-1} \chi(h^{pt'_1+a_1} + \ldots + h^{pt'_{s-1}+a_{s-1}} - h^{a_s}). \quad \square$$

ЛЕММА 3.4. *При* $r, s \geqslant 1$ *выполнено равенство*

$$[a_1, \ldots, a_s, b_1, \ldots, b_r]$$

$$= 2k[a_1, \ldots, a_s][b_1, \ldots, b_r] + \sum_{c=0}^{p-1} [a_1, \ldots, a_s, c][b_1, \ldots, b_r, c].$$

Доказательство. Пусть $A_i \equiv h^{a_i} \pmod q$ и $B_j \equiv h^{b_j} \pmod q$. Тогда

$$2kp^{s+r}[a_1, \ldots, a_s, b_1, \ldots, b_r] = N,$$

где N — количество решений $(x_1, \ldots, x_s, y_1, \ldots, y_r)$ сравнения $\sum_{i=1}^{s} A_i X_i^p + \sum_{j=1}^{r} B_j Y_j^p \equiv 0 \pmod q$, удовлетворяющих условию $1 \leqslant x_i, y_j \leqslant q-1$. Пусть N' обозначает число решений $(x_1, \ldots, x_s)$ сравнения $\sum_{i=1}^{s} A_i X_i^p \equiv 0 \pmod q$, таких, что $1 \leqslant x_i \leqslant q-1$, а N'' — число решений сравнения $\sum_{j=1}^{r} B_j Y_j^p \equiv 0 \pmod q$.

Для каждого $d = 0, 1, \ldots, q-2$ через N'_d обозначим число решений $(x_1, \ldots, x_s)$ сравнения

$$\sum_{i=1}^{s} A_i X_i^p + h^d \equiv 0 \pmod q$$

при $1 \leqslant x_i \leqslant q-1$, а через N''_d — число решений $(y_1, \ldots, y_r)$ сравнения

$$\sum_{j=1}^{r} B_j Y_j^p p - h^d \equiv 0 \pmod q$$

при $1 \leqslant y_j \leqslant q-1$. Тогда $N' = 2kp^s[a_1, \ldots, a_s]$, $N'' = 2kp^r[b_1, \ldots, b_r]$ и из леммы 3.3 мы получим

$$N'_d = p^s \sum_{t'_1, \ldots, t'_s = 0}^{2k-1} \chi\left(\sum_{i=1}^{s} h^{pt'_i + a_i} + h^d\right) = p^s[a_1, \ldots, a_s, d],$$

$$N''_d = p^r \sum_{t'_1, \ldots, t'_r = 0}^{2k-1} \chi\left(\sum_{j=1}^{r} h^{pt'_j + b_j} - h^d\right) = p^r[b_1, \ldots, b_r, d].$$

Справедливо соотношение $N = N'N'' + \sum_{d=0}^{q-2} N'_d N''_d$. Но

$$[a_1, \ldots, a_s, d] = [a_1, \ldots, a_s, c],\ [b_1, \ldots, b_r, d] = [b_1, \ldots, b_r, c],$$

если $d \equiv c \pmod p$. Таким образом,

$$\begin{aligned} 2kp^{s+r}&[a_1, \ldots, a_s, b_1, \ldots, b_r] \\ &= 4k^2 p^{s+r}[a_1, \ldots, a_s][b_1, \ldots, b_r] \\ &\quad + 2kp^{s+r} \sum_{c=0}^{p-1} [a_1, \ldots, a_s, c][b_1, \ldots, b_r, c], \end{aligned}$$

и, разделив на $2kp^{s+r}$, мы получим необходимое равенство. □

ЛЕММА 3.5. *Для любых целых чисел a_1, a_2, c справедливо равенство*

$$\sum_{d=0}^{p-1}[a_1, a_2, c+d] = 2k - [a_1, a_2].$$

В частности, эта сумма не зависит от выбора числа c.

ДОКАЗАТЕЛЬСТВО. По лемме 3.3 мы имеем

$$\sum_{d=0}^{p-1}[a_1, a_2, c+d] = \sum_{d=0}^{p-1}[c+d, a_1, a_2]$$
$$= \sum_{d=0}^{p-1}\left(\sum_{t,u=0}^{2k-1}\chi(h^{pt+d+c} + h^{pu+a_1} + h^{a_2})\right).$$

Обозначим через U_1 множество всех целых чисел u, $0 \leqslant u \leqslant 2k-1$, таких, что $h^{pu+a_1} + h^{a_2} \equiv 0 \pmod q$. Тогда по лемме 3.3 количество элементов множества U_1 есть $\#U_1 = \sum_{u=0}^{2k-1}\chi(h^{pu+a_1} + h^{a_2}) = [a_1, a_2]$. Пусть U_2 обозначает множество всех целых чисел u, $0 \leqslant u \leqslant 2k-1$, не лежащих в U_1. Тогда $\#U_2 = 2k - [a_1, a_2]$. Справедливо соотношение

$$\sum_{d=0}^{p-1}[a_1, a_2, c+d] = \sum_{u\in U_1}\sum_{d=0}^{p-1}\sum_{t=0}^{2k-1}\chi(h^{pt+d+c} + h^{pu+a_1} + h^{a_2})$$
$$+ \sum_{u\in U_2}\sum_{d=0}^{p-1}\sum_{t=0}^{2k-1}\chi(h^{pt+d+c} + h^{pu+a_1} + h^{a_2}).$$

Если $u \in U_1$, то $\chi(h^{pt+d+c} + h^{pu+a_1} + h^{a_2}) = \chi(h^{pt+d+c}) = 0$. А если $u \in U_2$, то существует ровно одна пара (d, t), такая, что $h^{pt+d+c} + h^{pu+a_1} + h^{a_2} \equiv 0 \pmod q$. Поэтому $\sum_{d=0}^{p-1}[a_1, a_2, c+d] = \#U_2 = 2k - [a_1, a_2]$. □

ЛЕММА 3.6. *Для любых целых чисел a_1, a_2, a_3, a_4 справедливо равенство*

$$\sum_{d=0}^{p-1}[a_1 + d, a_2 + d, a_3, a_4]$$
$$= (q-1)[a_1, a_2][a_3, a_4] + (2k - [a_1, a_2])(2k - [a_3, a_4]).$$

Доказательство. Из лемм 3.4 и 3.2 получим

$$\begin{aligned}\sum_{d=0}^{p-1}[a_1+d,a_2+d,a_3,a_4] &= 2k\left(\sum_{d=0}^{p-1}[a_1+d,a_2+d]\right)[a_3,a_4]\\ &\quad+\sum_{d,c=0}^{p-1}[a_1+d,a_2+d,c][a_3,a_4,c]\\ &= 2kp[a_1,a_2][a_3,a_4]\\ &\quad+\left(\sum_{d'=0}^{p-1}[a_1,a_2,d']\right)\left(\sum_{c=0}^{p-1}[a_3,a_4,c]\right)\end{aligned}$$

(где $d' \equiv c-d \pmod p$, $0 \leqslant d' \leqslant p-1$). Применение леммы 3.5 завершает доказательство. □

Для всех целых чисел n и m положим

$$\alpha_{n,m} = \sum_{d=0}^{p-1}[d, m+nd, 0]. \tag{3.6}$$

Лемма 3.7. *Справедливы следующие свойства чисел* $\alpha_{n,m}$:

(1) $\alpha_{0,m} = 2k-[m,0]$, $\alpha_{1,m} = 2k-[m,0]$;

(2) *если* $n \equiv n' \pmod p$ *и* $m \equiv m' \pmod p$, *то* $\alpha_{n,m} = \alpha_{n',m'}$;

(3) $\sum_{m=0}^{p-1}\alpha_{n,m} = q-2$.

Доказательство. (1) По леммам 3.2 и 3.5 мы получаем

$$\alpha_{0,m} = \sum_{d=0}^{p-1}[d,m,0] = \sum_{d=0}^{p-1}[m,0,d] = 2k-[m,0].$$

Аналогично

$$\alpha_{1,m} = \sum_{d=0}^{p-1}[d,m+d,0] = \sum_{d'=0}^{p-1}[0,m,d'] = \sum_{d'=0}^{p-1}[m,0,d'] = 2k-[m,0],$$

где $d' \equiv -d \pmod p$, $0 \leqslant d' \leqslant p-1$.

(2) Из леммы 3.2 следует, что $\alpha_{n,m}$ зависят только от классов вычетов n и m по модулю p.

(3) Наконец, в силу леммы 3.5 мы имеем

$$\begin{aligned}\sum_{m=0}^{p-1}\alpha_{n,m} &= \sum_{m=0}^{p-1}\sum_{d=0}^{p-1}[d, m+nd, 0]\\ &= \sum_{d=0}^{p-1}\sum_{m=0}^{p-1}[d, 0, m+nd]\\ &= \sum_{d=0}^{p-1}(2k-[d,0])\\ &= 2kp-1 = q-2. \quad \square\end{aligned}$$

Для всех целых чисел n и m положим

$$\sigma_{n,m} = \sum_{d=0}^{p-1}\alpha_{n,d}\alpha_{n,d+m} = \sum_{d,c,e=0}^{p-1}[c, d+nc, 0][e, d+m+ne, 0]. \quad (3.7)$$

Лемма 3.8. *При всех m, n справедливо соотношение*

$$\begin{aligned}\sigma_{n,m} = \sum_{j=0}^{p-1}\{&(q-1)[(n-1)j+m, 0][nj+m, 0]\\ &+(2k-[(n-1)j+m, 0])(2k-[nj+m, 0])\}-2k,\end{aligned}$$

а при $n \not\equiv 0, 1 \pmod p$ выполняются равенства

$$\sigma_{n,m} = \begin{cases} 2k(q-4)+q, & \text{если } m \equiv 0 \pmod p,\\ 2k(q-4), & \text{если } m \not\equiv 0 \pmod p.\end{cases}$$

Доказательство. Преобразуем выражение для $\sigma_{n,m}$ следующим образом:

$$\begin{aligned}\sigma_{n,m} &= \sum_{c,e=0}^{p-1}\left(\sum_{d=0}^{p-1}[c, d+nc, 0][e, d+m+ne, 0]\right)\\ &= \sum_{c,e=0}^{p-1}\left(\sum_{d=0}^{p-1}[c-nc, -nc, d][e-ne-m, -ne-m, d]\right).\end{aligned}$$

Из леммы 3.4 следует, что эта сумма равна

$$\sum_{c,e=0}^{p-1}([c-nc,-nc,e-ne-m,-ne-m]$$
$$-2k[c-nc,-nc][e-ne-m,-ne-m])$$
$$=\sum_{c,e=0}^{p-1}([c-nc,-nc,e-ne-m,-ne-m]-2k[c,0][e,0])\,.$$

По леммам 3.1 и 3.2 последняя сумма равна

$$\sum_{e=0}^{p-1}\left(\sum_{c=0}^{p-1}[c-nc+ne+m,-nc+ne+m,e,0]\right)-2k.$$

Пусть $j=e-c$ (для любого фиксированного e). Тогда $c-nc+ne-+m=(n-1)j+m+e$ и $-nc+ne+m=nj+m$. Поэтому рассматриваемая сумма равна

$$\sum_{e=0}^{p-1}\left\{\sum_{j=0}^{p-1}[(n-1)j+m+e,e,nj+m,0]\right\}-2k$$
$$=\sum_{j=0}^{p-1}\left\{\sum_{e=0}^{p-1}[(n-1)j+m+e,e,nj+m,0]\right\}-2k,$$

что согласно лемме 3.6 равняется

$$\sum_{j=0}^{p-1}\{(q-1)[(n-1)j+m,0][nj+m,0]$$
$$+(2k-[(n-1)j+m,0])(2k-[nj+m,0])\}-2k.$$

Если $n\not\equiv 0,1 \pmod p$ и $m\equiv 0 \pmod p$, то

$$\begin{aligned}\sigma_{n,m} &= \sum_{j=0}^{p-1}\{(q-1)[(n-1)j,0][nj,0]\\ &\qquad +(2k-[(n-1)j,0])(2k-[nj,0])\}-2k\\ &= (q-1)+4pk^2-2k-2k+1-2k\\ &= q+2k(q-1)-6k\\ &= q+2k(q-4).\end{aligned}$$

А если $n \not\equiv 0, 1 \pmod{p}$ и $m \not\equiv 0 \pmod{p}$, то, используя аналогичные выкладки, мы получим, что

$$\sigma_{n,m} = 4(p-2) + 4k(2k-1) - 2k = 2k(q-4). \quad \square$$

ЛЕММА 3.9. *При $n \not\equiv 0, 1 \pmod{p}$ для каждого целого числа m справедливы неравенства*

$$q - 2 - (p-1)\sqrt{q} < p\alpha_{n,m} < q - 2 + (p-1)\sqrt{q}.$$

ДОКАЗАТЕЛЬСТВО. Мы показали, что

$$\sigma_{n,0} = \alpha_{n,0}^2 + \alpha_{n,1}^2 + \ldots + \alpha_{n,p-1}^2 = 2k(q-4) + q,$$

а если $r \not\equiv 0 \pmod{p}$, то

$$\sigma_{n,r} = \alpha_{n,0}\alpha_{n,r} + \alpha_{n,1}\alpha_{n,r+1} + \ldots + \alpha_{n,p-1}\alpha_{n,r+p-1} = 2k(q-4).$$

Таким образом,

$$\begin{aligned}(\alpha_{n,0} - \alpha_{n,r})^2 + (\alpha_{n,1} - \alpha_{n,r+1})^2 + \ldots + (\alpha_{n,p-1} - \alpha_{n,r+p-1})^2 \\ = 2\left(\sum_{c=0}^{p-1} \alpha_{n,c}^2\right) - 2\left(\sum_{c=0}^{p-1} \alpha_{n,c}\alpha_{n,r+c}\right) \\ = 2[2k(q-4) + q] - 4k(q-4) = 2q.\end{aligned}$$

Следовательно,

$$\begin{aligned}2q &\geqslant (\alpha_{n,m} - \alpha_{n,m+r})^2 + (\alpha_{n,m-r} - \alpha_{n,m})^2 \\ &= 2\left[\left(\alpha_{n,m} - \frac{\alpha_{n,m+r} + \alpha_{n,m-r}}{2}\right)^2 + \left(\frac{\alpha_{n,m+r} - \alpha_{n,m-r}}{2}\right)^2\right] \\ &\geqslant 2\left(\alpha_{n,m} - \frac{\alpha_{n,m+r} + \alpha_{n,m-r}}{2}\right)^2.\end{aligned}$$

Поскольку число $\sqrt{q}$ иррационально, справедливы строгие неравенства

$$\sqrt{q} > \alpha_{n,m} - \frac{\alpha_{n,m+r} + \alpha_{n,m-r}}{2} > -\sqrt{q}.$$

Эти неравенства выполнены при каждом $r = 1, 2, \ldots, p-1$. Складывая их и учитывая, что

$$\sum_{r=1}^{p-1} \frac{\alpha_{n,m+r} + \alpha_{n,m-r}}{2} = -\alpha_{n,r} + \sum_{r=0}^{p-1} \frac{\alpha_{n,m+r} + \alpha_{n,m-r}}{2}$$

и согласно лемме 3.7

$$\sum_{r=0}^{p-1}\alpha_{n,m+r}=\sum_{r=0}^{p-1}\alpha_{n,m-r}=\sum_{j=0}^{p-1}\alpha_{n,j}=q-2,$$

получим, что

$$(p-1)\sqrt{q}>(p-1)\alpha_{n,m}-(-\alpha_{n,m}+q-2)>-(p-1)\sqrt{q},$$

поэтому

$$q-2-(p-1)\sqrt{q}<p\alpha_{n,m}<q-2+(p-1)\sqrt{q}.\ \square$$

Доказав эти леммы, перейдем к исследованию сравнения

$$AX^p+BY^p+CZ^p\equiv 0 \pmod q, \tag{3.8}$$

где A, B и C — ненулевые целые числа. Пусть $A\equiv h^a \pmod q$, $B\equiv$ $\equiv h^b \pmod q$ и $C\equiv h^c \pmod q$, где $0\leqslant a,b,c\leqslant q-2$.

(3А) *Во введенных выше обозначениях*

$$p[a,b,c]=6k+2-q-\nu+\sum_{n=2}^{p-1}\alpha_{n,b-c-n(a-c)},$$

где

$$\nu=[a,b]+[b,c]+[c,a]$$
$$=\begin{cases}0, & \textit{если } a,b,c \textit{ попарно несравнимы по модулю } p,\\ 3, & \textit{если } a,b,c \textit{ сравнимы друг с другом},\\ 1, & \textit{если ровно два из чисел } a,b,c \textit{ сравнимы друг с другом}.\end{cases}$$

Доказательство. Вычислим сумму $S=\sum_{n=0}^{p-1}\alpha_{n,d-ne}$, где d и e — целые числа. По определению

$$S=\sum_{n=0}^{p-1}\sum_{j=0}^{p-1}[j,d-ne+nj,0].$$

Если $j\equiv e \pmod p$, то при любом n справедливо сравнение $d-$ $-ne+nj\equiv d \pmod p$. А если $j\not\equiv e \pmod p$, то $\{d-ne+nj \mid n=$ $=0,1,\ldots,p-1\}$ есть множество целых чисел, попарно несравнимых

по модулю p. Таким образом, по лемме 3.5 мы получаем

$$S = p[e,d,0] + \sum_{t=0}^{p-1} \sum_{\substack{j=0 \\ j \not\equiv e \pmod p}}^{p-1} [j,t,0]$$

$$= p[e,d,0] + \sum_{\substack{j=0 \\ j \not\equiv e \pmod p}}^{p-1} (2k - [j,0]).$$

Значит,

$$S = p[e,d,0] + 2k(p-1) + [e,0] - \sum_{j=0}^{p-1} [j,0]$$

$$= p[e,d,0] + 2kp - 2k + [e,0] - 1$$

$$= p[e,d,0] + [e,0] + q - 2 - 2k.$$

Но $\alpha_{0,d} = 2k - [d,0]$ и $\alpha_{1,d-e} = 2k - [d-e,0] = 2k - [d,e]$, поэтому

$$p[e,d,0] = \sum_{n=2}^{p-1} \alpha_{n,d-ne} + 6k - (q-2) - \{[d,0] + [d,e] + [e,0]\}.$$

Пусть $e = a-c$, $d = b-c$. Тогда $p[a,b,c] = p[a-c,b-c,0] = p[e,d,0] = \sum_{n=2}^{p-1} \alpha_{n,b-c-n(a-c)} + 6k - (q-2) - \nu$. □

Теперь мы можем доказать теорему Гурвица (1909).

(3B) *Число N решений (x,y,z) сравнения* (3.8), *таких, что* $1 \leqslant x,y,z \leqslant q-1$, *удовлетворяет неравенствам*

$$(q-1)[(q+1) - (p-1)(p-2)\sqrt{q} - p\nu] < N$$
$$< (q-1)[(q+1) + (p-1)(p-2)\sqrt{q} - p\nu].$$

Доказательство. По лемме 3.9 имеем

$$(p-2)[q-2-(p-1)\sqrt{q}] < p\sum_{n=2}^{p-1} \alpha_{n,b-c-n(a-c)} < (p-2)[q-2+(p-1)\sqrt{q}].$$

Поэтому, учитывая результат (3A), получим

$$p(6k+2-q-\nu) + (p-2)[(q-2) - (p-1)\sqrt{q}]$$
$$< p^2[a,b,c] < p(6k+2-q-\nu) + (p-2)[(q-2) + (p-1)\sqrt{q}],$$

то есть

$$q+1-\nu p-(p-2)(p-1)\sqrt{q} < p^2[a,b,c] < q+1-\nu p+(p-2)(p-1)\sqrt{q}.$$

Но $N=(q-1)p^2[a,b,c]$ (по формуле (3.5)), поэтому

$$(q-1)[(q+1)-(p-1)(p-2)\sqrt{q}-p\nu] < N < (q-1)[(q+1)+(p-1)(p-2)\sqrt{q}-p\nu]. \quad \square$$

Для доказательства существования решения сравнения (3.8) достаточно убедиться, что при некоторых условиях выражение $q+1-(p-1)(p-2)\sqrt{q}-p\nu$ неотрицательно.

(3C) *Если* $q \geqslant (p-1)^2(p-2)^2+2(p\nu-1)$, *то* $N>0$.

Доказательство. В части (2) результата (2C) было показано, что если $q \geqslant (p-1)^2(p-2)^2+2(p\nu-1)$, то $q \geqslant (p-1)(p-2)\sqrt{q}+p\nu-1$. Тогда из утверждения (3B) следует, что $N>0$. $\square$

Список литературы

1909 Hurwitz, A., *Über die Kongruenz* $ax^e+by^e+cz^e \equiv 0 \pmod p$, J. Reine Angew. Math., **136** (1909), 272–292.

X.4. Сравнение Ферма по модулю, равному степени простого числа

Здесь мы рассмотрим сравнение

$$X^{p^m}+Y^{p^m}+Z^{p^m} \equiv 0 \pmod{p^n},$$

где p — нечетное простое число и $n>m \geqslant 1$. Согласно утверждению (1B) достаточно ограничиться рассмотрением сравнения

$$X^{p^m}+Y^{p^m}+Z^{p^m} \equiv 0 \pmod{p^{m+1}}. \tag{4.1}$$

Мы уже приступали к изучению этого сравнения в разд. VI.1. Напомним (см. утверждение (1H) гл. VI), что целые числа x,y и z, не делящиеся на p и удовлетворяющие сравнению (4.1), существуют тогда и только тогда, когда найдется такое число a, $1 \leqslant a \leqslant (p-3)/2$, что $1+a^{p^m} \equiv (1+a)^{p^m} \pmod{p^{m+1}}$.

Теперь рассмотрим общий случай. Пусть $k \geqslant 3$, $m \geqslant 1$ и p — нечетное простое число. Мы будем изучать сравнение

$$X_1^{p^m}+X_2^{p^m}+\ldots+X_k^{p^m} \equiv 0 \pmod{p^{m+1}}. \tag{4.2}$$

Решением (нетривиальным) назовем такой набор $(x_1, x_2, \ldots, x_k)$ целых чисел, что $1 \leqslant x_i \leqslant p^{m+1} - 1$, $p \nmid x_i$ (для всех $i = 1, \ldots, k$), $x_1^{p^m} + x_2^{p^m} + \ldots + x_k^{p^m} \equiv 0 \pmod{p^{m+1}}$. Два решения $(x_1, x_2, \ldots, x_k)$ и $(y_1, y_2, \ldots, y_k)$ называются *эквивалентными*, если существуют целое число a, не делящееся на p, $1 \leqslant a \leqslant p^{m+1} - 1$, и перестановка π множества $\{1, 2, \ldots, k\}$, такие, что $y_i \equiv a x_{\pi(i)} \pmod{p^{m+1}}$ при $i = 1, \ldots, k$. Ясно, что это есть отношение эквивалентности на множестве решений.

Для каждого целого числа a положим $\bar{a} = a \pmod{p^{m+1}}$ и обозначим через $\left(\mathbb{Z}/p^{m+1}\right)^\bullet$ приведенную систему вычетов по модулю p^{m+1}. Пусть

$$U = U(p^{m+1}) = \{\bar{b} \mid \text{существует число } a, \text{ взаимно простое с } p, \text{ такое, что } \bar{b} = \bar{a}^{p^m}\}$$

и

$$V = V(p^{m+1}) = \{\bar{b} \mid b \equiv 1 \pmod{p}\}.$$

Хорошо известно, что U и V являются подгруппами группы $(\mathbb{Z}/p^{m+1})^\bullet$, причем U содержит $p - 1$ элемент, а V состоит из p^m элементов, и

$$(\mathbb{Z}/p^{m+1})^\bullet \cong U \times V \tag{4.3}$$

(см. литературу по элементарной теории чисел или книгу Рибенбойма по алгебраическим числам (1999)).

Положим $hU = \{\sum_{i=1}^h \overline{a_i} \mid \overline{a_i} \in U \text{ при } i = 1, \ldots, h\}$ для каждого натурального числа h. Сравнение (4.2) разрешимо тогда и только тогда, когда $\bar{0} \in kU$.

Пусть, например, $m = 1$. Если $p = 3$, то $U = \{\bar{1}, \bar{8}\}$ и легко проверить, что $\bar{0} \notin 3U, 5U, 7U$ и $\bar{0} \in hU$ для всех $h \neq 1, 3, 5, 7$.

Покажем, что куб не может быть суммой двух, четырех или шести кубов, если они не делятся на 3. Допустим противное: если, к примеру, $y^3 = \sum_{i=1}^6 x_i^3$, то $(-y)^3 + \sum_{i=1}^6 x_i^3 = 0$ и, следовательно, $(-\bar{y})^3 + \sum_{i=1}^6 \bar{x}_i^3 = \bar{0}$ (где $\overline{-y}$, $\overline{x_i}$ принадлежат U), а это невозможно.

Аналогично, если $p = 5$, то $U = \{\bar{1}, \bar{7}, \overline{18}, \overline{24}\}$. Легко убедиться, что $\bar{0} \notin U, 3U, 5U$ и $\bar{0} \in hU$ для всех $h \neq 1, 3, 5$. Таким образом, пятая степень целого числа не может быть суммой двух или четырех пятых степеней целых чисел, если эти числа не делятся на 5.

Пусть g — первообразный корень по модулю p, $1 < g < p$, и пусть $r \equiv g^{p^m} \pmod{p^{m+1}}$, $1 < r < p^{m+1}$. Тогда числа $1, r, r^2, r^3, \ldots, r^{p-2}$ попарно несравнимы по модулю p^{m+1} и $U = \{\bar{1}, \bar{r}, \bar{r}^2, \bar{r}^3, \ldots, \bar{r}^{p-2}\}$. Другими словами, при заданном r каждый элемент $\bar{x}^{p^m} \in U$ ра-

вен некоторой степени $\bar{r}^i$, $0 \leqslant i \leqslant p-2$. Таким образом, каждому решению сравнения (4.2) соответствует представление нуля в виде суммы степеней элемента $\bar{r}$ в $(\mathbb{Z}/p^{m+1})^\bullet$, т. е. сравнение

$$r^{i_1} + r^{i_2} + \ldots + r^{i_k} \equiv 0 \pmod{p^{m+1}},$$

где $0 \leqslant i_t \leqslant p-2$ (при $t = 1, \ldots, k$), причем это соответствие есть биекция.

Два представления нуля $(r^{i_1}, \ldots, r^{i_k})$ и $(r^{j_1}, \ldots, r^{j_k})$ называются *эквивалентными*, если соответствующие решения сравнения (4.2) эквивалентны, т. е. существуют перестановка π множества $\{1, 2, \ldots, k\}$ и целое число h, $0 \leqslant h \leqslant p-2$, такие, что $i_t \equiv j_{\pi(t)} + h \pmod{(p-1)}$ при $t = 1, \ldots, k$.

Представление нуля $(r^{i_1}, \ldots, r^{i_k})$ называется *нормированным*, если $i_1 = 0 \leqslant i_2 \leqslant \ldots \leqslant i_k \leqslant p-2$. Легко видеть, что каждое представление эквивалентно некоторому нормированному. Однако, как мы увидим ниже, класс эквивалентных представлений нуля может содержать и более одного нормированного представления нуля.

Циклическим решением сравнения (4.2) назовем такое решение $(x_1, x_2, \ldots, x_k)$, что $x_1 \equiv 1 \pmod{p^{m+1}}$ и $x_j \equiv a^{j-1} \pmod{p^{m+1}}$ для $j = 2, \ldots, k$, где a — некоторое целое число, не делящееся на p. Соответствующее циклическому решению представление нуля назовем *циклическим*. Оно имеет вид (относительно заданного первообразного корня по модулю p)

$$1 + r^i + r^{2i} + \ldots + r^{(k-1)i} \equiv 0 \pmod{p^{m+1}} \qquad (4.4)$$

(при некотором i, $0 \leqslant i \leqslant p-2$).

(4A) *Если $p \equiv 1 \pmod{k}$, то существует циклическое представление нуля. А именно, можно положить $i = (p-1)/k$.*

Доказательство. Справедлива цепочка сравнений

$$(1 + r^i + \ldots + r^{(k-1)i})(1 - r^i) \equiv 1 - r^{ki} \equiv 1 - r^{p-1} \equiv 0 \pmod{p^{m+1}}.$$

Но $r \equiv g^{p^m} \pmod{p^{m+1}}$, поэтому $r \equiv g \pmod{p}$, а значит, r есть первообразный корень по модулю p. Если $r^i \equiv 1 \pmod{p}$, то $p-1$ делит число $i = (p-1)/k$, следовательно, $k = 1$, что противоречит определению циклического представления. Таким образом, элемент $(1 - r^i) \pmod{p^{m+1}}$ обратим, так что $1 + r^i + \ldots + r^{(k-1)i} \equiv 0 \pmod{p^{m+1}}$. □

В частном случае, когда $k = 3$ и $m = 1$, мы получаем циклическое представление $1 + r^i + r^{2i} \equiv 0 \pmod{p^2}$, где $i = (p-1)/3$, $r \equiv g^p$

(mod p^2). Тогда $r^i \equiv (g^{(p-1)/3})^p \pmod{p^2}$ и $(r^i)^3 \equiv g^{(p-1)p} \equiv 1 \pmod{p^2}$, поэтому r^i есть кубический корень из единицы по модулю p^2.

Следующий признак для теоремы Ферма основывается на существовании нециклического представления (см. Клёсген, 1970).

(4B) *Пусть $m \geqslant 1$, p — нечетное простое число, и пусть существуют такие целые числа x, y и z, не делящиеся на p, что $x^{p^m} + y^{p^m} + z^{p^m} = 0$. Тогда существует нециклическое представление нуля по модулю p^{3m+1}.*

Доказательство. По предположению

$$(x^{p^{m-1}})^p + (y^{p^{m-1}})^p + (z^{p^{m-1}})^p = 0,$$

поэтому в соответствии с результатом Поллачека, который был сформулирован в утверждении (2S) гл. VI, мы получаем

$$x^{2p^{m-1}} + (xy)^{p^{m-1}} + y^{2p^{m-1}} \not\equiv 0 \pmod{p}$$

и, следовательно,

$$x^2 + xy + y^2 \not\equiv 0 \pmod{p}.$$

Пусть w — целое число, такое, что $wx \equiv y \pmod{p}$. Тогда

$$1 + w + w^2 \not\equiv 0 \pmod{p}.$$

Из равенства $x^{p^m} + y^{p^m} + z^{p^m} = 0$ следует, что $x^{p^{3m}} + y^{p^{3m}} + z^{p^{3m}} \equiv 0 \pmod{p^{3m+1}}$ (см. утверждение (1M) гл. VI). Также справедливо сравнение $x + y + z \equiv 0 \pmod{p}$. Поэтому $z \equiv -(x+y) \equiv -x(1+w) \pmod{p}$ и, следовательно,

$$z^{p^{3m}} \equiv -x^{p^{3m}}(1+w)^{p^{3m}} \pmod{p^{3m+1}}.$$

Таким образом,

$$x^{p^{3m}}(1 + w^{p^{3m}} - (1+w)^{p^{3m}}) \equiv 0 \pmod{p^{3m+1}},$$

а значит,

$$1 + w^{p^{3m}} - (1+w)^{p^{3m}} \equiv 0 \pmod{p^{3m+1}}.$$

Если $-(1+w)^{p^{3m}} \equiv w^{2p^{3m}} \pmod{p^{3m+1}}$, то $-(1+w) \equiv w^2 \pmod{p}$. Тогда $1 + w + w^2 \equiv 0 \pmod{p}$, и мы получаем противоречие.

Если $w^{p^{3m}} \equiv (1+w)^{2p^{3m}} \pmod{p^{3m+1}}$, то $w \equiv (1+w)^2 \pmod{p}$, а значит, $1 + w + w^2 \equiv 0 \pmod{p}$, и мы снова приходим к противоречию. Следовательно, мы нашли нециклическое представление нуля по модулю p^{3m+1}. □

Пусть, например, $p \equiv 1 \pmod 3$, и пусть единственное представление нуля по модулю p^4 является циклическим и имеет вид

$$1 + r^i + r^{2i} \equiv 0 \pmod{p^4},$$

где g — первообразный корень по модулю p, $r \equiv g^{p^3} \pmod{p^4}$. Тогда первый случай теоремы Ферма выполняется для показателя p.

Следуя Клёсгену и сохраняя введенные обозначения, докажем такой факт.

(4C) (1) *Пусть* $1+r^i+r^j \equiv 0 \pmod{p^{m+1}}$, *где* $1 \leqslant i < j \leqslant p-2$, — *нормированное представление. Тогда всякое эквивалентное ему нормированное представление совпадает с одним из трех следующих представлений:*

(R_1) $1 + r^i + r^j \equiv 0 \pmod{p^{m+1}}$;
(R_2) $1 + r^{j-i} + r^{p-1-i} \equiv 0 \pmod{p^{m+1}}$;
(R_3) $1 + r^{p-1-j} + r^{p-1-j+i} \equiv 0 \pmod{p^{m+1}}$.

При $j = 2i$ *представления* (R_1), (R_2), (R_3) *совпадают. При* $j \neq 2i$ *эти представления различны.*

(2) *Если* $1 + 1 + r^j \equiv 0 \pmod{p^{m+1}}$ — *нормированное представление, то* $j \geqslant 1$ *и всякое нормированное представление, эквивалентное данному, совпадает с одним из двух следующих представлений:*

(R'_1) $1 + 1 + r^j \equiv 0 \pmod{p^{m+1}}$;
(R'_2) $1 + r^{p-1-j} + r^{p-1-j} \equiv 0 \pmod{p^{m+1}}$.

В этом случае представления (R'_1) *и* (R'_2) *различны и* $2^{p^m} \equiv 2 \pmod{p^{m+1}}$.

Доказательство. (1) Представление (R_2) получается из представления (R_1) умножением на r^{p-1-i}:

$$r^{p-1-i} + r^{p-1} + r^{p-1-i+j} \equiv 0 \pmod{p^{m+1}}.$$

Тогда $1 + r^{j-i} + r^{p-1-i} \equiv 0 \pmod{p^{m+1}}$, и это нормированное представление (так как $1 \leqslant j - i < p - 1 - i \leqslant p - 2$), эквивалентное представлению (R_1).

