НАУКА — МАССАМ

А. Я. ХИНЧИН

ВЕЛИКАЯ ТЕОРЕМА ФЕРМА

ОНТИ
ГТТИ
1934

Ферма
1608—1655

ПОПУЛЯРНАЯ БИБЛИОТЕКА ПО МАТЕМАТИКЕ
ПОД ОБЩЕЙ РЕДАКЦИЕЙ ПРОФ. Л. А. ЛЮСТЕРНИКА

А. Я. ХИНЧИН

ВЕЛИКАЯ ТЕОРЕМА ФЕРМА

ИЗДАНИЕ ТРЕТЬЕ

ОНТИ
ГОСУДАРСТВЕННОЕ
ТЕХНИКО-ТЕОРЕТИЧЕСКОЕ ИЗДАТЕЛЬСТВО
МОСКВА 1934 ЛЕНИНГРАД

Т 23-6-4

Редакция *Р. Н. Бончковского*. Оформление *С. Л. Дымач*.
Корректура *В. И. Сидоровой*. Выпускающий *Д. А. Липсе*.
Сдано в производство 31/III 1934. Подписано к печати 20/VI 1934 г.
Листов $3^1/_4$. Тираж 5000. Формат $82\times110^1/_{32}$. Печ. знаков в листе 38400.
Заказ № 390. ГТТИ № 57. Уполномоченный Главлита В-77295.

16-я типография треста «Полиграфкнига». Москва, Трехпрудный пер., д. 9.

ПРЕДИСЛОВИЕ К ПЕРВОМУ ИЗДАНИЮ.

Интерес к Великой теореме Ферма в нашем обществе растет с каждым годом; об этом свидетельствуют многочисленные запросы и попытки доказательств, получаемые нашими научными обществами и учреждениями. Между тем на русском языке не существует сколько-нибудь доступной литературы по этому вопросу, да и в странах Европы дело обстоит в этом отношении немногим лучше. Поэтому я охотно согласился на любезное предложение научного отдела Государственного издательства написать небольшую книжку, которая всем интересующимся могла бы дать необходимые справки, касающиеся проблемы Ферма, ее истории и современного состояния, а также по возможности осветить ее со стороны принципиальной и методологической.

Чтение этой книжки (за исключением дополнения) доступно каждому, кто знает элементарную арифметику.

А. Хинчин.

Москва, 16 июля 1925 г.

ОГЛАВЛЕНИЕ.

1. ПОСТАНОВКА ЗАДАЧИ.

Предложение, которое обычно называют Великой теоремой Ферма, родилось около середины XVII столетия; и во всей последующей истории математической мысли вряд ли можно найти другую задачу, которая в такой степени привлекала бы к себе научные усилия на протяжении столетий, как задача доказательства этой теоремы,—задача, не разрешенная и по настоящее время.

В то время, в XVII столетии, не было организованных научных обществ и не было научных журналов. Научное общение осуществлялось, главным образом, путем переписки. Отдельные гиганты математической мысли писали друг другу о своих достижениях и надеждах, писали редко и не спеша, потому что общий темп жизни был медленным и потому что почта тоже не спешила и ответа приходилось дожидаться долго. С другой стороны, и ученых было мало, так что каждый из них мог по пальцам пересчитать тех, кому интересно было бы узнать о его работах. Всем этим объясняется то, что от многих математических истин, открытых в то время, до нас дошли одни формулировки; доказательств история часто не сохраняла, и их приходилось восстанавливать заново. В особенности это относится к предложениям теории чисел. В сущности этой науки тогда еще не существовало; по крайней мере не было попыток соединить ее достижения в одно систематическое здание, и современники были склонны видеть в проблемах арифметики отдельные занятные, часто забавные, способные доставить изощренному уму тонкое наслаждение задачи; поэтому понятно, что в решении этих задач создалось соревнование, принимавшее характер спорта. Один писал другому: «Я умею решить такую-то задачу, умеешь ли ты ее решить?» А другой отвечал: «Нет, я ее решить не могу, и ты, очевидно, гениальный человек; но зато я знаю решение такой-то другой задачи; что ты можешь сказать о ней?» и т. д.

Ферма, Френикль, Декарт, Паскаль и другие часто и много переписывались между собою именно в этом роде; поэтому вполне понятно, что в большинстве случаев до нас от этой

переклички гигантов дошли одни названия их достижений; пути остались скрытыми. И если в большинстве случаев потомки, владевшие более сильными методами, сумели восстановить потерянные историей доказательства, то по крайней мере в одном случае — в случае Великой теоремы Ферма — им этого сделать не удалось.

Вот краткая история рождения этой задачи.

Пьер Ферма (Pierre Fermat), бесспорно наиболее выдающийся французский математик XVII столетия, обычно по справедливости почитается отцом современной теории чисел; первые достижения этой науки возникли при попытках решения целого ряда задач, им поставленных.

В 1670 г. сын Пьера Ферма издал книгу александрийского математика Диофанта, причем были перепечатаны также и примечания Пьера Ферма, оставленные им на полях одного из экземпляров этого сочинения. Одно из этих примечаний и содержит предложение, получившее наименование Великой теоремы Ферма. Вот его смысл:

Если n означает какое угодно целое положительное число, большее, нежели 2, то уравнению

$$x^n + y^n = z^n \tag{1}$$

не могут удовлетворять никакие три целых положительных числа x, y, z.

К этому Ферма прибавляет:

Я нашел удивительное доказательство этого предложения, но поля книги слишком узки, чтобы оно могло на них поместиться.

Таким образом доказательство, которым обладал сам Ферма, осталось необнародованным. С тех пор прошло почти триста лет, и мы еще не имеем ни доказательства, ни опровержения Великой теоремы Ферма; и это несмотря на то, что, как уже сказано, задаче этой непрерывно посвящали и продолжают посвящать свое внимание многие крупные ученые и еще большее количество неспециалистов, которых соблазняет простота формулировки проблемы.

Вопрос о том, имел ли действительно Ферма строгое доказательство своего предложения или же он заблуждался (в искренности его, повидимому, сомневаться не приходится), — этот вопрос, хотя он и часто обсуждается в литературе, очевидно, может иметь только историческое значение, почему мы здесь и не станем на нем останавливаться.

2. УКАЗАНИЯ НА МЕТОД.

Если бы удалось в научных трудах или записках самого Ферма отыскать хоть какие-нибудь указания на тот метод, каким он мог пользоваться при доказательстве своей теоремы, то это имело бы, разумеется, большое научное значение. К сожалению, определенных указаний на этот счет обнаружить нигде не удалось. Но косвенные намеки все же могли быть отысканы, и мы должны уделить им некоторое внимание.

Ферма вообще почти никогда не говорит о тех методах, какими он пользовался при своих исследованиях. Тем более ценным является одно его письмо к Каркави, в котором Ферма весьма подробно останавливается на одном замечательном способе математического рассуждения — способе, который, по его словам, позволил ему доказать много важных арифметических предложений и которым, кстати сказать, и после Ферма охотно пользовались выдающиеся исследователи. Этот способ Ферма называет методом «*бесконечного спуска*» (descente infinie). Вот в чем он состоит: *чтобы доказать, что какое-нибудь уравнение не может быть решено в целых положительных числах, показывают, что если бы оно удовлетворялось какими-нибудь целыми положительными числами, то оно должно было бы удовлетворяться кроме этих чисел еще и другими, и притом существенно меньшими.*

Если это удастся доказать для какого-нибудь уравнения, то мы можем считать доказанным, что это уравнение не имеет никаких целых положительных решений. В самом деле, если бы оно удовлетворялось какой-нибудь системой таких чисел, то оно, по доказанному, должно было бы удовлетворяться системой чисел меньших; а тогда, снова по доказанному, оно должно было бы удовлетворяться системой чисел еще меньших и т. д. Это рассуждение мы могли бы повторять сколько угодно раз и получали бы все новые системы решений, и притом все меньшие и меньшие; это же приводит нас к явной нелепости, ибо не может существовать безграничного ряда все меньших и меньших целых положительных чисел. Следовательно, уравнение не может вовсе иметь целых решений.

Ферма перечисляет целый ряд уравнений, невозможность которых ему удалось доказать именно методом бесконечного спуска. Среди них имеется уравнение.

$$x^3 + y^3 = z^3,$$

представляющее собою частный случай уравнения (1) (при $n = 3$). Можем ли мы считать вероятным, что и Великую теорему свою

Ферма доказывал методом спуска? Во всяком случае следует отметить, что многие предложения, высказанные Ферма без доказательства и доказанные позднее его последователями, были доказаны именно этим способом. Этот же прием дал возможность доказать и некоторые простейшие частные случаи Великой теоремы, на чем мы несколько подробнее остановимся ниже; кстати, мы будем иметь случай подробно проследить конкретное применение метода бесконечного спуска.

3. ФОРМУЛЫ ИНДУСОВ.

В формулировке Великой теоремы Ферма число n непременно должно быть больше, чем 2. И в самом деле, уже всякому ученику средней школы хорошо известно, что уравнение

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

может быть разрешено в целых положительных числах (например: $x = 3$, $y = 4$, $z = 5$). На основании теоремы Пифагора это приводится к тому общеизвестному факту, что существуют прямоугольные треугольники, все три стороны которых выражаются целыми числами.

Не ограничиваясь этим, мы поставим себе целью найти *все* решения уравнения (2), т. е. все тройки чисел, которые, как тройка 3, 4, 5, удовлетворяют этому уравнению.

Решение этой задачи уже в глубокой древности было известно индусам.

Прежде всего заметим, что числа x, y и z можно считать попарно не имеющими общих делителей. В самом деле, если бы какие-нибудь два из них, например x и y, имели какого нибудь общего делителя $r > 1$, то, как показывает уравнение (2), и z должно было бы делится на r, так что все уравнение можно было бы сократить на r^2. Поэтому можно предполагать, что числа x, y и z с самого начала попарно не имеют общих делителей.

Далее, нетрудно заметить, что из чисел x и y одно непременно должно быть четным, а другое нечетным.

В самом деле, если бы они оба были четными, то это значило бы, что у них есть общий делитель 2, — случай, который мы исключили. Если же оба были бы нечетны, например

$$x = 2k + 1, \quad y = 2l + 1,$$

то мы имели бы:

$$z^2 = x^2 + y^2 = 4(k^2 + k + l^2 + l) + 2, \qquad (3)$$

откуда видно, что z^2, а, следовательно, и z есть четное число,

$$z = 2m,$$

например, откуда $z^2 = 4m^2$, т. е. z^2 должно делиться на 4; но равенство (3) ясно показывает, что z^2 при делении на 4 дает в остатке 2. Таким образом предположение, что числа x и y оба нечетны, приводит нас к противоречию, и мы можем считать доказанным, что из двух чисел x и y одно должно быть четным, а другое нечетным. Заметим, что в таком случае z^2, равное $x^2 + y^2$, есть число обязательно нечетное, а следовательно, и z должно быть нечетным числом.

Пусть, для определенности, x четно, так что мы можем положить

$$x = 2u.$$

Написав уравнение (2) в виде

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

мы замечаем, что оба множителя правой части суть числа четные, а следовательно,

$$a = \frac{z + y}{2} \quad \text{и} \quad b = \frac{z - y}{2}$$

суть числа целые. Мы получаем:

$$x^2 = 4u^2 = 2a \cdot 2b = 4ab,$$

откуда

$$ab = u^2.$$

Но легко видеть, что числа a и b не могут иметь общих делителей. В самом деле, если бы оба они делились на какое-нибудь число r, то сумма и разность их, т. е. числа z и y, также должны были бы делиться на это число r, мы же предположили с самого начала, что эти числа не имеют общих делителей. Итак, числа a и b не имеют общих делителей, и произведение их есть квадрат некоторого целого числа. Но в таком случае, как известно, каждое из них в отдельности есть квадрат некоторого целого числа, и мы можем написать:

$$a = m^2, \quad b = n^2;$$

при этом числа m и n, очевидно, также не могут иметь общих делителей. Отсюда

$$z = a + b = m^2 + n^2, \quad y = a - b = m^2 - n^2,$$
$$u^2 = m^2 n^2,$$

и далее

$$u = mn, \quad x = 2mn.$$

Мы пришли к такому выводу: если числа x, y, z попарно не имеют общих делителей и удовлетворяют уравнению (2), то они обязательно выражаются формулами:

$$\left.\begin{aligned} x &= 2mn, \\ y &= m^2 - n^2, \\ z &= m^2 + n^2, \end{aligned}\right\} \tag{4}$$

где m и n суть два целых числа, не имеющих общих делителей.