Так же доказывается, что представление (R_3) эквивалентно представлению (R_2). Пусть $r^h + r^{h+i} + r^{h+j} \equiv 0 \pmod{p^{m+1}}$ — эквивалентное данному нормированное представление. Тогда выполняется один из трех следующих случаев:

(a) $h \equiv 0 \pmod{(p-1)}$, это есть представление (R_1);
(b) $h + i \equiv 0 \pmod{(p-1)}$, это есть представление (R_2);
(c) $h + j \equiv 0 \pmod{(p-1)}$, это есть представление (R_3).

Если $j = 2i$, то $1 + r^i + r^{2i} \equiv 0 \pmod{p^{m+1}}$, $1 + r^i + r^{p-1-i} \equiv 0 \pmod{p^{m+1}}$ и $1 + r^{p-1-2i} + r^{p-1-i} \equiv 0 \pmod{p^{m+1}}$. Тогда $r^{2i} \equiv r^{p-1-i} \pmod{p^{m+1}}$. Следовательно, $2i \equiv p-1-i \pmod{p-1}$. Но $1 \leqslant 2i$ и $p-1-i \leqslant p-2$, поэтому $2i = p-1-i$, значит, $i = (p-1)/3$. Отсюда мы заключаем, что представления (R_1), (R_2) и (R_3) совпадают с циклическим представлением $1+r^{(p-1)/3}+r^{2(p-1)/3} \equiv 0 \pmod{p^{m+1}}$.

Теперь докажем, что в противном случае эти представления будут различными.

Если представления (R_1) и (R_2) совпадают, то $i = j - i$, значит, $j = 2i$, а это противоречит предположению. Аналогично, если представления (R_1) и (R_3) совпадают, то $i = p-1-j$, $j = p-1-j+i$, и мы вновь получим, что $i = (p-1)/3$ и $j = 2(p-1)/3 = 2i$.

Наконец, если представления (R_2) и (R_3) совпадают, то $j - i = p-1-j$, $p-1-i = p-1-j+i$ и опять $2i = j$.

(2) Если $1 + 1 + r^j \equiv 0 \pmod{p^{m+1}}$, то нормированное представление (R'_2), эквивалентное данному, получается умножением на r^{p-1-j}. Отметим также, что $j \neq 0$, так как $p^{m+1} > 3$. Поэтому представление (R'_2) не совпадает с представлением (R'_1). В этом случае $2 + r^j \equiv 0 \pmod{p^{m+1}}$. Используя сравнение $r \equiv g^{p^m} \pmod{p^{m+1}}$ и заметив, что $g^{p^m} \equiv g \pmod{p}$, мы получим, что $2+g^j \equiv 0 \pmod{p}$, а значит, $g^j \equiv -2 \pmod{p}$. Следовательно, $g^{jp^m} \equiv -2^{p^m} \pmod{p^{m+1}}$, и, таким образом, $2^{p^m} \equiv 2 \pmod{p^{m+1}}$. □

Приведем другую формулировку этого результата.

(4D) *Классы эквивалентных решений сравнения*

$$1 + X_2^{p^m} + X_3^{p^m} \equiv 0 \pmod{p^{m+1}}$$

состоят из шести различных решений, за исключением следующих случаев:

(a) $p \equiv 1 \pmod 6$, $a \not\equiv 1 \pmod{p^2}$ *и* $a^3 \equiv 1 \pmod{p^2}$; *в этом случае существует класс эквивалентных решений, состоящий из решений вида* $(1, \overline{a}, \overline{a}^2)$ *и* $(1, \overline{a}^2, \overline{a})$;

(b) $2^{p^m} \equiv 2 \pmod{p^{m+1}}$; *в этом случае существует класс эквивалентных решений, состоящий из решений вида* $(\overline{1}, \overline{1}, -\overline{2})$, $(\overline{1}, -\overline{2}, \overline{1})$ *и* $\left(\overline{1}, (-\overline{2})^{p^m(p-2)}, (-\overline{2})^{p^m(p-2)}\right)$.

Доказательство. Согласно утверждению (4C) при $p \equiv 1 \pmod 6$ данное сравнение имеет циклическое решение и его класс эквивалентности состоит ровно из двух решений (одно из которых норми-

ровано). Если $p \not\equiv 1 \pmod 6$, то не существует циклического решения. Если $1+1+r^j \equiv 0 \pmod{p^{m+1}}$, то существует в точности три решения в этом классе эквивалентности (два из которых нормированы), причем в этом случае $2^{p^m} \equiv 2 \pmod{p^{m+1}}$. В остальных случаях каждый класс эквивалентности состоит ровно из шести различных решений. □

Покажем, что в некоторых случаях можно получить новое решение сравнения (4.1) из данного (см. Пешль, 1965).

(4E) *Пусть* $1+r^i+r^j \equiv 0 \pmod{p^{m+1}}$, *где* $j \equiv 3i+(p-1)/2 \pmod{(p-1)}$. *Тогда* $1+r^{4i}+r^{(p-1)/2+5i} \equiv 0 \pmod{p^{m+1}}$, *и это представление не эквивалентно данному.*

Доказательство. Так как $r^{(p-1)/2} \equiv -1 \pmod{p^{m+1}}$, справедливо сравнение $1+r^i-r^{3i} \equiv 0 \pmod{p^{m+1}}$. Поэтому $-r^i-r^{2i}+r^{4i} \equiv 0 \pmod{p^{m+1}}$ и $r^{2i}+r^{3i}-r^{5i} \equiv 0 \pmod{p^{m+1}}$. Складывая эти сравнения, получим, что $1+r^{4i}-r^{5i} \equiv 0 \pmod{p^{m+1}}$, т. е. $1+r^{4i}+r^{(p-1)/2+5i} \equiv 0 \pmod{p^{m+1}}$.

Если это нормированное представление эквивалентно данному, то из утверждения (4C) получим один из трех следующих случаев:

(a) $4i \equiv i \pmod{p-1}$ и $5i \equiv 3i \pmod{p-1}$; тогда имеем $i \equiv 0 \pmod{p-1}$, следовательно, $i=0$ и $1+1-1 \equiv 0 \pmod{p^{m+1}}$, а это невозможно;

(b) $4i \equiv 2i+(p-1)/2 \pmod{p-1}$ и $(p-1)/2+5i \equiv p-1-i \pmod{p-1}$; мы, как и выше, приходим к противоречию;

(c) $4i \equiv (p-1)/2-3i \pmod{p-1}$ и $(p-1)/2+5i \equiv (p-1)/2-2i \pmod{p-1}$; это также невозможно. □

Аналогичным образом можно получить следующий результат.

(4F) *Пусть* $p \equiv 1 \pmod 4$ *и*

$$1 \pm r^{(p-1)/4}+r^j \equiv 0 \pmod{p^{m+1}}.$$

Тогда

$$1+1 \pm r^{2j+(p-1)/4} \equiv 0 \pmod{p^{m+1}},$$

и это представление не эквивалентно данному.

Доказательство. Из сравнения

$$1 \pm r^{(p-1)/4}+r^j \equiv 0 \pmod{p^{m+1}}$$

следует, что

$$\mp r^{(p-1)/4}+1 \mp r^{j+(p-1)/4} \equiv 0 \pmod{p^{m+1}}$$

и

$$\pm r^{j+(p-1)/4} - r^j \pm r^{2j+(p-1)/4} \equiv 0 \pmod{p^{m+1}}.$$

Складывая эти сравнения, получим

$$1 + 1 \pm r^{2j+(p-1)/4} \equiv 0 \pmod{p^{m+1}}.$$

Заметим, что $r^{(p-1)/4} \not\equiv \pm 2 \pmod{p^{m+1}}$, так как в противном случае выполнялось бы сравнение $-1 \equiv r^{(p-1)/2} \equiv 4 \pmod{p^{m+1}}$, что невозможно. Поэтому $j \not\equiv 0 \pmod{p-1}$ и $j \not\equiv (p-1)/4 \pmod{p-1}$, а следовательно, полученное представление не эквивалентно данному. □

Перейдем теперь к изучению числа решений сравнения (4.2). При этом используем такой же метод, как и при доказательстве теоремы Диксона из разд. 2.

Введем обозначения. Пусть $p > 2$ — простое число, $m \geqslant 0$, $k \geqslant 3$. Обозначим через $F(p, m, k)$ количество наборов $(x_1, \ldots, x_k)$, таких, что $1 \leqslant x_i \leqslant p-1$ (при $i = 1, \ldots, k$) и

$$x_1^{p^m} + x_2^{p^m} + \ldots + x_k^{p^m} \equiv 0 \pmod{p^{m+1}}.$$

Пусть a — целое число, $1 \leqslant a \leqslant p-1$. Обозначим через $F(p, m, k; a)$ число наборов $(x_1, \ldots, x_k)$, таких, что $1 \leqslant x_i \leqslant p-1$ (при $i = 1, \ldots, k$) и

$$x_1^{p^m} + x_2^{p^m} + \ldots + x_k^{p^m} \equiv ap^m \pmod{p^{m+1}}.$$

Через $N(p, m, k)$ обозначим число наборов $(x_2, \ldots, x_k)$, таких, что $1 \leqslant x_i \leqslant p-1$ (при $i = 2, \ldots, k$) и

$$1 + x_2^{p^m} + \ldots + x_k^{p^m} \equiv 0 \pmod{p^{m+1}}.$$

При $k = 3$ и $m = 1$ мы будем просто записывать $F(p) = F(p, 1, 3)$, $F(p; a) = F(p, 1, 3; a)$, $N(p) = N(p, 1, 3)$.

Сначала отметим некоторые соотношения между введенными величинами. Затем получим индуктивные формулы, в которых эти величины выражаются через периоды круговых полей и через круговые суммы Якоби.

Для $m = 0$ выполняется следующее утверждение.

(4G) *Справедливы равенства*

$$F(p, 0, k) = (p-1)\frac{(p-1)^{k-1} + (-1)^k}{p},$$

$$N(p, 0, k) = \frac{(p-1)^{k-1} + (-1)^k}{p}.$$

В частности,

$$F(p,0,3) = (p-1)(p-2),$$
$$N(p,0,3) = p-2.$$

Доказательство. Пусть $1 \leqslant x_i \leqslant p-1$ при $i = 1,\ldots,k-2$ и $x_1 + \ldots + x_{k-2} \not\equiv 0 \pmod p$. Тогда мы можем выбрать $p-2$ чисел x_{k-1}, таких, что $1 \leqslant x_{k-1} \leqslant p-1$, $x_1 + \ldots + x_{k-2} + x_{k-1} \not\equiv 0 \pmod p$. Существует единственное число x_k, $1 \leqslant x_k \leqslant p-1$, такое, что $x_1 + \ldots + x_{k-1} + x_k \equiv 0 \pmod p$. Таким образом, мы получили уже $[(p-1)^{k-2} - F(p,0,k-2)](p-2)$ решений.

Пусть теперь $1 \leqslant x_i \leqslant p-1$ при $i = 1,\ldots,k-2$ и $x_1+\ldots+x_{k-2} \equiv 0 \pmod p$. Тогда можно выбрать $p-1$ чисел x_{k-1} (которые определяют число x_k). Следовательно, мы получили $F(p,0,k-2)(p-1)$ решений. Таким образом, если $k \geqslant 3$, то

$$\begin{aligned} &F(p,0,k) \\ &\quad = [(p-1)^{k-2} - F(p,0,k-2)](p-2) + F(p,0,k-2)(p-1) \\ &\quad = (p-1)^{k-2}(p-2) + F(p,0,k-2). \end{aligned}$$

В частности, $F(p,0,3) = (p-1)(p-2)$, $F(p,0,4) = (p-1)^2(p-2) + (p-1)$. Из полученных соотношений найдем

$$\begin{aligned} F(p,0,2k+1) &= (p-1)^{2k-1}(p-2) + F(p,0,2k-1), \\ F(p,0,2k-1) &= (p-1)^{2k-3}(p-2) + F(p,0,2k-3), \\ &\vdots \\ F(p,0,3) &= (p-1)(p-2). \end{aligned}$$

Тогда

$$\begin{aligned} F(p,0,2k+1) &= (p-1)(p-2)\sum_{j=0}^{k-1}(p-1)^{2j} \\ &= (p-1)\left[\sum_{j=0}^{k-1}(p-1)^{2j+1} - \sum_{j=0}^{k-1}(p-1)^{2j}\right] \\ &= (p-1)\frac{(p-1)^{2k}-1}{(p-1)+1} = (p-1)\frac{(p-1)^{2k}-1}{p}. \end{aligned}$$

Аналогично

$$F(p,0,2k) = (p-2)\sum_{j=0}^{k-1}(p-1)^{2j} + 1$$

$$= \sum_{j=0}^{k-1}(p-1)^{2j+1} - \sum_{j=0}^{k-1}(p-1)^{2j} + 1$$

$$= (p-1)\left[\sum_{j=0}^{k-1}(p-1)^{2j} - \sum_{j=1}^{k-1}(p-1)^{2j-1}\right]$$

$$= (p-1)\frac{(p-1)^{2k-1}+1}{(p-1)+1} = (p-1)\frac{(p-1)^{2k-1}+1}{p}.$$

Таким образом, вне зависимости от четности числа k мы имеем

$$F(p,0,k) = (p-1)\frac{(p-1)^{k-1}+(-1)^k}{p}.$$

Точно так же можно убедиться, что

$$N(p,0,k) = (p-1)^{k-3}(p-2) + N(p,0,k-2).$$

Поэтому

$$N(p,0,2k+1) = (p-1)^{2k-2}(p-2) + N(p,0,2k-1)$$

и

$$N(p,0,2k+1) = (p-2)\sum_{j=0}^{k-1}(p-1)^{2j} = \frac{(p-1)^{2k}-1}{p}.$$

Аналогично $N(p,0,2k) = ((p-1)^{2k-1}+1)/p$, а следовательно, для **любого** k мы получаем

$$N(p,0,k) = \frac{(p-1)^{k-1}+(-1)^k}{p}. \quad \square$$

Приведем более общее утверждение.

(4Н) *Во введенных выше обозначениях справедливы следующие* **равенства.**

(1) $F(p,m,k) = (p-1)N(p,m,k)$.
(2) $F(p,m,k;1) = F(p,m,k;2) = \ldots = F(p,m,k;p-1)$. *Эту величину будем обозначать через* $F^*(p,m,k)$.
(3) $N(p,m,k) = N(p,m-1,k) - F^*(p,m,k)$ *для* $m \geqslant 1$. *В частности,* $N(p,1,k) = ((p-1)^{k-1}+(-1)^k)/p - F^*(p,1,k)$.

Доказательство. (1) Рассмотрим множества $\mathcal{F} = \{(x_1,\ldots,x_k) \mid 1 \leqslant x_i \leqslant p-1$ при $i = 1,\ldots,k$ и $x_1^{p^m} + \ldots + x_k^{p^m} \equiv 0 \pmod{p^{m+1}}\}$ и $\mathcal{N} = \{(x_2,\ldots,x_k) \mid 1 \leqslant x_i \leqslant p-1$ при $i = 2,\ldots,k$ и $1 + x_2^{p^m} +$

$+ \ldots + x_k^{p^m} \equiv 0 \pmod{p^{m+1}}\}$. Пусть y — целое число, $1 \leqslant y \leqslant p-1$, $(x_2, \ldots, x_k) \in \mathcal{N}$, и пусть $y_1 = y$, $y_i \equiv yx_i \pmod{p}$ при $i = 2, \ldots, k$. Тогда $(y_1, y_2, \ldots, y_k) \in \mathcal{F}$. Различным значениям y соответствуют различные решения сравнения $X_1^{p^m} + X_2^{p^m} + \ldots + X_k^{p^m} \equiv 0 \pmod{p^{m+1}}$.

Пусть $(x_2, \ldots, x_k) \in \mathcal{N}$, $(x_2', \ldots, x_k') \in \mathcal{N}$, $(x_2, \ldots, x_k) \neq (x_2', \ldots, x_k')$, y и y' — целые числа, $1 \leqslant y, y' \leqslant p-1$. Тогда указанный выше способ позволяет получить различные решения $(y_1, y_2, \ldots, y_k) \neq \neq (y_1', y_2', \ldots, y_k')$. Действительно, если $y \neq y'$, то $y_1 \neq y_1'$, а если $y = y'$ и, например, $x_i \neq x_i'$, то $y_i \neq y_i'$.

Также ясно, что каждое решение $(y_1, y_2, \ldots, y_k) \in \mathcal{F}$ может быть получено таким способом, а именно, мы можем выбрать те значения x_i, $1 \leqslant x_i \leqslant p-1$, для которых $y_i \equiv y_1 x_i \pmod{p}$ при $i = 2, \ldots, k$. Поэтому $F(p, m, k) = (p-1)N(p, m, k)$.

(2) Пусть $1 \leqslant a, b \leqslant p-1$, и пусть число c удовлетворяет условиям $b \equiv ca \pmod{p}$, $1 \leqslant c \leqslant p-1$. Пусть, далее, $1 \leqslant x_i \leqslant p-1$ и

$$x_1^{p^m} + x_2^{p^m} + \ldots + x_k^{p^m} \equiv ap^m \pmod{p^{m+1}}.$$

Тогда если $1 \leqslant y_i \leqslant p-1$, $y_i \equiv cx_i \pmod{p}$, то $y_i^{p^m} \equiv c^{p^m} x_i^{p^m} \pmod{p^{m+1}}$. Из сравнения $c^{p^m} \equiv c \pmod{p}$ следует, что

$$y_1^{p^m} + y_2^{p^m} + \ldots + y_k^{p^m} \equiv c^{p^m} ap^m \equiv bp^m \pmod{p^{m+1}}.$$

Таким образом, мы установили взаимно однозначное соответствие между множеством решений сравнения

$$X_1^{p^m} + X_2^{p^m} + \ldots + X_k^{p^m} \equiv ap^m \pmod{p^{m+1}}$$

и множеством решений сравнения

$$X_1^{p^m} + X_2^{p^m} + \ldots + X_k^{p^m} \equiv bp^m \pmod{p^{m+1}}.$$

Следовательно, $F(p, m, k; a) = F(p, m, k; b)$.

(3) Пусть $x_1^{p^{m-1}} + \ldots + x_k^{p^{m-1}} \equiv 0 \pmod{p^m}$, где $1 \leqslant x_i \leqslant p-1$ (при $i = 1, \ldots, k$). Тогда $x_1^{p^m} + \ldots + x_k^{p^m} \equiv 0 \pmod{p^m}$, так как $x_i^{p^m} \equiv x_i^{p^{m-1}} \pmod{p^m}$. Поэтому существует число a, $0 \leqslant a \leqslant p-1$, такое, что

$$x_1^{p^m} + \ldots + x_k^{p^m} \equiv ap^m \pmod{p^{m+1}}.$$

Следовательно, $(x_1, \ldots, x_k)$ — решение сравнения

$$X_1^{p^m} + \ldots + X_k^{p^m} \equiv 0 \pmod{p^{m+1}}$$

или сравнения

$$X_1^{p^m} + \ldots + X_k^{p^m} \equiv ap^m \pmod{p^{m+1}}$$

при некотором a, $1 \leqslant a \leqslant p-1$. Верно и обратное утверждение.

Поэтому, как следует из из части (2),

$$F(p, m-1, k) = F(p, m, k) + (p-1)F^*(p, m, k),$$

а из части (1) мы получаем

$$N(p, m-1, k) = N(p, m, k) + F^*(p, m, k).$$

В случае когда $m = 1$, из утверждения (4F) следует, что

$$N(p, 1, k) = \frac{(p-1)^{k-1} + (-1)^k}{p} - F^*(p, 1, k). \quad \square$$

При $p > 3$ положим

$$\delta(p) = \begin{cases} 0, & \text{если } p \equiv -1 \pmod 6, \\ 1, & \text{если } p \equiv 1 \pmod 6, \end{cases}$$

и

$$\gamma(p, m) = \begin{cases} 1, & \text{если } 2^{p^m} \equiv 2 \pmod{p^{m+1}}, \\ 0, & \text{если } 2^{p^m} \not\equiv 2 \pmod{p^{m+1}}. \end{cases}$$

(4I) *Справедливы следующие сравнения:*

$$F^*(p, m, 3) \equiv 3\gamma(p, m) + 3\gamma(p, m-1) \pmod 6,$$
$$N(p, m, 3) \equiv 3\gamma(p, m) + 2\delta(p) \pmod 6.$$

Доказательство. Разобьем решения сравнения $1 + X_2^{p^m} + X_3^{p^m} \equiv 0 \pmod{p^{m+1}}$ на классы эквивалентности. Согласно утверждению (4D) эти классы состоят из шести элементов, за исключением случая, когда $p \equiv 1 \pmod 6$ и существует класс из двух элементов, и случая, когда $2^{p^m} \equiv 2 \pmod{p^{m+1}}$ и существует класс из трех элементов. Поэтому

$$N(p, m, 3) \equiv 3\gamma(p, m) + 2\delta(p) \pmod 6.$$

Из утверждения (4H) получим

$$\begin{aligned} F^*(p, m, 3) &= N(p, m-1, 3) - N(p, m, 3) \\ &\equiv 3\gamma(p, m-1) - 3\gamma(p, m) \\ &\equiv 3\gamma(p, m-1) + 3\gamma(p, m) \pmod 6. \quad \square \end{aligned}$$

В случае когда $m = 1$ и $k = 3$, справедливы сравнения

$$F^*(p) = F^*(p,1,3) \equiv 3\gamma(p,1) + 3 \pmod 6,$$
$$N(p) \equiv 3\gamma(p,1) + 2\delta(p) \pmod 6.$$

Чтобы указать верхнюю границу для $N(p)$ (при $p > 3$), нам необходимо более подробно изучить многочлены Коши по модулю p. Напомним, что, как было показано в разд. VII.2,

$$(X+1)^p - X^p - 1 = pX(X+1)(X^2+X+1)^\varepsilon C_p(X),$$

где $C_p(X) \in \mathbb{Z}[X]$,

$$\varepsilon = \begin{cases} 1, & \text{если } p \equiv -1 \pmod 6, \\ 2, & \text{если } p \equiv 1 \pmod 6. \end{cases}$$

Многочлен $C_p(X)$ не делится на X^2+X+1 и является приведенным симметрическим многочленом. Кроме того, $C_p(-1-X) = C_p(X)$, поэтому $C_p(0) = C_p(-1) = 1$. Пусть

$$q(X) = \frac{(X+1)^p - X^p - 1}{p} \in \mathbb{Z}[X]$$

и $\overline{q}(X) \equiv q(X) \pmod p$, $\overline{C}_p(X) \equiv C_p(X) \pmod p$.

(4J) *Если $p > 3$, то справедливы следующие утверждения.*

(1) *Все корни многочлена $\overline{q}(X)$ (отличные от $\overline{0}$ и $\overline{-1}$) в $\mathbb{F}_p$ и все корни многочлена $\overline{C}_p(X)$ в $\mathbb{F}_p$ имеют кратность 2.*

(2) *Если α — корень многочлена $\overline{C}_p(X)$, то каждый элемент множества*

$$M_\alpha = \left\{\alpha, \frac{1}{\alpha}, -(1+\alpha), -\frac{1}{1+\alpha}, -\frac{\alpha}{1+\alpha}, -\frac{1+\alpha}{\alpha}\right\}$$

есть также корень многочлена $\overline{C}_p(X)$. Если множество M_α состоит менее чем из шести различных элементов, то $M_\alpha = \{\overline{1}, -\overline{2}, (p-1)/2 \pmod p\}$ (в этом случае $2^p \equiv 2 \pmod{p^2}$) или $p \equiv -1 \pmod 6$ и $\alpha^2 + \alpha + \overline{1} = \overline{0}$, $\alpha \notin \mathbb{F}_p$.

(3) *Многочлен $X^2 + X + \overline{1} \in \mathbb{F}_p[X]$ не делит $\overline{C}_p(X)$.*

Доказательство. (1) Пусть $\alpha \in \mathbb{F}_p$ и $\overline{q}(\alpha) = \overline{0}$. Нетрудно видеть, что $\overline{q}'(X) = (X+\overline{1})^{p-1} - X^{p-1}$. Если $\alpha \neq \overline{0}, \overline{-1}$, то $(\alpha+\overline{1})^{p-1} = \alpha^{p-1} = \overline{1}$, и тогда $\overline{q}'(\alpha) = \overline{0}$. Так как $\overline{q}''(X) = (p-\overline{1})[(X+\overline{1})^{p-2} - X^{p-2}]$, мы получаем

$$\overline{q}''(\alpha) = -[(\alpha+\overline{1})^{p-2} - \alpha^{p-2}] = \frac{\overline{1}}{\alpha+\overline{1}} - \frac{\overline{1}}{\alpha} = -\frac{\overline{1}}{\alpha(\alpha+\overline{1})} \neq \overline{0}.$$

Следовательно, $\alpha \neq \overline{0}, -\overline{1}$ есть двукратный корень многочлена $\overline{q}(X)$.

Из равенства $\overline{q}(X) = X(X+\overline{1})(X^2+X+\overline{1})^{\varepsilon}\overline{C}_p(X)$ получаем, что если $\overline{C}_p(\alpha) = \overline{0}$, то $\overline{q}(\alpha) = \overline{0}$. Вычисляя производную, убедимся, что $\overline{0} = (\alpha^2+\alpha+\overline{1})^{\varepsilon}\overline{C}_p'(\alpha)$. Заметим, что $\alpha^2+\alpha+\overline{1} \neq \overline{0}$, поскольку в противном случае выполнялось бы сравнение $p \equiv 1 \pmod 6$, так как $\alpha \in \mathbb{F}_p$ (см. лемму 4.1 гл. I). Поэтому $\varepsilon = 2$ и $\overline{C}_p(\alpha) \neq \overline{0}$, поскольку α — корень кратности 2 многочлена $\overline{q}(X)$. Таким образом, $\overline{C}_p'(\alpha) = \overline{0}$, т. е. α — двукратный корень многочлена $\overline{C}_p(X)$.

(2) Так как $C_p(X)$ — симметрический многочлен и $C_p(-1-X) = C_p(X)$, $C_p(0) = C_p(-1) = 1$, при условии $\overline{C}_p(\alpha) = \overline{0}$ каждый элемент $\beta \in M_\alpha$ также будет корнем многочлена $C_p(X)$. Предположим, что множество M_α имеет менее шести элементов. Тогда возможен один из следующих случаев:

(i) $\alpha = 1/\alpha$, тогда $\alpha = \pm\overline{1}$;

(ii) $\alpha = -(1+\alpha)$, тогда $\alpha = (p-1)/2 \pmod p$;

(iii) $\alpha = -1/(1+\alpha)$, тогда $\alpha^2+\alpha+\overline{1} = \overline{0}$;

(iv) $\alpha = -\alpha/(1+\alpha)$, тогда $\alpha = \overline{0}$ или $\alpha = -\overline{2}$;

(v) $\alpha = -(1+\alpha)/\alpha$, тогда $\alpha^2+\alpha+\overline{1} = \overline{0}$.

Но $\overline{0}$ и $-\overline{1}$ не являются корнями многочлена $\overline{C_p}(X)$. Если $\alpha = \overline{1}, -\overline{2}$ или $(p-1)/2 \pmod p$, то $M_\alpha = \{\overline{1}, -\overline{2}, (p-1)/2 \bmod p\}$ и из соотношения $((1+1)^p - 1^p - 1)/p \equiv 0 \pmod p$ следует, что $2^p \equiv 2 \pmod{p^2}$. Если $\alpha^2+\alpha+\overline{1} = \overline{0}$, где $\alpha \in \mathbb{F}_p$, то $p \equiv 1 \pmod 6$, и тогда $\varepsilon = 2$. Так как α — корень кратности 2 многочлена $\overline{q}(X)$, он не может быть корнем многочлена $\overline{C_p}(X)$. Таким образом, $\alpha \notin \mathbb{F}_p$ и $p \equiv -1 \pmod 6$.

(3) Пусть $p \equiv 1 \pmod 6$. Тогда $\varepsilon = 2$ и многочлен $X^2+X+\overline{1}$ имеет корень $\alpha \in \mathbb{F}_p$, который является двукратным корнем многочлена $\overline{q}(X)$, а значит, не является корнем многочлена $\overline{C_p}(X)$. Следовательно, $X^2+X+\overline{1}$ не делит $\overline{C_p}(X)$.

Пусть $p \equiv -1 \pmod 6$. Тогда $\varepsilon = 1$. Корни многочлена $\overline{C_p}(X)$ можно разбить на множества из шести различных элементов, за исключением следующих случаев:

(i) множество из трех двукратных корней

$$\{\overline{1}, -\overline{2}, (p-1)/2 \bmod p\},$$

(ii) множество из двух корней многочлена $X^2+X+\overline{1}$ (которые лежат вне $\mathbb{F}_p$).

Если $\overline{C}_p(X) = (X^2 + X + \overline{1})^r \overline{H}(X)$, где $r \geqslant 1$ и $X^2 + X + \overline{1}$ не делит многочлен $\overline{H}(X) \in \mathbb{F}_p[X]$, то

$$\deg \overline{C}_p(X) = 2r + \deg \overline{H}(X) \equiv 2r \pmod 6.$$

Если $p = 6n - 1$, то $\deg \overline{C}_p(X) = 6(n-1)$, значит, $2r \equiv 0 \pmod 6$, поэтому $r \equiv 0 \pmod 3$ и, следовательно, $r \geqslant 3$. Таким образом, если $\alpha^2 + \alpha + \overline{1} = \overline{0}$, то α — корень кратности 3 многочлена $\overline{C}_p(X)$, а значит, и многочлена $\overline{q}(X)$. Следовательно, многочлены

$$\overline{q}'(X) = (X + \overline{1})^{p-1} - X^{p-1}$$

и

$$\overline{q}''(X) = (p-1)[(X + \overline{1})^{p-2} - X^{p-2}]$$

обращаются в нуль при $X = \alpha$, поэтому

$$(\alpha + \overline{1})^{p-1} = \alpha^{p-1}, \qquad (\alpha + \overline{1})^{p-2} = \alpha^{p-2}.$$

Сравнивая эти равенства, получим

$$\alpha^{p-1} = (\alpha + \overline{1})(\alpha + \overline{1})^{p-2} = (\alpha + \overline{1})\alpha^{p-2} = \alpha^{p-1} + \alpha^{p-2},$$

следовательно, $\alpha^{p-2} = \overline{0}$, значит, $\alpha = \overline{0}$. Полученное противоречие завершает доказательство. □

(4K) *Справедливы следующие оценки для величины* $N(p)$.

(1) *При* $2^p \not\equiv 2 \pmod{p^2}$ *выполняется неравенство*

$$N(p) \leqslant \begin{cases} \dfrac{p-9}{2}, & \text{если } p \equiv 1 \pmod{12}, \\ \dfrac{p-5}{2}, & \text{если } p \equiv 5 \pmod{12}, \\ \dfrac{p-3}{2}, & \text{если } p \equiv 7 \pmod{12}, \\ \dfrac{p-11}{2}, & \text{если } p \equiv 11 \pmod{12}. \end{cases}$$

(2) *При* $2^p \equiv 2 \pmod{p^2}$ *выполняется неравенство*

$$N(p) \leqslant \begin{cases} \dfrac{p-3}{2}, & \text{если } p \equiv 1 \pmod{12}, \\ \dfrac{p-11}{2}, & \text{если } p \equiv 5 \pmod{12}, \\ \dfrac{p-9}{2}, & \text{если } p \equiv 7 \pmod{12}, \\ \dfrac{p-5}{2}, & \text{если } p \equiv 11 \pmod{12}. \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Напомним, что нетривиальные решения сравнения $1 + X_1^p + X_2^p \equiv 0 \pmod{p^2}$ соответствуют нетривиальным решениям сравнения $1 + X^p \equiv (1+X)^p \pmod{p^2}$, т. е. корням многочлена

$$\overline{q}(X) = \frac{(X+1)^p - X^p - 1}{p} \pmod{p} \in \mathbb{F}_p[X],$$

лежащим в $\mathbb{F}_p$ и отличным от $\overline{0}$ и $-\overline{1}$.

(1) Пусть $p = 12n+1$. Тогда

$$q(X) = X(X+1)(X^2+X+1)^2 C_p(X),$$

$\deg q(X) = p-1$, $\deg C_p(X) = p-7 = 12n-6$. Так как каждый корень многочлена $\overline{C_p}(X)$ из $\mathbb{F}_p$ имеет кратность 2 и все корни можно разбить на множества из шести элементов,

$$N(p) \leqslant 2 + 6\left[\frac{6n-1}{6}\right] = 2 + 6n - 6 = 6n - 4$$
$$= \frac{p-1}{2} - 4 = \frac{p-9}{2}.$$

Если $p = 12n+5$, то $q(X) = X(X+1)(X^2+X+1)C_p(X)$. Точно так же (замечая, что многочлен $X^2+X+\overline{1}$ не имеет корней в $\mathbb{F}_p$) можно показать, что $\deg C_p(X) = 12n$, $N(p) \leqslant 6n = (p-5)/2$. В случаях $p = 12n+7$ и $p = 12n+11$ поступаем аналогично.

(2) Пусть $2^p \equiv 2 \pmod{p^2}$. Тогда $\overline{q}(X) = X(X+\overline{1})(X^2+X+\overline{1})^\epsilon \times$ $\times (X-\overline{1})^2(X+\overline{2})^2(X-(p-1)/2 \bmod p)^2\overline{A}(X)$ и все корни многочлена $\overline{A}(X) \in \mathbb{F}_p[X]$ можно разбить на множества из шести различных двукратных корней.

Если $p = 12n+1$, то $\deg \overline{A}(X) = 12(n-1)$ и $N(p) \leqslant 2+3+6(n-1) =$ $= 6n-1 = (p-3)/2$.

Точно так же мы можем получить верхнюю границу и в остальных случаях. □

Полученные результаты не позволяют еще найти явную формулу для числа решений рассматриваемых сравнений. Ниже мы увидим, как такие формулы могут быть получены с помощью периодов Гаусса и круговых сумм Якоби, как в разд. 2.