Легко теперь убедиться, что и обратно, если числа x, y, z имеют выражения (4), где m и n — какие угодно целые числа, то x, y, z удовлетворяют уравнению (2). Это мы можем прямо проверить, подставляя выражения (4) в это уравнение.

Таким образом все решения уравнения (2) (не имеющие попарно общих делителей) найдутся по формулам (4), и обратно — для любых значений m и n формулы (4) дают нам тройку чисел, удовлетворяющих уравнению (2). В этом смысле говорят, что формулы (4) представляют собою *полное решение* уравнения (2). Это обстоятельство в древнюю эпоху было известно индусам, вследствие чего мы и будем называть формулы (4) *формулами индусов*. В частности, полагая $m=2$, $n=1$, мы получаем известное решение уравнения (2): $x = 4$, $y = 3$, $z = 5$.

Формулы индусов представляют очень большую ценность. Прежде всего они показывают, что в случае $n=2$ уравнение Ферма (1) имеет бесчисленное множество решений. Но этим их значение не исчерпывается: как мы сейчас увидим, они с успехом могут быть применены к доказательству одного частного случая Великой теоремы Ферма.

4. ДОКАЗАТЕЛЬСТВО ВЕЛИКОЙ ТЕОРЕМЫ ФЕРМА ДЛЯ СЛУЧАЯ n = 4

Убедимся теперь, что уравнение (1) при $n = 4$, т. е. уравнение

$$x^4 + y^4 = z^4,$$

не может быть решено в целых положительных числах. Так как четвертая степень всякого целого числа есть вместе с тем квадрат некоторого целого числа, то наше предположение будет доказано, если мы покажем, что более общее уравнение

$$x^4 + y^4 = z^2 \tag{5}$$

неразрешимо в целых положительных числах. Постараемся доказать это, пользуясь методом бесконечного спуска.

Итак допустим, что уравнению (5) удовлетворяет тройка целых положительных чисел x, y и z. На том же основании, как в предыдущем параграфе, мы имеем право допустить, что эти числа попарно не имеют общих делителей. Соотношение (5) мы можем представить в виде:

$$(x^2)^2 + (y^2)^2 = z^2;$$

это показывает, что числа x^2, y^2 и z удовлетворяют уравнению (2), а следовательно, должны, как доказано в предыдущем параграфе, выражаться по формулам индусов (4):

$$x^2 = 2mn,$$
$$y^2 = m^2 - n^2,$$
$$z = m^2 + n^2,$$

где m и n — два числа, не имеющие общих делителей. Теперь мы утверждаем, что число m — нечетное, а n — четное. В самом деле, если бы они были оба четные или оба нечетные, то y и z оба должны были бы быть четными, что противоречит нашему предположению. Поэтому остается показать невозможность того случая, когда m четно, а n нечетно. Итак, допустим, что

$$m = 2k, \quad n = 2l + 1.$$

Тогда

$$y^2 = m^2 - n^2 = 4(k^2 - l^2 - l) - 1,$$
$$y^2 = 4(k^2 - l^2 - l - 1) + 3;$$

это показывает, что y^2 при делении на 4 дает в остатке 3; значит, y^2, а следовательно и y, число нечетное, и мы можем положить $y=2s+1$, откуда

$$y^2 = 4(s^2 + s) + 1;$$

это же показывает, что y^2 при делении на 4 дает в остатке единицу. Мы, таким образом, приходим к противоречию, которое показывает, что наше предположение недопустимо. Поэтому мы можем считать доказанным, что число m должно быть нечетным, а n — четным, и мы можем положить

$$n = 2n'.$$

Так как x число четное, $x=2u$, то

$$x^2 = 4u^2 = 2mn = 4mn',$$

откуда

$$mn' = u^2$$

Но числа m и n' не могут иметь общих делителей, а значит, каждое из них в отдельности должно быть квадратом целого числа, и мы можем положить

$$m = a^2, \quad n' = b^2, \quad n = 2b^2;$$

подставляя же выражения, найденные нами для m и n, в выражение для y^2, находим:

$$y^2 = (a^2)^2 - (2b^2)^2,$$

откуда

$$y^2 + (2b^2)^2 = (a^2)^2.$$

Числа m и n, т. е. a^2 и $2b^2$, как мы знаем, не имеют общих делителей. Значит, и из трех чисел

$$y, \quad 2b^2, \quad a^2$$

никакие два не могут иметь общих делителей, ибо тогда, как показывает последнее уравнение, и третье должно было бы на него делиться. С другой стороны, последнее уравнение показывает, что эти три числа удовлетворяют уравнению (2). На основании предыдущего параграфа мы заключаем, что эти три числа должны выражаться по формулам индусов (4):

$$\left.\begin{aligned} y &= g^2 - h^2, \\ 2b^2 &= 2gh, \\ a^2 &= g^2 + h^2, \end{aligned}\right\} \tag{6}$$

где g и h — целые числа, не имеющие общего делителя. Поэтому второе из этих уравнений,

$$gh = b^2,$$

показывает, что из чисел g и h каждое есть квадрат некоторого целого числа, т. е. мы можем положить

$$g = p^2, \quad h = q^2;$$

подставляя эти выражения в последнее из уравнений (6), мы получаем:

$$p^4 + q^4 = a^2. \tag{7}$$

Уравнение (7) имеет такой же вид, как уравнение (5), и числа p и q также не могут иметь общих делителей.

Но так как

$$a = \sqrt{m},$$
$$z = m^2 + n^2,$$

то число a обязательно меньше, чем z. Таким образом мы доказали следующее: *если уравнение* (5) *удовлетворяется тремя це-*

лыми положительными числами без общих делителей, то оно непременно должно удовлетворяться еще другой тройкой таких же чисел, причем последнее число второй тройки меньше соответствующего числа первой тройки.

Это же есть как раз то, что нам нужно для применения метода бесконечного спуска, потому что из существования второй тройки решений на основании доказанного будет следовать существование третьей и т. д. Таким образом, если бы уравнение (5) имело хоть одну тройку решений, то оно должно было бы иметь таких троек бесчисленное множество, бесконечный ряд, и в этом ряду последнее из трех чисел от тройки к тройке становилось бы все меньше и меньше, оставаясь целым и положительным, что создает очевидную нелепость. Отсюда следует, что уравнение (5), а следовательно, и уравнение

$$x^4 + y^4 = z^4,$$

не может удовлетворяться никакой тройкой целых положительных чисел. Тем самым доказан частный случай Великой теоремы Ферма, когда $n=4$.

Приведенное нами доказательство принадлежит Эйлеру.

5. ДРУГИЕ ПРОСТЫЕ СЛУЧАИ.

Доказанное нами в предыдущем параграфе предложение имеет значение не только частного случая. Оно легко позволяет значительно ограничить задачу полного доказательства Великой теоремы.

В самом деле, мы теперь легко можем показать, что нам в дальнейшем достаточно рассматривать уравнения вида

$$x^p + y^p = z^p, \tag{8}$$

где число p — абсолютно простое, т. е. не имеющее других делителей, кроме единицы и самого себя. Действительно, если бы уравнение

$$x^n + y^n = z^n \tag{1}$$

удовлетворялось целыми x, y, z при каком-нибудь $n>2$, то n должно было бы делиться либо на 4, либо на какое-нибудь нечетное абсолютно простое число p. Но в первом случае, полагая $n=4k$, мы могли бы написать соотношение (1) в виде:

$$(x^k)^4 + (y^k)^4 = (z^k)^4,$$

невозможность которого мы доказали в предыдущем параграфе.

Во втором же случае, полагая $n=pl$, мы приводим уравнение (1) к виду:

$$(x^l)^p + (y^l)^p = (z^l)^p.$$

Если бы нам удалось показать, что уравнение (8) не допускает решения в целых числах, то последнее соотношение также было бы невозможно, а стало быть и уравнение (1) не могло бы допускать целых решений.

Итак, для полного доказательства Великой теоремы Ферма остается показать, что уравнение (8) ни при каком абсолютно простом нечетном числе p не может иметь целых положительных решений. Здесь мы должны сделать одно важное замечание, которым нам придется пользоваться ниже. Мы до сих пор говорили всегда о неразрешимости уравнения (1) в целых *положительных числах* x, y и z; легко видеть, что этот вопрос совершенно равносилен вопросу о разрешимости уравнения (1) в *каких угодно отличных от нуля* целых числах. Это представляется самоочевидным в случае, когда число n четное. Если же n нечетно, то допустим, что уравнение (1) удовлетворяется тройкой отличных от нуля чисел x, y, z; если все три числа отрицательны, мы изменим знаки всех трех и тем самым убедимся, что уравнение (1) имеет и положительную тройку решений; если же из чисел x, y, z два имеют один знак, а третье — противоположный, то прежде всего ясно, что этим третьим числом не может быть z; пусть, для определенности, это будет x, так что числа y и z имеют один и тот же знак, противоположный знаку числа x; помня, что n нечетно, мы можем представить уравнение (1) в виде:

$$x^n + (-z)^n = (-y)^n,$$

где числа x, $-z$ и $-y$ имеют один и тот же знак; таким образом мы приходим к тому, что уравнение (1) имеет положительную тройку решений.

Итак, если уравнение (1) для какого-нибудь n удовлетворяется тремя целыми, отличными от нуля числами, то оно при том же n имеет и целые *положительные* решения. Мы поэтому в дальнейшем можем не делать никакого различия между этими двумя постановками задачи.

Естественно, что усилия ближайших последователей Ферма были направлены на доказательство неразрешимости в целых числах уравнения (8) для простейших значений числа p, т. е. $p = 3,5,7,\ldots$ Пытались применять к этим уравнениям метод бесконечного спуска и ряд других элементарных приемов. Для отдельных значений p эти попытки привели к хорошим резуль-

татам; так, Эйлер доказал теорему для $p = 3$ (его доказательство позднее было улучшено Лежандром). Лежандр и Дирихле доказали теорему для $p = 5$, Ламэ и Лебег — для $p = 7$.

Однако общего доказательства теоремы Ферма на этом пути получить не удалось; не удалось доказать ее и для более или менее обширных групп показателей, вследствие чего эти простейшие приемы постепенно были математиками оставлены и заменены другими, более сильными, которые привели ко многим интересным результатам, краткий обзор которых мы приведем в дальнейшем.

Сейчас же мы перейдем к доказательству, данному Эйлером для случая $p = 3$, и изложим его во всей подробности; оно не только покажет нам еще один пример применения метода бесконечного спуска, но вместе с тем, что гораздо важнее, даст нам первое указание на ту роль, какую играют так *называемые алгебраические числа* в вопросах, связанных с теоремой Ферма.

Нам надлежит показать, что уравнение

$$x^3 + y^3 = z^3 \tag{9}$$

не может иметь решений в целых числах; при этом мы можем теперь учитывать возможность отрицательных решений ввиду нечетности показателя.

Допустим, что существует тройка целых, отличных от нуля чисел, удовлетворяющих уравнению (9); прежде всего мы можем так же, как в предыдущем параграфе, считать эти числа x, y и z попарно не имеющими общих делителей.

Для большей ясности мы разобьем последующее рассуждение на отдельные этапы.

1. Числа x и y не могут быть оба четными, так как мы предположили их не имеющими общих делителей. Отсюда легко следует, что мы вправе считать одно их них четным, а другое нечетным; в самом деле, если бы они оба были нечетными, то, как показывает уравнение (9), z было бы числом четным, и мы бы могли заставить его играть роль прежнего y, переписав уравнение (9) в виде:

$$x^3 + (-z)^3 = (-y)^3$$

2. Итак, будем считать x четным а y — нечетным; уравнение (9) показывает, что z в таком случае нечетно, и следовательно, числа

$$p = \frac{z + y}{2}$$

и

$$q = \frac{z-y}{2}$$

целые. Так как $z=p+q$ и $y=p-q$, то из чисел p и q одно должно быть четным, а другое нечетным. Мы получаем:

$$z^3 - y^3 = 2q^3 + 6p^2q = 2q(q^2+3p^2).$$

Таким образом, при наших предположениях, выражение $2q(q^2+3p^2)$ также должно быть кубом целого числа; при этом, очевидно, мы можем считать p и q целыми числами, не имеющими общих делителей; более того, соотношение

$$x^3 = 2q(q^2+3p^2) \tag{10}$$

показывает нам, что числа x, q и p мы можем считать положительными, не ограничивая этим общности задачи; относительно p это ясно само собою; x и q, как показывает соотношение (10), имеют одинаковые знаки; если бы они были отрицательными, мы могли бы, изменив знаки чисел x, y и z (благодаря чему q, как показывает его выражение, также только переменило бы знак), сделать числа x и q положительными.

3. Мы уже заметили выше, что число x — четное; полагая $x=2u$, получаем:

$$u^3 = \frac{1}{4}q(q^2+3p^2);$$

но так как числа q и p — разной четности, то q^2+3p^2 есть число нечетное; следовательно, написанное равенство требует, чтобы q делилось на 4.

4. Таким образом произведение чисел $\frac{1}{4}q$ и q^2+3p^2 должно быть кубом целого числа; если сомножители не имеют общих делителей, то отсюда следует, что каждый из них в отдельности должен быть кубом некоторого целого числа. Посмотрим же, могут ли эти сомножители, или, что то же, могут ли числа q и q^2+3p^2 иметь общие делители. Если такой делитель есть, то вместе с числом q на него будет делиться и q^2, а следовательно, и разность

$$(q^2+3p^2) - q^2 = 3p^2;$$

а так как p и q, по доказанному, общих делителей не имеют, то этим делителем может быть только число 3.

5. Мы должны будем во всем дальнейшем резко различать два случая: если q не делится на три, то числа q и q^2+3p^2 не могут иметь общих делителей; это — первый случай.

Если же q делится на три, то q^2+3p^2, очевидно, также делится на три, и притом число три, как мы видели, есть наибольший общий делитель этих двух чисел; это — второй случай.

6. *Первый случай.* Если q не делится на три и, следовательно, числа $\frac{1}{4}q$ и q^2+3p^2 не имеют общих делителей, то, как мы уже видели, каждое из них должно быть кубом некоторого целого числа.

Теперь мы вступаем в область так называемых целых алгебраических чисел. Заметим, что

$$q^2+3p^2=(q+p\sqrt{-3})(q-p\sqrt{-3});$$

числа вида $a+b\sqrt{-3}$, где a и b — обыкновенные целые числа, и представляют собою тот частный случай целых алгебраических чисел, с которым нам здесь придется иметь дело. Для этих чисел можно построить всю арифметику так же, как мы ее строим для наших обыкновенных целых чисел. Определения делимости, делителя, кратного, абсолютно простого числа и т. д. остаются теми же, как в обычной арифметике. Сохраняется и бóльшая часть ее предложений; в частности, если произведение двух чисел этого нового вида равно кубу некоторого числа того же вида и если сомножители не имеют общих делителей, то каждый из них в отдельности будет кубом некоторого алгебраического числа того же вида.

Произведение чисел

$$q+p\sqrt{-3}$$

и

$$q-p\sqrt{-3}$$

есть, как мы показали, куб некоторого обыкновенного целого числа; но всякое обыкновенное целое число a принадлежит классу наших новых целых чисел, ибо может быть представлено в виде $a+0\cdot\sqrt{-3}$. Можно показать (мы не будем входить в эти подробности), что числа $q+p\sqrt{-3}$ и $q-p\sqrt{-3}$ не могут иметь общих делителей того же вида. Таким образом каждое из этих чисел должно быть кубом некоторого числа, и нетрудно

убедиться, что эти новые числа должны отличаться друг от друга только знаком при $\sqrt{-3}$; в самом деле, полагая

$$q + p\sqrt{-3} = (t + u\sqrt{-3})^3, \tag{11}$$

мы непосредственно убеждаемся, что число $q - p\sqrt{-3}$ должно быть кубом числа $t - u\sqrt{-3}$.

Отсюда мы находим:

$$q^2 + 3p^2 = (q + p\sqrt{-3})(q - p\sqrt{-3}) = (t^2 + 3u^2)^3;$$

кроме того, раскрывая соотношение (11), мы получаем:

$$q = t^3 - 9tu^2 = t(t^2 - 9u^2),$$
$$p = 3t^2u - 3u^3 = 3u(t^2 - u^2).$$

7. Так как p — число нечетное, то последняя формула показывает нам, что u должно быть числом нечетным, а t — четным.

Так как, далее, число $\frac{1}{4}q$, а следовательно, и число $2q$, должно быть кубом целого числа, то выражение

$$2t(t^2 - 9u^2) = 2t(t + 3u)(t - 3u)$$

также должно быть кубом целого числа.

Три множителя $2t$, $t + 3u$ и $t - 3u$ этого произведения попарно не могут иметь общих делителей, в чем легко убедиться, замечая, что число t — четное и не может делиться на три, так как тогда и q делилось бы на три, в противоречие с нашим предположением. Отсюда следует, что каждый из этих множителей в отдельности должен быть кубом целого числа. Полагая

$$t + 3u = f^3,$$
$$t - 3u = g^3,$$
$$2t = h^3,$$

мы, очевидно, получаем:

$$f^3 + g^3 = h^3;$$

таким образом числа f, g и h также удовлетворяют уравнению (9); легко подсчитать, что эти новые числа по абсолютному значению меньше чисел x, y, z первоначальной тройки. Мы поэтому находимся в условиях применимости принципа бесконечного спуска и можем считать предложение доказанным.

8 *Второй случай* легко приводит нас к аналогичному заключению. Пусть q делится на три; положим $q=3r$; r, подобно q, должно быть четным числом и не может иметь общих делителей с p; так как

$$\frac{1}{4}q(q^2+3p^2)=\frac{3}{4}r(9r^2+3p^2)=\frac{9}{4}r(3r^2+p^2)$$

должно быть кубом целого числа и так как числа $\frac{9}{4}r$ и $3r^2+p^2$, как легко убедиться, не могут иметь общих делителей, то каждое из этих чисел в отдельности есть куб некоторого целого числа.

9. Из того, что $3r^2+p^2$ есть куб целого числа, мы, так же как в первом случае, заключаем, что

$$p=t(t^2-9u^2),$$
$$r=3u(t^2-u^2),$$

причем на этот раз, как легко видеть, t должно быть нечетным, а u — четным числом.

Последняя формула показывает, что r делится на три.

10. Из того, что $\frac{9}{4}r$ должно быть кубом целого числа, мы, помножая это число на $\frac{8}{27}$ и помня, что r делится на три, находим, что и

$$\frac{2}{3}r=2u(t+u)(t-u)$$

должно быть кубом целого числа. А так как множители $2u$, $t+u$ и $t-u$ этого произведения, очевидно, попарно не могут иметь общих делителей, то каждый из них в отдельности должен быть кубом целого числа. Полагая

$$2u=f^3,$$
$$t+u=g^3,$$
$$t-u=h^3,$$

находим:

$$f^3+h^3=g^3;$$

таким образом мы и во втором случае приходим к существованию новой тройки чисел, удовлетворяющих исходному уравне-

нию (9), и эти новые числа опять, как легко проверить, по абсолютной величине меньше первоначальных.

Таким образом мы во всех случаях приходим к возможности применять принцип бесконечного спуска и, следовательно, можем считать наше предложение окончательно доказанным.

6. РЕЗУЛЬТАТЫ КУММЕРА.

Как мы уже указывали, тот путь, которым мы шли в последних параграфах, позволил доказать теорему Ферма еще для нескольких частных случаев; но результатов сколько-нибудь общих на этом пути получить не удалось. Это заставило математиков искать других путей — идейно более сложных и технически более громоздких, лишь бы ими удалось получить результаты более общего характера.

Из всех достижений, полученных на этих путях, безусловно наиболее значительными являются результаты немецкого ученого Куммера, найденные им около середины прошлого столетия. Методы Куммера в особенности замечательны тем, что с помощью их удалось не только значительно продвинуть вперед разрешение загадки, оставленной нам гением Ферма, но и создать новую, стройную и цельную ветвь современной арифметики — теорию алгебраических чисел.

Разумеется, эта заслуга Куммера должна стоять на первом плане, ибо мы не должны забывать, что Великая теорема Ферма, несмотря на весь интерес, который она к себе вызывала и продолжает вызывать, все же является проблемой частного характера, то или иное решение которой само по себе вряд ли могло бы значительно расширить горизонт научной мысли в ее современном состоянии.

Здесь мы не имеем возможности сколько-нибудь подробно остановиться на работах Куммера и должны ограничиться самыми краткими указаниями и перечислением результатов. В дополнении основные идеи работ Куммера изложены более подробно, и к нему мы отсылаем читателя, желающего глубже проникнуть в этот интересный круг мыслей.

В своих работах Куммер исходил из разложения суммы x^p+y^p на множители:

$$x^p + y^p = (x + y)(x + \alpha y)(x + \alpha^2 y) \ldots (x + \alpha^{p-1} y), \qquad (12)$$

где α есть комплексное число, удовлетворяющее уравнению

$$\alpha^p = 1.$$

Это разложение хорошо известно из алгебры. Такая постановка вопроса сейчас же выводит нас из круга обыкновенных целых чисел и заставляет вступить в область чисел, подобных тем, с какими нам пришлось иметь дело в последнем параграфе; это прежде всего число α и его различные степени, затем — различные комбинации, получаемые сложением и вычитанием этих степеней; все эти числа, подобно числам вида

$$a + b\sqrt{-3},$$

с которыми мы встречались выше, называются *алгебраическими целыми числами*; вообще целым алгебраическим числом называется всякое число x, удовлетворяющее уравнению вида:

$$x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n = 0,$$

где

$$a_1,\ a_2,\ \ldots,\ a_n$$

суть какие-нибудь обыкновенные целые числа.

Целые алгебраические числа делятся на *области*; внутри каждой области (с одной из таких областей мы имели дело в предыдущем параграфе) имеют место законы делимости и разложения чисел на множители, во многом напоминающие (а часто и прямо повторяющие) аналогичные законы для обыкновенных целых чисел; но в одном пункте имеется замечательное различие: именно, всякое обыкновенное целое число, как мы знаем, может быть разложено на абсолютно простые множители *единственным образом*; *алгебраическое же целое число, вообще говоря, несколькими различными способами может быть разложено на простые множители*. Это обстоятельство делает теорию делимости для алгебраических чисел гораздо более сложной, чем для чисел обыкновенных; именно оно и послужило главным препятствием на пути к доказательству теоремы Ферма. Но вместе с тем это же обстоятельство дало повод Куммеру положить основание для стройной теории делимости алгебраических чисел — теории, составляющей в настоящее время одно из самых прекрасных созданий математической науки.

В формуле (12) сумма $x^p + y^p$ представлена в виде произведения множителей очень простого типа, в которых число α и его степени встречаются в качестве коэфициентов; это, естественно, наводит на мысль, что следует и самые числа x, y и z искать не в области одних только обыкновенных целых чисел, а в гораздо более широкой области алгебраических целых чисел, связанных с числом α; на первый взгляд кажется, что

задача этим усложняется; в самом деле, ведь Ферма хотел показать невозможность своего уравнения только для обыкновенных целых чисел; мы же, следуя Куммеру, хотим показать сверх того, что оно не может выполняться еще и для целой области алгебраических чисел. Но интуиция Куммера повела его по верному пути: кажущееся усложнение проблемы сторицею окупилось тем обилием новых идей и методов, с которыми мысль встретилась, как только задача была поставлена в той области, с которой она предметно по сущности своей была связана. Мы теперь приведем основной результат Куммера, причем формулируем его только для обыкновенных целых чисел.

Куммер доказал, что *уравнение* (8) *не допускает решения в целых, отличных от нуля числах, для целого ряда простых чисел* p, *в том числе для всех простых чисел, меньших, нежели* 100, т. е. кроме $p = 3, 5, 7$ (что было известно раньше), для

$$p = 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,$$
$$47,\ 53,\ 59,\ 61,\ 67,\ 71,\ 73,\ 79,\ 83,\ 89,\ 97.$$

Это, разумеется, представляет собою огромный шаг вперед; и не только потому, что значительно расширилась область показателей, для которых доказана теорема Ферма, но главным образом потому, что был, наконец, найден *общий метод*, позволяющий рассматривать зараз целые обширные группы показателей, вместо того чтобы строить доказательство для каждого показателя в отдельности, как это делалось в предшествующих работах.

По господствующему в настоящее время среди представителей науки мнению, полного решения проблемы Ферма следует вероятнее всего ожидать от систематического дальнейшего развития тех идей, основание которым было положено работами Куммера.