Пусть p — нечетное простое число, $m \geqslant 1$, h — первообразный корень по модулю p^{m+1}, ζ — первообразный корень степени p^m из единицы и ρ — первообразный корень степени p^{m+1} из единицы, $\rho^p = \zeta$. Периоды Гаусса $\eta_i = \eta_i(p, m, h)$ задаются следующим обра-

зом:

$$\begin{cases} \eta_0 &= \rho + \rho^{h^{p^m}} + \rho^{h^{2p^m}} + \ldots + \rho^{h^{(p-2)p^m}}, \\ &\vdots \\ \eta_i &= \rho^{h^i} + \rho^{h^{p^m+i}} + \rho^{h^{2p^m+i}} + \ldots + \rho^{h^{(p-2)p^m+i}}, \\ &\vdots \\ \eta_{p^m-1} &= \rho^{h^{p^m-1}} + \rho^{h^{2p^m-1}} + \rho^{h^{3p^m-1}} + \ldots + \rho^{(p-1)p^m-1}. \end{cases} \tag{4.5}$$

Для удобства определим η_j для любого индекса j, полагая $\eta_j = \eta_i$ при $j \equiv i \pmod{p^m}$, $0 \leqslant i \leqslant p^m - 1$.

Если g — другой первообразный корень по модулю p^{m+1}, то $g \equiv h^r \pmod{p^{m+1}}$ и НОД$(r, p^m(p-1)) = 1$. Пусть ${\eta_i}' = \eta_i(p, m, g)$. Тогда ${\eta_i}' = \eta_{ri}$ (при $i = 0, 1, \ldots, p^m - 1$). Действительно, $\{(jrp^m + ri) \bmod p^m(p-1) \mid j = 0, 1, \ldots, p-2\} = \{(tp^m + ri) \bmod p^m(p-1) \mid t = 0, 1, \ldots, p-2\}$ при $jr \equiv t \pmod{(p-1)}$, $0 \leqslant t \leqslant p-2$, так как $j \not\equiv j' \pmod{p^m}$ тогда и только тогда, когда $jr \not\equiv j'r \pmod{p^m}$, поэтому

$${\eta_i}' = \sum_{j=0}^{p-2} \rho^{g^{jp^m+i}} = \sum_{j=0}^{p-2} \rho^{h^{jrp^m+ri}} = \sum_{t=0}^{p-2} \rho^{h^{tp^m+ri}} = \eta_{ri}.$$

Таким образом, меняя нумерацию, мы убедимся, что периоды Гаусса не зависят от выбора первообразного корня по модулю p^{m+1}.

Заметим, что каждый период η_i — вещественное число. Действительно, период η_i есть сумма $(p-1)/2$ пар комплексно сопряженных чисел, т. е.

$$\rho^{h^{jp^m+i}} + \rho^{h^{((p-1)/2+j)p^m+i}} = \rho^{h^{jp^m+i}} + \rho^{-h^{jp^m+i}} = \rho^{h^{jp^m+i}} + \overline{\rho^{h^{jp^m+i}}} \in \mathbb{R}.$$

Также справедлива грубая оценка

$$|\eta_i| \leqslant \sum_{j=0}^{p-2} \left|\rho^{h^{jp^m+i}}\right| < p - 1 \tag{4.6}$$

(равенство достигается лишь в том случае, когда все числа $\rho^{h^{jp^m+i}}$ с положительной действительной частью делятся на одно из них).

Для каждого числа t, не делящегося на p, определим $\operatorname{ind}_h(t) = s$, где $0 \leqslant s \leqslant (p-1)p^m - 1$ и $t \equiv h^s \pmod{p^{m+1}}$.

Суммы Якоби $\tau_j = \tau_j(p, m, h)$ (для $j = 0, 1, \ldots, p^m - 1$) определяются формулой

$$\tau_j = \langle \zeta^j, \rho \rangle = \sum_{\substack{t=1 \\ p \nmid t}}^{p^{m+1}-1} \zeta^{j \operatorname{ind}_h(t)} \rho^t. \tag{4.7}$$

В частности,

$$\tau_0 = 0. \tag{4.8}$$

Действительно,

$$\tau_0 = \langle 1, \rho \rangle = \sum_{\substack{t=1 \\ p \nmid t}}^{p^{m+1}-1} \rho^t,$$

т. е. τ_0 есть сумма первообразных корней степени (p^{m+1}) из единицы. Поэтому τ_0 совпадает с коэффициентом при степени $\varphi(p^{m+1})-1$ кругового многочлена

$$\Phi_{p^{m+1}}(X) = \frac{X^{p^{m+1}}-1}{X^{p^m}-1} = X^{(p-1)p^m} + X^{(p-2)p^m} + \ldots + X^{p^m} + 1,$$

следовательно, $\tau_0 = 0$.

Покажем, что $\tau_j \neq 0$ тогда и только тогда, когда $p \nmid j$. Для этого нам понадобится следующая лемма.

Лемма 4.1.

(1) *Пусть $n > 1$ и ξ — первообразный корень степени n из единицы. Тогда для любого целого числа a справедливо соотношение*

$$\sum_{x=1}^{n} \xi^{ax} = \begin{cases} n, & \text{если } n \mid a, \\ 0, & \text{если } n \nmid a. \end{cases}$$

(2) *Пусть p — нечетное простое число, $m \geqslant 0$ и ρ — первообразный корень степени p^{m+1} из единицы. Тогда для любого целого числа a справедливо соотношение*

$$\sum_{\substack{x=1 \\ p \nmid x}}^{p^{m+1}} \rho^{ax} = \begin{cases} \varphi(p^{m+1}), & \text{если } p^{m+1} \mid a, \\ -p^m, & \text{если } p^m \mid a,\ p^{m+1} \nmid a, \\ 0, & \text{если } p^m \nmid a. \end{cases}$$

Доказательство. (1) Пусть $d = \text{НОД}(n, a)$, $n = dn'$, $a = da'$. Тогда $\text{НОД}(n', a') = 1$. Так как ξ^d — первообразный корень степени n' из единицы, $\xi^{da'}$ — тоже первообразный корень степени n' из единицы. Поэтому

$$\sum_{x=1}^{n} \xi^{ax} = \sum_{x=1}^{n} (\xi^{da'})^x.$$

Сделаем замену переменной суммирования x, $1 \leqslant x \leqslant n$, вида $x = hn' + y$, $1 \leqslant y \leqslant n'$, $0 \leqslant h \leqslant d-1$.

Тогда

$$\begin{aligned}\sum_{x=1}^{n}\xi^{ax} &= \sum_{x=1}^{n}\left(\xi^{da'}\right)^{x}\\ &= \sum_{h=0}^{d-1}\sum_{y=1}^{n'}\left(\xi^{da'}\right)^{hn'+y}\\ &= \sum_{h=0}^{d-1}\sum_{y=1}^{n'}\left(\xi^{da'}\right)^{y}\\ &= \begin{cases} n'd=n, & \text{если } n'=1, \text{ т. е. } n\mid a,\\ 0, & \text{если } n'>1, \text{ т. е. } n\nmid a.\end{cases}\end{aligned}$$

(2) Если $p^{m+1}\mid a$, то сумма

$$S=\sum_{\substack{x=1\\ p\nmid x}}^{p^{m+1}}\rho^{ax},$$

очевидно, равна $\varphi(p^{m+1})$. Если $p^{m+1}\nmid a$ и $p^m\mid a$, то $a=bp^m$ и $p\nmid b$. Тогда $\zeta=\rho^{bp^m}$ — первообразный корень степени p из единицы. Каждое число x, $1\leqslant x\leqslant p^{m+1}$, можно представить в виде $x=hp+y$, $0\leqslant h\leqslant p^m-1$, $1\leqslant y\leqslant p$. Кроме того, $p\nmid x$ при $y\neq p$. Поэтому

$$S=\sum_{\substack{x=1\\ p\nmid x}}^{p^{m+1}}\zeta^{x}=\sum_{h=0}^{p^m-1}\sum_{y=1}^{p-1}\zeta^{y}=\sum_{h=0}^{p^m-1}(-1)=-p^m.$$

Если $p^m\nmid a$, то из части (1) следует, что

$$S+\sum_{\substack{p\mid x\\ 1\leqslant x\leqslant p^{m+1}}}\rho^{ax}=\sum_{x=1}^{p^{m+1}}\rho^{ax}=0,$$

поскольку $p^{m+1}\nmid a$.

Заметим, что $\rho^p=\zeta$ есть первообразный корень степени p^m из единицы. Каждое число x, $1\leqslant x\leqslant p^{m+1}$, делящееся на p, запишем в виде $x=py$, $1\leqslant y\leqslant p^m$. Тогда из части (1) мы получаем

$$\sum_{\substack{x=1\\ p\mid x}}^{p^{m+1}}\rho^{ax}=\sum_{y=1}^{p^m}\zeta^{ay}=0,$$

так как $p^m\nmid a$. Отсюда заключаем, что $S=0$. □

Последующие леммы связаны со свойствами индексов.

ЛЕММА 4.2. *Пусть p — нечетное простое число, $m \geqslant 0$, h — первообразный корень по модулю p^{m+1}, i — целое число, $1 \leqslant i \leqslant p-1$. Тогда*

$$\operatorname{ind}_h(1+ip^m) \equiv iap^{m-1} \pmod{p^m},$$

где a — некоторое целое число, не делящееся на p.

ДОКАЗАТЕЛЬСТВО. Пусть $s = \operatorname{ind}_h(1+ip^m)$. Тогда $h^s \equiv 1+ip^m \pmod{p^{m+1}}$. Поэтому

$$h^{sp} \equiv (1+ip^m)^p \equiv 1+ip^{m+1} \equiv 1 \pmod{p^{m+1}}.$$

Следовательно, $sp \equiv 0 \pmod{p^m(p-1)}$, т. е. $sp = -bp^m(p-1) = bp^m - bp^{m+1}$. Таким образом, $s = bp^{m-1} - bp^m$, а значит, $s \equiv bp^{m-1} \pmod{p^m}$. Так как $p \nmid i$, существует число a, такое, что $b \equiv ia \pmod{p}$, поэтому $s \equiv iap^{m-1} \pmod{p^m}$.

Осталось показать, что $p \nmid a$. В самом деле, если $p \mid a$, то $s \equiv 0 \pmod{p^m}$, т. е. $1+ip^m \equiv h^{p^m c} \pmod{p^{m+1}}$ (для некоторого целого числа c). Из формулы (4.3) следует, что $(1+ip^m) \bmod p^{m+1} = h^{p^m c} \bmod p^{m+1} \in U \cap V = \{\overline{1}\}$, поэтому $i \equiv 0 \pmod{p}$. Полученное противоречие завершает доказательство. □

Для каждого $j = 0, 1, \ldots, p^m(p-1)-1$ положим

$$U_j = \{\overline{a} \in (\mathbb{Z}/p^{m+1})^\bullet \mid \operatorname{ind}_h(\overline{a}) \equiv j \pmod{p^m}\}.$$

Поскольку $U = \{\overline{a}^{p^m} \mid \overline{a} \in (\mathbb{Z}/p^{m+1})^\bullet\}$, множество U_j есть смежный класс группы $(\mathbb{Z}/p^{m+1})^\bullet$ по подгруппе U. В дальнейшем для вычисления сумм квадратов периодов нам потребуются описания этих смежных классов.

При $1 \leqslant k \leqslant m$ и $i = 0, 1, \ldots, p^{m-k}-1$ положим

$$\mathcal{S}_i = \{U_i, U_{i+p^{m-k}}, U_{i+2p^{m-k}}, \ldots, U_{i+(p^k-1)p^{m-k}}\}$$

и

$$\mathcal{S}'_i = \{\overline{(1+ip)} \cdot U, \overline{[1+(i+p^{m-k})p]} \cdot U, \overline{[1+(i+2p^{m-k})p]} \cdot U, \ldots, \overline{[1+(i+(p^k-1)p^{m-k})p]} \cdot U\}.$$

Во-первых, заметим, что для каждого i смежные классы $U_{i+lp^{m-k}}$ и $U_{i+l'p^{m-k}}$ (при $l \neq l'$) не совпадают. Действительно, в противном случае выполнялось бы сравнение $i+lp^{m-k} \equiv i+l'p^{m-k} \pmod{p^m}$, поэтому мы получили бы $l \equiv l' \pmod{p^k}$, что противоречит предположению. Итак, $\#\mathcal{S}_i = p^k$.

Если $i \neq i'$, то $\mathcal{S}_i \cap \mathcal{S}_{i'} = \varnothing$. В самом деле, если это пересечение непусто, то мы получим $i + lp^{m-k} \equiv i' + l'p^{m-k} \pmod{p^m}$, поэтому $i \equiv i' \pmod{p^{m-k}}$, т. е. $i = i'$.

Таким образом, множество $\bigcup_{i=0}^{p^{m-k}-1} \mathcal{S}_i$ содержит p^m смежных классов, т. е. состоит из всех смежных классов по модулю U. Аналогично смежные классы

$$\overline{[1 + (i + lp^{m-k})p]} \cdot U, \qquad \overline{[1 + (i + l'p^{m-k})p]} \cdot U$$

(при $l \neq l'$) не совпадают, так как в противном случае должно выполняться условие

$$\overline{1 + (i + lp^{m-k})p} \cdot \left(\overline{[1 + (i + l'p^{m-k})p]}\right)^{-1} \in V \cap U = \{\bar{1}\},$$

а значит,

$$1 + (i + lp^{m-k})p \equiv 1 + (i + l'p^{m-k})p \pmod{p^{m+1}},$$

следовательно, $l \equiv l' \pmod{p^k}$. Таким образом, $\#\mathcal{S}_i' = p^k$.

Если $i \neq i'$, то $\mathcal{S}_i' \cap \mathcal{S}_{i'}' = \varnothing$, поскольку, предположив противное, мы получим

$$\overline{[1 + (i + lp^{m-k})p]} \cdot U = \overline{[1 + (i' + l'p^{m-k})p]} \cdot U,$$

поэтому

$$1 + (i + lp^{m-k})p \equiv (1 + i' + l'p^{m-k})p \pmod{p^{m+1}},$$

т. е. $i \equiv i' \pmod{p^{m-k}}$, а значит, $i = i'$. Таким образом, множество $\bigcup_{i=0}^{p^{m-k}-1} \mathcal{S}_i'$ содержит p^m смежных классов, а следовательно, состоит из всех смежных классов по модулю U.

Лемма 4.3. *Существует такая перестановка π множества $\{0, 1, \ldots, p^{m-k} - 1\}$, что $\mathcal{S}_i' = \mathcal{S}_{\pi(i)}$.*

Доказательство. Пусть $\operatorname{ind}\overline{(1 + ip)} = j$, т. е. $\overline{(1 + ip)} \cdot U = U_j$. Сначала покажем, что для каждого $l = 0, 1, \ldots, p^k - 1$ справедливо равенство

$$\operatorname{ind}\overline{[1 + (i + lp^{m-k})p]} = j + sp^{m-k},$$

где число s удовлетворяет условию $0 \leqslant s \leqslant p^k - 1$. Это равносильно тому, что

$$\overline{[1 + (i + lp^{m-k})p]} \cdot U = U_{j+sp^{m-k}}.$$

Если мы положим $\pi(i) = j$, то получим $\mathcal{S}_i' = \mathcal{S}_{\pi(i)}$. Пусть число i' таково, что $(1 + i'p)(1 + ip) \equiv 1 \pmod{p^{m+1}}$, и пусть $l = l'p^r$,

$p \nmid l'$, $0 \leqslant r \leqslant k$. Определим число b, $1 \leqslant b \leqslant p^{k-r} - 1$, из сравнения $l'(1 + i'p) \equiv b \pmod{p^{k-r}}$. Тогда

$$\begin{aligned}[1 + (i + lp^{m-k})p][1 + i'p] &\equiv 1 + l(1 + i'p)p^{m-k+1} \\ &\equiv 1 + l'(1 + i'p)p^{m-k+r+1} \\ &\equiv 1 + bp^{m-k+r+1} \pmod{p^{m+1}}.\end{aligned}$$

Поскольку

$$(1 + bp^{m-k+r+1})^{p^{k-r}} \equiv 1 \pmod{p^{m+1}},$$

мы получаем

$$1 + bp^{m-k+r+1} \equiv h^{t(p-1)p^{m-k+r}} \pmod{p^{m+1}}.$$

Положим $s = t(p-1)p^r$. Тогда

$$1 + (i + lp^{m-k})p \equiv (1 + ip)h^{sp^{m-k}} \equiv h^{j+sp^{m-k}} \pmod{p^{m+1}},$$

что и требовалось доказать.

Покажем, что $\pi(i) \neq \pi(i')$ при $i \neq i'$. Допустим противное. Пусть $h^j \equiv 1+ip \pmod{p^{m+1}}$, $h^{j'} \equiv 1+i'p \pmod{p^{m+1}}$, $j \equiv j' \pmod{p^{m-k}}$, т. е. $j' = j + sp^{m-k}$. Тогда $1 + i'p \equiv (1 + ip)h^{sp^{m-k}} \pmod{p^{m-k}}$, следовательно, $h^{sp^{m-k}} \in V$. Поэтому число sp^{m-k} делится на $(p-1)$, а значит, и на $(p-1)p^{m-k}$, т. е. $sp^{m-k} = t(p-1)p^{m-k}$. Пусть $h^{p-1} \equiv \equiv 1 + ap \pmod{p^{m+1}}$. Тогда $h^{sp^{m-k}} \equiv (1 + ap)^{tp^{m-k}} \equiv 1 + atp^{m-k+1} \pmod{p^{m-k+1}}$. Следовательно, $1 + i'p \equiv (1 + ip)(1 + atp^{m-k+1}) \equiv \equiv 1 + (i + atp^{m-k})p \pmod{p^{m-k+2}}$. Отсюда получаем, что $i' \equiv i \pmod{p^{m-k}}$, т. е. $i' = i$.

Таким образом, π есть искомая перестановка. □

Выведем некоторые формулы для сумм Якоби и периодов Гаусса, аналогичные полученным в разд. IX.2.

Лемма 4.4. *Суммы Якоби удовлетворяют следующим условиям:*

(1) $\overline{\tau}_j = \tau_{p^m-j}$ *при* $j = 1, \ldots, p^m - 1$ ($\overline{\tau_j}$ *обозначает комплексное число, сопряженное с* τ_j);

(2) $\tau_j\overline{\tau_j} = \begin{cases} p^{m+1}, & \text{если } p \nmid j, \\ 0, & \text{если } p \mid j; \end{cases}$

(3) $\tau_j \neq 0$ *тогда и только тогда, когда* p *не делит* j.

Доказательство. (1) Нетрудно видеть, что

$$\overline{\tau}_j = \sum_{\substack{x=1 \\ p \nmid x}}^{p^{m+1}} \zeta^{-j \operatorname{ind}_h(x)} \rho^{-x}.$$

Так как $\operatorname{ind}_h(-x) \equiv \operatorname{ind}_h(-1)+\operatorname{ind}_h(x) \pmod{p^m(p-1)}$ и $\operatorname{ind}_h(-1) = \frac{1}{2}p^m(p-1)$, мы получаем, что $\zeta^{\operatorname{ind}_h(-1)} = 1$. Поэтому

$$\overline{\tau_j} = \sum_{\substack{x=1 \\ p \nmid x}}^{p^{m+1}} \zeta^{-j \operatorname{ind}_h(-x)} \rho^{-x} = \tau_{p^m-j}.$$

(2) Преобразуем произведение $\tau_j\overline{\tau_j}$ следующим образом:

$$\tau_j\overline{\tau_j} = \left(\sum_{\substack{x=1 \\ p \nmid x}}^{p^{m+1}-1} \zeta^{j \operatorname{ind}_h(x)} \rho^{x}\right)\left(\sum_{\substack{y=1 \\ p \nmid y}}^{p^{m+1}-1} \zeta^{-j \operatorname{ind}_h(y)} \rho^{-y}\right)$$

$$= \sum_{\substack{x=1 \\ p \nmid x}}^{p^{m+1}-1} \sum_{\substack{y=1 \\ p \nmid x}}^{p^{m+1}-1} \zeta^{j(\operatorname{ind}_h(x)-\operatorname{ind}_h(y))} \rho^{x-y}.$$

Для всех x и y определим t, $1 \leqslant t \leqslant p^{m+1}-1$, из сравнения $y \equiv xt \pmod{p^{m+1}}$. Тогда $p \nmid t$ и $\operatorname{ind}_h(y) \equiv \operatorname{ind}_h(x)+\operatorname{ind}_h(t) \pmod{p^m(p-1)}$. Поэтому

$$\tau_j\overline{\tau}_j = \sum_{\substack{x=1 \\ p \nmid x}}^{p^{m+1}-1} \sum_{\substack{t=1 \\ p \nmid t}}^{p^{m+1}-1} \zeta^{-j \operatorname{ind}_h(t)} \rho^{x(1-t)}$$

$$= \sum_{\substack{t=1 \\ p \nmid t}}^{p^{m+1}-1} \zeta^{j \operatorname{ind}_h(t)} \left(\sum_{\substack{x=1 \\ p \nmid x}}^{p^{m+1}-1} \rho^{x(1-t)}\right).$$

Используя лемму 4.1, получим

$$\tau_j\overline{\tau}_j = p^m(p-1) + (-p^m)\sum_{i=1}^{p-1} \zeta^{-j \operatorname{ind}_h(1+ip^m)},$$

где первое слагаемое соответствует $t = 1$, а члены суммы — $t = 1 + ip^m$; при других значениях t сумма равна нулю. Как следует из леммы 4.2,

$$\operatorname{ind}_h(1 + ip^m) \equiv iap^{m-1} \pmod{p^m},$$

где $p \nmid a$, а значит,

$$\tau_j\overline{\tau}_j = p^m(p-1) + (-p^m)\sum_{i=1}^{p-1} \zeta^{-jiap^{m-1}}$$

$$= \begin{cases} p^m(p-1) + p^m = p^{m+1}, & \text{если } p \nmid j, \\ p^m(p-1) - p^m(p-1) = 0, & \text{если } p \mid j. \end{cases}$$

(3) Это утверждение, очевидно, следует из части (2). □

Отметим важные соотношения между периодами Гаусса и суммами Якоби. Рассмотрим матрицу $Z = (\zeta^{ij})_{i,j=0,1,\ldots,p^m-1}$ и векторы

$$\tau = \begin{pmatrix} \tau_0 \\ \tau_1 \\ \vdots \\ \tau_{p^m-1} \end{pmatrix}, \qquad \eta = \begin{pmatrix} \eta_0 \\ \eta_1 \\ \vdots \\ \eta_{p^m-1} \end{pmatrix}.$$

ЛЕММА 4.5. *Справедливы следующие равенства:*

(1) $Z\overline{Z} = p^m I$ (I — *единичная матрица*), *т. е.*

$$\sum_{k=1}^{p^m} \zeta^{ik}\zeta^{-kj} = p^m \delta_{ik}$$

(*при* $i, j = 0, 1, \ldots, p^m - 1$);

(2) $\overline{Z}\tau = p^m\eta$, *т. е.*

$$\sum_{j=0}^{p^m-1} \zeta^{-ij}\tau_j = p^m\eta_i$$

(*при* $i = 0, 1, \ldots, p^m - 1$);

(3) $\tau = Z\eta$, *т. е.*

$$\sum_{j=0}^{p^m-1} \zeta^{ij}\eta_j = \tau_i$$

(*при* $i = 0, 1, \ldots, p^m - 1$).

ДОКАЗАТЕЛЬСТВО. (1) По лемме 4.1(1) получим

$$\sum_{k=1}^{p^m} \zeta^{ik}\zeta^{-kj} = \sum_{k=1}^{p^m-1} \zeta^{(i-j)k} = \begin{cases} p^m, & \text{если } p^m \mid (i-j), \text{ т. е. } j = i, \\ 0, & \text{если } j \neq i. \end{cases}$$

(2) Нетрудно видеть, что

$$\sum_{j=0}^{p^m-1} \zeta^{-ij}\tau_j = \sum_{j=0}^{p^m-1} \zeta^{-ij} \sum_{\substack{x=1 \\ p \nmid x}}^{p^{m+1}} \zeta^{j\,\mathrm{ind}_h(x)}\rho^x$$

$$= \sum_{\substack{x=1 \\ p \nmid x}}^{p^{m+1}} \rho^x \left(\sum_{j=0}^{p^m-1} \zeta^{j(-i+\mathrm{ind}_h(x))} \right).$$

Но из леммы 4.1(1) следует, что

$$\sum_{j=0}^{p^m-1} \zeta^{j(-i+\mathrm{ind}_h(x))} = \begin{cases} p^m, & \text{если } \mathrm{ind}_h(x) \equiv i \pmod{p^m}, \\ 0 & \text{в противном случае,} \end{cases}$$

поэтому оцениваемая сумма, деленная на p^m, равна

$$\sum_{\mathrm{ind}_h(x)\equiv i \pmod{p^m}} \rho^x = \sum_{a=0}^{p-2} \rho^{h^{ap^m+i}} = \eta_i,$$

поскольку сравнение $\mathrm{ind}_h(x) \equiv i \pmod{p^m}$, $1 \leqslant x \leqslant p^m - 1$, эквивалентно сравнению $x \equiv h^{ap^m+i} \pmod{p^{m+1}}$, где $0 \leqslant a \leqslant p-1$.

(3) Умножив соотношение $Z\tau = p^m\eta$ на Z, получим, что $p^m\tau = Z\overline{Z}\tau = p^m Z\eta$, а значит, $\tau = Z\eta$. □

В качестве следствия предыдущей леммы покажем, что следующая сумма периодов равна нулю.

Лемма 4.6. *Пусть p — нечетное простое число, $m \geqslant 1$, $1 \leqslant k \leqslant m$, $i = 0, 1, \ldots, p^{m-k} - 1$. Тогда*

$$\sum_{x=0}^{p^k-1} \eta_{i+xp^{m-k}} = 0.$$

Доказательство. По лемме 4.5(2) мы получаем

$$p^m \left(\sum_{x=0}^{p^k-1} \eta_{i+xp^{m-k}} \right) = \sum_{x=0}^{p^k-1} \sum_{j=0}^{p^m-1} \zeta^{-(i+xp^{m-k})j} \tau_j$$

$$= \sum_{j=0}^{p^m-1} \zeta^{-ij} \tau_j \left(\sum_{x=0}^{p^k-1} \zeta^{-xp^{m-k}j} \right)$$

$$= \sum_{j=0}^{p^m-1} \zeta^{-ij} \tau_j \left(\sum_{x=0}^{p^k-1} \xi^{-xj} \right),$$

где $\xi = \zeta^{p^{m-k}}$. Так как ξ — первообразный корень степени p^k из единицы, из леммы 4.1(1) следует, что

$$\sum_{x=0}^{p^k-1} \xi^{-xj} = \begin{cases} p^k, & \text{если } p^k \mid j, \\ 0 & \text{в противном случае.} \end{cases}$$

Поэтому

$$p^m \left(\sum_{x=0}^{p^k-1} \eta_{i+xp^{m-k}} \right) = p^k \left(\sum_{\substack{j=0 \\ p^k \mid j}}^{p^m-1} \zeta^{-ij} \tau_j \right) = 0$$

в силу леммы 4.4(3). □

Рассмотрим примеры. Если $m = 1$, то $k = 1$ и, как нам уже известно, $\sum_{j=0}^{p-1} \eta_j = 0$. При $m = 2$ и $k = 1$ мы получаем

$$\sum_{j=0}^{p-1} \eta_{i+jp} = 0 \qquad \text{для} \quad i = 0, 1, \ldots, p-1. \tag{4.9}$$

Если $m = 2$ и $k = 2$, то $\sum_{j=0}^{p^2-1} \eta_j = 0$. При $m = 3$ и $k = 1$ мы имеем

$$\sum_{j=0}^{p-1} \eta_{i+jp^2} = 0 \qquad \text{для} \quad i = 0, 1, \ldots, p^2-1. \tag{4.10}$$

Если $m = 3$ и $k = 2$, то

$$\sum_{j=0}^{p^2-1} \eta_{i+jp} = 0 \qquad \text{для} \quad i = 0, 1, \ldots, p-1, \tag{4.11}$$

и, наконец, при $m = 3$ и $k = 3$ мы получаем уже известное нам равенство $\sum_{j=0}^{p^3-1} \eta_j = 0$.

Мы также можем вычислить некоторые суммы квадратов периодов.

Лемма 4.7. *Пусть p — нечетное простое число, $m \geqslant 1$, $1 \leqslant k \leqslant m$, $i = 0, 1, \ldots, p^{m-k} - 1$. Тогда*

$$\sum_{x=0}^{p^k-1} \eta_{i+xp^{m-k}}^2 = p^k(p-1).$$

Доказательство. Пусть $U_j = \{\bar{a} \in (\mathbb{Z}/p^{m+1})^\bullet \mid \operatorname{ind}_h(a) \equiv j \pmod{p^m}\}$ при $j = 0, 1, \ldots, p^m(p-1)$. Тогда U_j есть смежный класс по модулю U. По определению

$$\eta_j = \sum_{\substack{0 \leqslant s \leqslant (p-1)p^m \\ \bar{s} \in U_j}} \rho^{h^s}.$$

Сохраним обозначения, введенные перед леммой 4.3:

$$\begin{aligned}\mathcal{S}_i &= \{U_i, U_{i+p^{m-k}}, U_{i+2p^{m-k}}, \dots, U_{i+(p^k-1)p^{m-k}}\},\\ \mathcal{S}'_i &= \{\overline{(1+ip)}\cdot U, \overline{[1+(i+p^{m-k})p]}\cdot U,\\ &\qquad \dots, \overline{[1+(i+(p^k-1)p^{m-k})p]}\cdot U\}.\end{aligned}$$

Пусть π — перестановка множества $\{0,1,\dots,p^{m-k}-1\}$, такая, что $\mathcal{S}'_i = \mathcal{S}_{\pi(i)}$ (см. лемму 4.3). Тогда

$$\sum_{x=0}^{p^k-1}\eta^2_{i+xp^{m-k}} = \sum_{U_j\in\mathcal{S}_i}\eta_j^2 = \sum_{U_j\in\mathcal{S}'_{\pi^{-1}(i)}}\eta_j^2.$$

Таким образом, нам необходимо вычислить суммы

$$S_i = \sum_{x=0}^{p^k-1}\left(\sum_{a=1}^{p-1}\rho^{(1+ip+xp^{m+1-k})a^{p^m}}\right)^2.$$

Полагая $\zeta = \rho^p$ и $\xi = \rho^{p^{m+1-k}}$ (следовательно, $\xi^{p^k}=1$), получим

$$\begin{aligned}S_i &= \sum_{x=0}^{p^k-1}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\rho^{(1+ip+xp^{m+1-k})(a^{p^m}+b^{p^m})}\\ &= \sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\rho^{a^{p^m}+b^{p^m}}\zeta^{i(a^{p^{m-1}}+b^{p^{m-1}})}\sum_{x=0}^{p^k-1}\xi^{x(a^{p^{k-1}}+b^{p^{k-1}})},\end{aligned}$$

так как $a^{p^m}\equiv a^{p^{m-1}} \pmod{p^m}$, $a^{p^m}\equiv a^{p^{k-1}} \pmod{p^k}$ и аналогичные соотношения выполняются для b.

Из леммы 4.1 получим

$$S_i = p^k\sum_{a=1}^{p-1}\rho^{a^{p^m}-a^{p^m}}\zeta^{i(a^{p^{m-1}}-a^{p^{m-1}})} = p^k(p-1),$$

что и завершает доказательство. □

В частности, при $k=m$ имеем

$$\sum_{j=0}^{p^m-1}\eta_j^2 = p^m(p-1). \tag{4.12}$$

Рассмотрим случай $m=1$. Определим число a, $1\leqslant a\leqslant p-1$, следующим образом. Пусть $s = \operatorname{ind}_h(1+p)$. Тогда $h^s\equiv 1+p \pmod{p^2}$, следовательно, $h^{sp}\equiv(1+p)^p\equiv 1 \pmod{p^2}$. Поэтому

$p(p-1)$ делит sp, а значит, $p-1$ делит s, и мы можем определить число a из равенства $a(p-1)=s$.

ЛЕММА 4.8. *Пусть* $m=1$ *и* $a(p-1)=\operatorname{ind}_h(1+p)$. *Тогда* $\operatorname{ind}_h(1+cp)\equiv -ca \pmod p$ *для каждого* $c=0,1,\dots,p-1$.

ДОКАЗАТЕЛЬСТВО. Из сравнения $h^{a(p-1)}\equiv 1+p \pmod{p^2}$ получим $h^{ca(p-1)}\equiv (1+p)^c\equiv 1+cp \pmod{p^2}$. Поэтому $\operatorname{ind}_h(1+cp)\equiv ca(p-1) \pmod{p(p-1)}$. В частности, $\operatorname{ind}_h(1+cp)\equiv cap-ca\equiv -ca \pmod p$. □

ЛЕММА 4.9. *Для* $m=1$ *суммы Якоби* (*при* $i=0,1,\dots,p-1$) *задаются формулой*

$$\tau_i=p\rho^{(ai)^p},$$

где $a(p-1)=\operatorname{ind}_h(1+p)$.

ДОКАЗАТЕЛЬСТВО. По определению

$$\tau_i=\sum_{x=0}^{p^2-1}\zeta^{i\operatorname{ind}_h(x)}\rho^x.$$

Из формулы (4.3) следует, что мы можем единственным образом записать

$$x\equiv h^{pb}(1+cp) \pmod{p^2},$$

где $0\leqslant b,c\leqslant p-1$. Согласно лемме 4.8 справедливы сравнения $\operatorname{ind}_h(x)\equiv pb+\operatorname{ind}_h(1+cp)\equiv -ca \pmod p$. Следовательно, замечая, что $\rho^p=\zeta$, получим

$$\tau_i=\sum_{c=0}^{p-1}\zeta^{-ica}\sum_{b=0}^{p-1}\rho^{h^{pb}(1+cp)}=\sum_{b=0}^{p-1}\rho^{h^{pb}}\sum_{c=0}^{p-1}\zeta^{c(h^{pb}-ia)}.$$

Так как $ia\not\equiv 0 \pmod p$, мы заключаем, что $(ia)^p \pmod{p^2}\in U$. Поэтому существует число b_0, $1\leqslant b_0\leqslant p-1$, такое, что $(ia)^p\equiv h^{pb_0} \pmod{p^2}$. Как следует из леммы 4.1(1),

$$\sum_{c=0}^{p-1}\zeta^{c(h^{pb}-ia)}=\begin{cases}p, & \text{если } b=b_0,\\ 0, & \text{если } b\neq b_0.\end{cases}$$

Отсюда получим

$$\tau_i=\rho^{h^{pb_0}}=\rho^{(ia)^p}. \quad \square$$

По аналогии с утверждением (2B) найдем индуктивные выражения для величин $N(p,m,k)$ и $F(p,m,k)$ через периоды (см. Клёсген, 1970).

(4L) *Справедливы следующие равенства:*

$$(1)\quad F(p,m,k)=\frac{1}{p}F(p,m-1,k)+\frac{p-1}{p^{m+1}}\sum_{i=0}^{p^m-1}\eta_i^k;$$

$$(2)\quad N(p,m,k)=\frac{1}{p}N(p,m-1,k)+\frac{1}{p^{m+1}}\sum_{i=0}^{p^m-1}\eta_i^k.$$

Доказательство. (1) Из леммы 4.1(1) получим

$$\begin{aligned}
p^{m+1}F(p,m,k) &= \sum_{x_1=1}^{p-1}\sum_{x_2=1}^{p-1}\dots\sum_{x_k=1}^{p-1}\sum_{y=0}^{p^{m+1}-1}\rho^{y(x_1^{p^m}+\dots+x_k^{p^m})}\\
&= \sum_{y=0}^{p^{m+1}-1}\sum_{x_1=1}^{p-1}\rho^{yx_1^{p^m}}\dots\sum_{x_k=1}^{p-1}\rho^{yx_k^{p^m}}\\
&= \sum_{y=0}^{p^{m+1}-1}\left(\sum_{x=1}^{p-1}\rho^{yx^{p^m}}\right)^k\\
&= \sum_{\substack{\nu=0\\ p\mid\nu}}^{p^{m+1}-1}\left(\sum_{x=1}^{p-1}\rho^{yx^{p^m}}\right)^k+\sum_{\substack{\nu=0\\ p\nmid\nu}}^{p^{m+1}-1}\left(\sum_{x=1}^{p-1}\rho^{yx^{p^m}}\right)^k\\
&= \sum_{t=0}^{p^m-1}\left(\sum_{x=1}^{p-1}\zeta^{tx^{p^m-1}}\right)^k+\sum_{\substack{\nu=0\\ p\nmid\nu}}^{p^{m+1}-1}\left(\sum_{x=1}^{p-1}\rho^{yx^{p^m}}\right)^k,
\end{aligned}$$

поскольку $\rho^p=\zeta$ и $x^{p^m}\equiv x^{p^{m-1}}\pmod{p^m}$. Так как

$$p^mF(p,m-1,k)=\sum_{t=0}^{p^m-1}\left(\sum_{x=1}^{p-1}\zeta^{tx^{p^m-1}}\right)^k,$$

используя такие же вычисления, получим

$$p^{m+1}F(p,m,k)=p^mF(p,m-1,k)+\sum_{\substack{y=0\\ p\nmid y}}^{p^{m+1}-1}\left(\sum_{x=1}^{p-1}\rho^{yx^{p^m}}\right)^k.$$

Каждое число y, $0\leqslant y\leqslant p^{m+1}-1$, $p\nmid y$, может быть единственным образом представлено в виде $y\equiv h^i\pmod{p^{m+1}}$, где $0\leqslant i\leqslant p^m(p-1)$. Также каждое число x^{p^m} (при $1\leqslant x\leqslant p-1$) может быть единственным образом представлено в виде $x^{p^m}\equiv h^{cp^m}$

(mod p^{m+1}), где $0 \leqslant c \leqslant p-2$. Следовательно,

$$\sum_{\substack{\nu=0 \\ p \nmid \nu}}^{p^{m+1}-1} \left(\sum_{x=1}^{p-1} \rho^{yx^{p^m}} \right)^k = \sum_{i=0}^{p^m(p-1)-1} \left(\sum_{c=0}^{p-2} \rho^{h^{i+cp^m}} \right)^k$$

$$= \sum_{i=0}^{p^m(p-1)-1} \eta_i^k$$

$$= (p-1) \sum_{i=0}^{p^m-1} \eta_i^k.$$

Таким образом,

$$F(p,m,k) = \frac{1}{p} F(p,m-1,k) + \frac{p-1}{p^{m+1}} \sum_{i=0}^{p^m-1} \eta_i^k.$$

(2) Разделив на $p-1$ и принимая во внимание утверждение (4G), получим рекуррентное соотношение для $N(p,m,k)$. □

Как следствие с учетом утверждения (4G) найдем

$$F(p) = \frac{(p-1)(p-2)}{p} + \frac{p-1}{p^2} \sum_{i=0}^{p-1} \eta_i^3, \tag{4.13}$$

$$N(p) = \frac{p-2}{p} + \frac{1}{p^2} \sum_{i=0}^{p-1} \eta_i^3. \tag{4.14}$$

Пусть $S(p^m,k) = \sum_{i=0}^{p-1} [\eta_i(p,m)]^k$. Из рекуррентных формул утверждения (4L) получим следующие выражения.

(4M) *Справедливы соотношения*

(1) $F(p,m,k) = \dfrac{p-1}{p^{m+1}} [(p-1)^k + (-1)^k + S(p^m,k) + S(p^{m-1},k) + \\ + \ldots + S(p,k)]$;

(2) $N(p,m,k) = \dfrac{1}{p^{m+1}} [(p-1)^{k-1} + (-1)^k + S(p^m,k) + S(p^{m-1},k) + \\ + \ldots + S(p,k)]$.

Доказательство. (1) Нетрудно видеть, что

$$\begin{aligned} F(p,m,k) &= \frac{1}{p}F(p,m-1,k)+\frac{p-1}{p^{m+1}}S(p^m,k),\\ \frac{1}{p}F(p,m-1,k) &= \frac{1}{p^2}F(p,m-2,k)+\frac{p-1}{p^{m+1}}S(p^{m-1},k),\\ &\vdots\\ \frac{1}{p^{m-1}}F(p,1,k) &= \frac{1}{p^m}F(p,0,k)+\frac{p-1}{p^{m+1}}S(p,k). \end{aligned}$$

Учитывая утверждение (4G), получим

$$\begin{aligned} F(p,m,k) = \frac{p-1}{p^{m+1}}[&(p-1)^k+(-1)^k+S(p^m,k)+S(p^{m-1},k)\\ &+\ldots+S(p,k)]. \end{aligned}$$

(2) Эта формула получается из предыдущей делением на $p-1$. □

Из доказанной формулы при $k=2$ следует, что $N(p,m,2)=1$ (тривиально). Тогда утверждение (4M) позволяет получить результат леммы 4.7 при $k=m$. Действительно, если $m=1$, то

$$1=N(p,1,2)=\frac{1}{p^2}[(p-1)+1+S(p,2)],$$

и тогда

$$S(p,2)=\sum_{j=0}^{p^2-1}[\eta_j(p,1)]^2=p(p-1).$$

По предположению индукции при $r<m$ имеем

$$S(p^r,2)=\sum_{j=0}^{p^r-1}[\eta_i(p,r)]^2=p^r(p-1),$$

а значит,

$$\begin{aligned} 1 &= N(p,m,2)\\ &= \frac{1}{p^{m+1}}[(p-1)+1+S(p^m,2)+p^{m-1}(p-1)+\ldots+p(p-1)]. \end{aligned}$$

Поэтому $S(p^m,2)=p^m(p-1)$. Таким образом, $S(p^m,2)$ есть целое число, делящееся на p^m.

Чтобы получить дальнейшие результаты, связанные с суммами степеней периодов Гаусса, нам понадобится лемма о q-адических значениях произведения факториалов.

ЛЕММА 4.10. *Пусть q — простое число, $s \geqslant 1$, $\mu > 1$, и пусть $r_1, r_2, \ldots, r_\mu$ — такие положительные целые числа, что $q^s = r_1 + r_2 + \ldots + r_\mu$. Тогда*

$$v_q(r_1! r_2! \ldots r_\mu!) \leqslant q v_q(q^{s-1}!)$$

и если $\mu = q$, $r_1 = r_2 = \ldots = r_q = q^{s-1}$, то $v_q(q^{s-1}! \ldots q^{s-1}!) = q v_q(q^{s-1}!)$.

ДОКАЗАТЕЛЬСТВО. Применим метод математической индукции по s. При $s = 1$ утверждение леммы тривиально (так как $\mu > 1$).

Нетрудно видеть, что $[r_1/q] + \ldots + [r_\mu/q] \leqslant q^{s-1}$, поэтому при некотором $r_0' \geqslant 0$ получим $r_0' + [r_1/q] + \ldots + [r_\mu/q] = q^{s-1}$. По предположению индукции

$$v_q(r_0'!) + v_q\left(\left[\frac{r_1}{q}\right]!\right) + \ldots + v_q\left(\left[\frac{r_\mu}{q}\right]!\right) \leqslant q v_q(q^{s-2}!).$$

В утверждении (1А) гл. II было показано, что для любого целого числа $t \geqslant 1$ выполняется соотношение

$$v_q(t!) = \left[\frac{t}{q}\right] + \left[\frac{t}{q^2}\right] + \left[\frac{t}{q^3}\right] + \ldots$$

и для любого вещественного $x \geqslant 0$ и целого числа $a \geqslant 1$ справедливо равенство $[x/a] = [[x]/a]$. Тогда

$$\begin{aligned}
&v_q(r_1!) + v_q(r_2!) + \ldots + v_q(r_\mu!) \\
&\quad = \sum_{i=1}^{\mu} \left(\left[\frac{r_i}{q}\right] + \left[\frac{r_i}{q^2}\right] + \left[\frac{r_i}{q^3}\right] + \ldots \right) \\
&\quad = \sum_{i=1}^{\mu} \left[\frac{r_i}{q}\right] + \sum_{i=1}^{\mu} \left(\left[\frac{[r_i/q]}{q}\right] + \left[\frac{[r_i/q]}{q^2}\right] + \ldots \right) \\
&\quad \leqslant q^{s-1} + v_q(r_0'!) + \sum_{i=1}^{\mu} v_q\left(\left[\frac{r_i}{q}\right]!\right) \\
&\quad \leqslant q^{s-1} + q v_q(q^{s-2}!) \\
&\quad = q^{s-1} + q(q^{s-3} + \ldots + q + 1) \\
&\quad = q(q^{s-2} + q^{s-3} + \ldots + q + 1) = q v_q(q^{s-1}!).
\end{aligned}$$

Последнее утверждение тривиально. □

(4N) *Справедливы следующие свойства сумм* $S(p^m, k)$:

(1) $S(p^m, k) = p^m[pN(p, m, k) - N(p, m-1, k)] = p^m[F(p, m, k) - F^*(p, m, k)]$;

(2) *если* q *— простое число,* $k = q^s$, *то* $S(p^m, q^s)$ *делится на* q.

Доказательство. (1) Из утверждений (3L) и (4H) найдем

$$\begin{aligned} S(p^m, k) &= p^m[pN(p, m, k) - N(p, m-1, k)] \\ &= p^m[(p-1)N(p, m, k) - F^*(p, m, k)] \\ &= p^m[F(p, m, k) - F^*(p, m, k)]. \end{aligned}$$

(2) Как следует из утверждения (1), мы можем предположить, что $q \neq p$, и нам достаточно показать, что q делит $F(p, m, q^s)$ и $F^*(p, m, q^s) = F(p, m, q^s; c)$, где $1 \leqslant c \leqslant p-1$, $c \equiv q \pmod p$ (см. результат (4H)). Пусть $x_1, x_2, \ldots, x_k \in \mathbb{Z}$ и $x_1^{p^m} + x_2^{p^m} + \ldots + x_k^{p^m} \equiv 0 \pmod{p^{m+1}}$, соответственно $x_1^{p^m} + x_2^{p^m} + \ldots + x_k^{p^m} \equiv c \pmod{p^{m+1}}$, где $1 \leqslant x_i \leqslant p^{m+1} - 1$ при $i = 1, \ldots, k$, $k = q^s$. Любая перестановка решения $(x_1, x_2, \ldots, x_k)$ остается решением сравнения. Следовательно, множество решений разбивается на непересекающиеся классы эквивалентных (относительно перестановки) решений. Таким образом, достаточно доказать, что число решений, эквивалентных данному, делится на q.

Пусть набор $(x_1, x_2, \ldots, x_k)$ имеет ровно μ различных компонент и $r_1, r_2, \ldots, r_\mu$ — число их повторений ($r_i \geqslant 1$). Заметим, что $\mu \neq 1$, так как в противном случае $x_1 = x_2 = \ldots = x_k$ и мы получим $qx_1^{p^m} \equiv \equiv 0$, соответственно $q \pmod p$, что невозможно. Отсюда следует, что $r_1 < k, \ldots, r_\mu < k$.

Число решений, полученных перестановками набора $(x_1, x_2, \ldots, \ldots, x_k)$, равно $k!/(r_1! r_2! \ldots r_\mu!)$. Поэтому нам необходимо доказать, что q делит это число. Нетрудно видеть, что

$$v_q(k!) = q^{s-1} + q^{s-2} + \ldots + q + 1.$$

Так как $r_1 + r_2 + \ldots + r_\mu = q^s$ и $\mu > 1$, мы получаем $v_q(r_1! r_2! \ldots r_\mu!) \leqslant \leqslant q(q^{s-2} + q^{s-3} + \ldots + q + 1) = q^{s-1} + q^{s-2} + \ldots + q^2 + q$.

Следовательно, q-адическое значение числа $k!/(r_1! r_2! \ldots r_\mu!)$ по меньшей мере равно единице, что и требовалось доказать. □

Выразим верхнюю границу величины $N(p)$ через периоды. Ввиду формулы (4.14) нам необходимо найти верхнюю границу для суммы $\sum_{i=0}^{p-1} \eta_i^3$. Для этого докажем следующую лемму.

ЛЕММА 4.11. *Пусть $n \geqslant 3$ и f — функция n действительных переменных,*

$$f(y_1, \ldots, y_n) = \sum_{i=1}^{n} y_i^3,$$

определенная на множестве D всех таких точек $(y_1, \ldots, y_n)$, что $\sum_{i=1}^n y_i = 0$ и $\sum_{i=1}^n y_i^2 = n(n-1)$.

(1) *Если $(y_1, \ldots, y_n)$ — точка максимума или минимума функции, то существует такое целое число T, $1 \leqslant T \leqslant n-1$, что (с точностью до перестановки множества $\{1, \ldots, n\}$)*

$$\begin{cases} y_1 = \ldots = y_T = (n-T)\sqrt{\dfrac{n-1}{T(n-T)}}, \\ y_{T+1} = \ldots = y_n = -T\sqrt{\dfrac{n-1}{T(n-T)}}. \end{cases}$$

Пусть, далее, y^T — точка, координаты которой удовлетворяют указанным выше равенствам. Тогда

(2) $f(y^T) = n(n-1)(n-2T)\sqrt{(n-1)/(T(n-T))}$, $f(y^{n-T}) = -f(y^T)$, $f(y^T) > 0$ *при* $1 \leqslant T < (n-1)/2$;

(3) *если* $T = 1$, *то* $f(y^T) = n(n-1)(n-2)$ *есть абсолютный максимум функции f на множестве D;*

(4) *если* $1 \leqslant T \leqslant n-1$, *то* $f(y^T)$ *есть абсолютный максимум функции f на множестве точек $y = (y_1, \ldots, y_n) \in D$, удовлетворяющих условию* $y_i \leqslant (n-T)\sqrt{(n-1)/(T(n-T))}$.

ДОКАЗАТЕЛЬСТВО. (1) Для нахождения точек максимума или минимума функции f на множестве D применим метод множителей Лагранжа. Пусть

$$F(y_1, \ldots, y_n) = f(y_1, \ldots, y_n) + \lambda\left(\sum_{i=1}^{n} y_i\right) + \mu\left(\sum_{i=1}^{n} y_i^2 - n(n-1)\right),$$

где λ, μ — параметры. Если $(y_1, \ldots, y_n)$ — точка экстремума, то $(\partial F/\partial y_i)(y_1, \ldots, y_n) = 0$ (при $i = 1, \ldots, n$), т. е.

$$3y_i^2 + \lambda + 2\mu y_i = 0 \qquad (\text{при } i = 1, \ldots, n). \tag{4.15}$$

Сложив эти равенства, найдем, что $3n(n-1) + n\lambda = 0$, следовательно, $\lambda = -3(n-1)$. Подставляя это значение в формулу (4.15), получим $3y_i^2 + 2\mu y_i - 3(n-1) = 0$, поэтому

$$y_i = \frac{-\mu \pm \sqrt{\mu^2 + 9(n-1)}}{3}. \tag{4.16}$$

Поскольку существует только два возможных значения координат, найдется такое целое число T, $0 \leqslant T \leqslant n$, что с точностью до перестановки множества $\{1, \ldots, n\}$ выполняются равенства

$$y_1 = \ldots = y_T = \frac{-\mu + \sqrt{\mu^2 + 9(n-1)}}{3},$$

$$y_{T+1} = \ldots = y_n = \frac{-\mu - \sqrt{\mu^2 + 9(n-1)}}{3}.$$

Заметим, что все координаты не могут быть равными, так как $\sum_{i=1}^{n} y_i = 0$. Значит, $1 \leqslant T \leqslant n-1$. Кроме того,

$$0 = -\frac{\mu}{3}(T + n - T) + \frac{1}{3}\sqrt{\mu^2 + 9(n-1)}(T - n + T),$$

следовательно,

$$n\mu = (2T - n)\sqrt{\mu^2 + 9(n-1)},$$

поэтому

$$n^2\mu^2 = (2T - n)^2[\mu^2 + 9(n-1)]$$

и, наконец,

$$\mu = \frac{3(2T-n)}{2}\sqrt{\frac{n-1}{T(n-T)}},$$

$$\mu^2 + 9(n-1) = \frac{9(n-1)n^2}{4T(n-T)}.$$

Подставив полученные выражения в формулу (4.16), найдем

$$y_i = \begin{cases} (n-T)\sqrt{\dfrac{n-1}{T(n-T)}}, \\ -T\sqrt{\dfrac{n-1}{T(n-T)}}. \end{cases} \tag{4.17}$$

(2) Если координаты точки y^T удовлетворяют указанным выше предположениям, то

$$\sum_{i=1}^{n} y_i^3 = T(n-T)^3 \frac{n-1}{T(n-T)}\sqrt{\frac{n-1}{T(n-T)}}$$

$$-(n-T)T^3 \frac{n-1}{T(n-T)}\sqrt{\frac{n-1}{T(n-T)}}$$

$$= n(n-1)(n-2T)\sqrt{\frac{n-1}{T(n-T)}}.$$

Пусть

$$\tilde{f}(t) = n(n-1)(n-2t)\sqrt{\frac{n-1}{t(n-t)}}$$

при $0 < t < n$. Тогда $\tilde{f}(n-t) = -\tilde{f}(t)$, $\tilde{f}(t) > 0$ при $0 < t < n/2$ и $f(y^T) = \tilde{f}(T)$ при $T = 1, 2, \ldots, n-1$. Легко видеть, что $t(n-t) \leqslant (t+1)(n-t-1)$ при $0 < t \leqslant (n-1)/2$. Таким образом,

$$\frac{n-2t}{\sqrt{t(n-t)}} > \frac{n-2t-2}{\sqrt{(t+1)(n-t-1)}}$$

и, следовательно, $f(y^T) > f(y^{T+1}) > 0$ при $T = 1, 2, \ldots, [n/2] - 1$.

(3) При $T = 1$ имеем $f(y^1) = n(n-1)(n-2)$. Так как функция f определена и непрерывна на замкнутом и ограниченном множестве, она достигает на нем максимального и минимального значения. Из (1) и (2) следует, что y^1 — точка абсолютного максимума функции f.

(4) Пусть $1 \leqslant T \leqslant n-1$ и D_T — подмножество множества D, состоящее из точек, координаты которых удовлетворяют неравенствам $y_i \leqslant (n-T)\sqrt{(n-1)/(T(n-T))}$. Если $1 \leqslant T' \leqslant n-1$, то $y^{T'} \in D_T$ в точности тогда, когда $T \leqslant T'$. Следовательно, поскольку $f(y^{T'-1}) > f(y^{T'}) > 0$ при $2 \leqslant T' \leqslant [n/2]$ и $f(y^{T'}) < 0$ при $T' > [n/2]$, мы заключаем, что $f(y^T)$ есть абсолютный максимум функции f на множестве D_T. □

Во введенных выше обозначениях имеем такой результат.

(4О) *Пусть* $M = \max\{\eta_i \mid i = 0, \ldots, p-1\}$ *и* T — *наибольшее целое число, удовлетворяющее условию*

$$M \leqslant (p-T)\sqrt{\frac{p-1}{T(p-T)}}.$$

Тогда

$$N(p) < 1 + (p-2T)\sqrt{\frac{p-1}{T(p-T)}}.$$

Доказательство. Так как $\sum_{i=0}^{p-1} \eta_i = 0$, справедливо неравенство $0 < M$. Из неравенства (4.6) следует, что $M < p-1$. Функция

$$g(t) = (p-t)\sqrt{\frac{p-1}{t(p-t)}}$$

убывает, и $g(1) = p-1$, $g(p-1) = 1$. Следовательно, существует максимальное целое число T, $1 \leqslant T \leqslant p-1$, такое, что

$$M \leqslant (p-T)\sqrt{\frac{p-1}{T(p-T)}}.$$

Поскольку

$$\sum_{i=0}^{p-1} \eta_i = 0, \qquad \sum_{i=0}^{p-1} {\eta_i}^2 = p(p-1),$$

мы заключаем, что $(\eta_0, \eta_1, \ldots, \eta_{p-1}) \in D_T$. По лемме 4.11 значение $f(y_1^T)$ есть абсолютный максимум функции f на D_T, поэтому

$$\sum_{i=0}^{p-1} {\eta_i}^3 = f(\eta_0, \ldots, \eta_{p-1}) \leqslant f(y^T) = p(p-1)(p-2T)\sqrt{\frac{p-1}{T(p-T)}}.$$

Из равенства (4.14) найдем

$$\begin{aligned} N(p) &= \frac{p-2}{p} + \frac{1}{p^2}\sum_{i=0}^{p-1}\eta_i^3 \\ &\leqslant \frac{p-2}{p} + \frac{(p-1)(p-2T)}{p}\sqrt{\frac{p-1}{T(p-T)}} \\ &< 1 + (p-2T)\sqrt{\frac{p-1}{T(p-T)}}. \quad \square \end{aligned}$$

Заметим, что если

$$M = (p-T)\sqrt{\frac{p-1}{T(p-T)}},$$

то $N(p) < 1 + M$. Действительно, при доказательстве утверждения (4O) мы получили оценку

$$\begin{aligned} N(p) &\leqslant \frac{p-2}{p} + \frac{(p-1)(p-2T)}{p}\sqrt{\frac{p-1}{T(p-T)}} \\ &= \frac{p-2}{p} + \frac{p-1}{p}\frac{p-2T}{p-T}M \\ &< 1 + M. \end{aligned}$$

Исследуем теперь поведение $F(p, m, k)$ и $N(p, m, k)$ при $k \to \infty$.

(4P) *Справедливо равенство*

$$\lim_{k\to\infty} \frac{N(p,m,k)}{(p-1)^{k-1}/p^{m+1}} = 1.$$

Доказательство. Из утверждения (4M) имеем

$$\frac{N(p,m,k)}{(p-1)^{k-1}/p^{m+1}} = 1 + \frac{(-1)^k}{(p-1)^{k-1}} + (p-1)\sum_{j=1}^{m} \frac{S(p^j,k)}{(p-1)^k}$$

$$= 1 + \frac{(-1)^k}{(p-1)^{k-1}} + (p-1)\sum_{j=1}^{m}\sum_{i=1}^{p^j-1} \left\{\frac{\eta_i(p,j)}{p-1}\right\}^k.$$

Так как $|\eta_i(p,j)| < p-1$, из неравенства (4.6) следует, что

$$\lim_{k\to\infty} \left\{\frac{\eta_i(p,j)}{(p-1)}\right\}^k = 0,$$

поэтому $\lim_{k\to\infty} N(p,m,k)/((p-1)^{k-1}/p^{m+1}) = 1$. □

Рассмотрим вопрос о существовании p-адических решений конкретного сравнения. Пусть $\hat{U}_p$ обозначает мультипликативную группу корней степени $(p-1)$ из единицы в кольце $\hat{\mathbb{Z}}_p$ целых p-адических чисел. Справедливо следующее утверждение.

(4Q)

(1) *Существует целое число* $m_0 = m_0(k,p) \geqslant 1$, *такое, что для любого* $m \geqslant m_0$ *выполняется равенство* $N(p,m,k) = N(p,m_0,k)$.

Обозначим для краткости $N(p,m_0,k)$ *через* $N(p,k)$, $N(p,k) \geqslant 0$.

(2) *Величина* $N(p,k)$ *совпадает с числом решений уравнения* $1 + X_2 + \ldots + X_k = 0$ *в элементах из* $\hat{U}_p$.

Доказательство. (1) В утверждении (4H) было показано, что $0 \leqslant N(p,m,k) \leqslant N(p,m-1,k)$. Поэтому существует число m_0 с указанным свойством.

(2) Пусть $m \geqslant m_0$ и

$$1 + \sum_{i=2}^{k} x_i^{p^m} \equiv 0 \pmod{p^{m+1}},$$

где $p \nmid x_i$. Так как $x_i^{p^{m+1}} \equiv x_i^{p^m} \pmod{p^{m+1}}$, мы получаем

$$1 + \sum_{i=2}^{k} x_i^{p^{m+1}} \equiv 0 \pmod{p^{m+1}},$$

а значит,

$$1 + \sum_{i=2}^{k} x_i^{p^{m+1}} \equiv ap^{m+1} \pmod{p^{m+2}},$$

где число a удовлетворяет условию $0 \leqslant a \leqslant p-1$. Так как $m+1 > m_0$, из утверждения (4H) имеем $F^*(p, m+1, k) = 0$, поэтому $a = 0$, следовательно,

$$1 + \sum_{i=2}^{k} x_i^{p^{m+1}} \equiv 0 \pmod{p^{m+2}}.$$

Мы установили отображение

$$(x_2 \bmod p^{m+1}, \ldots, x_k \bmod p^{m+1}) \\ \to (x_2 \bmod p^{m+2}, \ldots, x_k \bmod p^{m+2})$$

множества S_m решений сравнения

$$1 + X_2^{p^m} + \ldots + X_k^{p^m} \equiv 0 \pmod{p^{m+1}}$$

в соответствующее множество S_{m+1}. Ясно, что это отображение инъективно.

Таким образом, элементам $(x_2 \bmod p^{m_0+1}, \ldots, x_k \bmod p^{m_0+1}) \in \in S_{m_0}$ мы ставим в соответствие последовательности $(\alpha_{m,i})_{m \geqslant m_0}$, $\alpha_{m,i} = x_i^{p^m}$ (при $i = 2, \ldots, k$). Поскольку $x_i^{p^{m+1}} \equiv x_i^{p^m} \pmod{p^{m+1}}$, мы имеем $\alpha_{m+1,i} \equiv \alpha_{m,i} \pmod{p^m}$, следовательно, последовательность $(\alpha_{m,i})_m$ является p-адически сходящейся.

Пусть $\alpha_i = \lim_{m \to \infty} \alpha_{m,i}$. Тогда $1 + \alpha_2 + \ldots + \alpha_k = 0$ в $\hat{\mathbb{Z}}_p$. Так как $\alpha_{m,i}^{p-1} \equiv 1 \pmod{p^{m+1}}$ при $m \geqslant m_0$, справедливо равенство $\alpha_i^{p-1} = = 1$, следовательно, $\alpha_i \in U_p$ и $(\alpha_2, \ldots, \alpha_k) \in \hat{S}$, где $\hat{S}$ — множество решений в $\hat{U}_p$ уравнения $1 + X_2 + \ldots + X_k = 0$. Таким образом, мы построили инъективное отображение σ множества S_{m_0} в $\hat{S}$.

С другой стороны, пусть $\alpha_i \in \hat{U}_p$, $\alpha_i = (y_{m,i})_{m \geqslant 0}$ (при $i = = 2, \ldots, k$) и $1 + \alpha_2 + \ldots + \alpha_k = 0$. Так как $\alpha_i^{p-1} = 1$, выполняется сравнение $y_{m,i}^{p-1} \equiv 1 \pmod{p^{m+1}}$ (при $i = 2, \ldots, k$ и для всех достаточно больших m). Следовательно, $y_{m,i} \equiv x_{m,i}^{p^m} \pmod{p^{m+1}}$ и

$$1 + x_{m,2}^{p^m} + \ldots + x_{m.k}^{p^m} \equiv 0 \pmod{p^{m+1}}.$$

В частности,

$$1 + x_{m,2}^{p^{m_0}} + \ldots + x_{m,k}^{p^{m_0}} \equiv 0 \pmod{p^{m_0+1}},$$

поэтому $(x_{m,2}, \ldots, x_{m,k}) \in S_{m_0}$. Таким образом, σ отображает множество S_{m_0} на множество $\hat{S}$, т. е. σ — сюръекция. Отсюда следует, что количество элементов множества $\hat{S}$ равно $N(p,k) = \#S_{m_0}$. □

Как следствие имеем такой результат.

(4R) *Пусть* $p \equiv 1 \pmod{k}$. *Тогда существуют корни степени* $(p-1)$ *из единицы* $\alpha_2, \ldots, \alpha_k \in \hat{U}_p$, *такие, что* $1 + \alpha_2 + \ldots + \alpha_k = 0$.

Доказательство. Из утверждения (4A) следует, что для любого $m \geqslant 1$ сравнение $1 + X_2^{p^m} + \ldots + X_k^{p^m} \equiv 0 \pmod{p^{m+1}}$ имеет нетривиальное решение. В частности, $N(p,k) \geqslant 1$, поэтому из утверждения (4Q) получим, что существуют $\alpha_2, \ldots, \alpha_k \in \hat{U}_p$, такие, что $1 + \alpha_2 + \ldots + \alpha_k = 0$. □

Ниже приведены таблицы значений величины $N(p,m,k)$ при малых значениях аргумента, вычисленных Клёсгеном.

Таблица для $N(p,1,k)$:

	3	4	5	6	7
5	0	9	0	100	35
7	2	15	60	340	1680
11	0	31	24	1600	5250
13	2	33	200	2260	21630
17	0	57	140	6220	50120
19	2	51	390	6880	101430

Таблица для $N(p,2,k)$ (курсивом выделены значения, отличные от соответствующих значений в предыдущей таблице):

	3	4	5	6	7
5	0	9	0	100	*0*
7	2	15	60	340	1680
11	0	*27*	24	*1090*	*2520*
13	2	33	*180*	*1930*	*15540*
17	0	*45*	*0*	*3160*	*945*
19	2	51	*300*	*4600*	*44520*

В заключение рассмотрим эвристический метод, который позволяет найти вероятность того, что сравнение

$$1 + Y^p + Z^p \equiv 0 \pmod{p^2}$$

имеет заданное число классов эквивалентных нетривиальных решений. Исключим из рассмотрения также циклические решения.

Пусть $1 \leqslant a \leqslant p-2$ и

$$M_a = \left\{ a \bmod p, \frac{1}{a} \bmod p, -(1+a) \bmod p, -\frac{1}{(1+a)} \bmod p, -\frac{(a+1)}{a} \bmod p, -\frac{a}{(a+1)} \bmod p \right\}.$$

Множество M_a состоит из шести различных решений (все они отличны от $\overline{0}$ и $-\overline{1}$), за исключением следующих случаев:

(a) $a = 1, p-2$ или $(p-1)/2$; тогда $M_a = \{1 \bmod p, (p-2) \bmod p, (p-1)/2 \bmod p\}$;

(b) $a \neq 1$, $a^3 \equiv 1 \pmod{p}$; тогда $M_a = \{a \bmod p, a^2 \bmod p\}$.

Последний случай возможен тогда и только тогда, когда $p \equiv 1 \pmod 6$.

Таким образом, множество $\{\overline{1}, \overline{2}, \ldots, \overline{p-2}\}$ разбивается на непересекающиеся классы. Если $p = 6n \pm 1$, то число таких классов M_a (содержащих более двух элементов) равно n. Действительно, если $p = 6n+1$, то число классов равно $1 + (p-2-2-3)/6 = n$. Если $p = 6n-1$, то это число снова равно $1 + (p-2-3)/6 = n$. В каждом классе M_a (содержащем более двух элементов) через $\tilde{a}$ обозначим наименьшее целое число, $1 \leqslant \tilde{a} \leqslant p-2$. Ясно, что $\tilde{a} \leqslant (p-1)/2$.

Если $1 + y^p + z^p \equiv 0 \pmod{p^2}$, то $z \equiv -(1+y) \pmod{p}$. Этому решению соответствует значение $\tilde{y}$. Заметим, что $(1+\tilde{y})^p - 1 - \tilde{y}^p \equiv 0 \pmod{p^2}$. Пусть $1 + y'^p + z'^p \equiv 0 \pmod{p^2}$. Это решение эквивалентно приведенному выше тогда и только тогда, когда $y' \bmod p \in M_y$, т. е. $\tilde{y'} = \tilde{y}$.

По малой теореме Ферма $(1+t)^p - 1 - t^p \equiv 0 \pmod{p}$ при $t \geqslant 1$, следовательно, $(1+t)^p - 1 - t^p \equiv t(p)p \pmod{p^2}$, где $0 \leqslant t(p) \leqslant p-1$. Поэтому решения сравнения соответствуют целым числам t, $1 \leqslant t \leqslant (p-1)/2$, таким, что $t(p) = 0$.

Рассмотрим последовательность $(t(p))_{t \leqslant (p-1)/2}$.

(4S) *Пусть $(t(p))_{t \leqslant (p-1)/2}$ — случайная последовательность. Тогда для всех простых чисел $p = 6n \pm 1$ справедливы следующие утверждения.*

(1) *Вероятность того, что сравнение* $1 + Y^p + Z^p \equiv 0 \pmod{p^2}$ *имеет лишь тривиальные или циклические решения, равна* $((p-1)/p)^n$.

(2) *Вероятность того, что сравнение* $1 + Y^p + Z^p \equiv 0 \pmod{p^2}$ *имеет* r *(нетривиальных, нециклических) классов эквивалентных решений, равна*

$$\frac{1}{p^r}\binom{n}{r}\left(\frac{p-1}{p}\right)^{n-r}.$$

(3) ***Плотность простых чисел, для которых существует ровно*** r ***(нетривиальных, нециклических) классов эквивалентных решений, равна***

$$\frac{1}{r!\,6^r}\frac{1}{\sqrt[6]{e}}.$$

Доказательство. (1) Как уже было отмечено, существует n классов эквивалентности во множестве $\{\overline{1}, \overline{2}, \ldots, \overline{p-2}\}$, состоящих по меньшей мере из трех элементов. Обозначим их через $M_{\tilde{x}_1}, M_{\tilde{x}_2}, \ldots, M_{\tilde{x}_n}$.