7. КРАТКИЙ ОБЗОР ДРУГИХ ВАЖНЕЙШИХ РЕЗУЛЬТАТОВ.

Мы теперь должны остановиться на одной группе попыток доказательства теоремы Ферма — попыток, приведших к довольно замечательным результатам и основанных на весьма простом замечании, которое еще в 1823 г. было высказано Лежандром и широко использовано последующими математиками вплоть до наших дней.

Перенося влево все члены уравнения (8) и замечая, что p — число нечетное и что знаки чисел x, y и z находятся в нашем распоряжении, мы можем формулировать утверждение Ферма

следующим образом: не существует трех целых, отличных от нуля чисел x, y и z, для которых

$$x^p + y^p + z^p = 0.$$

Очевидно (и в этом и состоит замечание Лежандра), что для того, чтобы в этом убедиться, достаточно показать, что для некоторого подходяще выбранного числа k выражение

$$x^p + y^p + z^p \tag{13}$$

не может делиться на k, каковы бы ни были целые, отличные от нуля числа x, y и z.

В самом деле, так как нуль делится на любое число, то тем самым будет показано, что число (13) не может обращаться в нуль. Таким образом вместо изучения величины числа (13) мы обращаемся к изучению вопроса о его делимости на те или иные числа; а это, разумеется, сейчас же дает нам ряд новых способов для исследования вопроса.

За число k (выбором которого мы можем, понятно, распоряжаться как нам угодно) в большинстве случаев принимался показатель p. Реже, но зато с более значительным успехом, выбирались абсолютно простые числа, дающие единицу в остатке при делении на p (т. е. имеющие вид $np+1$); пользовались с успехом и простыми числами вида $2np+1$.

Характерным для всех этих попыток является то, что при этом приходится отказаться от рассмотрения таких возможных решений уравнения (8), в которых одно из трех чисел (x, y, z) может делиться на p. Таким образом, если вообще что-нибудь удается доказать, то полученный результат всегда гласит так: *Уравнение* (8) *при данном значении числа p не может иметь таких целых положительных решений x, y, z, в которых ни одно из этих трех чисел не делится на p.* Однако с этим ограничением теорему можно считать доказанной для очень многих значений p. В недавней сводке работ по этому вопросу Диксон показывает, что *за исключением числа* $p = 6857$ *этот случай (т. е. отсутствие решений, не делящихся на p) доказан для всех простых чисел p, не превышающих* 7000.

Что касается возможных решений, в которых одно из чисел x, y, z может делиться на p, по этому вопросу известно то, что дают работы Куммера, рассмотренные в предыдущем параграфе.

Было замечено, что, принимая за k абсолютно простое число вида $2np + 1$, довольно часто удается показать, что выражение

(13) может делиться на k только в том случае, если по крайней мере одно из трех чисел x, y и z делится на k; это обстоятельство в свое время дало надежду притти к доказательству теоремы Ферма следующим путем: показать, что для всякого абсолютно простого числа p найдется среди чисел вида

$$k = 2np + 1$$

бесчисленное множество абсолютно простых чисел, обладающих только что указанным свойством [т. е. таких, что выражение (13) может делиться на k не иначе, как при условии, что одно из трех чисел x, y и z делится на k]. Если бы это удалось показать, то отсюда теорема Ферма следовала бы в нескольких словах; в самом деле, если бы уравнению (8) удовлетворяла какая-нибудь тройка чисел x, y и z, то, так как нуль делится на любое число, отсюда вытекало бы, что для любого из чисел k упомянутого бесконечного множества выражение (13), составленное для выбранной тройки, должно было бы делиться на k; а это в свою очередь на основании того, что мы предположили доказанным, сейчас же приводит нас к тому, что по меньшей мере одно из чисел x, y и z должно иметь бесконечное множество различных абсолютно простых делителей, что, очевидно, нелепо.

Однако на этом пути не только не удалось доказать теоремы Ферма, но, более того, удалось убедиться, что путь этот в отношении к данной цели является безнадежным. Именно Диксон доказал следующую интересную теорему, которую мы приводим ввиду того интереса, который она возбудила среди математиков, работающих над проблемой Ферма (хотя значение теоремы Диксона для этой проблемы — чисто отрицательное): *каково бы ни было абсолютно простое число p, для всякого достаточно большого абсолютно простого числа k найдутся три числа x, y, z, не делящихся на k, и таких, что выражение* (13) *делится на k.*

Очевидно, что теорема Диксона обнаруживает безнадежность намеченного нами пути, ибо из нее следует, что чисел k, о которых мы выше упоминали, для каждого p может существовать лишь конечное число (если они вообще существуют).

Наконец следует еще указать на интересные работы Вифериха и Мириманова, обратившие на себя большое внимание простотою своих результатов. Виферих доказал следующее:

Для того чтобы уравнение (8) *могло быть решено в целых числах x, y, z, не делящихся на p, нужно, чтобы число*

$$2^p - 2$$

делилось без остатка на p^2.

Так как не было известно простых чисел, удовлетворяющих этому условию, то были основания предполагать, что таких чисел нет вовсе. Проф. Граве во втором издании своего «Элементарного курса теории чисел» (1913 г., стр. 315) сообщил, что ему известно, что таких чисел не существует; однако соответствующее доказательство, насколько мне известно, обнародовано не было. Но в том же 1913 г. Мейсснер нашел абсолютно простое число, именно $p = 1093$, для которого условие Вифериха фактически выполняется.

Мириманов доказал, между прочим, что в условиях теоремы Вифериха не только $2^p - 2$, но и число

$$3^p - 3$$

должно делиться на p^2.

Те исследования, о которых мы сообщали в настоящем параграфе, почти все проведены совершенно элементарными методами, но ни в одном из них не применяется «метод бесконечного спуска». Поэтому естественно возникает вопрос о том, насколько методы тех или других из числа этих исследований могут оказаться родственными тому пути, которым шел сам Ферма в своем доказательстве.

Существует мнение, что Ферма мог найти свое доказательство на пути, не очень далеком от указанного ряда исследований. Может быть, его гению удалось каким-либо искусным приемом сразу достигнуть того, к чему в первую очередь стремятся современные математики: доказать, что уравнение (8) не может удовлетворяться целыми числами, не делящимися на p. Допускают, что если это так, то вторую часть теоремы, т. е. невозможность уравнения (8) в предположении, что одно из чисел x, y, z делится на p, Ферма мог доказать именно методом спуска (повидимому, этот случай проблемы наиболее приспособлен для применения метода спуска).

Допускают, однако, и то, что доказательство Ферма (если только оно не содержало ошибки) могло быть построено на совершенно других основаниях; может быть, не напрасно сам автор в других случаях сдержанный в своих оценках, назвал его «удивительным доказательством».

8. НОВЫЙ АНГЛИЙСКИЙ МЕТОД В АДДИТИВНОЙ ТЕОРИИ ЧИСЕЛ.

Все исследования, о которых мы до сих пор говорили (включая и работы Куммера), пользовались методами элементарными в том смысле, что для решения арифметических задач привлека-

лись только арифметические и алгебраические средства. Между тем современная теория чисел, вообще говоря, для доказательства своих предложений широко пользуется средствами анализа: теорией пределов, бесконечных рядов и произведений, теорией функций и вообще всем тем арсеналом орудий, который дается изучением непрерывного изменения величин. И вот, в применении к интересующей нас задаче, нам не известно в литературе ни одной попытки подхода, которая опиралась бы на тот или иной *аналитический* путь. Как это объяснить?

Великая теорема Ферма принадлежит к числу предложений так называемой *аддитивной* теории чисел. Так называется ветвь арифметики, изучающая законы, по которым числа могут быть составлены из слагаемых того или иного вида, в противоположность *мультипликативной* теории, занимающейся изучением того, как числа составлены из множителей.

И вот, если теория чисел по справедливости считается одной из труднейших ветвей математики, если о ней часто говорят, что она, несмотря на древнее свое происхождение, еще не нашла своего метода, — то все это в особенности верно по отношению к аддитивной теории. Здесь в сущности до самого последнего времени не было ничего, что могло бы объединить между собою отдельные разрозненные достижения этой науки, да и самых достижений этих было очень немного (проблема Ферма представляет собою далеко не единственную простую задачу этой области, до сих пор сопротивляющуюся всем попыткам решения). В частности, попытки применения средств анализа к сколько-нибудь глубоким задачам этой области до сих пор почти никогда не приводили к цели.

Однако существует один очень старый, принадлежащий еще Эйлеру, аналитический метод, позволяющий найти по крайней мере первый аналитический подход ко всякой почти задаче аддитивной теории чисел. Мы в нескольких словах изложим сущность этого метода на примере проблемы Ферма, причем мы предполагаем у читателя знакомство с основными понятиями теории степенных рядов.

Рассмотрим бесконечный ряд

$$x^{1^p} + x^{2^p} + \ldots + x^{n^p} + \ldots, \qquad (14)$$

где x — комплексное переменное, а p — то самое абсолютно простое число, которое встречается в уравнении (8); известно, что ряд этот будет сходиться, коль скоро $|x| < 1$, и сумма его будет, следовательно, некоторой функцией комплексного переменного

x, которую мы обозначим через $f(x)$. Известно, что функция $[f(x)]^2$ также будет разлагаться в степенной ряд и что этот новый степенной ряд

$$a_1x + a_2x^2 + \ldots + a_nx^n + \ldots$$

мы получим, если ряд (14) помножим на самого себя так, как в алгебре перемножаются многочлены. Так как при перемножении различных степеней переменного x показатели складываются, то ясно, что коэфициент a_n последнего ряда будет представлять собою число, показывающее, сколькими различными способами число n может быть представлено в виде

$$k^p + l^p,$$

где k и l — целые положительные числа.

Чтобы доказать теорему Ферма, достаточно поэтому установить, что a_n обращается в нуль всякий раз, как число n имеет вид m^p, где m — целое.

С другой стороны, теория функций комплексного переменного дает нам средства выражать коэфициенты степенного ряда через значения функции, им представляемой; таким образом проблема сводится к изучению свойств функции $f(x)$; к сожалению, функция эта является весьма сложной; правда, путем ряда преобразований удается свести проблему к изучению других функций, с которыми специалисты по аналитической теории чисел гораздо лучше знакомы; но решение проблемы требует детального знания таких тонких свойств этих функций, какое совершенно недоступно современному состоянию науки, и, по всей вероятности, может быть добыто только постепенными систематическими усилиями ряда поколений. И надо сказать, что метод Эйлера, соблазнительный на первый взгляд, каждый раз, когда его пытались применять к конкретным задачам, приводил к неодолимым трудностям; вследствие этого он, как безнадежный, был уже давно почти совсем оставлен математиками, занимавшимися аддитивной теорией чисел.

И вот совсем недавно, уже после мировой войны, метод этот внезапно был воскрешен и, подкрепленный всем арсеналом современных знаний в области математического анализа, с новыми силами и новой, юношеской свежестью дал ряд неожиданных и блестящих результатов, и притом отчасти в подходе к проблемам, к которым, несмотря на их значительную давность, до тех пор решительно никаких подходов не существовало и которые, стало быть, находились в положении более печальном,

чем проблема Ферма. Так обстояло дело, например, с так называемой первой проблемой Гольдбаха: *доказать, что всякое четное число кроме двух может быть представлено как сумма двух абсолютно простых чисел.* Доказательства этой теоремы (кстати сказать, по возрасту немного уступающей теореме Ферма) мы не имеем до сих пор; но уже после первых работ в новом направлении определенно чувствуется, что данная задача, к которой раньше мы не знали никаких подходов, наконец схвачена крепким, могучим и многообещающим методом.

Творцы нового метода — английские математики Харди и Литтльвуд и молодой индус Рамануйян (недавно безвременно скончавшийся). Сущность и сила нового метода заключается в том, что он дает способ изучения функций, определяемых степенными рядами [функция $f(x)$ в нашем примере], в областях, близких к кругу сходимости ряда, т. е. там, где поведение функции наиболее сложно.

О значении нового метода читатель может судить по словам одного из наиболее выдающихся современных работников теории чисел, проф. Ландау, который заканчивает свой реферат об этом методе такой фразой: «Я счастлив, что мне удалось дожить до того времени, когда аддитивная теория чисел обрела себе метод».