Класс $M_{\tilde{x}_i}$ состоит из решений сравнения $(1+t)^p \equiv 1 + t^p \pmod{p^2}$ в точности тогда, когда $\tilde{x}_i(p) = 0$. Поскольку $(\tilde{x}_i(p))_{\tilde{x}_i \leqslant (p-1)/2}$ — случайная последовательность, вероятность этого события равна $1/p$. Поэтому вероятность того, что ни один из n классов $M_{\tilde{x}_i}(p)$ не состоит из решений, равна $(1-1/p)^n$.

(2) Точно так же убедимся, что вероятность того события, что r из n классов $M_{\tilde{x}_i}$ состоят из решений, равна

$$\binom{n}{r}\frac{1}{p^r}\left(1-\frac{1}{p}\right)^{n-r}.$$

(3) Искомая плотность равна

$$D = \lim_{p\to\infty}\frac{1}{p^r}\binom{n}{r}\left(\frac{p-1}{p}\right)^{n-r}$$

$$= \lim_{n\to\infty}\frac{n^r\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\ldots\left(1-\frac{r-1}{n}\right)}{6^r r! n^r\left(1\pm\frac{1}{6n}\right)^r}\left(\frac{p-1}{p}\right)^{n-r}.$$

Если $p = 6n+1$, то

$$D = \frac{1}{6^r r!}\lim_{n\to\infty}\left(\frac{6n}{6n+1}\right)^{6n/6} = \frac{1}{6^r r!}\frac{1}{\sqrt[6]{e}}.$$

Аналогично, если $p = 6n - 1$, то

$$D = \frac{1}{6^r r!} \lim_{n\to\infty} \left(\frac{6n-2}{6n-1}\right)^{(6n-2)/6} \times \left(1 - \frac{1}{6n-1}\right)^{1/3}$$
$$= \frac{1}{6^r r!} \frac{1}{\sqrt[6]{e}}. \quad \square$$

Клёсген вычислил решения сравнения $1 + Y^p + Z^p \equiv 0 \pmod{p^2}$ для всех простых чисел $p < 20\,000$.

Пусть $r \geqslant 0$. Обозначим через v_r^+ (соответственно через v_r^-) количество простых чисел $p < 20\,000$, $p \equiv 1 \pmod 6$ (соответственно $p \equiv -1 \pmod 6$), для которых сравнение $1 + Y^p + Z^p \equiv 0 \pmod{p^2}$ имеет ровно r (нетривиальных, нециклических) классов эквивалентных решений.

Существует 1124 простых чисел p, таких, что $p \equiv 1 \pmod 6$ и $p < 20\,000$.

Клёсген показал, что

$v_0^+ = 970$, $v_0^+/1124 = 86.30\%$, вероятность 84.35%;
$v_1^+ = 144$, $v_1^+/1124 = 12.81\%$, вероятность 14.11%;
$v_2^+ = 9$, $v_2^+/1124 = 0.80\%$, вероятность 1.18%;
$v_3^+ = 1$, $v_3^+/1124 = 0.09\%$, вероятность 0.07%.

А если $p \equiv -1 \pmod 6$, $p < 20\,000$, то

$v_0^- = 957$, $v_0^-/1136 = 84.24\%$, вероятность 84.35%;
$v_1^- = 166$, $v_1^-/1136 = 14.61\%$, вероятность 14.11%;
$v_2^- = 13$, $v_2^-/1136 = 1.15\%$, вероятность 1.18%.

Список литературы

1965 Peschl, E., *Remarques sur la résolubilité de la congruence* $x^p + y^p + z^p \equiv 0 \pmod{p^2}$, $xyz \not\equiv 0 \pmod p$ *pour un nombre premier impair* p, Mém. Acad. Sci. Inscriptions Belles Lettres Toulouse, 14^e série, **6** (1965), 121–127.

1970 Klösgen, W., *Untersuchungen über Fermatsche Kongruenzen*, Gesellschaft Math. Datenverarbeitung, No. 36, 1970, 124 pp., Bonn.

1999 Ribenboim, P., *Classical Theory of Algebraic Numbers*, Springer-Verlag, New York, 1999.

Глава XI

Эпилог

Эта книга о последней теореме Ферма была написана для того, чтобы ею наслаждались любители. Почти все доказательства весьма подробны и используют исключительно элементарные и легко воспринимаемые методы. По этой причине мы были вынуждены исключить результаты, основанные на изучении идеалов числовых полей или на более замысловатых теориях. Однако в этой заключительной части мы укажем наиболее важные достижения, о которых нельзя говорить, оставаясь в рамках элементарных методов. Мы также вкратце наметим подход к знаменитому доказательству последней теоремы Ферма. В помощь читателю, желающему расширить свои познания в указанных вопросах, здесь также имеется список наиболее важных статей.

XI.1. Попытки

В этом разделе мы представим краткий обзор различных подходов к доказательству последней теоремы Ферма. Подходы эти не увенчались полным успехом, но пренебрегать ими не следует. В свое время эти результаты вселяли надежду на то, что последняя теорема Ферма будет наконец доказана, и приводили к новым задачам, представляющим самостоятельный интерес.

A. Теорема Куммера

В 1847 г. Куммер доказал следующую важную теорему.

Если $p > 2$ — регулярное простое число, то последняя теорема Ферма справедлива для показателя p.

Понятие *регулярного простого числа* нуждается в пояснении. Оно может быть определено в терминах числа классов круговых полей или с помощью *чисел Бернулли*.

Числа Бернулли $B_0, B_1, B_2, \ldots$ определяются рекуррентно: $B_0 = 1$, и если $n \geqslant 1$, то

$$\binom{n+1}{1} B_n + \binom{n+1}{2} B_{n-1} + \ldots + \binom{n+1}{n} B_1 + 1 = 0.$$

Таким образом, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0, \ldots$ Легко видеть, что $B_{2k+1} = 0$ для всех $k \geqslant 1$. Простое число p ***регулярно***, если p не делит числители чисел Бернулли $B_2, B_4, \ldots, B_{p-5}, B_{p-3}$. Пусть p — нечетное простое число, и пусть

$$\zeta_p = \cos(2\pi/p) + i \sin(2\pi/p)$$

есть первообразный корень степени p из 1. Пусть, далее, $\mathbb{Q}(\zeta_p)$ — p-е круговое поле. Оно состоит из всех комплексных чисел вида

$$r_0 + r_1\zeta_p + \ldots + r_{p-2}\zeta_p^{p-2},$$

где $r_0, r_1, \ldots, r_{p-2} \in \mathbb{Q}$. *Число классов* h_p поля $\mathbb{Q}(\zeta_p)$ есть определенное положительное целое число, связанное с $\mathbb{Q}(\zeta_p)$. Оно представляет собой число классов идеалов поля $\mathbb{Q}(\zeta_p)$, но мы не будем углубляться в эти понятия (см. любую книгу по теории алгебраических чисел, к примеру книгу Боревича и Шафаревича (1966) или же собственную книгу автора (1999)). Куммер показал, что простое число p регулярно тогда и только тогда, когда p не делит h_p.

Наименьшее иррегулярное простое число — 37. Известно, что иррегулярных простых чисел бесконечно много. С другой стороны, высказано предположение, которое до сих пор не доказано, что существует бесконечно много регулярных простых чисел.

Метод Куммера может быть распространен также и на многие иррегулярные простые числа. Как бы то ни было, с помощью этих методов не удавалось установить справедливость последней теоремы Ферма для бесконечного множества простых показателей.

Определить, регулярно простое число p или нет, для больших значений p не так-то просто, поскольку числители чисел Бернулли также становятся очень большими. Заметив, что достаточно убедиться, что показатель p не делит числители чисел $B_2, \ldots, B_{p-3}$ (а не требуется вычисление самих этих числителей), Д. Лемер, Э. Лемер и Вандивер указали критерий, который можно было применить для практических вычислений. Таким способом было показано (в то время, когда доказательство ПТФ еще не было получено). что ПТФ верна для всех простых показателей, вплоть до 4×10^6 (см. Булер и др. (1993)).

Список литературы

1847 Kummer, E.E., *Extrait d'une lettre de M. Kummer à M. Liouville*, J. Math. Pures Appl., **12** (1847), 136.

1851 Kummer, E.E., *Mémoire sur les nombres complexes composés de racines de l'unité et de nombres entiers*, J. Math. Pures Appl., **16** (1851), 377–498.
(The above papers are reprinted in *Collected Papers of E. E. Kummer*, Vol. 1 (editor A. Weil), Springer-Verlag, Berlin, 1975.)

1966 Borevich, Z.I. and Shafarevich, I.R., *Number Theory*, Academic Press, New York, 1966.

1993 Buhler, J., Crandall, R.E., Ernvall, R., and Metsänkyla, T., *Irregular primes and cyclotomic invariants to four million*, Math. Comp., **61** (1993), 151–153.

1999 Ribenboim, P., *Classical Theory of Algebraic Numbers*, Springer-Verlag, New York, 1999.

B. Теорема Вифериха

В 1909 г. Виферих доказал следующее утверждение.

Если первый случай ПТФ не выполнен для показателя p, то

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

В это условие[1] входит только конкретный показатель p и не входят гипотетические ненулевые решения x, y, z уравнения $X^p + Y^p = Z^p$. Было сразу же замечено, что ни одно достаточно малое простое число p не удовлетворяет указанному сравнению. Еще до эпохи компьютеров, в 1913 г., Мейснер доказал, что $p = 1093$ — наименьшее простое число, обладающее вышеуказанным свойством. Трудно представить тот объем вычислений, который для этого потребовался. Еще один пример, $p = 3511$, был найден Бигером в 1921 г. Последующие вычисления Д. Лемера, Келлера, Кларка и позднее Крэндалла, Дильхера и Померанса показали, что никакое другое простое число $p < 4 \times 10^{12}$ не удовлетворяет этому сравнению.

Дальнейшие условия подобного рода были найдены Миримановым, Вандивером, Фробениусом, Поллачеком, Россером, а также Грэнвиллем и Монаганом, которые доказали следующее утверждение.

---

[1] Если простое число p *не* удовлетворяет данному сравнению, то первый случай ПТФ справедлив для показателя p. — *Прим. перев.*

Если первый случай ПТФ не выполнен для показателя p, то

$$l^{p-1} \equiv 1 \pmod{p^2}$$

для всех простых чисел $l \leqslant 89$.

Остроумная комбинаторная комбинация этих условий, принадлежащая Гундерсону и Копперсмиту, и последовавшие за ней трудоемкие вычисления (Грэнвилль и Монаган, Таннер и Вагштаф) позволили показать, что первый случай ПТФ справедлив для каждого показателя $p < 6.93 \times 10^{17}$. Все это было сделано еще до того, как ПТФ была доказана для всех показателей.

Список литературы

1909 Wieferich, A., *Zum letzten Fermat'schen Theorem*, J. Reine Angew. Math., **136** (1909), 293–302.

1911 Mirimanoff, D., *Sur le dernier théorème de Fermat*, J. Reine Angew. Math., **139** (1911), 309–324.

1917 Pollaczek, F., *Über den grossen Fermat'schen Satz*, Sitzungsber. Akad. Wiss. Wien, Abt. IIa, **126** (1917), 45–59.

1988 Granville, A. and Monagan, M.B., *The First Case of Fermat's last theorem is true for all prime exponents up to 714,591,116,091,389*, Trans. Amer. Math. Soc., **306** (1988), 329–359.

1989 Tanner, J.W. and Wagstaff, S.S., Jr., *New bound for the first case of Fermat's last theorem*, Math. Comp., **53** (1989), 743–750.

1990 Coppersmith, D., *Fermat's last theorem (case 1) and the Wieferich criterion*, Math. Comp., **54** (1990), 895–902.

C. Первый случай последней теоремы Ферма для бесконечно многих простых показателей

Используя методы решета, Адлеман, Хиз-Браун и Фуври в 1985 г. доказали следующее утверждение.

Существует бесконечное множество S простых чисел, такое, что первый случай последней теоремы Ферма справедлив для каждого показателя $p \in S$.

Более сильный результат, справедливый не только для первого случая, нельзя было установить теми же методами. В то время эта теорема представляла собой важный шаг вперед. Метод доказательства родился из классических идей Софи Жермен и связан

с оценкой величины наименьшего простого числа в арифметических прогрессиях. При этом была использована усовершенствованная техника решета.

Бесконечное множество S, существование которого гарантирует эта теорема, определено неэффективно, так что использованный метод не позволяет доказать, что первый случай ПТФ справедлив для некоторого наперед заданного показателя p.

Здесь вновь следует отметить, что эта важная теорема устарела благодаря открытию доказательства ПТФ для всех показателей $n > 2$.

Список литературы

1985 Fouvry, E., *Théorème de Brun–Titchmarsh. Application au théorème de Fermat*, Invent. Math., **79** (1985), 383–407.

1985 Adleman, L.M. and Heath-Brown, D.R., *The first case of Fermat's last theorem*, Invent. Math., **79** (1985), 409–416.

D. Теорема Фалтингса

Морделл заметил и высказал в качестве гипотезы, что на неприводимых кривых, определяемых однородными многочленами высокой степени от трех переменных с рациональными коэффициентами, должно существовать лишь конечное число рациональных точек, при условии, что эти кривые имеют малое число сингулярностей и все они низкого порядка. Точная формулировка гипотезы выражается в терминах *рода* кривой, а это понятие выходит за рамки данной книги. В своей знаменитой статье Фалтингс доказал, среди множества других теорем, гипотезу Морделла. В частном случае уравнения Ферма его результат можно сформулировать следующим образом.

Для каждого $n > 3$ существует не более чем конечное число троек (x, y, z), таких, что x, y, z — целые числа, все не равные 0, НОД$(x, y, z) = 1$ *и* $x^n + y^n = z^n$.

Несмотря на свою важность, этот результат не приводит к доказательству ПТФ. Однако он был использован независимо Грэнвиллем и Хиз-Брауном для доказательства того факта, что множество показателей $n \geqslant 3$, для которых ПТФ верна, имеет плотность единица. Метод Грэнвилля—Хиз-Брауна применим также к очень широкому классу показательных диофантовых уравнений (см. Рибенбойм (1993)) и приводит к заключению о нулевой плотности по-

казателей, при которых эти уравнения имеют нетривиальные решения.

Список литературы

1983 Faltings, G., *Endlichkeitssätze für Abelsche Varietäten über Zahlkörpern*, Invent. Math., **73** (1983), 349–366.

1984 Filaseta, M., *An application of Faltings' results to Fermat's last theorem*, C. R. Math. Rep. Acad. Sci. Canada, **6** (1984), 31–32.

1985 Granville, A., *The set of exponents for which Fermat's last theorem is true, has density one*, C. R. Math. Rep. Acad. Sci. Canada, **7** (1985), 55–60.

1985 Heath-Brown, D.R., *Fermat's last theorem is true for almost all exponents*, Bull. London Math. Soc., **17** (1985), 15–16.

1989 Tzermias, P., *A short note on Fermat's last theorem*, C. R. Math. Rep. Acad. Sci. Canada, **11** (1989), 259–260.

1990 Brown, T.C. and Friedman, A.R., *The uniform density of sets of integers and Fermat's last theorem*, C. R. Math. Rep. Acad. Sci. Canada, **12** (1990), 1–6.

1993 Ribenboim, P., *Density results on families of diophantine equations with finitely many solutions*, Enseign. Math., **39** (1993), 3–23.

E. (abc)-гипотеза

Авторство (abc)-гипотезы приписывается Массеру и Эстерле. Она была выдвинута при рассмотрении одного из результатов Мэйсона о многочленах. Эта гипотеза звучит так.

Для любого $\varepsilon > 0$ существует число $C(\varepsilon) > 0$, такое, что если a, b, c — целые числа, $1 \leqslant a < b < c$, $c = a + b$ и $\text{НОД}(a, b, c) = 1$, то $c < C(\varepsilon) r^{1+\varepsilon}$, где r есть произведение различных простых делителей числа abc.

На интуитивном уровне, если, к примеру, $a = 2^m$, $b = 3^n$, где m, n велики, то $c = a + b$ велико, и гипотеза утверждает, что c должно иметь большой простой делитель либо иметь большое число простых делителей, так что r велико.

Легко показать, что (abc)-гипотеза влечет следующий результат.

ПТФ верна для всех достаточно больших показателей.

В самом деле, пусть $n > 3$, и пусть x, y, z — положительные целые числа, такие, что $\text{НОД}(x, y, z) = 1$ и $x^n + y^n = z^n$. Положив

$\varepsilon = \frac{1}{2}$, по (abc)-гипотезе получим, что $z^n < C(\frac{1}{2})r^{3/2}$, где

$$r = \prod_{p|x^n y^n z^n} p = \prod_{p|xyz} p \leqslant xyz \leqslant z^3,$$

а значит, $z^n < C(\frac{1}{2})z^{9/2}$. Следовательно, существует такое n_0, что $n \leqslant n_0$. Другими словами, ПТФ верна для каждого показателя $n > n_0$, или, короче, ПТФ асимптотически верна.

Известно, что из (abc)-гипотезы следует множество других недоказанных утверждений теории чисел, а также гипотеза Морделла, которая была доказана Фалтингсом. Доказательство (abc)-гипотезы представляется весьма трудным, и в настоящее время она является объектом интенсивных исследований.

Список литературы

1984 Mason, R.C., *Diophantine Equations over Function Fields*, London Math. Soc. Lecture Notes Ser., No. 96, Cambridge University Press, Cambridge, 1984.

1985 Masser, D.W., *Some open problems*, Symp. Analytic Number Theory, Imperial College, London, 1985 (unpublished).

1988 Oesterlé, J., *Nouvelles approches au théorème de Fermat*, Sém. Bourbaki, 40ème année, No. 694, Février 1988, 1987–1988.

1990 Masser, D.W., *More on a conjecture of Szpiro*, Astérisque, **183** (1990), 19–24.

1991 Elkies, N.D., *ABC implies Mordell*, Duke Math. J., Intern. Math. Res. Notes, **7** (1991), 99–109.

XI.2. Победа, или Вторая смерть Ферма

Решать задачи — долг математиков. Когда же столь долгожданное доказательство, такое, как доказательство последней теоремы Ферма, наконец, найдено, время кричать «ПОБЕДА!».

23 июня 1993 г. на своей третьей лекции в Институте Ньютона в Кембридже, Англия, Уайлс объявил о доказательстве последней теоремы Ферма. В рукописи Уайлса, тщательно изученной различными экспертами, обнаружились пробелы, которые требовали устранения. С помощью Тейлора неутомимый Уайлс преодолел все трудности и в октябре 1994 г. опубликовал две рукописи, одна из которых была написана в соавторстве с Тейлором. Они содержали доказательство гипотезы Шимуры—Таниямы для случая полу-

устойчивых эллиптических кривых, которая, согласно предшествовавшей работе Рибета, влечет за собой справедливость ПТФ. Для большинства математиков это ознаменовало собой окончание увлекательной саги. Своим достижением Уайлс заслужил восхищение всех математиков. Использованный метод уже применен к другим диофантовым уравнениям. Работа Уайлса была заключительным шагом в новой стратегии, на которой мы вскоре остановимся.

Некоторые математики не удовлетворены методом доказательства, использующим эллиптические кривые и модулярные формы, которые рассматриваются (вероятно, несправедливо? или справедливо?) как чуждые этой проблеме. Вполне разумна задача попытаться найти другое, более простое, доказательство ПТФ. Но то, что проблема Ферма решена, кроме всего прочего таит в себе и негативный аспект, и слезы об утраченном неизбежны, потому что математики и их исследования в своей тяге к нерешенным задачам подобны ночным мотылькам, которых влекут к себе яркие источники света. 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. В попытках доказать теорему Ферма, старых и новых, прославленные ученые привнесли массу интересных идей в разнообразные направления теории чисел. Неужели этот стимул исчезнет теперь, когда ПТФ доказана? Отнюдь нет. Варианты задачи, обобщения на высшие размерности, будут продолжать терзать математиков. Итак, мы празднуем эту блестящую победу и восхищаемся нашими коллегами, которые, благодаря своим усилиям и изобретательности, преуспели в решении этой задачи.

Доказательство последней теоремы Ферма должно проводиться «от противного». Мы предполагаем, что существуют $n \geqslant 3$ и натуральные числа a, b, c, такие, что $a^n + b^n = c^n$. Цель состоит в том, чтобы получить заведомо ложное утверждение. Не были найдены противоречия ни с утверждениями из элементарной теории чисел, ни с утверждениями о числовых полях, ни с какими-либо другими утверждениями, пока ПТФ не была выражена в терминах эллиптических кривых. Доказательство ПТФ включает в себя несколько этапов.

(I) Связать эллиптическую кривую с гипотетическим нетривиальным решением уравнения Ферма с произвольным показателем $n \geqslant 5$.

(II) Получить противоречие с предположением об истинности определенной гипотезы об эллиптических кривых и модулярных формах.

(III) Доказать истинность этой гипотезы.

Шаги эти требуют весьма замысловатых понятий и теорий, далеко выходящих за рамки этой книги и за рамки знаний, обычно ожидаемых от любителей и даже от профессиональных математиков, работающих в других областях. Моя задача трудна, если не сказать безнадежна. Последующее изложение весьма упрощено и поверхностно, но все равно оно может оказаться загадочным и, возможно, даже непонятным для того, кто еще не знаком с обсуждаемыми понятиями. Необходимые ключевые понятия — это эллиптические кривые, модулярные формы и представления Галуа.

A. Кривые Фрея

Для взаимно простых натуральных чисел A, B, где A делится на 16, Фрей рассмотрел эллиптическую кривую, задаваемую уравнением

$$Y^2 = X(X - A)(X + B) \tag{2.1}$$

(см. п. A6 разд. VIII.1), и изучил ее свойства.

Если последняя теорема Ферма неверна для простого показателя $q \geqslant 5$, то пусть a, b, c — натуральные попарно взаимно простые числа, такие, что число a четно и $a^q + b^q = c^q$. Пусть $A = a^q$, $B = b^q$. Соответствующая кривая Фрея демонстрирует свойства, резко отличающиеся от свойств других эллиптических кривых. Фрей пришел к убеждению, что такая ситуация невозможна, и наметил идею метода, позволяющего получить противоречие с тогда уже известной гипотезой Шимуры—Таниямы (см. ниже). Однако нужно было преодолеть серьезные препятствия, что потребовало многих лет работы (см. ниже).

Вот некоторые свойства указанных кривых Фрея. Минимальный дискриминант кривой Фрея есть

$$\Delta = \frac{a^{2q}b^{2q}(a^q + b^q)^2}{2^8} = \frac{(abc)^{2q}}{2^8}.$$

Поскольку $\Delta \neq 0$, кривая несингулярна, так что это есть эллиптическая кривая.

Для каждого простого числа p, не делящего Δ, рассмотрим сравнение

$$Y^2 \equiv X(X - a^q)(X + b^q) \pmod{p} \tag{2.2}$$

Оно определяет кривую в двумерном пространстве над конечным полем $\mathbb{F}_p$. Поскольку p не делит Δ, кривая несингулярна, так что это опять эллиптическая кривая. С другой стороны, если бы число p делило Δ, то кривая была бы сингулярна. Тип сингулярностей кодируется в инварианте, называемом *кондуктором*. Простые числа p, делящие кондуктор, в точности те же, которые делят дискриминант, т. е. это те простые числа p, для которых кривая в произведении $\mathbb{F}_p \times \mathbb{F}_p$ имеет сингулярность. Степень числа p указывает тип сингулярности. В данном случае, когда сингулярности есть узлы, кондуктор N свободен от квадратов, так что он равен

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

Эллиптические кривые с кондуктором, свободным от квадратов, называются *полуустойчивыми*. Таким образом, кривые Фрея полуустойчивые. Как было известно ранее, если предположить, что последняя теорема Ферма неверна для простого показателя q, то число q должно быть очень большим, к тому же, поскольку уравнение Ферма однородно, дискриминант есть степень целого числа, и все это вместе представляется маловероятным.

Далее мы займемся подсчетом числа точек на кривой Фрея по модулю p (для каждого p, не делящего Δ). Мы учитываем также одну дополнительную точку, которая соответствует бесконечно удаленной точке на соответствующей проективной кривой. Пусть ν_p обозначает число точек, и пусть $a_p = p + 1 - \nu_p$ (числа a_p необязательно положительные). Вспомним, что в разд. 1.1 мы исследовали уравнение Пифагора $X^2 + Y^2 = 1$ по модулю всех нечетных простых чисел и доказали, что введенные там числа N_p (которые являются аналогом чисел ν_p) легко определяются с помощью несложного сравнения, которому удовлетворяет простое число p. Рассмотрения подобного рода используются для изучения всех эллиптических кривых (не только кривых Фрея). Их дискриминант, кондуктор и целые числа a_p (для простых чисел p, не делящих дискриминант) определяются и исследуются аналогичным образом. Эллиптические кривые, которые допускают задание с помощью некоторого уравнения с коэффициентами из $\mathbb{Q}$, называются определенными

над $\mathbb{Q}$. Правило определения целых чисел a_p основано на модулярных формах.

B. Модулярные формы и гипотеза Шимуры—Таниямы

Пусть $N \geqslant 1$ — целое число, и пусть $\Gamma_0(N)$ есть множество всех 2×2 матриц

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

где a, b, c, d — целые числа, N делит c и $ad - bc = 1$. Множество $\Gamma_0(N)$ есть мультипликативная группа, которая называется *конгруэнц-группой ступени* N. Пусть H обозначает верхнюю полуплоскость, т. е. $H = \{z = x + iy \in \mathbb{C} \mid y > 0\}$. Группа $\Gamma_0(N)$ действует на H по формуле

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az + b}{cz + d} \tag{2.3}$$

для всех матриц из $\Gamma_0(N)$ и $z \in H$. Существует конечное множество специальных точек, связанных с группой $\Gamma_0(N)$, которые называются *точками заострения* (мы их здесь не определяем). Это бесконечно удаленная точка полупрямой $\{iy \mid y \geqslant 0\}$ и некоторые другие точки из множества $\mathbb{Q}$ (в случае $N > 1$).

Модулярная форма ступени N (и веса 2 — только такие мы будем рассматривать) есть отображение f из $H^* = H \cup \{\text{точки заострения } \Gamma_0(N)\}$ в $\mathbb{C}$, такое, что

(i) для всех $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ и $z \in H^*$ выполняется соотношение

$$f\left(\frac{az + b}{cz + d}\right) = (cz + d)^2 f(z); \tag{2.4}$$

(ii) функция f голоморфна в каждой точке множества H^* (это требует надлежащего определения в точках заострения).

Модулярная форма, которая обращается в нуль во всех точках заострения, называется *параболической формой*.

Теория модулярных форм очень богата. Вот некоторые важные для нас факты (которые мы приводим без намека на доказательство).

(1) Множество $\mathcal{M}_2(N)$ модулярных форм ступени N и веса 2 есть конечномерное векторное пространство над $\mathbb{C}$, а подмножество

$S_2(N)$ параболических форм есть подпространство. Для ступени $N = 2$ это подпространство параболических форм состоит только из нулевой формы.

(2) Существует естественное скалярное произведение, определенное на $S_2(N)$, так что можно рассматривать ортогональность в $S_2(N)$.

(3) Пусть $N \geqslant 1$. Если M делит N, то $M_2(M) \subseteq M_2(N)$. Также существует следующее вложение $M_2(M)$ в $M_2(N)$: если $f \in M_2(N)$, положим $\tilde{f}(z) = f((N/M)z)$ для каждого $z \in H^*$. Тогда $\tilde{f} \in M_2(N)$.

(4) Форма $f \in M_2(N)$ называется ***старой формой***, если f лежит в подпространстве $M_2(N)$, порожденном образами вложений, рассмотренных в (3), для всех чисел M, делящих N и не совпадающих с N. Форма $f \in M_2(N)$ называется ***новой формой***, если она лежит в подпространстве, которое ортогонально подпространству старых форм.

(5) Поскольку

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N),$$

мы получаем, что $f(z+1) = f(z)$ для каждой модулярной формы и каждого z. Таким образом, f разлагается в ряд Фурье вида

$$f(z) = \sum_{n=0}^{\infty} c_n e^{2\pi i n z}. \tag{2.5}$$

Для параболических форм $c_0 = 0$.

(6) Гекке определил для каждого $n \geqslant 1$, взаимно простого со ступенью N, линейный оператор T_n в пространстве $M_2(N)$. Операторы Гекке коммутируют: $T_m \circ T_n = T_n \circ T_m$ для всех чисел m и n, взаимно простых со ступенью. Модулярная форма, которая является собственным значением всех операторов Гекке T_n, называется *собственной формой*.

Также вводятся и другие операторы, связанные с целыми числами n, не взаимно простыми с N. Вместе с указанными операторами Гекке T_n они порождают более широкую алгебру Гекке, обладающую полезными свойствами (см. Уайлс и Тейлор, а также Ленстра). Новые формы ступени N, которые являются собственными формами каждого оператора T_n (где n взаимно просто с N), являются также собственными формами операторов алгебры Гекке.

Сейчас мы обсудим взаимосвязь между эллиптическими кривыми и модулярными формами. Для данной эллиптической кривой числа a_p (для всех простых чисел p, не делящих дискриминант) содержат очень важную «локальную» информацию об этой кривой (для каждого p). Ключевой момент состоит в том, чтобы связать эти локальные данные с некоторым объектом[2] при помощи некоторого «глобального» инварианта[3].

Эта важная идея есть чудесное преображение того факта, что каждое натуральное число единственным образом разлагается в произведение степеней простых чисел. Так, Эйлер уже обнаружил подобную взаимосвязь между бесконечным произведением, распространенным на все простые числа, и бесконечным рядом Дирихле по всем натуральным числам:

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Во времена Эйлера рассматривали вещественные числа s, большие единицы. Для таких s обе части равенства сходятся и равны между собой. Риман выдвинул смелую и глубокую идею, состоящую в том, что s может быть любым комплексным числом, удовлетворяющим условию $\mathrm{Re}(s) > 1$. Тогда указанный ряд есть дзета-функция Римана. Чтобы доказать существование бесконечного множества простых чисел в арифметической прогрессии, Дирихле рассмотрел «закрученный» L-ряд, числители членов которого уже не равны 1, а совпадают со значениями характеров надлежащих конечных абелевых групп. Каждый такой ряд тоже имеет абсциссу сходимости и допускает эйлерово произведение, отражающее также мультипликативное свойство характеров.

Как и дзета-функция Римана, L-ряды характеров имеют только полюса и не имеют существенных особенностей на границе области сходимости. Риман доказал, что определенные выше функции могут быть продолжены на всю комплексную плоскость посредством аналитического продолжения и, что еще более удивительно, значения справа и слева от критической прямой[4] связаны функциональным уравнением, содержащим гамма-функцию. Величайшее

---

[2] Аналитической функцией комплексного переменного. — *Прим. ред.*

[3] Бесконечного произведения по простым числам. — *Прим. ред.*

[4] Критической прямой называется прямая $\mathrm{Re}(s) = \frac{1}{2}$ на комплексной плоскости. — *Прим. ред.*

открытие. И «царская дорога» аналитическим методам в теорию чисел.

В своем поразительном сходстве с числовыми полями эллиптические кривые также демонстрируют очень важные аналитические свойства такого же типа. Локальные числа a_p, определенные выше (с учетом конечного числа множителей, связанных с простыми числами, делящими дискриминант), мультипликативно группируются и определяют числа a_n (для каждого $n \geqslant 1$), приводя тем самым к ряду Дирихле, называемому L-рядом этой эллиптической кривой. Эти ряды сходятся при $\mathrm{Re}(s) > \frac{3}{2}$. При изучении численных примеров было замечено, что такие L-ряды допускают аналитические продолжения и функциональные уравнения. Хассе выдвинул гипотезу, что это должно быть верно для каждой эллиптической кривой. Дойринг доказал ее для тех эллиптических кривых, которые допускают больше «симметрий», а именно для кривых с комплексным умножением.

В определенный момент в процессе вычислений было обнаружено, что для многих специфических эллиптических кривых числа a_p совпадают с коэффициентами c_p ряда Фурье некоторой модулярной формы. Эллиптические кривые с таким свойством были названы модулярными эллиптическими кривыми или эллиптическими кривыми Вейля.

В 1955 г. во время конференции «Токио—Никко» по теории чисел Танияма выдвинул на обсуждение задачи, две из которых были связаны (пусть еще не совсем явно) с указанным вопросом. Если бы гипотеза Хассе была верна, был бы L-ряд связан с некоторой автоморфной функцией или даже с модулярной формой? Эти задачи обсуждались с Шимурой и Вейлем. Около 1964 г. Шимура обнародовал на своих лекциях один весьма точный вариант гипотезы (который, однако, не был опубликован в печати). Вейль внес важный вклад в исследование модулярности эллиптических кривых. В его статье 1967 г. подтверждается предшествовавшее общение с Шимурой, но не содержится формулировки этой гипотезы, которую Вейль рассматривал, даже позднее, как сомнительную. В соответствии с хорошо документированным исследованием Ленга (1995) мы примем для обозначения этого проницательного утверждения термин «гипотеза Шимуры—Таниямы».

(7) **Гипотеза Шимуры—Таниямы:** *Каждая эллиптическая кривая модулярна.*

Это краткое выражение следующего факта.

Если E — произвольная эллиптическая кривая, определенная над $\mathbb{Q}$, и если N — ее кондуктор, то существует новая параболическая собственная форма f ступени N, коэффициенты Фурье c_n которой — целые числа, такая, что для каждого простого числа p, не делящего N, выполняется равенство $c_p = a_p$ (где числа a_p определяются с использованием подсчета числа точек кривой E в поле $\mathbb{F}_p$).

Эта гипотеза утверждает, что некоторая модулярная форма позволяет получить правило нахождения целых чисел a_p.

(8) Шимура доказал обращение гипотезы Шимуры—Таниямы. Пусть форма $f \in S_2(N)$ такова, что ее коэффициенты Фурье лежат в $\mathbb{Z}$. Мы объясним, как можно связать с ней эллиптическую кривую. Пусть $z_0 \in H$. Для каждого $\gamma \in \Gamma_0(N)$ рассмотрим интеграл

$$w_{z_0}(\gamma) = \int_{z_0}^{\gamma(z_0)} f(z)\,dz.$$

Он не зависит от пути. Множество $\{w_{z_0}(\gamma) \mid \gamma \in \Gamma_0(N)\}$ не зависит от z_0, так что оно зависит только от f. Используя то обстоятельство, что коэффициенты Фурье формы f — целые числа, получаем, что указанное множество есть решетка в H, т. е. множество всех линейных комбинаций двух чисел из множества H^* (*периодов* формы f) с целыми коэффициентами. Эта решетка стандартным образом приводит к аналитическому тору, а значит, к эллиптической кривой E, имеющей уравнение с коэффициентами из $\mathbb{Z}$ (так что E определена над $\mathbb{Q}$). Пусть $C_2(N) = \{f \in \mathcal{M}_2(N) \mid f$ есть параболическая собственная форма с целыми коэффициентами Фурье$\}$. Указанная конструкция связывает с каждой формой $f \in C_2(N)$ эллиптическую кривую E, определенную над $\mathbb{Q}$. Кроме того, кондуктор кривой E есть ступень N формы f, и для каждого простого числа p, не делящего дискриминант кривой E, коэффициент Фурье c_p формы f равен числу a_p (связанному с E и p так, как сказано выше).

Аналитические методы, использующие L-ряды эллиптических кривых, их эйлерово произведение, аналитическое продолжение и функциональное уравнение, играют фундаментальную роль в доказательстве.

C. Работы Рибета и Уайлса

Работа Рибета включала условное доказательство ПТФ методом спуска, связанное с представлениями Галуа и модулярными формами. Здесь необходимо объяснить, как Серр связал представления Галуа с произвольной эллиптической кривой E, определенной над $\mathbb{Q}$, т. е. допускающей уравнение с целыми коэффициентами. Множество точек кривой с комплексными координатами (к которым добавлена бесконечно удаленная точка) образует аддитивную абелеву группу, которая полностью определяется соглашением, что бесконечно удаленная точка должна быть нулем по сложению. Сложение определяется посредством следующего правила: если P, Q, R — точки на этой кривой, то $P+Q+R=0$, когда P, Q, R лежат на одной прямой (необходимы уточнения, когда $P=Q$ и в некоторых других особых случаях). Пусть K есть подполе поля $\mathbb{C}$, и пусть $E(K)$ — множество пар элементов поля K, которые удовлетворяют уравнению кривой E. Тогда $E(K)$ есть подгруппа группы $E(\mathbb{C})$.

Для каждого простого числа p также можно определить аддитивную группу $E(\mathbb{F}_p)$. В абелевой группе $E(\mathbb{C})$ рассмотрим множество $E(\mathbb{C})[p]$ всех элементов, порядок которых делит p. Это точка 0 и точки P, такие, что $P+P+\ldots+P$ (p раз) равно 0. Тогда $E(\mathbb{C})[p]$ есть подгруппа порядка p^2, которая изоморфна $\mathbb{Z}/p \times \mathbb{Z}/p$. Координаты точек в множестве $E(\mathbb{C})[p]$ лежат в некотором расширении Галуа K конечной степени над $\mathbb{Q}$. Элементы группы Галуа поля $K|\mathbb{Q}$ действуют линейно на $E(K)$ и переставляют между собой элементы группы $E(\mathbb{C})[p]$. Ввиду изоморфизма с группой $\mathbb{Z}/p \times \mathbb{Z}/p$ это приводит к линейным преобразованиям $\mathbb{Z}/p \times \mathbb{Z}/p$. Таким образом, мы имеем представление группы Галуа поля $K|\mathbb{Q}$, связанное с кривой E. Далее обычно рассматривается поле $\overline{\mathbb{Q}}$ всех алгебраических чисел, имеющее бесконечную степень и содержащее K. Группа Галуа поля $K|\mathbb{Q}$ есть факторгруппа группы Галуа G поля $\overline{\mathbb{Q}}|\mathbb{Q}$. Итак, мы получили представление $\rho_{E,p}$ группы G группой 2×2-матриц с элементами в $\mathbb{Z}/p = \mathbb{F}_p$ (здесь также необходимо обратить внимание на естественную топологию Крулля группы G). Подобные рассуждения приводят к представлениям ρ_{E,p^n} группами 2×2-матриц с элементами в $\mathbb{Z}/p^n$ (для всех $n \geqslant 1$). Все такие представления ρ_{E,p^n} (для $n \geqslant 1$) совмещаются и порождают представление $\rho_{E,\mathbb{Q}_p}$ группы G группой 2×2-матриц с элементами в поле $\mathbb{Q}_p$ p-адических чисел.

Также можно связать с произвольной собственной формой f с коэффициентами Фурье из $\mathbb{Z}$ представление $\rho_{f,\mathbb{Q}_p}$ группы G группой 2×2-матриц с элементами в $\mathbb{Q}_p$. Если E есть эллиптическая кривая, связанная с f таким образом, как показано выше, то представления $\rho_{f,\mathbb{Q}_p}$ и $\rho_{E,\mathbb{Q}_p}$ изоморфны.

Приведем набросок доказательства Рибета. Допустим, что ПТФ неверна для показателя q, и пусть E — кривая Фрея, связанная с гипотетическим решением. Тогда E — полуустойчивая эллиптическая кривая. Если гипотеза Шимуры—Таниямы справедлива, то существует новая параболическая собственная форма f веса 2, ступень которой равна кондуктору N кривой E. Тогда $\rho_{f,\mathbb{Q}_q}\cong\rho_{E,\mathbb{Q}_q}$.

Рибет доказал, что если p — нечетное простое число, делящее N, $N_1=N/p$, то существует новая параболическая собственная форма f_1 веса 2 и ступени N_1, такая, что $\rho_{f_1,\mathbb{Q}_p}=\rho_{E,\mathbb{Q}_p}$. Последовательно применяя это рассуждение, приходим к ненулевой параболической форме веса 2 и ступени 2, что невозможно.

Уайлс доказал, что гипотеза Шимуры—Таниямы справедлива для полуустойчивых эллиптических кривых, в частности для указанной кривой Фрея. Теория деформации представлений, созданная Мазуром, играет в доказательстве очень большую роль, равно как и результат (доказанный совместно с Тейлором, а также позднее Ленстрой) о структуре коммутативной алгебры, порожденной операторами Гекке. При доказательстве были существенно развиты и использованы когомологические результаты. Это в высшей степени изощренное доказательство, так что невозможно доступно изложить его в этой книге. Среди обзорных статей, указанных в списке литературы, мы можем порекомендовать статью Говеа, который приводит схему доказательства, опуская технические подробности, что делает его изложение доступным для храбреца-любителя.

XI.3. Руководство к дальнейшему изучению

Для моих храбрых читателей, у которых еще остался энтузиазм, я включил библиографию, которая содержит не только научные работы, но и материал справочного и обзорного характера, а также те статьи, с которыми следует ознакомиться читателям, желающим глубже проникнуть в существо доказательства Уайлса.

Для удобства читателя ссылки разбиты на группы.

A. Эллиптические кривые, модулярные формы: базовый материал

1962 Gunning, R.C., *Lectures on Modular Forms*, Princeton University Press, Princeton, NJ, 1962.

1971 Shimura, G., *Introduction to the Theory of Automorphic Functions*, Princeton University Press, Princeton, NJ, 1971.

1972 Ogg, A., *Survey of modular functions of one variable*, in: *Modular Functions of One Variable* (editor W. Kuyk), Springer-Verlag, New York, 1972.

1974 Tate, J., *The arithmetic of elliptic curves*, Invent. Math., **23** (1974), 179–206.

1976 Lang, S., *Introduction to Modular Forms*, Springer-Verlag, New York, 1976.

1984 Koblitz, N., *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York, 1984.

1986 Silverman, J.H., *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

1986 Cornell, G. and Silverman, J.H. (editors), *Arithmetic Geometry*, Springer-Verlag, Berlin, 1986.

1989 Miyake, T., *Modular Forms*, Springer-Verlag, New York, 1989.

1989 Hida, H., *Theory of p-adic Hecke algebras and Galois representations*, Sûgaku Expositions, **2** (1989), 75–102.

1989 Gouvêa, F.Q., *Formas Modulares, uma Introdução*, Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 1989.

1991 Cassels, J.W.S., *Lectures on Elliptic Curves*, Cambridge University Press, Cambridge, 1991.

1992 Tate, J. and Silverman, J.H., *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.

B. Обзоры

1988 Cipra, B.A., *Fermat's last corollary?*, Focus, March–April 1988, pp. 2 and 6.

1989 Shimura, G., *Yataku Taniyama and his time. Very personal recollections*, Bull. London Math. Soc., **21** (1989), 186–196.

1990 Ribet, K.A., *From the Taniyama–Shimura conjecture to Fermat's last theorem*, Ann. Fac. Sci. Toulouse Math., (5), **11** (1990), no. 1, 116–139.

1993 Murty, M. Ram, *Fermat's last theorem, an outline*, Gaz. Sc. Math. Québec, **16** (1993), No. 1, 4–13.

1993 Murty, M. Ram, *Topics in Number Theory*, Mehta Res. Inst. Lect. Notes, No. 1, Allahabad, 1993.

1993 Frey, G., *Über A. Wiles' Beweis der Fermatschen Vermutung*, Math. Semesterber., **40** (1993), no. 2, 177–191.

1993 Ribet, K.A., *Modular elliptic curves and Fermat's last theorem*, Videocassette, 100 min., Amer. Math. Soc., Providence, RI.

1994 Gouvêa, F.Q., *A marvelous proof*, Amer. Math. Monthly, **101** (1994), 203–222. (Updated Portuguese translation: Matem. Univ., no. 19, Dec. 1995, pp. 16–43.)

1994 Cox, D.A., *Introduction to Fermat's last theorem*, Amer. Math. Monthly, **101** (1994), 3–14.

1994 Rubin, K. and Silverberg, A., *Wiles' Cambridge lecture*, Bull. Amer. Math. Soc., **11** (1994), 15–38.

1994 Ribet, K.A. and Hayes, B., *Fermat's last theorem and modern arithmetic*, American Scientist, March–April 1994, pp. 146–156.

1993 Ribet, K.A., *Wiles proves Taniyama's conjecture; Fermat's last theorem follows*, Notices Amer. Math. Soc., **40** (1993), no. 6, 575–576.

1995 Ribenboim, P., *Fermat's last theorem before June 23, 1993*, in: *Proc. Fourth Conference Canad. Number Theory Assoc.*, Halifax, July 1994 (editor K. Dilcher), Amer. Math. Soc., Providence, RI, 1995, pp. 279–293.

1995 Schoof, R., *Wiles' proof of Taniyama–Weil conjecture for semi-stable elliptic curves over* $\mathbb{Q}$, Gaz. Math., Soc. Math. France, No. 66 (1995), 7–24.

1995 Edixhoven, B., *Le rôle de la conjecture de Serre dans la démonstration du théorème de Fermat*, Gaz. Math., Soc. Math. France, No. 66 (1995), 25–41. (Erratum and addendum: Gaz. Math., Soc. Math. France, No. 67 (1996), 19.)

1995 Lang, S., *Some history of the Shimura–Taniyama conjecture*, Notices Amer. Math. Soc., **42** (1995), no. 11, 1301–1307.

1995 Faltings, G., *The proof of Fermat's last theorem by R. Taylor and A. Wiles*, Notices Amer. Math. Soc., **42** (1995), no. 7, 743–746.

1995 Serre, J.-P., *Travaux de Wiles (et Taylor, ...), Partie I*, Séminaire Bourbaki, Vol. 1994/95. Astérisque, No. 237 (1996), Exp. No. 803, 5, 319–332.

1995 Oesterlé, J., *Travaux de Wiles (et Taylor, ...), Partie II*, Séminaire Bourbaki, Vol. 1994/95. Astérisque, No. 237 (1996), Exp. No. 804, 5, 333–355.

1995 Darmon, H., Diamond, F., and Taylor, R., *Fermat's last theorem.* In: *Current Developments in Mathematics*, 1995 (editors R. Bott, A. Jaffe, and S.T. Yau), pp. 1–154, Internat. Press, Cambridge, MA, 1995. Also in: *Elliptic curves, modular forms & Fermat's last theorem* (Hong Kong, 1993), pp. 2–140, Internat. Press, Cambridge, MA, 1997.

1995 Gouvêa, F.Q., *Deforming Galois representations: a survey.* In: *Seminar on Fermat's Last Theorem* (Toronto, ON, 1993–1994), pp. 179–207, CMS Conf. Proc., No. 17, Amer. Math. Soc., Providence, RI, 1995.

1995 Mazur, B., *Fermat's last theorem*, Videocassette, 60 min., American Math. Soc., Providence, RI.

1996 Darmon, H. and Levesque, C., *Sommes infinies, équations diophantiennes et le dernier théorème de Fermat*, Gaz. Soc. Math. Québec, **18** (1996), 3–18.

1996 van der Poorten, A., *Notes on Fermat's Last Theorem*, Wiley, New York, 1996.

1997 Cornell, G., Silverman, J.H., and Stevens, G. (editors), *Modular Forms and Fermat's Last Theorem*, Springer-Verlag, New York, 1997.

1997 Singh, S., *Fermat's Enigma*, Viking, London, 1997.

1997 Singh, S. and Ribet, K.A., *Fermat's last theorem*, Scientific American, **277** (1997), no. 5, 36–41.

1997 Kani, E., *Fermat's last theorem*, Queen's Math. Communicator (Queen's University at Kingston, Ontario, Canada), Summer 1997, pp. 1–8.

1997 Frey, G., *The way to the proof of Fermat's last theorem*, preprint, 20 pp., 1997.

C. Исследования

1958 Shimura, G., *Correspondances modulaires et les fonctions zeta de courbes algébriques*, J. Math. Soc. Japan, **10** (1958), 1–28.

1961 Shimura, G., *On the zeta-functions of the algebraic curves uniformized by certain automorphic functions*, J. Math. Soc. Japan, **13** (1961), 275–331.

1967 Shimura, G., *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math., (2), **85** (1967), 58–159.

1967 Weil, A., *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen.* Math. Ann., **168** (1967), 149–156.

1975 Hellegouarch, Y., *Points d'ordre 2p sur les courbes elliptiques*, Acta Arith., **26** (1975), 253–263.

1977 Mazur, B., *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math., **47** (1977), 33–186 (1978).

1982 Frey, G., *Rationale Punkte auf Fermatkurven und getwisteten Modulkurven*, J. Reine Angew. Math., **331** (1982), 185–191.

1986 Frey, G., *Elliptic curves and solutions of* $A - B = C$, in: *Sém. Th. Nombres*, Paris, 1985–1986 (editor C. Goldstein), Progress in Mathematics, Birkhäuser, Boston, 1986, pp. 39–51.

1986 Frey, G., *Links between elliptic curves and certain diophantine equations*, Ann. Univ. Sarav. Ser. Math., **1** (1986), No. 1, 1–40.

1987 Frey, G., *Links between elliptic curves and solutions of* $A-B = C$, J. Indian Math. Soc., **51** (1987), 117–145.

1987 Frey, G., *Links between solutions of* $A-B = C$ *and elliptic curves*, in: *Number Theory* (Ulm, 1987) (editors H.-P. Schlickewei and E. Wirsing), Springer Lect. Notes in Math., No. 1380, Springer-Verlag, New York, 1989.

1987 Serre, J.-P., *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$, Duke Math. J., **54** (1987), 179–230.

1987–1990 Ribet, K.A., *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$, preprint, 1987. Invent. Math., **100** (1990), 115–139.

1989 Mazur, B., *Deforming Galois representations*, in: *Galois Groups over* $\mathbb{Q}$ (editors Y. Ihara, K.A. Ribet, and J.-P. Serre), Math. Sci. Res. Inst. Publ., Vol. 16, Springer-Verlag, New York, 1989.

1990 Ribet, K.A., *From the Taniyama–Shimura conjecture to Fermat's last theorem*, Ann. Sci. Univ. Toulouse, (5), **11** (1990), 115–139.

1991 Ribet, K.A., *Lowering the levels of modular representations without multiplicity one*, Internat. Math. Res. Notices **1991**, no. 2, 15–19.

1991 Kolyvagin, V., *Euler systems*, in: *The Grothendieck Festschrift*, Vol. 2, pp. 435–483, Birkhäuser, Boston, 1991.

1992 Flach, M., *A finiteness theorem for the symmetric square of an elliptic curve*, Invent. Math., **109** (1992), 307–327.

1993 Lenstra, H.W. Jr., *Complete intersections and Gorenstein rings*, preprint (September 27, 1993).

1993 Ramakrishna, R., *On a variation of Mazur's deformation functor*, Compositio Math., **87** (1993), 269–286.

1995 Ribet, K.A., *Galois representations and modular forms*, Bull. Amer. Math. Soc., **32** (1995), 375–401.

1995 Wiles, A., *Modular elliptic curves and Fermat's last theorem*. Ann. of Math., (2), **141** (1995), 443–551.
1995 Taylor, R. and Wiles, A., *Ring theoretic properties of certain Hecke algebras*, Ann. of Math., (2), **141** (1995), 553–572.

XI.4. Электронная почта в действии

В заключение приведем «горячие» сообщения Карла Рубина, которые получили широкое распространение.

Электронное письмо № 1:

Дата: 23 *июня* 1993 *г.*, 05:52:30
Тема: *большие новости*

Эндрю Уайлс только что объявил у нас, в конце своей третьей лекции, что он доказал последнюю теорему Ферма. Он сделал это, доказав, что каждая полуустойчивая эллиптическая кривая над $\mathbb{Q}$ *(т. е. кондуктор свободен от квадратов) модулярна. Но описанные Фреем кривые, которые возникают в результате рассмотрения контрпримеров к теореме Ферма, полуустойчивы, и, согласно работе Рибета, они не могут быть модулярными, так что все доказано.*

Проделанная им работа поистине удивительна.
Карл

Электронное письмо № 2:

Дата: 25 *октября* 1994 *г.*, 10:24:46
Тема: *новое о последней теореме Ферма*
Сегодня утром были обнародованы две рукописи:

Модулярные эллиптические кривые и последняя теорема Ферма
Эндрю Уайлс
Теоретико-кольцевые свойства определенных алгебр Гекке
Ричард Тейлор и Эндрю Уайлс.

Первая (длинная) рукопись объясняет, среди прочего, о доказательстве последней теоремы Ферма и ссылается на вторую (короткую) с целью обоснования одного ключевого шага.

Почти все вы знаете, что в рассуждении, которое было описано Уайлсом на его лекциях в Кембридже, обнаружился серьезный

пробел, а именно в построении эйлеровой системы. После тщетных попыток исправить это построение Уайлс вернулся к другому подходу, который он пробовал раньше, но отказался от него в пользу идеи эйлеровой системы. Ему удалось завершить свое доказательство в предположении, что определенные алгебры Гекке представляют собой локальные полные пересечения. Подробное изложение этой идеи наряду с остальными, описанными на лекциях Уайлса в Кембридже, составляет предмет первой рукописи. Во второй статье Тейлор и Уайлс совместными усилиями установили нужное им свойство алгебр Гекке.

В своих основных чертах это рассуждение сходно с тем, которое Уайлс описал в Кембридже. Новый подход стал значительно проще и короче, нежели первоначальный, благодаря отказу от эйлеровой системы. (На самом деле после ознакомления с этими рукописями Фалтингс, по-видимому, добился дальнейшего существенного упрощения этой части рассуждения.)

Варианты этих рукописей находились в руках небольшого количества людей в некоторых случаях до нескольких недель. И хотя разумно еще некоторое время проявлять осторожность, причины для оптимизма, несомненно, есть.

Карл Рубин

Волнение, осторожность и изумление перед лицом величайшего подвига в Математике.

Приложение А

Ссылки на ошибочные доказательства

Все прекрасно знают, что 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.

С момента учреждения Премии Вольфскеля в 1908 г. только за первый год поступило 621 ошибочное решение, а сегодня в Гёттингене хранится почти трехметровый архив переписки и предложенных решений задачи Ферма.

Ниже мы приводим список, разумеется, неполный, некоторых печально известных ошибочных попыток решить эту задачу. В него угодили даже высокопрофессиональные математики.

Примечательно присутствие в нем Ф. Линдемана, который открыл трансцендентность числа π. Но в отношении последней теоремы Ферма все его попытки были неудачны.

Ф. Поле был, кажется, одним из самых упорных: в период с 1841 по 1862 г. он двенадцать раз представлял доказательство Парижской Академии Наук, но за это время не продвинулся в исследованиях ни на шаг.

За редким исключением, мы не упоминаем ошибочные решения, опубликованные авторами в виде отдельных книг или брошюр. Некоторые из них указаны Флеком и Менхеном (1908–1912), Миримановым (1909), а также Перроном (1916). Вместо этого мы сосредоточимся на целенаправленных, но неудавшихся попытках решения, опубликованных в математических журналах или в трудах конференций.

Вначале мы приводим подборку книг и статей, содержащих ссылки на неверные доказательства. Затем следует список ошибочных статей, включающий указание на место обсуждения той или иной ошибки[1].

XII.1. Статьи и книги, содержащие списки ошибочных доказательств

1908 Hoffmann, F., *Der Satz vom Fermat. Sein seit dem Jahr 1658 gesuchter Beweis*, J. Singer, Strasbourg, 1908.

1909 Lampe, E., Jahrbuch Fortschritte Math., **40** (1909), 258–261.

1909/10/11/12/16 Fleck, A. and Maennchen, A., *Vermeintliche Beweise des Fermatschen Satzes*, Arch. Math. Phys., (3),
14 (1909), 284–286, 370–372;
15 (1909), 108–111;
16 (1910), 105–109 and 372–375;
17 (1911), 108–109 and 370–374;
18 (1912), 105–109 and 204–206;
25 (1916), 267–268.

1910 Lind, B., *Über das letzte Fermatsche Theorem*, Abh. Geschichte Math. Wiss., **26** (1910), 23–65.

1920 Dickson, L.E., *History of the Theory of Numbers*, Vol. II, Carnegie Institution, Washington, DC, 1920; reprinted by Chelsea, New York, 1971.

1973 Besenfelder, H.J[2]., *Das Fermat-Problem*, Diplomarbeit, Universität Karlsruhe, 1973, 61 pp.

XII.2. Статьи, содержащие ошибочные доказательства

1810 Barlow, P., *Demonstration of a curious numerical proposition*, J. Nat. Phil. Chem. Arts, **27** (1810), 193–205.

1811 Barlow, P., *An Elementary Investigation of Theory of Numbers*, pp. 160–169, J. Johnson, St. Paul's Church-Yard, London, 1811.

1845 Drach, S.M., *Proof of Fermat's undemonstrated theorem that* $x^n + y^n = z^n$ *is only possible in whole numbers when* $n = 1$ *or* 2, Phil. Mag., **27** (1845), 286–289.

---

[1] Статья Яхьи использует неверный результат Капферера (1933).

[2] В августе 1979 г. автор сменил фамилию «Безенфельдер» на «Бентц»

Таблица 1. Ошибочные доказательства

Год	Автор	Кем указана ошибка	Год
1810,	Барлоу	Смит	1860
1811		Тэлбот	1864
1845	Драх	Диксон, с. 738	1820
1847	Ламе	Лиувилль	1847
		Куммер	1847
		Диксон, с. 739/40	1920
1855	Кальцолари	Линд, с. 48	1910
/57/64		Диксон, с. 743, 744, 746	1920
1864	Годен	Диксон, с. 746	1920
1890	Лефебюр	Пепен	1880
1889	Вариско	Ландсберг	1890
		Диксон, с. 754	1920
1893	Корнек	Пикар и Пуанкаре	1894
		Диксон, с. 756	1920
1901/	Линдеман	Флек и Менхен	1909
1907/		Фуртвенглер, Флек	1909
1909		Иванов	1910
		Диксон, с. 759, 762	1920
1908	Веребрюсов	Диксон, Вормс де Ромилли, Дюран-Лорига, Куржель	1908
		Диксон, с. 762	1920
1910	Линд	Флек	1910
		Диксон, с. 760	1920
1913	Фабри	Мириманов	1913
1955	Беккер	Егган	1981
1956	Фрага Торрехон	Родеха,	1956
1957	Вилласеньор	*Math. Rev.*, **19**, № 251f	1958
1957	Ногуэра	*Math. Rev.*, **19**, № 16e	1958
	Барренече	*Math. Rev.*, **20**, № 1658	1959
1958/9	Дрегер	Моришима	1960
1958/73	Яхья	Ганди и Стафф	1975
1973/77		Инкери	1984
1966	Сарантопулос	Гаррисон	1967
1978	Зиновьев	Крейзель	1978
1979	Кларк и Шеннон	Устное сообщение Дж. Г. Урселла	1983
1980	Маггу	Егган	1980
1980	Лаллу-Сингх	Ямагучи	1982

1847 Lamé, G., *Mémoire sur la résolution en nombres complexes de l'équation* $A^n + B^n + C^n = 0$, J. Math. Pures Appl., **12** (1847), 172- 184.

1847 Lamé, G., *Démonstration générale du théorème de Fermat sur l'impossibilité en nombres entiers de l'équation* $x^n + y^n = z^n$, C. R. Acad. Sci. Paris, **24** (1847), 310 -314.

1847 Lamé, G., *Note au sujet de la démonstration du théorème de Fermat*, C. R. Acad. Sci. Paris, **24** (1847), 352.

1847 Lamé, G., *Second mémoire sur le dernier théorème de Fermat*, C. R. Acad. Sci. Paris, **24** (1847), 569 572.

1847 Lamé, G., *Troisième mémoire sur le dernier théorème de Fermat*, C. R. Acad. Sci. Paris, **24** (1847), 888.

1847 Kummer, E. E., *Extrait d'une lettre de M. Kummer à M. Liouville*, J. Math. Pures Appl., **12** (1847), 136; reprinted in *Collected Papers*, Vol. I, p. 298. Springer-Verlag, Berlin, 1975.

1847 Liouville, J., *Remarques à l'occasion d'une communication de M. Lamé sur un théorème de Fermat*, C. R. Acad. Sci. Paris, **24** (1847), 315–316.

1855 Calzolari, L., *Tentativo per dimostrare il teorema di Fermat sull'-equazione indeterminata* $x^n + y^n = z^n$, Ferrara, 1855.

1857 Calzolari, L., *Dimostrazione dell'ultimo teorema di Fermat*, Annali Sci. Mat. B. Tortolini, **8** (1857), 339- 349.

1860 Smith, H.J.S., *Report on the Theory of Numbers, Part II, Art. 61, "Application to the Last Theorem of Fermat", Collected Math. Papers*, Vol. I, 1894, pp. 131 -137 Clarendon Press, Oxford, 1894; reprinted by Chelsea, New York, 1965.

1864 Calzolari, L., *Impossibilità in numeri interi dell'equazione* $z^n = x^n + y^n$ *quando* $n > 2$, Ann. Mat., **6** (1864), 280–286.

1864 Gaudin, A., *Impossibilité de l'équation* $(x + h)^n - x^n = z^n$, C. R. Acad. Sci. Paris, **59** (1864), 1036 -1038.

1864 Talbot, W.H.F., *On the theory of numbers*, Trans. Roy. Soc. Edinburgh, **23** (1864), 45–52.

1880 Lefébure, A., *Sur la résolution de l'équation* $x^n + y^n = z^n$ *en nombres entiers*, C. R. Acad. Sci. Paris, **90** (1880), 1406–1407.

1880 Pepin, T., *Sur diverses tentatives de démonstration du théorème de Fermat*, C. R. Acad. Sci. Paris, **91** (1880), 366–367.

1889 Varisco, D., *Ricerche aritmetiche contenente la dimostrazione generale del teorema di Fermat*, Giorn. Mat., **27** (1889), 371–380.

1890 Landsberg, O., *Lettera al redattore*, Giorn. Mat., **28** (1890), 52.

1893 Korneck, G., *Beweis des Fermatschen Satzes von der Unmöglichkeit der Gleichung $x^n + y^n = z^n$ für rationale Zahlen und $n > 2$.* Arch. Math. Phys., (2), **13** (1893), 1–9.

1893 Korneck, G., *Nachtrag zum Beweis des Fermatschen Satzes*, Arch. Math. Phys., (2), **13** (1893), 263–267.

1894 Picard, E. and Poincaré, H., *Rapport verbal sur les articles de M. G. Korneck*, C. R. Acad. Sci. Paris, **118** (1894), 841.

1901 Lindemann, F., *Über den Fermatschen Satz betreffend die Unmöglichkeit der Gleichung $x^n = y^n + z^n$*, Sitzungsber. Akad. Wiss. München, Math., **31** (1901), 185–202; corrigenda, p. 495.

1907 Lindemann, F., *Über das sogenannte letzte Fermatsche Theorem*, Sitzungsber. Akad. Wiss. München, Math., **37** (1907), 287–352.

1908 Dickson, L. E., *Dernier théorème de Fermat*, L'Interm. Math., **15** (1908), 174.

1908 Curjel, H. W., *Dernier théorème de Fermat* (*Question 612 de Worms de Romilly*), L'Interm. Math., **15** (1908), 247.

1908 Duran-Loriga, J. J., *Sur le dernier théorème de Fermat* (*Réponse de M. Werebrusow*), L'Interm. Math., **15** (1908), 177.

1908 Werebrusow, A. S., *Impossibilité de l'équation $x^n = y^n + z^n$* (*Question 612 de Worms de Romilly*), L'Interm. Math., **15** (1908), 79–81.

1908 Worms de Romilly, A. S., *Le dernier théorème de Fermat*, L'Interm. Math., **15** (1908), 175–177.

1909 Lindemann, F., *Über den sogenannten letzten Fermatschen Satz*, Veit, Leipzig, 1909, 83 pp.

1909 Fleck, A. and Maennchen, A.: See in List I.

1909 Furtwängler, P., *Review of Lindemann's "Über den sogenannten letzten Fermatschen Satz,"* Jahrbuch Fortschritte Math., **40** (1909), 258.

1910 Ivanov, I.I., *Über den von Prof. F. Lindemann vorgeschlagenen Beweis des Fermatschen Satzes* (*Brief an die Redaktion*), Jahrbuch Fortschritte Math., **41** (1910), 238.

1910 Lind, B.: See in List I.

1913 Fabry, E., *Un essai de démonstration du théorème de Fermat*, C. R. Acad. Sci. Paris, **156** (1913), 1814–1816.

1913 Mirimanoff, D., *Remarque sur une communication de M. Eugène Fabry*, C. R. Acad. Sci. Paris, **157** (1913), 491–492.

1920 Dickson, L.E., See in List I.

1933 Kapferer, H., *Über die diophantischen Gleichungen $z^3 - y^2 = 3^3 \cdot 2^\lambda x^{\lambda+2}$ und deren Abhängigkeit von der Fermatschen Vermutung.*

Heidelberger Akad. Math. Naturwiss. Klasse, Abh. **2** (1933). 32-37.

1956 Fraga Torrejón, E. de, *Note on Fermat's last theorem*, Las Ciências, **21** (1956), 5–13.

1956 Rodeja, F., E.G., *On Fermat's last theorem*, Las Ciências, **21** (1956), 382–383.

1957 Noguera Barreneche, R., *Solución general de la ecuación algebraico-exponencial* $X^\nu + Y^\nu = Z^\nu$, Studia Rev. Univ. Atlantico, **2** (1957), 119–126.

1957 Noguera Barreneche, R., *Historically the first proof incontrovertible, complete and universal of the grand theorem of Fermat, with the Davidic algebra of the "principle of the amateurs" in mathematical investigation* (*in Spanish*), Studia Rev. Univ. Atlantico, **2** (1957), 199–209.

1957 Villaseñor Z., F., *El celebre teorema de Fermat y su demonstración*, Mexico, 1957, 127 pp.

1958 Yahya, Q.A.M.M., *Complete proof of Fermat's last theorem*, Author's publication, Pakistan Air Force, Kohat, Pakistan, 1958, 14 pp.

1958/9 Draeger, M., *Das Fermat-Problem*, Wiss. Z. Techn. Hochsch. Dresden, **8** (1958/9), 941–946.

1960 Morishima, T., *Review of the paper by Draeger "Das Fermat-Problem,"* Math. Rev., **23** (1960), A2375.

1969 Sarantopoulos, S., *Du premier cas du théorème de Fermat*. Bull. Soc. Math. Grèce (N.S.), **10** (1969), 76–115.

1971 Garrison, B., Review of the above paper by Sarantopoulos (with a remark by E.G. Straus), Math. Rev., **42** (1971), No. 4483.

1973 Yahya, Q.A.M.M., *On general proof of Fermat's last theorem*, Portugal. Math., **32** (1973), 157–170.

1975 Gandhi, J.M. and Stuff, M., *Comments on certain results about Fermat's last theorem*, Notices Amer. Math. Soc., **22** (1975), A-502.

1978 Kreisel, G., Letter to Ribenboim (6 June 1978). Atlantis Hotel, Zürich.

1979 Clarke, J.H. and Shannon, A.G., *Some observations on Fermat's last theorem*, New Zealand Math. Mag., **16** (1979), 80–83.

1979 Zinoviev, A. A., *Complete* (*rigorous*) *induction and Fermat's great theorem* (*with a report by G. Kreisel*), Logique et Anal., **22** (1979), no. 87, 243–263.

1980 Maggu, P.L., *On the proof of Fermat's last theorem*, Pure Appl. Math. Sci., **12** (1980), 7–9.
1981 Eggan, L.C., Review of the above paper by Maggu, Math. Rev., **81g** (1981), No. 10032.
1984 Inkeri, K., *On certain equivalent statements for Fermat's last theorem – with requisite corrections*, Ann. Univ. Turku., Ser. AI, **186** (1984) 12–22; reprinted in *Collected Papers of Kustaa Inkeri* (editor P. Ribenboim), Queen's Papers in Pure and Applied Mathematics, Vol. 91, Kingston, Ontario, 1992.

XII.3. Неудовлетворительные попытки

Этот список мы дополним некоторыми публикациями, которые используют методы, явно недостаточные для решения данной задачи.