Я счел полезным сообщить читателю об этом новом методе, хотя в направлении теоремы Ферма этот метод до сих пор не дал еще ничего. Даст ли он что-нибудь в будущем? Трудно сколько-нибудь уверенно ответить на этот вопрос, но необходимо учитывать, что большинство проблем, решенных этим методом до сих пор, ставилось так, что требовалось доказать *возможность* представления того или иного числа в виде суммы слагаемых определенного вида. В теореме Ферма речь идет напротив, о *невозможности* некоторого представления. Этот «отрицательный» характер проблемы делает ее значительно более трудной для нового метода; но в принципе подход к ней средствами нового метода возможен и, несомненно, в ближайшее время будет испробован.

9. ЗАКЛЮЧЕНИЕ.

Задача, которую гений Ферма поставил грядущим поколениям, остается, таким образом, нерешенной.

Для всякого, кто интересуется теоремой Ферма не с одной только спортивной стороны, должен возникнуть основной вопрос: какое место занимает эта теорема в ряду актуальных математических задач современности, и какое место займет она

в сокровищнице наших знаний, если когда-нибудь будет доказана?

Мы уже указывали (да это и непосредственно ясно), что задача доказательства теоремы Ферма сама по себе есть весьма частная проблема аддитивной теории чисел. Но если так, то стоит ли она тех усилий, которые на нее тратятся, стоит ли того усиленного внимания, какое уделяют ей математики вот уже почти три столетия?

Вспомним, что Куммер, пытаясь доказать Великую теорему, положил основание одному из самых стройных и законченных зданий современной арифметики.

Случайно ли обязаны мы возникновением этого здания теореме Ферма? Есть некоторые основания полагать, что это не случайно. Размышляя о Великой теореме Ферма, математический ум неизменно чувствует себя в кругу самых острых и существенных соотношений и закономерностей, какие только знает арифметика. Откуда является это чувство, чем оно обосновано и что оно нам может обещать, о чем свидетельствовать?

Основу арифметики составляют арифметические действия, или операции. Первую ступень этих действий образует сложение (обратное действие — вычитание), вторую — умножение (обратное — деление), третью — возведение в степень (обратные действия — извлечение корня и логарифмирование). Законы этих операций и соотношения между ними составляют в сущности задачу арифметики. И вот история арифметики обнаружила факт чрезвычайной важности: в то время как понятия, возникающие из действий одной и той же ступени, оказываются связанными между собою весьма простыми законами и обнаружение этих законов не вызывает никаких затруднений, — в то же самое время связь между операциями различных ступеней и между понятиями, возникающими из этих операций, оказывается часто столь трудно поддающейся обнаружению, что ум чувствует себя перед лицом неразрешимой проблемы. Кажется, что понятия, например, аддитивной и мультипликативной теории чисел столь далеки друг от друга, как будто бы они были взяты из двух научных дисциплин, не имеющих между собою ничего общего. И часто приходится для доказательства той или иной закономерности прибегать к анализу — области, глубоко чужеродной арифметике, — как к связующему звену, чтобы соединить понятия, возникшие из общего лона целого числа, но упорно не желающие признавать своего родства, не желающие иметь ничего общего друг с другом. Так, задача о том, содержит ли всякая арифметическая прогрессия бесконечное множество

абсолютно простых чисел, — эта задача, в своей постановке доступная каждому школьнику, до сих пор не получила чисто арифметического решения и могла быть решена только с помощью методов анализа, выходящих далеко за пределы арифметики; и трудность, присущая этой задаче, коренится, как знает каждый, кто над ней думал, именно в том, что здесь требуется найти закономерность, связывающую аддитивное понятие арифметической прогрессии с чисто мультипликативным понятием абсолютно простого числа. Совершенно то же самое можно сказать и о вышеприведенной проблеме Гольдбаха, представляющей собою типичную аддитивно-мультипликативную задачу.

То, что мы констатировали сейчас для понятий, связанных с операциями первой и второй ступени, дает себя чувствовать в еще большей степени, когда мы пытаемся связать между собою две ступени несоседние — первую и третью.

Мы не можем долго останавливаться на примерах, но достаточно упомянуть в этом ряду задач хотя бы знаменитую проблему Варинга, чисто арифметического решения которой мы тоже до сих пор не имеем (и лучшее решение которой, между прочим, получено Харди и Литтльвудом с помощью их нового метода).

Почти всегда бывало так, что те трудности, на какие мы сейчас указывали, оказывались сопряженными со значительностью (иногда не бросающейся в глаза) и чрезвычайной плодотворностью проблемы. Решение задачи об арифметической прогрессии, найденное Дирихле, помимо своего предметного значения является теперь классическим по своему методу, обогатившему науку целым рядом новых открытий. Решение проблемы Варинга Харди и Литтльвудом (не первое по времени, но лучшее по точности результата) совпало с созданием метода, обещающего стать одним из самых сильных в теории чисел. Наконец, здесь следует упомянуть и формулу бинома, открытую Ньютоном и всем хорошо известную, которая ведь представляет собою одну из простейших связей между действиями первой и третьей ступени и значение которой для арифметики хорошо известно и, по всей вероятности, еще далеко не исчерпано. Можно было бы указать еще ряд других примеров.

Но вернемся к Великой теореме Ферма. Что мы в ней увидим с нашей новой точки зрения? Одну из самых простых, естественных, непосредственно приходящих в голову задач о связи операций первой и третьей ступени! В самом деле, если мы задумаемся над этой связью, сможем ли мы придумать сразу вопрос более простой, чем этот: может ли сумма одинаковых

степеней двух чисел равняться такой же степени некоторого третьего числа? А это ведь и есть проблема Ферма.

Мы теперь склонны понять и простить ей ее трудность. Но вместе с тем мы понимаем и то чувство высокой значительности, которое охватывает всякого ученого, стремящегося проникнуть в загадку Великой теоремы, ибо он стоит перед лицом самых основ арифметики, перед лицом тех величайших законов, которыми управляется мир чисел и на которых основано все наше знание об этом мире.

ДОПОЛНЕНИЕ.

ПОДРОБНОЕ ИЗЛОЖЕНИЕ ИССЛЕДОВАНИЙ КУММЕРА.

В настоящем дополнении мы имеем в виду подробно изложить основную работу Куммера, содержащую доказательство теоремы Ферма для всех *регулярных* простых показателей, — работу, справедливо почитающуюся самым значительным из всего, что до сих пор сделано в направлении к доказательству Великой теоремы. Это изложение представляется нам не лишним по той причине, что мы не знаем не только в русской, но и в иностранной литературе такого изложения этого безусловно классического произведения, которое было бы доступно читателю, хотя бы даже знакомому с элементами теории алгебраических областей, но не являющемуся искушенным специалистом в этой ветви арифметики. Работа самого Куммера, помимо того, что она доступна только такому специалисту, содержит еще ряд неточностей и пробелов, заполнить которые может только хороший знаток; прекрасное изложение Гильберта в его известном «Bericht...» помещено в самом конце и для своего усвоения требует предварительного изучения всей огромной работы, написанной сжато и также с расчетом на знатока; наконец, имеющее претензию на популярность изложение Бахмана в его недавно вышедшей книге, специально посвященной теореме Ферма, настолько недоброкачественно в отношении логической отчетливости и строгости, что даже знатока может поставить втупик. Пусть читатель судит, в какой мере приводимое ниже изложение является удовлетворительным.

Мы в этом дополнении должны предполагать читателя имеющим некоторое арифметическое образование. Вполне ясным все последующее будет для читателя, знакомого хотя бы с элементами теории идеалов; на случай, если читатель этой теории не знает, мы в первом параграфе собрали все необходимые определения и теоремы (следовательно, читатель, знакомый с теорией идеалов, может этот первый параграф пропустить); формально читатель найдет здесь все необходимое; по существу

же, конечно, невозможно таким образом усвоить теорию, о которой не знаешь ничего, и мы хотели бы, чтобы в таком случае этот первый параграф послужил для читателя стимулом к изучению хотя бы элементов этой теории.

Наконец, совершенно необходимым минимумом для понимания последующего является знакомство с обычным университетским курсом теории чисел в объеме примерно учебника Д. Ф. Егорова.

Второй параграф содержит специальные сведения из теории простых круговых областей; в третьем помещено доказательство теоремы Куммера.

1. Необходимые сведения из общей теории алгебраических областей.

1. Число x называется *алгебраическим*, если оно удовлетворяет уравнению.

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0 \qquad (15),$$

где все a — обыкновенные целые числа; алгебраическое число x называется *целым*, если в уравнении (15) $a_n = 1$; целые алгебраические числа мы будем обозначать малыми латинскими и греческими буквами. В отличие от алгебраических иррациональных чисел обыкновенные целые числа называются *целыми рациональными*.

Сумма, разность и произведение двух целых алгебраических чисел также суть целые алгебраические числа.

2. Если x есть алгебраическое число, то совокупность чисел вида

$$\frac{\alpha_0 + \alpha_1 x + \cdots + \alpha_k x^k}{\beta_0 + \beta_1 x + \cdots + \beta_l x^l},$$

где все α и β—целые рациональные числа, называются *областью, определяемой числом* x, и обозначается через $K(x)$; все рациональные числа принадлежат всякой алгебраической области; сумма, разность, произведение и частное двух чисел*) какой-либо области также принадлежат этой области.

3. Если число x таково, что числа x и $\frac{1}{x}$ оба целые, то оно называется *единицей* данной области; область рациональных чи-

*) В случае частного надо, конечно, чтобы делитель был отличен от нуля.

сел содержит только две единицы: $+1$ и -1; алгебраическая область, вообще говоря, содержит бесконечное множество единиц; произведение и частное двух единиц есть всегда единица.

4. Делимость целых чисел данной области определяется совершенно так же, как для целых рациональных чисел. Два числа, делящиеся друг на друга, называются *ассоциированными*: их отношение есть, конечно, единица области; условимся называть целое число *простым* или *абсолютно простым*, если оно в данной области не имеет других делителей, кроме единиц и ассоциированных чисел, и само не есть единица; каждое число имеет лишь конечное число простых делителей (если не различать ассоциированных чисел); каждое число разлагается на произведение простых множителей, но, как мы уже знаем, вообще говоря, *не единственным образом*, даже при том условии, если мы не будем различать между собою ассоциированных чисел; в этом лежит главная трудность арифметической теории алгебраических чисел, и для преодоления ее, для того чтобы вернуть алгебраическим числам их однозначную разложимость, и создана Куммером та теория идеалов, к изложению основ которой мы сейчас переходим.

5. Пусть x — целое число некоторой области. Обозначим через (x) совокупность всех целых чисел данной области, делящихся на x; очевидно, что совокупность (x) однозначно определяет собою число x, из которого она возникла (если не различать чисел ассоциированных); совокупность эта обладает, очевидно, следующими важными свойствами:

1°. Сумма и разность любых двух чисел этой совокупности также принадлежат ей.

2°. Вместе с числом y этой совокупности принадлежит и всякое число данной области, делящееся на y.

Допустим теперь, наоборот, что нам дана некоторая совокупность I целых чисел данной области, про которую известно только, что она обладает свойствами 1° и 2°; можем ли мы, обратно, утверждать, что все числа совокупности I делятся на одно и то же число x и все числа, делящиеся на x, входят в эту совокупность? В области рациональных чисел — можем; в алгебраической области, вообще говоря, нет; и в этом лежит причина отсутствия однозначной разложимости.

Условимся теперь называть *идеалом* всякую совокупность I целых чисел данной области, обладающую свойствами 1° и 2°; в частности, совокупность (x) чисел, делящихся на число x, есть, как мы видели, идеал; такой идеал мы будем называть *главным идеалом*; в области, где все идеалы главные (например

в области рациональных чисел), существует однозначность разложения чисел на простые множители.

Идеалы мы вообще будем обозначать большими латинскими буквами; иногда мы будем обозначать через (x) главный идеал, определяемый числом x.

6. Если число x делится на число y, то все числа идеала (x) принадлежат к идеалу (y), как это непосредственно очевидно; мы будем в этом случае говорить, что идеал (x) *делится* на идеал (y).

Это сейчас же позволяет нам обобщить понятие делимости и на случай не главных идеалов; мы скажем, что идеал I *делится* на идеал I', если все числа первого входят и в последний; если идеал (x) делится на идеал I, то мы будем также говорить, что *число x делится на идеал I*; очевидно, эта делимость равносильна тому, что число x входит в состав идеала I.

Идеалы можно перемножать между собою. Какой идеал мы будем называть произведением двух данных идеалов, — на этом мы здесь останавливаться не будем. Важно то, что если идеал I делится на идеал K, то всегда найдется такой идеал L, что

$$I = KL;$$

этот факт, который в обычной арифметике есть определение делимости, в теории идеалов является теоремой (ибо здесь делимость, как мы видели, определяется существенно иным путем).

Наибольшим общим делителем двух идеалов называется такой их общий делитель, который делится на всякий другой их общий делитель.

7. Совокупность *всех* целых чисел данной области, очевидно, есть идеал; этот идеал мы будем обозначать через 1 и называть *основным идеалом* данной области. Он играет в теории делимости роль единицы, ибо на него делится всякий другой идеал, в силу принятого нами определения делимости. Идеал P, отличный от 1 и не имеющий других делителей кроме P и 1, мы будем называть *простым* или *абсолютно простым идеалом*.

Основная теорема теории идеалов состоит в том, что *всякий идеал может быть единственным образом представлен в виде произведения простых идеалов*. В частности, всякий главный идеал, иначе говоря, всякое целое число области единственным образом разлагается на произведение простых идеалов. Таким образом в известном смысле алгебраическим числам присуща, при этом расширенном их понимании, однозначность разложения на простые множители.

8. Два идеала I_1 и I_2 данной области называются *эквивалентными*,

$$I_1 \sim I_2,$$

если в данной области существуют два таких целых числа α_1 и α_2, что

$$I_1(\alpha_1) = I_2(\alpha_2);$$

два идеала, в отдельности эквивалентных третьему, эквивалентны между собою; это позволяет объединить все идеалы, эквивалентные между собою, в один *класс*. Все главные идеалы, очевидно, составляют один класс; этот класс называется *главным* классом, и легко убедиться, что и, обратно, этот класс содержит только главные идеалы. В областях, где числа однозначно разлагаются на простые множители, — все идеалы главные, и существует только один класс — главный; в общем случае *число классов всегда конечно*, и в этом одно из самых важных предложений теории идеалов. Соотношения эквивалентности

$$I_1 \sim I_2$$

обладают многими свойствами равенств; так, их можно почленно перемножать, а следовательно, в частности можно возводить в одну и ту же степень обе части такого соотношения.

Далее, весьма важную роль в теории идеалов играет число классов данной области, которое, как мы уже заметили, всегда конечно и которое мы будем обозначать через h. Отметим одно важное предложение, связанное с этим числом: *для любого идеала идеал I^h есть главный идеал.*

9. Сравнение

$$\alpha \equiv \beta \,(\mathrm{mod.}\, I)$$

по модулю, который есть идеал, означает, что разность $\alpha - \beta$ или, что то же, идеал $(\alpha - \beta)$ делится на идеал I; сравнения по идеальному модулю подчиняются всем тем законам, какие имеют место для обычных сравнений.

2. Необходимые сведения из теории круговых областей.

Мы должны теперь сообщить некоторые сведения из теории алгебраических областей одного специального типа, называемых *круговыми областями*.

1. Пусть p — нечетное (рациональное) абсолютно простое число, и α — один из комплексных корней уравнения

$$\alpha^p = 1;$$

алгебраическая область $K(\alpha)$ называется *круговой областью* (в связи с той ролью, какую играет число α в геометрической задаче деления круга на равные части). Число α есть единица этой области, так как α и $\alpha^{-1} = \alpha^{p-1}$ суть числа целые.

2. Можно показать, что всякое целое число области $K(\alpha)$ может быть представлено как многочлен, расположенный по степеням α, с целыми рациональными коэфициентами; ясно, что, обратно, всякий такой многочлен представляет собою целое число области $K(\alpha)$.

3. Положим

$$\lambda = 1 - \alpha;$$

из п. 2 ясно, что всякое целое число β области $K(\alpha)$ может быть представлено в виде:

$$\beta = a + a_1\lambda + a_2\lambda^2 + \dots,$$

где все a — целые рациональные числа.

4. Мы будем в дальнейшем обозначать через $e(\alpha)$ различные единицы области $K(\alpha)$.

Теорема. Если g есть целое положительное число, не делящееся на p, то число

$$\frac{1-\alpha^g}{1-\alpha}$$

есть единица области $K(\alpha)$.

В самом деле, прежде всего написанное число — целое, так как числитель даже алгебраически делится на знаменатель. Далее, находя такое целое положительное число k, чтобы

$$gk \equiv 1 \pmod{p},$$

мы получаем $gk - lp = 1$ (l — целое рациональное), и

$$1-\alpha = 1-\alpha^{gk-lp} = 1-\alpha^{gk},$$

$$\frac{1-\alpha}{1-\alpha^g} = \frac{1-\alpha^{gk}}{1-\alpha^g};$$

здесь снова числитель алгебраически делится на знаменатель, и следовательно теорема доказана.

5. Приведем без доказательства следующее предложение:

Всякая единица $e(\alpha)$ области $K(\alpha)$ может быть представлена в виде:

$$e(\alpha) = \alpha^s \varepsilon(\alpha),$$

где s — целое рациональное число, а $\varepsilon(\alpha)$ — *действительная единица* области $K(\alpha)$.

6. Приведем также без доказательства следующее предложение:

Если некоторая единица $e(\alpha)$ области $K(\alpha)$ по модулю p сравнима с каким-нибудь целым рациональным числом, то она может быть представлена в виде:

$$e(\alpha) = [e_1(\alpha)]^p,$$

где $e_1(\alpha)$ есть некоторая другая единица области $K(\alpha)$ *).

7. Из тождественного относительно x соотношения

$$\frac{x^p - 1}{x - 1} = \{x - \alpha\}\{x - \alpha^2\} \ldots \{x - \alpha^{p-1}\}$$

мы, заставляя x стремиться к единице, получаем в пределе:

$$p = \{1 - \alpha\}\{1 - \alpha^2\} \ldots \{1 - \alpha^{p-1}\} =$$

$$= \{1 - \alpha\}^{p-1} \cdot \frac{1 - \alpha^2}{1 - \alpha} \cdot \frac{1 - \alpha^3}{1 - \alpha} \cdots \frac{1 - \alpha^{p-1}}{1 - \alpha},$$

или на основании теоремы п. 4 настоящего параграфа

$$p = e(\alpha)\lambda^{p-1};$$

переходя к идеалам, мы получаем:

$$(p) = (\lambda)^{p-1} = L^{p-1},$$

где через L обозначен главный идеал (λ); можно показать, что этот идеал абсолютно простой. Всякое целое рациональное число, делящееся на идеал L, должно быть кратным p.

8. Назовем *полупервичным* **) такое целое число области $K(\alpha)$, которое, во-первых, не делится на идеал L и, во-вторых, сравнимо с некоторым рациональным целым числом (также, разумеется, не делящимся на L) по модулю L^2.

Теорема. Всякое целое число области $K(\alpha)$, не делящееся на L, можно сделать полупервичным, умножая его на некоторую целую положительную степень числа α.

---

*) Это предложение имеет место только для *регулярных* чисел p (определение см. ниже); но мы только с такими и будем иметь дело в дальнейшем.

**) Этот термин, звучащий непонятно в нашем конспективном изложении, мы сохранили, чтобы не расходиться с обычной терминологией.

В самом деле, обозначая данное число через β, мы имеем на основании п. 3 настоящего параграфа:

$$\beta \equiv a + a_1\lambda \pmod{L^2},$$

где a и a_1 — целые рациональные числа, не делящиеся на L; обозначая через k целое положительное число, будем иметь:

$$\begin{aligned}\alpha^k\beta &\equiv \alpha^k a + \alpha^k a_1\lambda \\ &\equiv \{1-\lambda\}^k a + \{1-\lambda\}^k a_1\lambda \\ &\equiv a + \{a_1 - ka\}\,\lambda \pmod{L^2};\end{aligned}$$

выбирая же k, что всегда возможно, так, чтобы было

$$ak \equiv a_1 \pmod{p},$$

мы будем иметь:

$$\alpha^k\beta \equiv a \pmod{L^2}$$

(так как p делится на L^2), чем теорема и доказана.

9. Обозначим через h число классов (п. 8 предыдущего параграфа) области $K(\alpha)$. Простое число p называется *регулярным*, если h не делится на p. Куммеру принадлежит доказательство следующего признака, позволяющего для каждого данного простого числа p решить вопрос о том, будет ли оно регулярным или нет.

Для того чтобы данное нечетное, абсолютно простое (рациональное) число p было регулярным, необходимо и достаточно, чтобы ни одно из первых $\frac{p-3}{2}$ чисел Бернулли

$$B_1,\ B_2,\ \ldots,\ B_{\frac{p-3}{2}}$$

не делилось на p.

Мы упомянули об этом признаке лишь для того, чтобы показать, что задача о регулярности данного простого числа p может быть всегда практически решена.

В дальнейшем мы нигде на этот признак опираться не будем, так что читатель, незнакомый с числами Бернулли, может спокойно забыть о нем.

3. Доказательство основной теоремы Куммера.

Мы теперь допустим, что абсолютно простое число p — регулярное и что $p \geqslant 7$ (случаи $p = 3$ и $p = 5$, как мы знаем, исчер-

нывающе решены элементарными способами). В этих предположениях требуется доказать, что уравнение

$$x^p + y^p + z^p = 0 \tag{16}$$

не может быть решено в целых рациональных, отличных от нуля числах. Напишем это уравнение в виде:

$$x^p + y^p = (-z)^p$$

и представим левую часть его в виде:

$$x^p + y^p = (x+y)\ (x+\alpha y)\ (x+\alpha^2 y) \ldots (x+\alpha^{p-1} y),$$

где α — первообразный корень уравнения

$$\alpha^p = 1,$$

т. е. первообразный *) корень из единицы степени p; тем самым мы вступаем в область алгебраических чисел $K(\alpha)$; как мы уже заметили выше, это обстоятельство наводит нас на мысль, что область $K(\alpha)$ является естественной областью интересующей нас проблемы; и действительно, в доказательстве Куммера является основною эта идея расширения той области, в какой мы ставим задачу. Итак, нашей целью будет показать, что *уравнение* (16) *не имеет решений в целых, отличных от нуля, числах области* $K(\alpha)$.

Положим $\lambda = 1 - \alpha$ и обозначим через L главный абсолютно простой идеал (λ) нашей области. Мы должны с самого начала различать два случая, требующих совершенно раздельного рассмотрения.

Первый случай. Допустим, что уравнение (8) удовлетворяется тремя целыми числами x, y, z области $K(\alpha)$, *ни одно из которых не делится на* L. Так как все три числа входят в это уравнение только в степени p и так как $\alpha^p = 1$, то уравнение останется в силе, если мы каждое из трех чисел x, y, z помножим на любую степень числа α; это обстоятельство, в связи с п. 8 предыдущего параграфа, позволяет нам с самого начала считать все три числа x, y и z *числами полупервичными*.

Напишем уравнение (16) в виде:

$$(x+y)(x+\alpha y)(x+\alpha^2 y) \ldots (x+\alpha^{p-1} y) = (-z)^p$$

и обозначим через D идеал, являющийся наибольшим общим делителем чисел x и y. Если какие-нибудь два из множителей

*) Так как число p простое, то первообразным является всякий комплексный корень.

левой части, например $x+\alpha^m y$ и $x+\alpha^n y$, делятся на какой-нибудь простой идеал P, то и выражения

$$(\alpha^m - \alpha^n)x \text{ и } (\alpha^m - \alpha^n)y$$

должны на него делиться, а так как

$$\alpha^m - \alpha^n = \alpha^m(1 - \alpha^{n-m}) = \alpha^m \frac{1-\alpha^{n-m}}{1-\alpha} \cdot (1-\alpha)$$

и так как

$$\alpha^m \frac{1-\alpha^{n-m}}{1-\alpha}$$

на основании п. 4 предыдущего параграфа есть единица области, то и число $1-\alpha$ должно делиться на P, если только D не делится на P; но идеал

$$(1-\alpha) = L$$

простой, и следовательно (в случае, если D не делится на P)

$$P = L;$$

следовательно, число z должно было бы делиться на L, что противно нашему предположению.