1951 Natucci, A., *Osservazioni sul problema di Fermat*, Bull. Un. Mat. Ital., (3), **6** (1951), 245–248.
1953 Natucci, A., *Ricerche sistematiche sull'ultimo teorema di Fermat*, Giorn. Mat., (5), **1(81)** (1953), 171–179.
1975 Peiulescu, V., *Teorema lui Fermat*, Ed. Litera, Bucureşti, 1975, 86 pp.
1976 Yahya, Q.A.M.M., *On general proof of Fermat's last theorem—epilogue*, Portugal. Math., **35** (1976), 9–15.
1977 Yahya, Q.A.M.M., *Fermat's last theorem—a topological verification*, Portugal. Math., **36** (1977), 25–31.
1979 De Fermate, J.F. (pseudonym of Guillotte, G.), *A Famous Problem in Number Theory of the First Kind Dating from 1637: $x^p + y^p = z^p, p > 2$*, Cowansville Printing, Cowansville, Quebec; Vol. I, 1979, 22 pp.; Vol. II, 1980, 8 pp.
1980 Singh, L., *The general proof of Fermat's last theorem*, J. Indian Acad. Math., **2** (1980), 43–50.

Также изрядное количество ошибок содержали связанные с последней теоремой Ферма статьи, направленные на получение частичных результатов, необходимых условий и т. д. Мы указываем на эти ошибки в соответствующем месте текста книги.

Приложение B

Общая библиография

XII.1. Труды Ферма

После смерти Ферма его избранные труды были опубликованы под руководством сына, Самюэля де Ферма.

1679 *Varia Opera Mathematica*, D. Petri de Fermat, Senatoris Tolosani. Tolosae, Apud Joannem Pec, Comitiorum Fuzensium Typographum justa Collegium P P. Societatis JESU.

Следующие книги представляют собой переиздание в четырех томах с приложением:

1891, 1894, 1896, 1912, 1922 *Oeuvres de Pierre de Fermat*, Publiées par les soins de MM. Paul Tannery et Charles Henry. Gauthier-Villars, Paris.

Среди писем Ферма следующие имеют отношение к предмету этой книги:

1636, April 26 Lettre à Mersenne[1], *Correspondance du Père Marin Mersenne*, Vol. 6, p. 50. Commencée par Mme. Paul Tannery, publiée et annotée par Cornelis de Waard. Ed. du C.N.R.S, Paris, 1962.

1636, Sept. Lettre à Mersenne [pour Sainte-Croix]. *Oeuvres de Fermat*, Vol. III, pp. 286–292.

1636, Nov. 4 Lettre à Roberval. *Oeuvres de Fermat*, Vol. II, p. 83.

1638, beg. June Lettre à Mersenne. *Correspondance du Père Marin Mersenne*, Vol. 7, pp. 272–283. Commencée par Mme. Paul Tannery, publiée et annotée par Cornelis de Waard. Ed. du C.N.R.S, Paris, 1962.

1640, May (?) Lettre à Mersenne. *Oeuvres de Fermat*, Vol. II, pp. 194–195.

---

[1] Согласно Итару (1948), дата написания этого письма — июнь 1638 г. Однако датой 26 апреля 1636 г. оно сопровождается в издании переписки Мерсенна.

1654, Aug. 29 Lettre à Pascal. *Oeuvres de Fermat*, Vol. II, pp. 307 310.

1657, Aug. 15 Lettre à Kenelm Digby. *Oeuvres de Fermat*, Vol. II, pp. 342–346.

XII.2. Книги, посвященные Ферма

1910 Lind, B., *Über das letzte Fermatsche Theorem*, Abh. Geschichte Math. Wiss., no. 26, 1910, pp. 23–65.

1919 Bachmann, P., *Das Fermatproblem in seiner bisherigen Entwicklung*, W. de Gruyter, Berlin, 1919; reprinted by Springer-Verlag, Berlin, 1976.

1927 Khinchin, A.I., *Velikai Teorema Ferma* (The Great Theorem of Fermat), Moskau-Leningrad, Staatsverlag, Vol. **76**, 1927.

1961 Bell, E.T., *The Last Problem*, Simon & Schuster, New York, 1961.

1966 Noguès, P., *Théorème de Fermat, son Histoire*, A. Blanchard, Paris, 1966.

1972 Mahoney, M.S., *The Mathematical Career of Pierre de Fermat, 1601–1665*, Princeton University Press, Princeton, NJ, 1973.

1977 Edwards, H.M., *Fermat's Last Theorem, A Genetic Introduction to Algebraic Number Theory*, Springer-Verlag, New York, 1977.

1979 Ribenboim, P., *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.

XII.3. Книги со ссылками на последнюю теорему Ферма

1859 Smith, H.J.S., *Report on the Theory of Numbers*, Part II, Art. 61, "Application to the last theorem of Fermat."Report of the British Association for 1859, pp. 228–267. Reprinted in *Collected Mathematical Works*, Vol. I, pp. 131–137, Clarendon Press, Oxford, 1894; reprinted by Chelsea, New York, 1965.

1897 Hilbert, D., *Die Theorie der algebraischen Zahlkörper*, Jahresber. Deutsch. Math.-Verein., **4** (1897), 175–546; reprinted in *Gesammelte Abhandlungen*, Vol. I, Chelsea, New York, 1965.

1910 Bachmann, P., *Niedere Zahlentheorie*, Vol. II, Teubner, Leipzig, 1910; reprinted by Chelsea, New York, 1968.

1920 Dickson, L.E., *History of the Theory of Numbers*, Vol. II. Carnegie Institution, Washington, DC, 1920; reprinted by Chelsea, 1971.

1927 Landau, E., *Vorlesungen über Zahlentheorie*, Vol. III, Hirzel, Leipzig, 1927; reprinted by Chelsea, New York, 1947.
1928 Vandiver, H.S. and Wahlin, G.E., *Algebraic Numbers*, Vol. II. Bull. Nat. Research Council No. 62, 1928; reprinted by Chelsea, New York, 1967.
1937 Bell, E.T., *Men of Mathematics*, Simon & Schuster, New York, 1937.
1951 Nagell, T., *Introduction to Number Theory*, Wiley, New York, 1951; reprinted by Chelsea, New York, 1962.
1956 Ostmann, H.H., *Additive Zahlentheorie*, Vol. II, Springer-Verlag, Berlin, 1956.
1962 Shanks, D., *Solved and Unsolved Problems in Number Theory*, Vol. I, Spartan, Washington, DC, 1962; reprinted by Chelsea, New York, 1978.
1966 Borevich, Z.I. and Shafarevich, I.R., *Number Theory*, Academic Press, New York, 1966.
1969 Mordell, L.J., *Diophantine Equations*, Academic Press, New York, 1969.
1982 Koblitz, N. (editor), *Number Theory Related to Fermat's Last Theorem*, Birkhäuser, Boston, 1982.
1984 Weil, A., *Number Theory, An Approach Through History from Hammurapi to Legendre*, Birkhäuser, Boston, 1984.

XII.4. Обзорные, исторические и библиографические статьи

1807 Gauss, C.F., Letter to Sophie Germain (Braunschweig, 30 April, 1807). *Werke*, Vol. X, Part I, pp. 70–74. Königl. Ges. Wiss., Göttingen, Teubner, Leipzig, 1917.
1816 Gauss, C.F., Letter to Wilhelm Olbers (March 21, 1816). *Werke*, Vol. X, Part I, pp. 75–76. Königl. Ges. Wiss., Göttingen, Teubner, Leipzig, 1917.
1841 Terquem, O., *Théorème de Fermat sur un trinôme, démonstration de M. Lamé, projet de souscription*, Nouv. Ann. Math., **6** (1847), 132–134.
1879 Henry, C., *Recherches sur les manuscripts de Pierre de Fermat*, Bull. Bibliografia Storia Scienze Matem. Fis., **12** (1879), 477–568 and 619–740.
1879 Mansion, P., *Remarques sur les théorèmes arithmétiques de Fermat*, Nouv. Corr. Math., **5** (1879), 88–91 and 122–125.

1880 Germain, S., *Cinq lettres de S. Germain à C.F. Gauss, publiées par B. Boncompagni*, Arch. Math. Phys., **63** (1880), 27–31; **66** (1881), 3–10.

1883 Tannery, P., *Sur la date des principales découvertes de Fermat*, Bull. Sci. Math. Sér. 2, **7** (1883), 116–128; reprinted by Sphinx-Oedipe, **3** (1908), 169ff.

1887 Henry, C., *Lettre à M. le Prince de Boncompagni sur divers points d'histoire des mathématiques*, Bull. Bibliografia Storia Scienze Matem. Fis., **20** (1887), 389–403.

1898 Gram, J.P., *Om Fermat og haus sidote Saetning*, Forhandlingar Skandinaviska Natursforskare, Götheborg, 1898, p. 182.

1901 Gambioli D., *Memoria bibliografica sull'ultimo teorema di Fermat*, Period. Mat., **16** (1901), 145–192.

1902 Gambioli, D., *Appendice alla mia memoria bibliografica sull'-ultimo teorema di Pietro Fermat*, Period. Mat., (2), IV, **17** (1902), 48–50.

1908 Hoffmann, F., *Der Satz vom Fermat. Sein seit dem Jahr 1658 gesuchter Beweis*, J. Singer, Strasbourg, 1908.

1908 Schönbaum, E., *Arbeiten von Kummer über den Fermatschen Satz*, Časopis Pěst. Mat., **37** (1908), 484–506.

1910 Gérardin, A., *État actuel de la démonstration du grand théorème de Fermat*, Assoc. Française Avanc. Sciences, Toulouse, I, **39** (1910), 55–56.

1912 *Wolfskehl Prize. Bekanntmachung*, Math. Ann., **72** (1912), 1–2.

1917 Dickson, L.E., *Fermat's last theorem and the origin and nature of the theory of algebraic numbers*, Ann. of Math., **18** (1917), 161–187.

1921 Mordell, L.J., *Three Lectures on Fermat's Last Theorem*, Cambridge University Press, Cambridge, 1921; reprinted by Chelsea, New York, 1962.

1925 Ore, O., *Fermat's theorem* (in Norwegian). Norske Mat. Tidsskrift, **7** (1925), 1–10.

1941 Brčić-Kostić, M., *Das Fermatproblem, $x^n + y^n = z^n$*, Zagreb, 1941.

1943 Hofmann, J.E., *Neues über Fermats zahlentheoretische Herausforderungen von 1657 (mit zwei bisherunbekannten Originalstuecken Fermats)*, Abh. Preussischen Akad. Wiss., Math.-Naturw. Kl., 1943, No. 9, 52 pp.

1946 Vandiver, H.S., *Fermat's last theorem*, Amer. Math. Monthly, **53** (1946), 555–578.

1948 Got, T., *Une enigmè mathématique: Le dernier théorème de Fermat* (a chapter in *Les Grands Courants de la Pensée Mathématique*, edited by F. Le Lionnais), Cahiers de Sud, Marseille, 1948. Reprinted by A. Blanchard, Paris, 1962. Translated into English (2 volumes). Dover, New York, 1971.

1948 Itard, J., *Sur la date à attribuer à une lettre de Pierre Fermat*, Rev. Historie Sci. Appl., **2** (1948), 95–98.

1957 *Un Mathématician de Génie: Pierre de Fermat, 1601–1665*, Lycée Pierre de Fermat, Toulouse, 1957.

1959 Schinzel, A., *Sur quelques propositions fausses de P. Fermat*, C. R. Acad. Sci. Paris, **249** (1959), 1604–1605.

1970 Smadja, R., *Le théorème de Fermat* (thèse de 3e cycle), Université de Paris VI, 1970.

1972 Mahoney, M.S., *Fermat's Mathematics: Proofs and Conjectures*, Science, **178** (1972), 30–36.

1973 Albis Gonzalez, V., *El señor Fermat y sus problemas*, Bol. Mat., Bogotà, **7** (1973), 219–232.

1973 Besenfelder, H.J. (now Bentz, H.J.), *Das Fermat-Problem*, Diplomarbeit, Univ. Karlsruhe, 1973, 61 pp.

1973 Fournier, J.C., *Sur le Dernier Théorème de Fermat* (thèse de 3e cycle). Université de Paris VI, 1973.

1974 Ferguson, R.P., *On Fermat's last theorem, I–II*, J. Undergrad. Math., **6** (1974), 1–14 and 85–98.

1974 Weil, A., *La cyclotomie jadis et naguère*, Enseign. Math., **20** (1974), 247–263. Reprinted in *Essais Historiques sur la Théorie des Nombres*. Monographie no. 22 de L'Enseignement Mathématique, 1975. Génève, 55 pp. Reprinted in *Collected Papers*, Vol. III, pp. 311–328. Springer-Verlag, New York, 1980.

1975 Edwards, H.M., *The background of Kummer's proof of Fermat's last theorem for regular primes*, Arch. History Exact Sci., **14** (1975), 219–236.

1975 Ferguson, R.P., *On Fermat's last theorem*, III, J. Undergrad. Math., **7** (1975), 35–45.

1976 Christy, D., *Le dernier thérème de Fermat et le théorème de Roth*, Sém. Alg. Th. Nombres, Caen, 1976/7, 12 pp.

1977 Edwards, H.M., *Postscript to: "The background of Kummer's proof of Fermat's last theorem for regular primes"*, Arch. History Exact Sci., **17** (1977), 381–394.

1980 de Rham, G., *Brève notice sur Dmitri Mirimanoff*, Cahiers Sém. Histoire Math. Paris, **1** (1980), 32–33.

1980 Cassinet, R., *La descente infinie de Campanus à Hilbert, 1260 1897*, Sém. Histoire Math. Toulouse, 1980, cahier no. 2, pp. B1 to B25.

1980 Ribenboim, P., *Les idées de Kummer sur le théorème de Fermat*, Séminaire de Philosophie et Mathématiques, École Normale Sup. Paris, 1979, 11 pp.

1980 Terjanian, G., *Fermat et son arithmétique*, Sém. Histoire Math. Toulouse, 1980, cahier no. 2, pp. A1 to A35.

См. также статьи в следующих словарях и энциклопедиях:

1961 Fermat; Fermat's last theorem. *Encyclopedia Americana*, Vol. 11, pp. 125–125, 1961 edition.

1977 Boyer, C.B., Fermat, Pierre de. *Encyclopaedia Britannica*, Macropaedia, Vol. 7, pp. 234–236, 1977 edition.

1977 Iyanaga, S. and Kawada, Y. (editors), Fermat's Problem. *Encyclopedic Dictionary of Mathematics* (by The Mathematical Society of Japan), pp. 512–513. Translation reviewed by K.O. May, MIT Press, Cambridge, MA, 1977.

1979 Bouvier, A., George, M., and Le Lionnais, F., Fermat, Pierre Simon de (1606–1665). *Dictionnaire des Mathématiques*, p 296. Presses Universitaires de France, Paris, 1979.

XII.5. Критические статьи и обзоры

1839 Cauchy, A. and Liouville, J., *Rapport sur un mémoire de M. Lamé relatif au dernier théorème de Fermat*, C. R. Acad. Sci. Paris, **9** (1839), 359–363; also appeared in J. Math. Pures Appl., **5** (1840), 211–215 and *Oeuvres Complètes*, Sér. 1, Vol. 4, pp. 494–504, Gauthier-Villars, Paris, 1884.

1856 Cauchy, A., *Rapport sur le concours relatif au dernier théorème de Fermat* (*Commissaires MM. Bertrand, Liouville, Lamé, Chasles; Cauchy rapporteur*), C. R. Acad. Sci. Paris, **44** (1856), p. 208.

1881 Catalan, E., *Jugement du concours annuel*, Bull. Acad. Roy. Sci. Belgique, (3), **6** (1881), 814–832.

1973 Weil, A., *Review of "The Mathematical Career of Pierre de Fermat" by M. S. Mahoney*, Bull. Amer. Math. Soc., **79** (1973). 1138–1149. Reprinted in *Oeuvres Scientifiques*, Vol. 3, pp. 266–277, Springer-Verlag, Berlin, 1979.

1977 Mazur, B., *Review of Kummer's "Collected Papers,"* Vols. I and II, Bull. Amer. Math. Soc., **83** (1977), 976–988.

Список литературы о теореме Ферма на русском языке

В списках литературы работы, имеющиеся на русском языке, **выделены** полужирным шрифтом. Здесь мы приводим их список (**они также** выделены) и некоторую дополнительную литературу, охватывающую период с 1905 г. до настоящего времени. Разумеется, **настоящий** список литературы, которая может быть использована при **изучении** теоремы Ферма, не претендует на полноту, но он будет, **по** нашему мнению, полезен русскоязычным читателям.

1905 Веребрюсов А. С. *Об уравнении* $x^5 + y^5 = Az^5$. — Московский Математический Сборник, 1905, т. 25, с. 466–473.

1922 Делоне Б. Н. *Решение неопределенного уравнения* $x^3q + y^3 = 1$. — Известия Российской АН. Сер. 6, 1922, т. 16, с. 273–280.

1934 Хинчин А. Я. *Великая теорема Ферма.* — Изд. третье — М.–Л.: ГТТИ, 1934.

1940 Гекке Э. *Лекции по теории алгебраических чисел*: Пер. с нем. — М.–Л.: ГТТИ, 1940.

1940 Делоне Б. Н., Фаддеев Д. К. *Теория иррациональностей третьей степени.* — Труды Математического института АН СССР, 1940, т. 11, с. 1–340.

1948 Риман Б. *Сочинения*: Пер. с нем. — М.–Л.: ГТТИ, 1948.

1959 Гаусс К. Ф. *Труды по теории чисел*: Пер. с нем. — М.: Издательство АН СССР, 1959.

1965 Дэвенпорт Г. *Высшая арифметика. Введение в теорию чисел*: Пер. с англ. — М.: Наука, 1965.

1969 Касселс Дж., Фрёлих А. *Алгебраическая теория чисел*: Пер. с англ. — М.: Мир, 1969.

1970 Кобелев В. В. *Доказательство великой теоремы Ферма для всех простых показателей, меньших* 5500. — Доклады АН СССР, 1970, т. 190, № 4, с. 767–768.

1971 Дэвенпорт Г. *Мультипликативная теория чисел*: Пер. с англ. — М.: Наука, 1971.

1972 Вейль А. *Основы теории чисел*: Пер. с англ. — М.: Мир, 1972.
1972 Постников М. М. *Теорема Ферма.* — М.: Наука, 1972.
1972 Серр Ж.-П. *Курс арифметики*: Пер. с англ. — М.: Мир, 1972.
1974 Диофант. *Арифметика и книга о многоугольных числах*: Пер. с древнегреческого — М.: Наука, 1974.
1979 Ленг С. *Введение в теорию модулярных форм*: Пер. с англ. — М.: Мир, 1979.
1980 Эдвардс Г. М. *Последняя теорема Ферма. Генетическое введение в алгебраическую теорию чисел*: Пер. с англ. — М.: Мир, 1980.
1981 Виноградов И. М. *Основы теории чисел.* — М.: Наука, 1981.
1982 Касселс Дж. *Рациональные квадратичные формы*: Пер. с англ. — М.: Мир, 1982.
1982 Коблиц Н. *p-адические числа, p-адический анализ и дзета-функции*: Пер. с англ. — М.: Мир, 1982.
1985 Боревич З. И., Шафаревич И. Р. *Теория чисел.* — Изд. третье, дополненное — М.: Наука, — 1985. — 504 с.
1987 Айерленд К., Роузен М. *Классическое введение в современную теорию чисел*: Пер. с англ. — М.: Мир, 1987. — 416 с.
1988 Коблиц Н. *Введение в эллиптические кривые и модулярные формы*: Пер. с англ. — М.: Мир, 1988.
1989 Бюлер В. *Гаусс*: Пер. с англ. — М.: Наука, 1989.
1990 *Труды семинара Н. Бурбаки за* 1988 *г.*: Пер. с франц. и англ. — М.: Мир, 1990.
1992 Воробьев Н. Н. *Числа Фибоначчи.* — Изд. шестое, дополненное — М.: Наука, 1992.
1997 Прасолов В. В., Соловьев Ю. П. *Эллиптические функции и алгебраические уравнения.* — М.: Факториал, 1997.
1998 Гильберт Д. *Избранные труды*: Пер. с нем., Т. 1. — М.: Факториал, 1998.
1998 Соловьев Ю. П. *Гипотеза Таниямы и последняя теорема Ферма.* — Соросовский образовательный журнал, 1998, № 2, с. 135–138.
1999 Виноградов И. М. *Элементы высшей математики.* — М.: Высшая школа, 1999.
2000 Гашков С. Б., Чубариков В. Н. *Арифметика. Алгоритмы. Сложность вычислений.* — Изд. второе, переработанное — М.: Высшая школа, 2000. — 320 с.
2000 Сингх С. *Великая теорема Ферма*: Пер. с англ. — М.: Издательство МЦНМО, 2000. — 288 с.

Именной указатель

Абель (Abel N.) 116, 121, 182, 212, 220
Аго (Agoh T.) 12
Адамар (Hadamard J.) 156
Адлеман (Adleman L.M.) 137, 140, 380, 381
Айгнер (Aigner M.) 111
Алу (Helou C.) 152, 156, 243, 251
Альберт (Albert A.A.) 110
Альбис Гонсалес (Albis Gonzalez V.) 411
Анри (Henry C.) 407, 409, 410
Арвин (Arwin A.) 199, 200
Артин (Artin E.) 106, 111
Архипов Г.И. 171

Банг (Bang A.S.) 28, 32, 106, 110, 125, 139, 142, 143, 145, 148, 151, 155
Баризьен (Barisien E.N.) 233, 237, 239, 250
Барлоу (Barlow P.) 28, 31, 116, 120, 121, 123, 210, 218, 401, 402
Бахман (Bachmann P.) 32, 116, 122, 139, 155, 233, 237, 320, 408
Баше (Bachet C. G.) 13, 22
Бегунц А.В. 8
Безенфельдер (Besenfelder H. J.) 401, 411
Безу (Bézout É.) 115
Бейтман (Bateman P.T.) 158, 159
Беккер (Becker H.W.) 225, 230, 402
Белл (Bell E.T.) 408, 409
Бендц (Bendz T.R.) 28, 32, 264, 269
Бентц (Bentz H.J.) 401, 411
Бергман (Bergmann G.) 37, 54
Бертран (Bertrand J.) 28, 32
Бехара (Behara M.) 181
Бигер (Beeger N.G.W.H.) 379
Бине (Binet J.) 150, 154, 174, 181
Бини (Bini U.) 213, 220, 233, 237, 284, 285, 292
Биркгоф (Birkhoff G.D.) 103, 106, 110, 189, 191, 192
Бойд (Boyd D.W.) 152, 156
Бойер (Boyer C.B.) 412
Бомбьери (Bombieri E.) 86
Бонкомпаньи (Boncompagni B.) 410
Боревич З.И. 378, 379, 409, 414
Борлетти (Borletti F.) 213, 220
Ботт (Bott R.) 396
Боттари А. (Bottari A.) 19, 23, 28, 32, 273, 292
Боттери В. (Botteri V.) 12
Боше (Bôcher M.) 112, 115, 292
Браун (Brown T.C.) 382
Брауэр (Brauer A.) 202, 211
Брент (Brent R.P.) 158, 159
Бройш (Breusch R.) 79, 80, 82, 83, 86
Брокар (Brocard H.) 231, 237, 240, 251
Броункер (Brouncker W.) 37
Брчич-Костич (Brčić-Kostić M.) 79, 86, 195, 200, 239, 251, 410
Бувье (Bouvier A.) 412
Булер (Buhler J.P.) 378, 379
Бурбаки (Bourbaki N.) 414
Бусси (Bussi C.) 272, 293
Бутен (Boutin A.) 233, 237
Бюлер (Bühler W.) 414

Вагштаф (Wagstaff S.) 192, 201
Вагштаф мл. (Wagstaff Jr. S.S.) 380
Валин (Wahlin G.E.) 409
Валле Пуссен (de la Vallée Poussin C.J.) 156
Валлис (Wallis J.) 25, 31, 37
Вандивер (Vandiver H.S.) 103, 106, 110, 134, 135, 139, 183, 184, 199, 200, 283, 314, 321, 322, 378, 379, 409, 410
Варинг (Waring E.) 236, 244, 246, 249
Вариско (Varisco D.) 402, 403
Вашет (Vachette A.) 233, 237
Вебб (Webb W.A.) 54, 56, 64
Вейль (Weil A.) 92, 314, 320, 322, 379, 390, 396, 409, 411, 412, 414
Вельш (Welsch) 53, 240, 251
Вендт (Wendt E.) 135, 138, 140, 142, 143, 155
Веребрюсов А.С. 72, 232, 237, 402, 404, 413
Виванти (Vivanti G.) 96, 111
Вилласеньор (Villaseñor Z.) 402, 405
Виноградов И.М. 5, 414
Вирзинг (Wirsing E.) 397
Виферих (Wieferich A.) 283, 379, 380
Вормс де Ромилли (Worms de Romilly A.S.) 402, 404
Воробьев Н.Н. 151, 155, 414
Врэнчеану (Vrănceanu G.) 27, 28, 33, 44, 46, 54, 267, 270

Гайяши (Hayashi T.) 72, 73, 79, 86
Гамбиоли (Gambioli D.) 28, 32, 47, 53, 72, 213, 220, 410
Ганди (Gandhi J.M.) 134–136, 139, 140, 154–156, 190, 192, 195, 201, 224, 230, 258, 270, 402, 405
Ганнинг (Gunning R.C.) 394
Гаррисон (Garrison B.) 402, 405
Гаусс (Gauss C.F.) 17, 23, 40, 55, 58, 64, 72, 163, 221, 231, 237, 314, 384, 409, 410, 413
Гашков С.Б. 414
Гекке (Hecke E.) 388, 413
Гензель (Hensel K.) 160, 169, 173
Гильберт (Hilbert D.) 33, 36, 408, 414
Гильот (Guillotte G.) 406
Глейшер (Glaisher J.W.L.) 239, 248–250
Говеа (Gouvêa F.Q.) 12, 393-396
Годен (Gaudin A.) 402, 403
Гольдзихер (Goldziher H.) 273, 292
Гольдштейн (Goldstein C.) 270, 397
Гольмбо (Holmboe B.M.) 116, 121
Гонсалес Кихано (Gonzalez Quijano P.M.) 233, 237
Гот (Got T.) 411
Гофман (Hofmann J.E.) 5, 6, 410
Грам (Gram J.P.) 410
Грей (Grey L.D.) 222, 230
Григорьев (Grigorieff E.) 239, 251
Гризелль (Griselle T.) 221, 230
Гроссвальд (Grosswald E.) 54, 139
Грэнвилль (Granville A.) 134, 140, 154, 156, 283, 379-382
Гундерсон (Gunderson N.G.) 380
Гурвиц (Hurwitz A.) 51, 53, 252, 256, 269, 313, 320, 322, 333, 334
Гут (Gut M.) 229
Гюнтер (Günther S.) 47, 52

Даймонд (Diamond F.) 396
Дармон (Darmon H.) 396
Де Ферма (De Fermate J.F.) (псевдоним Гильота) 406
Делоне Б.Н. 413
Дене (Dénes P.) 134, 139
Джеймс (James G.) 116, 118, 122, 184, 185, 200

Джексон (Jackson J.S.) 244, 249
Дженокки (Genocchi A.) 78, 79
Джероно (Gérono G.C.) 240, 250
Джонсон (Johnson W.) 196, 201
Джордж (George M.) 412
Дигби (Digby K.) 25, 31, 37, 51, 408
Диксон (Dickson L.E.) 15, 23, 82, 106, 110, 134, 139, 154, 155, 174, 181, 207, 211, 244, 312–316, 319, 320, 341, 401, 402, 404, 408, 410
Дильхер (Dilcher K.) 379, 395
Диофант (Diophantus) 13, 15, 23, 414
Дирихле (Dirichlet P.G.L.) 42, 65, 71, 82, 84, 85, 138, 156, 222, 389
Дитман (Dittmann G.) 219, 221
Дойринг (Deuring M.) 390
Драх (Drach S.M.) 401, 402
Дрегер (Draeger M.) 118, 123, 402, 405
Дуарте (Duarte F.J.) 47, 53
Дэвенпорт Г. (Davenport H.) 413
Дюбуа (Dubouis E.) 237, 320
Дюран-Лорига (Duran-Loriga J.J.) 402, 404

Евклид (Euclid) 15, 22
Егган (Eggan L.C.) 402, 406

Жакме (Jacquemet C.) 96, 110
Жерар (Girard A.) 249
Жерарден (Gérardin A.) 410
Жермен (Germain S.) 78, 82, 116, 118, 125, 126, 129, 135, 136, 138, 221, 229, 380, 409, 410
Жонкюре (Jonquières E. de) 213, 220, 287, 292

Зальшутц (Saalschütz L.) 244, 250
Зауэр (Sauer R.) 213, 220
Зибек (Siebeck H.) 174, 181
Зигель (Siegel C.L.) 263, 269
Зигмонди (Zsigmondy K.) 106, 110
Зиновьев (Zinoviev A.A.) 402, 405
Зоммер (Sommer J.) 33, 36, 53

Иванов (Ivanov I.I.) 402, 404
Извеков (Izvekoff J.) 213, 220
Инкери (Inkeri K.) 12, 96, 99, 103, 111, 184, 187, 200, 202, 204, 210–212, 217, 220, 258, 259, 262–264, 270, 283, 293, 402, 406
Итар (Itard J.) 407, 411
Иф (Yf P.) 37, 54
Ихара (Ihara Y.) 397
Иянага (Iyanaga S.) 412

Кавада (Kawada Y.) 412
Кальцолари (Calzolari L.) 47, 52, 402, 403
Кандидо (Candido G.) 239, 251
Кани (Kani E.) 12, 396
Канольд (Kanold H.J.) 106, 111
Капферер (Kapferer H.) 82, 86, 111, 137, 139, 244, 247, 251, 252, 258, 259, 263, 269, 275, 276, 280, 293, 401, 404
Каркави (Carcavi) 7, 25, 31, 37
Карлиц (Carlitz L.) 244, 246, 251
Кармайкл (Carmichael R.D.) 23, 28, 33, 37, 47, 53, 106. 110, 189–191, 193, 196, 199
Касселс (Cassels J.W.S.) 394. 413, 414
Кассине (Cassinet R.) 412
Каталан (Catalan E.) 116, 122, 217, 220, 231, 237, 239, 240, 250, 412
Каттанео (Cattaneo P.) 19, 23, 273, 292
Кауслер (Kausler C.F.) 28, 31, 47, 51, 82, 85
Квайн (Quine W.V.) 267, 270
Келле (Cailler R.) 281. 292
Келлер (Keller W.) 379

Кисс (Kiss P.) 288, 289, 293, 294
Кламкин (Klamkin M.S.) 290, 293
Кларк Д. (Clark D.) 379
Кларк Дж. (Clarke J.H.) 402, 405
Клёсген (Klösgen W.) 189, 193, 195, 201, 241, 243, 251, 306, 309, 315, 322, 337, 338, 361, 373, 376
Кобелев В.В. 413
Коблиц (Koblitz N.) 394, 409, 414
Ковалевская С.В. 244, 250
Кокотт (Kokott P.) 82, 86
Кокс (Cox D.A.) 395
Колывагин В. 397
Кон (Cohn P.M.) 112, 115
Копперсмит (Coppersmith D.) 380
Корнаккья (Cornacchia G.) 312, 313, 320
Корнек (Korneck G.) 402, 404
Корнелл (Cornell G.) 394, 396
ван дер Корпут (van der Corput J.G.) 47, 53, 72, 73
Коши (Cauchy A.M.) 78, 125, 192, 199, 238, 249, 412
Краснер (Krasner M.) 134, 139, 264, 269
Крей (Krey H.) 47, 53
Крейзель (Kreisel G.) 402, 405
Кристи (Christy D.) 411
Кристилль (Christilles W.E.) 136, 140, 252, 254, 270
Кришнасастри (Krishnasastri M.S.R.) 136, 139
Кронекер (Kronecker L.) 28, 32, 44, 52
Крэндалл (Crandall R.E.) 379
Куйк (Kuyk W.) 394
Куммер (Kummer E.E.) 91, 92, 96, 110, 210, 211, 221, 229, 233, 236, 377–379, 402, 403, 412
Куржель (Curjel H.W.) 402, 404
Кэли (Cayley A.) 239, 249
Кэри (Carey F.S.) 313, 320
Лагранж (Lagrange J.L.) 31, 96, 110, 285, 292, 367
Ламе (Lamé G.) 47, 52, 72, 73, 78, 79, 82, 84, 85, 231, 236, 238, 249, 402, 403
Лампе (Lampe E.) 401
Ландау (Landau E.) 37, 53, 319, 320, 409
Ландсберг (Landsberg O.) 402, 403
Ле Лионне (Le Lionnais F.) 411, 412
Лебег (Lebesgue V.A.) 28, 32, 72, 73, 79, 231, 237, 252, 269, 311, 312, 319
Левек В. (Leveque W.J.) 322
Левек К. (Levesque C.) 396
Лежандр (Legendre A.M.) 26, 28, 29, 31, 32, 37, 40, 47, 51, 61, 64, 65, 72, 73, 78, 82, 85, 90 92, 103, 110, 116, 118, 122, 125–127, 129, 133, 134, 138, 223, 310, 319
Лежандр Р. (Legendre R.) 37, 54
Лексель (Lexell A.J.) 86
Лемер Д. (Lehmer D.H.) 174, 181, 378, 379
Лемер Э. (Lehmer E.) 143–145, 151, 155, 314, 322, 378
Ленг (Lang S.) 390, 394, 395, 414
Ленстра (Lenstra H.) 12, 388
Ленстра мл. (Lenstra Jr. H.W.) 393, 397
Леонардо Пизанский (Фибоначчи) (Leonardo di Pisa) 16
Леопольдт (Leopoldt H.-W.) 111
Лефебюр (Lefébure A.) 402, 403
Либри (Libri G.) 310–312, 319
Линд (Lind B.) 82, 86, 116, 118, 122, 183, 199, 207, 211, 264, 269, 401, 402, 404, 408
Линдеман (Lindemann F.) 116, 122, 400, 402, 404
Линц (Lintz R.G.) 181

Литтлвуд (Littlewood J.E.) 158, 314
Лиувилль (Liouville J.) 78, 238, 249, 253, 269, 402, 403, 412
Лонг (Long L.) 222, 223, 230
Лузин Н.Н. 5
Любельский (Lubelski S.) 151, 155
Люка Ф. (Lucas F.) 96, 110, 247, 250
Люка Э. (Lucas E.) 30, 32, 51, 52, 92, 93, 174, 181, 212, 220, 239, 244, 250
Люнебург (Lüneburg H.) 106, 111