Итак, полагая

$$(x + \alpha^k y) = DI_k \quad (k = 0,\ 1, \ldots, p-1)$$

и условившись во всем дальнейшем число, заключенное в круглые скобки, понимать как главный идеал, мы будем иметь:

$$D^p I_0, I_1, \ldots, I_{p-1} = (-z)^p, \tag{17}$$

где идеалы $I_0, I_1, \ldots, I_{p-1}$ попарно взаимно простые. Отсюда следует прежде всего, что z делится на D и что потому последнее равенство мы можем сократить на D^p. Из того, что при этом останется, следует, что каждый из идеалов I_k в отдельности должен представлять собою p-ю степень некоторого идеала; мы получаем:

$$I_k = J_k^p,$$

и соотношения

$$(x + \alpha^k y) = DI_k$$

принимают вид:

$$(x + \alpha^k y) = DJ_k^p \quad (k = 0,\ 1,\ 2, \ldots, p-1);$$

из этих соотношений мы получаем:

$$(x + \alpha^k y) J_{p-1}^p = (x + \alpha^{p-1} y) J_k^p \; (k = 0, \; 1, \ldots, p-2), \qquad (18)$$

а это показывает, что все идеалы J_k^p принадлежат одному классу

$$J_n^p \sim J_{p-1}^p \; (k = 0, \; 1, \ldots, p-2); \qquad (19)$$

с другой стороны, обозначая через h число классов области $K(\alpha)$, мы, как известно, имеем:

$$J_k^h \sim J_{p-1}^h \; (k = 0, \; 1, \ldots, p-2); \qquad (20)$$

число p, по условию, регулярно, т. е. h не делится на p; следовательно, найдутся такие целые числа u и v, что

$$up + vh = 1;$$

возводя соотношения (19) в степень u, а соотношения (20) в степень v и перемножая результаты, находим, что

$$J_k \sim J_{p-1} \; (k = 0, \; 1, \ldots, p-2),$$

т. е. все идеалы J_k — одного класса.

Итак, для каждого k ($k = 0, 1, \ldots, p-2$) найдутся два таких целых числа области $K(\alpha)$, α_k и β_k, что

$$J_{p-1}(\alpha_k) = J_k(\beta_k) \; (k = 0, \; 1, \; 2, \ldots, p-2);$$

при этом, очевидно, мы можем предположить, что числа α_k и β_k не делятся одновременно ни на какой главный идеал (ибо в противном случае мы могли бы сократить равенство); в частности они не будут оба делиться на идеал L; но тогда, очевидно, не может случиться и так, чтобы одно из этих чисел делилось на L, ибо тогда, как показывает последнее равенство, и один из идеалов J_k должен был бы делиться на L, а тогда на основании (17) и z делилось бы на L, что противоречит нашему предположению; итак, мы вправе предполагать, что ни одно из чисел α_k, β_k не делится на L.

В силу соотношений (18) последние равенства дают нам:

$$(x + \alpha^k y)(\beta_k^p) = (x + \alpha^{p-1} y)(\alpha_k^p) \; (k = 0, \; 1, \ldots, p-1);$$

эти равенства содержат только главные идеалы; переходя от идеалов к числам (что символически выполняется опусканием скобок, а там, где этого нельзя сделать, — заменой круглых ско-

бок фигурными), мы должны в одной из частей присоединить в качестве множителя некоторую (неизвестную нам) единицу области. Поэтому на основании п. 5 предыдущего параграфа мы получаем (обозначая через ε_k — *действительные* единицы области и через e_k — целые рациональные числа):

$$\{x+\alpha^k y\}\,\beta_k^p=\alpha^{e_k}\varepsilon_k\,\{x+\alpha^{p-1}y\}\,\alpha_k^p \quad (k=0,1,\ldots,p-1). \tag{21}$$

Эти соотношения послужат отправным пунктом наших дальнейших рассуждений; теперь же заметим, что на основании п. 3 предыдущего параграфа мы можем числа α_k и β_k, входящие в какое-либо из последних соотношений, представить в виде:

$$\alpha_k=a_k+\lambda A_k,\quad \beta_k=b_k+\lambda B_k,$$

где a_k и b_k — целые рациональные числа, не делящиеся на L, а A_k и B_k — целые числа области $K(\alpha)$.

Отсюда

$$\alpha_k^p=a_k^p+p\lambda M_k,$$
$$\beta_k^p=b_k^p+p\lambda N_k,$$

где M_k и N_k снова суть некоторые целые числа области $K(\alpha)$; так как $(\lambda)=L$ и $(p)=L^{p-1}$, то из этих равенств следует:

$$\left.\begin{aligned}\alpha_k^p&\equiv a_k^p\ (\mathrm{mod.}\ L^p),\\ \beta_k^p&\equiv b_k^p\ (\mathrm{mod.}\ L^p);\end{aligned}\right\} \tag{22}$$

так как b_k не делится на p, то найдется такое целое рациональное число c_k, что

$$b_kc_k\equiv a_k\ (\mathrm{mod.}\ p),$$

т. е.

$$b_kc_k=a_k+u_kp,$$

где u_k — целое рациональное число; отсюда

$$b_k^pc_k^p\equiv a_k^p\ (\mathrm{mod.}\ p^2),$$

и следовательно, подавно

$$b_k^pc_k^p\equiv a_k^p\ (\mathrm{mod.}\ L^p);$$

поэтому соотношения (22) дают нам:

$$\beta_k^pc_k^p\equiv\alpha_k^p\ (\mathrm{mod.}\ L^p). \tag{23}$$

Вернемся теперь к соотношениям (21); на основании п. 8 предыдущего параграфа мы можем найти такое целое рациональное число g, чтобы число

$$\gamma = \alpha^g \{x + \alpha^{p-1} y\}$$

было полупервичным: полагая $e_k - g = g_k$, мы будем иметь:

$$\alpha^{e_k} \{x + \alpha^{p-1} y\} = \alpha^{g_k} \gamma,$$

а потому можем переписать соотношения (21) в виде:

$$\{x + \alpha^k y\} \beta_k^p = \alpha^{g_k} \varepsilon_k \gamma \alpha_k^p \ (k = 0, 1, \ldots, p-2);$$

рассматривая же эти соотношения как сравнения по модулю L^p и пользуясь сравнениями (23), мы находим:

$$\{x + \alpha^k y\} \equiv \alpha^{g_k} \varepsilon_k \gamma c_k^p \pmod{L^p} \ (k = 0, 1, \ldots, p-2).$$

Эти сравнения останутся справедливыми, если в обеих частях мы всюду заменим α через α^{-1}; в самом деле, каждое из написанных сравнений имеет тот смысл, что разность левой и правой его частей делится на λ^p, но при указанной замене λ^p переходит в $-\lambda^p$; измененная разность, следовательно, должна делиться на $-\lambda^p$, а следовательно, и на L^p. Обозначая через x', y', γ', те числа, в которые соответственно переходят x, y и γ при указанной замене, и замечая, что ε_k и c_k при этом не изменяются, мы находим новую группу сравнений:

$$\{x' + \alpha^{-k} y'\} \equiv \alpha^{-g_k} \varepsilon_k \gamma' c_k^p \pmod{L^p}$$
$$(k = 0, 1, \ldots, p-2);$$

перемножая, наконец, крест-накрест соответствующие друг другу сравнения обеих групп, получаем:

$$\{x + \alpha^k y\} \gamma' \equiv \alpha^{2g_k} \{x' + \alpha^{-k} y'\} \gamma \pmod{L^p}$$
$$(k = 0, 1, \ldots, p-2). \qquad (24)$$

Так как числа x, y и γ — полупервичные, то мы можем представить их в виде:

$$x = m + \lambda^2 R,$$
$$y = n + \lambda^2 S,$$
$$\gamma = t + \lambda^2 T,$$

где числа m, n, и t — целые, рациональные и не делящиеся на L-, а R, S и T — некоторые целые числа нашей области; так как при замене α на α^{-1} число λ^{-2} переходит в $\alpha^{-2}\lambda^{-2}$, а m, n и t остаются без перемены, то мы получаем отсюда:

$$\left.\begin{aligned} x' &\equiv x \equiv m \\ y' &\equiv y \equiv n \\ \gamma' &\equiv \gamma \equiv t \end{aligned}\right\} (\text{mod. } L^2). \tag{25}$$

Внося это в сравнения (24), мы найдем:

$$\{m + \alpha^k n\}\, t \equiv \alpha^{2g_k} \{m + \alpha^{-k} n\}\, t \,(\text{mod. } L^2) \quad (k = 0,\ 1,\ \ldots,\ p-2),$$

или, по сокращении и раскрытии скобок:

$$m + \alpha^k n \equiv \alpha^{2g_k} m + \alpha^{2g_k - k} n \ (\text{mod. } L^2)\ (k = 0,\ 1, \ldots, p-2).$$

Заметим теперь, что из соотношения

$$\alpha = 1 - \lambda$$

следует, для любого целого положительного (рационального) числа w:

$$\alpha^w \equiv 1 - w\lambda \ (\text{mod. } L^2);$$

пользуясь этим и замечая, что числа $2g - k$ мы можем считать положительными, получаем из нашей группы сравнений:

$$m + \{1 - k\lambda\}\, n \equiv \{1 - 2g_k\lambda\}\, m + \{1 - 2g_k\lambda + k\lambda\}\, n \ (\text{mod. } L^3)$$
$$(k = 0,\ 1, \ldots, p-2),$$

или, по сокращении:

$$2g_k \{m + n\} \equiv 2kn \,(\text{mod. } L)\,(k = 0,\ 1, \ldots, p-2). \tag{26}$$

Так как в эти сравнения входят только рациональные целые числа, то мы можем их прямо писать в виде сравнений по модулю p:

$$g_k \{m + n\} \equiv kn \,(\text{mod. } p)\ (k = 0,\ 1, \ldots, p-2). \tag{27}$$

Далее, из сравнений (25) следует, что

$$\alpha^g \{m + \alpha^{p-1} n\} \equiv t \,(\text{mod. } L^2). \tag{28}$$

Определим числа (целые рациональные) r и s из сравнений:

$$\left.\begin{aligned} tr &\equiv m \\ ts &\equiv n \end{aligned}\right\} (\text{mod. } p);$$

тогда сравнения (27) дадут нам:

$$g_k\{r+s\} \equiv ks (\text{mod. } p)\,(k = 0,\ 1,\ \ldots,\ p-2), \qquad (29)$$

а сравнение (28) приводится к виду:

$$\alpha^g r + \alpha^{g+p-1} s \equiv 1 (\text{mod. } L^2);$$

замечая же, что

$$\left.\begin{aligned} \alpha^g r &\equiv r \\ \alpha^{g+p-1} s &\equiv s \end{aligned}\right\} (\text{mod. } L),$$

находим отсюда:

$$r + s \equiv 1 (\text{mod. } L),$$

а значит и (mod. p), так как все числа, входящие в это сравнение, — целые рациональные. Вставляя этот результат в группу (29), находим окончательно:

$$g_k \equiv ks (\text{mod. } p),\ (k = 0,\ 1,\ \ldots,\ p-2),$$

т. е. приходим к тому весьма важному результату, что числа g пропорциональны своим номерам. На этом основана вся остающаяся часть рассуждения.