Маггу (Maggu P.L.) 402, 406
Мазур (Mazur B.) 393, 396, 397, 412
Макмагон (MacMahon P.A.) 250
Манн (Mann H.B.) 54, 56. 64
Мансьон (Mansion P.) 212, 220, 409
Мантель (Mantel W.) 319, 320
Мариани (Mariani J.) 19, 23
Марков (Markoff V.) 212, 220
Массер (Masser D.W.) 382, 383
Массутье (Massoutié L.) 201, 211
Махони (Mahoney M.S.) 408, 411, 412
Мейе (Maillet E.) 78, 79, 134, 137–139
Мейснер (Meissner W.) 190, 199, 379
Менхен (Maennchen A.) 400–402, 404
Меншен (Mention J.) 231, 233, 237
Мерсенн (Mersenne M.) 25, 26, 30, 31, 37, 407
Метро (Métrod G.) 291, 292
Метрополис (Metropolis N.) 201
Метсянкиля (Metsänkylä T.) 12, 379
Мёллер (Möller K.) 96, 111, 212, 216. 221
Мийяке (Miyake T.) 394
Мириманов Д. 72, 82, 86, 134, 139, 229, 241, 243, 250, 281, 283, 292, 379, 380, 400, 402, 404
Митчелл (Mitchell H.H.) 314, 320
Михальинеч (Mihaljinec M.) 273, 293
Монаган (Monagan M.B.) 379, 380
Морделл (Mordell L.J.) 51, 54, 61, 381, 409, 410
Моришима (Morishima T.) 402, 405
Мория (Moriya M.) 137
Муир (Muir T.) 141, 155, 239, 244, 245, 248, 250
Мурти (Murty M. Ram) 394, 395
Мэй (May K.O.) 412
Мэйсон (Mason R.C.) 382, 383
Мэтьюс (Matthews G.B.) 82, 85, 142, 143, 155, 250, 310, 320

Нагель (Nagell T.) 53, 71, 73, 79, 409
Натуччи (Natucci A.) 406
Невядомский (Niewiadomski R.) 184, 200, 207, 211, 291, 292
Нестер (Nester) 240, 251
Нетаньяху-Милейковский (Netanjahu-Mileikowsky E.M.) 213, 220
Нидермайер (Niedermeier F.) 221, 222, 229
Ногуэра Барренече (Noguera Barreneche R.) 402, 405
Ногуэс (Noguès P.) 408
Нутцхорн (Nutzhorn F.) 28, 32

Облаф (Obláth R.) 30, 33
Огг (Ogg A.) 394
Ольберс (Olbers W.) 409
Оре (Ore O.) 410
Остман (Ostmann H.H.) 409

Пальмстрем (Palmström A.) 53
Паскаль (Pascal B.) 7, 25, 31, 408
Пауэлл (Powell B.) 134, 137, 140
Пелле (Pellet A.E.) 310–312, 320
Пелль (Pell J.) 285
Пепен (Pepin T.) 28, 32, 37, 51, 52, 78, 79, 310–312, 319, 320, 402, 403
Перес-Качо (Pérez-Cacho L.) 118, 123, 183, 200, 201, 204, 211, 264, 267, 269, 271, 272, 274, 293
Перисастри (Perisastri M.) 136, 139, 140
Перрен (Perrin R.) 47, 52, 252, 255, 269
Перрон (Perron O.) 237, 244, 251, 400
Пешль (Peschl E.) 340, 376
Пеюлеску (Peiulescu V.) 406
Пиза (Pizá P.A.) 37, 54
Пикар (Picard E.) 402, 404
Пиньятаро (Pignataro S.) 285, 293
Пифагор (Pythagoras) 15
Платон (Plato) 15
Племель (Plemelj J.) 71, 73
Поклингтон (Pocklington H.C.) 252, 269
Поле (Paulet F.) 400
Поллачек (Pollaczek F.) 200, 210, 211, 283, 293, 337, 379, 380
Поме (Pomey L.) 118, 122, 137, 139, 183, 184, 200–202, 211
Померанс (Pomerance C.) 379
Попов О.В. 8
ван дер Портен (van der Poorten A.) 396
Постников М.М. 414
Прасолов В.В. 414
Преображенский С.Н. 8
Пуанкаре (Poincaré H.) 402, 404
Пьер (Pierre C.) 123, 124, 206, 211, 280, 281, 293

Раина (Raina B.L.) 224, 225, 230
Райт (Wright E. M.) 17, 23
Раклиш (Racliş N.) 116, 122, 185, 200
де Рам (de Rham G.) 411
Рамакришна (Ramakrishna R.) 397
Рамесвар Рао (Rameswar Rao D.) 208, 212, 273, 293
Ребу (Rebout E.) 231, 237
Редей (Rédei L.) 237, 244, 251
Рейс (Reis G.) 208
Ренч (Wrench J.W.) 158
Реталь (Retall V.) 239, 251
Рибенбойм (Ribenboim P.) 5, 8, 23, 64, 73, 151, 156, 173, 181, 258, 262, 270, 285, 293, 294, 335, 376, 379, 382, 395, 406, 408, 412
Рибет (Ribet K.A.) 264, 392–398
Ривуар (Rivoire P.) 134, 140, 142, 155, 264, 270
Риман (Riemann B.) 389, 413
Роберваль (Roberval) 7, 407
Родеха (Rodeja F.) 402, 405
Роллеро (Rollero A.) 208, 212
Россер (Rosser J.B.) 283, 379
Роткевич (Rotkiewicz A.) 228, 230
Роуз (Rose J.) 233, 237
Рубин (Rubin K.) 395, 398
Рыхлик (Rychlik K.) 28, 32, 47, 53, 72

Садовничий В.А. 171
Сайпра (Cipra B.A.) 394
Сарантопулос (Sarantopoulos S.) 402, 405
Свистак (Swistak J.M.) 272, 293
Свифт (Swift E.) 82, 86
Сегал (Segal D.) 185, 200
Секстон (Sexton C.R.) 158
Сен-Круа (Sainte-Croix Chevalier de) 25, 26, 30, 37, 407
Сен-Мартен (Saint-Martin) 25, 30
Серпинский (Sierpiński W.) 19, 23. 54

Серр (Serre J.-P.) 392, 395, 397, 414
Серре (Serret J.A.) 237, 244, 250
Сильверберг (Silverberg A.) 395
Сильверман (Silverman J.H.) 394, 396
Сильвестр (Sylvester J.J.) 51, 52, 64, 96, 110
Симмонс (Simmons G.J.) 208, 212
Сингх Л. (Singh L.) 402, 406
Сингх С. (Singh S.) 396, 414
Сколем (Skolem T.) 281, 293
Смит (Smith H.J.S.) 402, 403, 408
Соловьев Ю.П. 414
Споттисвуд (Spottiswoode W.) 141, 155
Стафф (Stuff M.) 258, 270, 402, 405
Стивенс (Stevens G.) 396
Стоун (Stone D.E.) 120, 122, 135, 136, 139
Стюарт (Stewart C.L.) 120, 123
Стюпу (Stupuy H.) 138, 229

Танияма (Taniyama Y.) 383, 385, 390
Таннер (Tanner J.W.) 380
Таннери (Tannery P.) 407, 410
Тафельмахер (Tafelmacher W.L.A.) 28, 32, 82, 85, 86, 116, 122
Тейлор (Taylor R.) 383, 388, 393, 396, 398
Тейт Дж. (Tate J.) 394
Тейт П. (Tait P.G.) 47, 52
Тержанян (Terjanian G.) 12, 72, 73, 79, 82, 84, 86, 221, 225, 227, 228, 230, 243, 251, 412
Теркем (Terquem O.) 28, 32, 252, 253, 269, 409
Тодхантер (Todhunter I.) 244, 249
Топен (Taupin) 239, 251
Трипанис (Trypanis A.A.) 193, 196, 200
Турешбаев Б.А. 8
Туэ (Thue A.) 47, 53, 82, 85
Тэбо (Thébault V.) 135, 136, 139
Тэлбот (Talbot W.H.F.) 213, 220, 402, 403

Уайлс (Wiles A.) 11, 252, 264, 309, 383, 384, 388, 392, 393, 398
Урселл (Ursell J.H.) 402
Урсус (Ursus) 239, 251

Фабри (Fabry E.) 402, 404
Фаддеев Д.К. 413
Фалтингс (Faltings G.) 381–383, 395, 399
Фейт (Feit W.) 314, 322
Фелл (Fell J.) 82, 85, 86
Фергюсон (Ferguson R.P.) 411
Ферентину-Николакопулу (Ferentinou-Nicolacopoulou J.) 188, 193, 200
Ферма (Fermat P. de) 5, 6, 7, 13, 17, 22, 23, 25, 30, 37, 40, 51, 285, 292, 407
Ферма Самуэль (Fermat Samuel de) 13, 407
Феррерс (Ferrers N.M.) 244, 249
Фи (Fee G.) 154, 156
Фибоначчи (Fibonacci) 16
Филасета (Filaseta M.) 243, 382
Флах (Flach M.) 397
Флек (Fleck A.) 116, 118, 122, 183, 184, 199, 209–211, 400–402, 404
Фли Сен-Мари (Flye Sainte-Marie C.) 319, 320
Фонг (Phong Bui Minh) 289, 293
Фрага Торрехон (Fraga Torrejón E. de) 402, 405
Фрей (Frey G.) 12, 252, 264, 270, 385, 395–398
Фрейм (Frame J.S.) 143, 145, 146, 148, 151–153, 156

Френикль (Frénicle de Bessy B.) 6, 22, 28, 31, 292
Фресней (Frasnay C.) 92
Фрёлих (Fröhlich A.) 413
Фридман (Friedman A.R.) 382
Фритш (Fritsch R.) 181
Фробениус (Frobenius F.G.) 183, 199, 379
Фуври (Fouvry E.) 137, 140, 380, 381
Фурнье (Fournier J.C.) 411
Фуртвенглер (Furtwängler P.) 137, 184, 402, 404
Фюетер (Fueter R.) 258, 269

Хантер (Hunter J.A.H.) 244, 246, 251
Харди (Hardy G.H.) 17, 23, 158, 314
Хассе (Hasse H.) 314, 390
Хейз (Hayes B.) 395
Хенкок (Hancock H.) 33, 36, 53
Херинг (Hering C.) 106, 111
Хида (Hida H.) 394
Хиз (Heath T. L.) 22
Хиз-Браун (Heath-Brown D.R.) 137, 140, 380–382
Хинчин А.Я. 408, 413
Хоггатт (Hoggatt V.E.) 151, 155
Холден (Holden H.) 37, 53
Хорн (Horn R.A.) 158, 159
Хоффман (Hoffmann F.) 401, 410
Хуа (Hua L.K.) 314, 321

Цермиас (Tzermias P.) 382

Чезаро (Cesàro E.) 244, 250
Човла (Chowla S.) 264, 270
Чубариков В.Н. 8, 171, 414

Шаумбергер (Schaumberger N.) 290, 293
Шафаревич И.Р. 378, 379, 409, 414
Шенкс (Shanks D.) 19, 23, 158, 159, 409
Шеннон (Shannon A.G.) 402, 405
Шимура (Shimura G.) 383, 385, 390, 391, 394, 396
Шинцель (Schinzel A.) 111, 159, 411
Шликевай (Schlickewei H.-P.) 397
Шмадья (Smadja R.) 411
Шмид (Schmid F.) 46, 54
Шопи (Schopis) 28, 31, 71, 72
Шпунар В.А. (Spunar V.A.) 185, 200
Шпунар В.М. (Spunar V.M.) 118, 122
Шрёнбаум (Schönbaum) 410
Штерн (Stern M.A.) 141, 155
Штокхаус (Stockhaus H.) 47, 53
Шумахер (Schumacher J.) 37, 53
Шур (Schur I.) 313, 320
Шуф (Schoof R.) 395

Эверетт (Everett C.J.) 201
Эдвардс (Edwards H.M.) 33, 37, 54, 408, 411, 414
Эдиксован (Edixhoven B.) 395
Эйзенштейн (Eisenstein F.G.) 54
Эйлер (Euler L.) 26, 28, 31, 37, 44, 51, 61, 86, 96, 110, 130, 262, 269, 389
Эконому (Oeconomou G.) 221, 223, 224, 230
Элкис (Elkies N.D.) 383
Эльгуарш (Hellegouarch Y.) 264, 270, 397
Эрнваль (Ernvall R.) 379
Эстерле (Oesterlé J.) 382, 383, 395

Юнгникель (Jungnickel D.) 111

Якоби, (Jacobi C.G.J.) 10, 17, 123, 225
Яу (Yau S.T.) 396
Яффе (Jaffe A.) 396
Яхья (Yahya Q.A.M.M.) 263, 270, 402, 405, 406

Предметный указатель

(*abc*)-гипотеза (*abc* conjecture) 382
L-ряд (*L*-series) 389, 390
— эллиптической кривой (— of elliptic curve) 390
p-адическая метрика (*p*-adic distance) 161
p-адические числа (*p*-adic numbers) 160, 392
— — целые (*p*-adic integers) 160, 162
p-адический анализ (*p*-adic analisys) 92
p-адическое (*p*-adic)
— значение (— value) 89
— нормирование (— valuation) 89, 160
p-целое число (*p*-integral) 89
— — рациональное (— rational number) 160

«Mathematical Reviews», 314
«Zahlbericht», 33
«Арифметика» (Arithmetica (Diophantus)) 23
«Начала» (Elements, The) 15
«метод ящиков» Дирихле (Dirichlet's pigeon-hole principle) 42

автоморфная функция (automorphic function) 390
алгебра Гекке (Hecke algebra) 388, 399
арифметическая алгебраическая геометрия (Arithmetic Algebraic Geometry) 384

биквадратное уравнение (biquadratic equation) 23
биномы (binomials) 95

великая теорема Ферма (Fermat's last theorem) 13

гамма-функция (gamma function) 389
гауссово поле (Gaussian field) 33
гауссово целое число (Gaussian integer) 33
— — — простое (prime — —) 33
гауссовы единицы (Gaussian units) 33
гауссовы целые числа (Gaussian integers) 33
— — — ассоциированные (associated — —) 33
— — — наибольший общий делитель (greatest common divisor of — —) 34
гауссовы числа (Gaussian numbers) 33, 34
гипотеза (conjecture)
— Абеля (Abel's —) 212, 217
— Морделла (Mordell's —) 381, 383
— Римана (Riemann hypothesis) 314
— Шимуры—Таниямы (Shimura—Taniyama —) 383, 385, 387, 390, 391, 393
гипотетические решения (hypothetical solutions) 116
группа (group)
— Галуа (Galois —) 295, 301
— классов (class —) 137

делители биномов (factors of binomials) 95
дзета-функция Римана (Riemann zeta function) 389
дискриминант (discriminant) 112, 113, 385, 390

единица (unit) 55, 162
— p-адическая (p-adic —) 307

закон взаимности Гаусса (Gauss' reciprocity law) 40, 225
золотое сечение (golden ratio) 150
золотое число (golden number) 150

индекс (index) 301
институт Ньютона (Newton Institute) 383
иррегулярное простое число (irregular prime) 378

квадратичные вычеты (quadratic residues) 18, 19
квадратичный закон взаимности (quadratic law of reciprocity) 40, 225
кольцо нормирования (valuation ring) 161
конгруэнц-группа (congruence group) 387
кондуктор (conductor) 386
конференция «Токио—Никко» (Tokyo-Nikko conference) 390
корни из 1 (roots of unity) 93
кривая (curve)
— Фрея (Frey —) 264, 385, 386
— эллиптическая (elliptic —) 264, 385, 390
— — Вейля (Weil — —) 390
— — модулярная (modular — —) 390
— — полуустойчивая (semistable — —) 384, 386
критерий Вендта (Wendt's criterion) 141, 142
круговое поле (cyclotomic field) 137, 378
— — число классов (class number of — —) 377
кубическое уравнение (cubic equation) 37, 55, 255

лемма (lemma)
— Гаусса (Gauss' —) 163
— Гензеля (Hensel's —) 169, 172, 305, 306
линейные рекуррентные последовательности (linear recurring sequences) 174
локальная проблема Ферма (local Fermat problem) 305

малая теорема Ферма (Fermat's little theorem) 136
метод (method)
— бесконечного спуска (infinite descent) 25
— множителей Лагранжа (Lagrange multipliers) 367
многочлен (polynomial)
— неприводимый (irreducible —) 163
— приведенный (monic —) 93, 169
— примитивный (primitive —) 162
многочлены (polynomials)
— Коши (Cauchy —) 241, 243, 277, 346
— взаимно простые (relatively prime —) 163
— деления круга (cyclotomic —) 93
модулярная форма (modular form) 385, 387, 390
— — собственная (eigenform) 388
модулярная эллиптическая кривая (modular elliptic curve) 390

новая форма (new form) 388

оператор Гекке (Hecke operator) 388
определитель Вендта (Wendt's determinant) 127, 142–144, 151, 319

параболическая форма (cusp form) 387
период модулярной формы (period of a modular form) 391
периоды Гаусса (Gaussian periods) 295, 304, 349
пифагореизм (Pythagoreanism) 19
пифагоров треугольник (Pythagorean triangle) 19, 23, 25
пифагоровы тройки (Pythagorean triples) 15, 17, 291
поле (field)
— p-адических чисел (— of p-adic numbers) 161
— Эйзенштейна (Eisenstein —) 54, 55
— вычетов (residue —) 161
полуустойчивая эллиптическая кривая (semistable elliptic curve) 384, 386
пополнение (completion) 161
последняя теорема Ферма (Fermat's last theorem) 13
правило Крамера (Cramer's rule) 166
представление Галуа (Galois representations) 385, 392
премия Вольфскеля (Wolfskehl Prize) 400, 410
примитивные решения (primitive solutions) 15, 17, 19
примитивный (primitive)
— делитель (— factor) 101
— (первообразный) корень (— root) 103
— — степени d (— dth root) 93
проблема Варинга (Waring's problem) 314
простое число (prime) 33, 55
— — инертное (inert —) 56
— — иррегулярное (irregular —) 378
— — разветвленное (ramified —) 56
— — разложимое (split —) 56
— — регулярное (regular —) 377, 378
простые числа (primes)
— — Жермен (Sophie Germain —) 158
— — Ферма (Fermat —) 130
— — близнецы (twin —) 158
— — в арифметической прогрессии (— in an arithmetical progression) 389

расширение Галуа (Galois extension) 301
регулярное простое число (regular prime) 377, 378
резольвенты Лагранжа (Lagrange resolvents) 62, 301, 304, 315
результант (resultant) 112, 113, 141
род кривой (genus) 381
ряд (series)
— Дирихле (Dirichlet —) 389, 390
— Фурье (Fourier —) 390

символ (symbol)
— Лежандра (Legendre —) 40, 223
— Якоби (Jacobi —) 123, 206, 225
собственная форма (eigenform) 388
соотношения Барлоу (Barlow's relations) 116, 123, 210, 218
сравнение (congruence)
— Гурвица (Hurwitz —) 322
— Ферма (Fermat's —) 140, 309
старая форма (old form) 388

сумма двух квадратов (sum of two squares) 17, 18
суммы (sums)
-- Гаусса (Gaussian --) 314
— Якоби (Jacobi --) 350

теорема Ферма (Fermat's theorem) 13, 15, 46, 254, 413
— — второй случай (second case of — —) 14
— — для показателя 3 (— — for the exponent three) 47, 56–58
— — для показателя 4 (— — for the exponent four) 27
— — малая (— little —) 136
— — первый случай (first case of — —) 14, 125, 133–135, 137, 380
— — — — для четных показателей (— — — — — for even exponents) 221
теорема (theorem)
— Безу (Bézout's —) 115
— Вендта (Wendt's —) 140
— Вифериха (Wieferich's —) 379
— Дирихле (Dirichlet's —) 138, 156, 222
— Жермен (Germain's —) 125, 126, 129, 135, 136
— Куммера (Kummer's —) 377
— Тержаняна (Terjanian's —) 225
— Фалтингса (Faltings' —) 381
теория Галуа (Galois theory) 93
теория полей классов (class field theory) 137, 184, 187, 229, 262
точка заострения (cusp) 387

уравнение Пифагора (Pythagorean equation) 15, 287
уравнение Ферма (Fermat's equation) 13, 116
-- — биквадратное (biquadratic — —) 23
— — десятого порядка (— — of degree ten) 83
— — квадратное (quadratic — —) 15
— — кубическое (cubic — —) 37, 55, 255
— — пятого порядка (quintic — —) 65
— — седьмого порядка (— — of degree seven) 73
— — шестого порядка (— — of degree six) 83

функция (function)
— Мёбиуса (Möbius —) 94, 273
— Эйлера (Euler's totient —) 93, 271

характеры (characters) 389

целая часть (integral part) 90
целые числа, ассоциированные (associated integers) 55
циклическое представление (cyclic representation) 336
циклическое решение (cyclic solution) 336
циркулянта (circulant) 141, 142

числа (numbers)
— Бернулли (Bernoulli —) 134, 377
— Люка (Lucas —) 150, 151, 174
— Фибоначчи (Fibonacci —) 150, 151, 174
— Эйлера (Euler —) 229
число классов (class number) 377, 378
числовое поле (number field) 390

эйлерова система (Euler system) 399
эйлерово произведение (Euler product) 389
эллиптическая кривая (elliptic curve) 264
— — Вейля (Weil -- —) 390

Оглавление

От редактора перевода 5
Предисловие 9
К читателю 11
Благодарности 12
Проблема 13
Глава I. Частные случаи 15
I.1. Уравнение Пифагора 15
I.2. Биквадратное уравнение 23
I.3. Гауссовы числа 33
I.4. Кубическое уравнение 37
I.5. Поле Эйзенштейна 54
I.6. Уравнение пятого порядка 65
I.7. Уравнение седьмого порядка 73
I.8. Другие частные случаи 79
I.9. Приложение: что скрывалось за «чудесным доказательством» Ферма? 86
Глава II. 4 эпизода 89
II.1. p-адическое нормирование 89
II.2. Многочлены деления круга 93
II.3. Делители биномов 95
II.4. Результант и дискриминант многочленов 111
Глава III. Алгебраические ограничения на гипотетические решения 116
III.1. Соотношения Барлоу 116
III.2. Дополнительные соотношения для гипотетических решений 123
Глава IV. Теорема Софи Жермен 125
IV.1. Теорема Софи Жермен 125
IV.2. Теорема Вендта 140
IV.3. Приложение: простые числа Жермен 156
Глава V. Эпизоды 5 и 6 160
V.1. p-адические числа 160
A. Поле p-адических чисел 160
B. Многочлены с p-адическими коэффициентами 162
C. Лемма К. Гензеля 169

V.2. Линейные рекуррентные последовательности второго порядка 174

Глава VI. Арифметические ограничения на гипотетические решения и показатель степени 182
VI.1. Сравнения 182
VI.2. Условия делимости 201
VI.3. Гипотеза Абеля 212
VI.4. Первый случай для четных показателей 221

Глава VII. Эпизоды 7 и 8 231
VII.1. Некоторые важные полиномиальные тождества . . 231
VII.2. Многочлены Коши 238

Глава VIII. Переформулировки, следствия и критерии . . . 252
VIII.1. Переформулировки и следствия из последней теоремы Ферма 252
A. Диофантовы уравнения, связанные с уравнением Ферма 252
B. Переформулировки последней теоремы Ферма 264
VIII.2. Различные утверждения, связанные с последней теоремой Ферма 270
A. Связь с функцией Эйлера 271
B. Связь с функцией Мёбиуса 273
C. Отсутствие нетривиальных решений в арифметической прогрессии 273
D. Связь с символом Лежандра 274
E. Связь с дискриминантом 275
F. Связь с кубическим сравнением 280
G. Связь с определителем 284
H. Связь с бинарной квадратичной формой 285
I. Отсутствие алгебраических соотношений между решениями уравнения Ферма 287
J. Связь с линейными рекуррентными последовательностями второго порядка 288
K. Возмущение показателя 290
L. Условие делимости для пифагоровых троек . . 291

Глава IX. Эпизоды 9 и 10 295
IX.1. Периоды Гаусса 295
IX.2. Резольвенты Лагранжа 300

Глава X. Локальная и модулярная проблемы Ферма **305**
X.1. Локальная проблема Ферма 305
X.2. Сравнение Ферма 309
X.3. Сравнение Гурвица 322
X.4. Сравнение Ферма по модулю, равному степени простого числа 334
Глава XI. Эпилог **377**
XI.1. Попытки 377
A. Теорема Куммера 377
B. Теорема Вифериха 379
C. Первый случай последней теоремы Ферма для бесконечно многих простых показателей 380
D. Теорема Фалтингса 381
E. (*abc*)-гипотеза 382
XI.2. Победа, или Вторая смерть Ферма 383
A. Кривые Фрея 385
B. Модулярные формы и гипотеза Шимуры—Таниямы 387
C. Работы Рибета и Уайлса 392
XI.3. Руководство к дальнейшему изучению 393
A. Эллиптические кривые, модулярные формы: базовый материал 394
B. Обзоры 394
C. Исследования 396
XI.4. Электронная почта в действии 398
Приложение A. Ссылки на ошибочные доказательства . . . **400**
XII.1. Статьи и книги, содержащие списки ошибочных доказательств 401
XII.2. Статьи, содержащие ошибочные доказательства . . 401
XII.3. Неудовлетворительные попытки 406
Приложение B. Общая библиография **407**
XII.1. Труды Ферма 407
XII.2. Книги, посвященные Ферма 408
XII.3. Книги со ссылками на последнюю теорему Ферма . 408
XII.4. Обзорные, исторические и библиографические статьи 409
XII.5. Критические статьи и обзоры 412
Список литературы о теореме Ферма на русском языке **413**
Именной указатель **415**
Предметный указатель **423**

Учебное издание

Пауло Рибенбойм

Последняя теорема Ферма
ДЛЯ ЛЮБИТЕЛЕЙ

Зав. редакцией академик В. И. Арнольд
Зам. зав. редакцией А. С. Попов
Ведущий редактор О. А. Васильева
Художник В. Р. Орловский
Художественный редактор В. А. Чуракова
Технические редакторы Е. В. Денюкова, О. Г. Лапко
Корректоры Л. В. Ким, Е. В. Кудряшова

Оригинал-макет подготовили А. В. Бегунц и С. Н. Преображенс
в пакете LaTeX 2ε с использованием
кириллических шрифтов семейства LH

Лицензия ЛР № 010174 от 20.05.97 г.

Подписано к печати 27.12.2002 г. Формат 60 × 90/16.
Гарнитура Computer Modern. Печать офсетная.
Объем 13,5 бум. л. Усл.-печ. л. 27,00. Уч.-изд. л. 23,45.
Изд. № 1/9769. Тираж 3 000 экз. Заказ -27

Издательство «Мир»
Министерства РФ по делам печати,
телерадиовещания и средств массовых коммуникаций
107996, ГСП-6, Москва, 1-й Рижский пер., 2.

Диапозитивы изготовлены в издательстве «Мир»

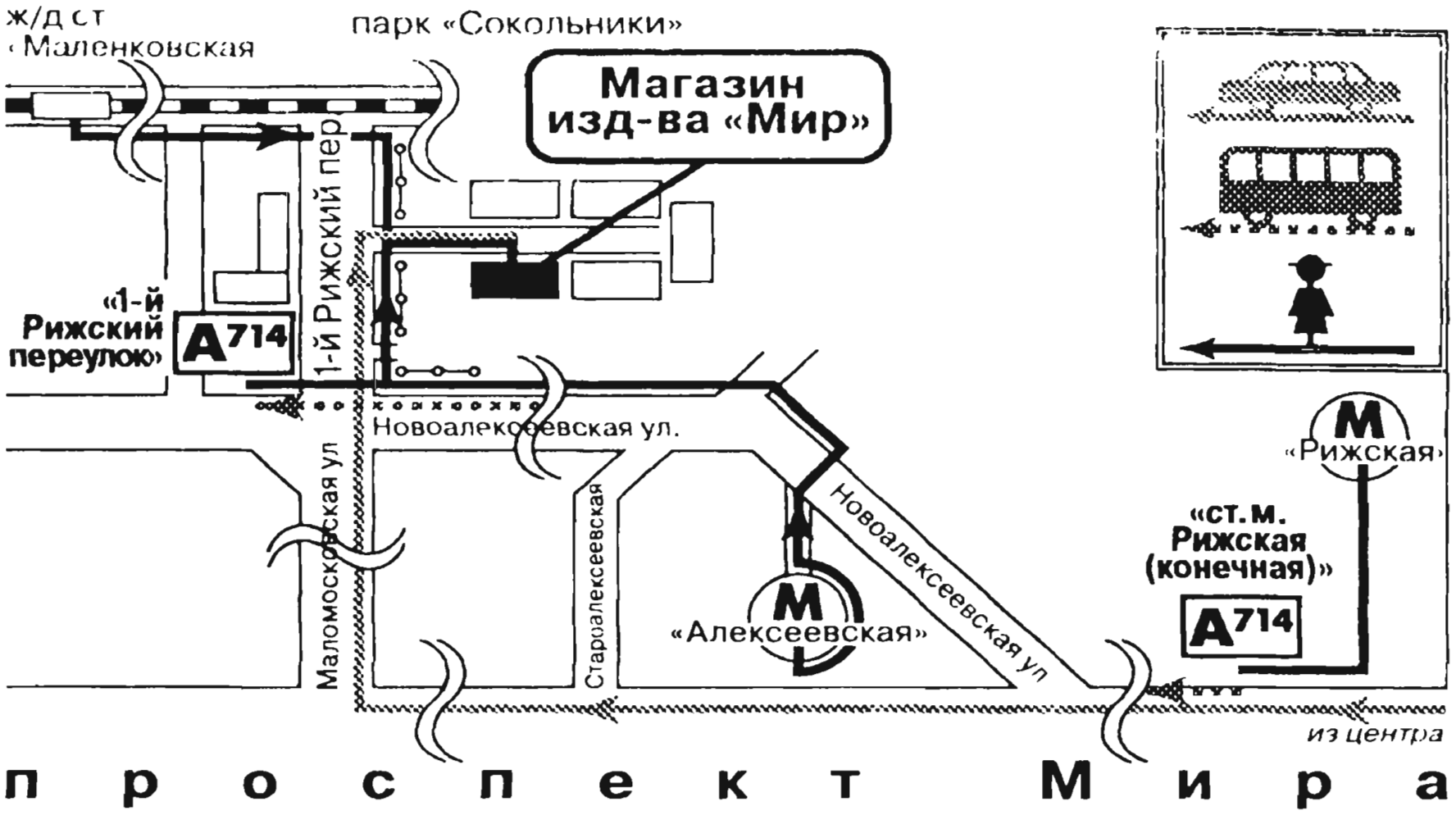
Отпечатано с готовых диапозитивов в
ОАО типография № 9
109033, Москва, ул. Волочаевская, 40

Книги издательства «Мир»

можно приобрести по издательским ценам в рекламно-коммерческом центре издательства по адресу:

Москва, 1-й Рижский пер., д. 2, корп. 1.
Тел.: (095) 286-84-55, 286-84-49

Проезд: метро «Рижская», далее авт. 714 до остановки «1-й Рижский переулок»



обычной почтой: 107996, ГСП-6, Москва, 1-й Рижский пер., д. 2
факсом: (095) 286-84-55
по электронной почте: info@mir-publishers.net (для информации)
com@mir-publishers.net (для заказов)
по сети Internet: http://www.mir-publishers.net

КНИГИ ИЗДАТЕЛЬСТВА «МИР»

также можно приобрести в следующих крупнейших магазинах:

Москва

- ГУП «Объединенный центр «Московский Дом книги» – ул. Новый Арбат, д. 8. Тел.: (095) 290-45-07
- ТД «Библио-глобус» – ул. Мясницкая, д. 6. Тел.: (095) 928-43-51
- «Дом технической книги» – Ленинский пр., д. 40. Тел.: (095) 137-60-38
- «Медицинская книга» – Комсомольский пр., д. 25. Тел.: (095) 245-39-33
- ДК «Молодая гвардия» – ул. Б. Полянка, д. 28. Тел.: (095) 238-50-01

Санкт-Петербург

- ГУП КТ «Санкт-Петербургский Дом книги» – Невский пр., д. 28. Тел.: (812) 219-49-15
- ГУП КТ «Техническая книга» – ул. Пушкинская, д. 6. Тел.: (812) 164-65-65

Новосибирск

- «Топ-книга» – ул. Арбузова, д. 1/1 Тел.: (3832) 36-10-28 http://www.top-kniga.ru

Екатеринбург

- «Дом книги» – ул. Валека, д. 12. Тел.: (3432) 59-42-00
- «Книжный магазин №14» – ул. Челюскинцев, д. 23. Тел.: (3432) 53-24-89

softline
www.softline.ru

119991 г. Москва,
ул. Губкина, д. 8
тел.: (095) 232-0023
e-mail: info@softline.ru

Все для науки

Научное ПО для исследований и расчетов

Почему студенты, преподаватели и научные работники приобретают нужные им программы в компании SoftLine?

- Низкие цены – компания работает напрямую с вендорами и является привилегированным партнером по образовательным программам для многих производителей ПО
- Возможность получения демо-версий и обновлений для широкого спектра программ
- Возможность удобного выбора программ по каталогу SoftLine-direct или на сайте *www.softline.ru*.
- Поддержка сообщества пользователей на сайте *www.exponenta.ru*.

Какое научное программное обеспечение поставляется SoftLine?

- Языки программирования математических задач (MathWorks)
- Моделирование электронных схем и устройств (Electronics Workbench, PCAD)
- Универсальные математические пакеты, обмен данными с AutoCAD (Wolfram Research, Waterloo Maple, MathSoft)
- ПО для химиков (CambridgeSoft)
- Статистические пакеты (MathSoft, StatSoft)
- Редакторы формул (Design Science, Multi Edit)
- Пакеты бизнес-анализа (Palisade)
- Математические надстройки к MS Office (Frontline Systems)

SoftLine – это свобода выбора

Обратившись в SoftLine, вы в кратчайшие сроки решите проблемы с программным обеспечением. Получив консультации менеджеров, вы подберете все необходимые инструменты для работы в вашей области. Компания SoftLine поможет вам также в выборе обучающих курсов и пригласит на регулярно проводимые семинары по математическим и статистическим пакетам.

The MATH WORKS Inc.

MathSoft
$\Sigma + \sqrt{} - = \int + \delta$

StatSoft

WOLFRAM RESEARCH

Waterloo Maple

Electronics Workbench

CambridgeSoft
Internet Chemistry Software Leader