На основании последней группы сравнений мы можем теперь переписать сравнения (24) в виде:

$$\{x + \alpha^k y\}\,\gamma' \equiv \alpha^{2ks}\{x' + \alpha^{-k} y'\}\,\gamma (\text{mod. } L^p)\,(k = 0, 1, \ldots, p-2).$$

Мы воспользуемся только четырьмя первыми

$$(k = 0,\ 1,\ 2,\ 3)$$

из этих сравнений, которые напишутся так:

$$\left.\begin{aligned} \gamma' x + \gamma' y - \gamma x' - \gamma y' &\equiv 0 \\ \gamma' x + \gamma' \alpha y - \gamma \alpha^{2s} x' - \gamma \alpha^{2s-1} y' &\equiv 0 \\ \gamma' x + \gamma' \alpha^2 y - \gamma \alpha^{4s} x' - \gamma \alpha^{4s-2} y' &\equiv 0 \\ \gamma' x + \gamma' \alpha^3 y - \gamma \alpha^{6s} x' - \gamma \alpha^{6s-3} y' &\equiv 0 \end{aligned}\right\} (\text{mod. } L^p).$$

Мы пришли, таким образом, к системе четырех линейных сравнений с четырьмя неизвестными x, y, x', y', которые заведомо удовлетворяются значениями этих неизвестных, не делящимися на модуль. Так как все сравнения однородны, то отсюда следует, что определитель системы должен делиться на L^p; а это сейчас же приводит нас к соотношению:

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^{2s} & \alpha^{2s-1} \\ 1 & \alpha^2 & \alpha^{4s} & \alpha^{4s-2} \\ 1 & \alpha^3 & \alpha^{6s} & \alpha^{6s-3} \end{vmatrix} \equiv 0 \pmod{L^p}.$$

Этот определитель легко вычислить так: вычитая сначала из второй строки первую, из третьей — вторую и из четвертой — третью, мы приведем его к определителю третьего порядка; вынося затем что можно за скобки и произведя еще раз такую же операцию, только на этот раз со столбцами, мы легко приведем последнее сравнение к виду:

$$\begin{aligned} &\{1-\alpha\}\{1-\alpha^{2s}\}\{1-\alpha^{2s-1}\}\{\alpha-\alpha^{2s}\}\cdot \\ &\cdot\{\alpha-\alpha^{2s-1}\}\{\alpha^{2s}-\alpha^{2s-1}\}\equiv 0 \pmod{L^p}. \end{aligned} \tag{30}$$

Теперь мы почти у цели, ибо невозможность полученного сравнения доказать очень легко. Прежде всего мы должны убедиться, что ни один из множителей левой части не может равняться нулю; так как a — первообразный корень уравнения $a^p=1$, то это было бы возможно только в том случае, если выполняется одно из следующих трех сравнений:

$$\left.\begin{aligned} s &\equiv 0 \\ s &\equiv 1 \\ 2s &\equiv 1 \end{aligned}\right\} \pmod{p}.$$

Но в случае первого из них мы имели бы:

$$y \equiv n \equiv ts \equiv 0 \pmod{L},$$

что противоречит нашему предположению; в случае второго мы имели бы в силу вышеуказанного соотношения $r+s\equiv 1 \pmod{L}$:

$$r \equiv 0 \pmod{L},$$

откуда

$$x \equiv m \equiv tr \equiv 0 \pmod{L},$$

что снова неверно. Наконец, в случае третьего сравнения, сопоставляя соотношения

$$\left.\begin{aligned} 2s &\equiv 1 \\ r+s &\equiv 1 \end{aligned}\right\} (\text{mod. } L),$$

мы нашли бы $r \equiv s$, а следовательно $tr \equiv ts$, $m \equiv n$, $x \equiv y$ (mod. L); но в наше исходное уравнение x, y и z входят совершенно равноправно; поэтому: либо мы имеем

$$x \equiv y \equiv z \,(\text{mod. } L), \tag{31}$$

либо (меняя в случае надобности обозначения y и z) мы можем утверждать, что и третья из наших гипотез отпадает.

Но соотношения (31) сейчас же приводят к противоречию, так как из них в силу самого исходного уравнения (16) следует, что

$$3x \equiv 0 \,(\text{mod. } L),$$

или, так как $p > 3$,

$$x \equiv 0 \,(\text{mod. } L),$$

что противоречит нашему предположению.

Итак, мы можем считать доказанным, что ни один из множителей левой части сравнения (30) не обращается в нуль. Теперь мы покажем, что ни один из этих множителей не может делиться на L^2; в самом деле, каждый из этих множителей имеет вид:

$$\alpha^u - \alpha^v,$$

где u и v — целые рациональные числа, причем, согласно доказанному, разность $u - v$ не делится на p; допустим для определенности, что $u < v$; тогда наш множитель можно представить в виде:

$$\alpha^u(1-\alpha^{v-u}) = \alpha^u \frac{1-\alpha^{v-u}}{1-\alpha} \cdot \lambda,$$

откуда и видно, что частное от деления этого множителя на λ есть единица нашей области (см. п. 4 предыдущего параграфа) и, следовательно, не может еще раз делиться на λ; а это и означает, что взятый нами множитель делится на L, но не делится на L^2.

Из доказанного следует, что левая часть сравнения (30) делится на L^6, но не делится ни на какую более высокую сте-

пень идеала L; а так как по условию $p > 6$, то сравнение (30) приводит к противоречию, что мы и хотели доказать.

Второй случай. Пусть теперь одно из чисел x, y, z делится на идеал L; пусть для определенности это будет число z; на том же основании, как и в элементарных случаях, мы можем допустить, что числа x, y, z попарно не имеют общих *числовых* делителей и что, следовательно, ни x, ни y не делятся на λ, или, что то же, на L. Представим число z в виде

$$z = \lambda^{\mu} z',$$

где μ — целое положительное число, а z' — целое число нашей области, не делящееся на λ; наше исходное уравнение принимает вид:

$$x^p + y^p = -\lambda^{\mu p} z'^p.$$

Рассмотрим более общее уравнение

$$x^p + y^p = e(\alpha)\lambda^{\mu p} z'^p,$$

где $e(\alpha)$ — произвольная единица нашей области, и покажем, что и это более общее уравнение ни при каком целом положительном μ не может удовлетворяться целыми, отличными от нуля, числами области $K(\omega)$; тем самым и подавно будет доказано наше более узкое утверждение.

Представим последнее уравнение в виде:

$$\{x + y\}\{x + \alpha y\} \ldots \{x + \alpha^{p-1} y\} = e(\alpha)\lambda^{\mu p} z'^p; \qquad (32)$$

по меньшей мере один из множителей левой части должен делиться на λ, так как $L = (\lambda)$ есть простой идеал. Но так как каждая из двух разностей

$$\left.\begin{aligned} \{x + \alpha^k y\} - \{x + \alpha^i y\} &= \{\alpha^k - \alpha^i\} y = \alpha^k \{1 - \alpha^{i-k}\} y, \\ \alpha^i \{x + \alpha^k y\} - \alpha^k \{x + \alpha^i y\} &= \{\alpha^i - \alpha^k\} x = \alpha^i \{1 - \alpha^{k-i}\} x \end{aligned}\right\} \qquad (33)$$

делится на $1 - a = \lambda$, то вместе с одним каким-нибудь из множителей должен делиться на λ и всякий другой; итак, каждый множитель левой части уравнения (32) должен делиться на λ.

Если мы теперь будем предполагать числа x и y полупервичными (на что мы имеем право по той же причине, как и в первом случае), то

$$x + y \equiv a \,(\mathrm{mod.}\, L^2),$$

где a — целое рациональное число; мы доказали, что $x + y$ делится на L; последнее сравнение показывает, что и a делится на L, а стало быть, и на p (п. 7 предыдущего параграфа); а так как $(p) = L^{p-1}$, то в таком случае последнее сравнение показывает, что $x + y$ делится на L^2.

Итак, все множители левой части уравнения (32) делятся на λ, а первый из этих множителей делится даже на λ^2; отсюда прежде всего следует, что все произведение делится на λ^{p-1}, а это показывает, что μ необходимо должно быть больше единицы.

Далее, легко убедиться, что ни один из множителей, кроме первого, не может делиться на λ^2; в самом деле, если бы вообще какие-нибудь два из этих множителей делились на λ^2; то, как показывают соотношения (33), числа

$$\alpha^k \{1 - \alpha^{i-k}\} y$$

и

$$\alpha^i \{1 - \alpha^{k-i}\} x$$

также должны были бы делиться на λ^2; а так как x и y на L не делятся и L есть простой идеал, то числа

$$\frac{\alpha^k \{1 - \alpha^{i-k}\}}{1 - \alpha}$$

$$\frac{\alpha^i \{1 - \alpha^{k-i}\}}{1 - \alpha}$$

должны были бы делиться на λ, что невозможно, так как эти числа суть единицы области $K(\alpha)$ (см. п. 4 предыдущего параграфа).

Таким образом мы приходим к следующему заключению: μ должно быть больше единицы; все множители левой части уравнения (32), кроме первого, делятся на λ, но не делятся на λ^2; первый множитель, следовательно, должен делиться на $\lambda^{p(\mu-1)+1}$ и не может делиться ни на какую более высокую степень числа λ.

Принимая все это во внимание, мы совершенно тем же путем, как в первом случае, обозначая через D идеал, служащий наибольшим общим делителем чисел x и y, придем к соотношениям:

$$(x + y) = L^{p(\mu-1)+1} J_0^p D,$$

$$(x + \alpha^k y) = L J_k^p D \; (k = 1, 2, \ldots, p - 1),$$

где $J_0, J_1, \ldots, J_{p-1}$ суть идеалы, не делящиеся на L. Перемножая последнее из этих равенств крест-накрест с каждым из предшествующих, мы находим:

$$L(x+y)J_{p-1}^p = L^{p(\mu-1)+1}(x+\alpha^{p-1}y)J_0^p,$$
$$L(x+\alpha^k y)J_{p-1}^p = L(x+\alpha^{p-1}y)J_k^p$$
$$(k=1,\ 2,\ \ldots,\ p-2),$$

откуда

$$J_k^p \sim J_{p-1}^p (k=0,\ 1,\ \ldots,\ p-2),$$

так как L — главный идеал.

Сопоставляя же эти соотношения с соотношениями

$$J_k^h \sim J_{p-1}^h (k=0,\ 1,\ \ldots,\ p-2)$$

и пользуясь регулярностью числа p, мы, так же как в первом случае, покажем, что

$$J_k \sim J_{p-1} (k=0,\ 1,\ \ldots,\ p-2),$$

т. е. что

$$J_{p-1}(\alpha_k) = J_k(\beta_k)\ (k=0,\ 1,\ \ldots,\ p-2),$$

где α_k и β_k — некоторые целые числа области $K(\alpha)$, которые мы, очевидно, можем считать не делящимися на L. Возводя равенства последней группы в степень p и помножая каждое из них крест-накрест с соответствующим равенством предшествующей группы, мы по сокращении найдем:

$$(x+y)(\beta_0)^p = L^{p(\mu-1)}(\gamma)(\alpha_0)^p,$$
$$(x+\alpha^k y)(\beta_k)^p = (\gamma)(\alpha_k)^p\ (k=1,\ 2,\ \ldots,\ p-2),$$

где положено $\gamma = x+\alpha^{p-1}y$; переходя от идеалов к числам, получаем:

$$\{x+y\}\beta_0^p = e_0(\alpha)\lambda^{p(\mu-1)}\gamma\alpha_0^p,$$
$$\{x+\alpha^k y\}\beta_k^p = e_k(\alpha)\gamma\alpha_k^p (k=1,\ 2,\ \ldots,\ p-2).$$

Из этих уравнений первые три дают нам:

$$\beta_0^p x + \beta_0^p y - e_0(\alpha)\lambda^{p(\mu-1)}\gamma\alpha^p = 0,$$
$$\beta_1^p x + \alpha\beta_1^p y - e_1(\alpha)\gamma\alpha_1^p = 0,$$
$$\beta_2^p x + \alpha^2\beta_2^p y - e_2(\alpha)\gamma\alpha^p = 0.$$

Условие совместности этих уравнений приводится к виду:

$$\begin{vmatrix} \beta_0^p & \beta_0^p & \gamma^{p(\mu-1)}\varepsilon_0(\alpha)\alpha_0^p \\ \beta_1^p & \alpha\beta_1^p & \varepsilon_1(\alpha)\alpha_1^p \\ \beta_2^p & \alpha^2\beta_2^p & \varepsilon_2(\alpha)\alpha_2^p \end{vmatrix} = 0;$$

раскрывая определитель и полагая

$$\alpha_1\beta_0\beta_2 = \tau_1,\ \alpha_2\beta_0\beta_1 = \tau_2,\ \alpha_0\beta_1\beta_2 = \tau_3,$$

мы находим:

$$\tau_1^p + \varepsilon'(\alpha)\tau_2^p = \lambda^{p(\mu-1)}\varepsilon(\alpha)\tau_3^p, \qquad (34($$

где $\varepsilon(\alpha)$ и $\varepsilon'(\alpha)$ суть некоторые новые единицы области [при выводе придется сократить все соотношение на λ и пользоваться тем, что $\frac{1-\alpha^2}{1-\alpha}$ есть единица области $K(\alpha)$].

Пусть теперь разложения чисел τ_1 и τ_2 по степеням λ (см. п. 3 предыдущего параграфа) начинаются так:

$$\tau_1 = a + a_1\lambda + \dots,$$
$$\tau_2 = b + b_1\lambda + \dots,$$

где целые рациональные числа a и b, очевидно, не делятся на λ; тогда

$$\left.\begin{aligned} \tau_1^p &= a^p \\ \tau_2^p &= b^p \end{aligned}\right\} (\mathrm{mod.}\ L^p),$$

и так как $\mu > 1$, то уравнение (34) дает нам:

$$a^p + \varepsilon'(\alpha)b^p \equiv 0\,(\mathrm{mod.}\ L^p); \qquad (35)$$

так как b не делится на λ и, следовательно, на p, то найдется такое целое рациональное число c, что

$$bc \equiv a\,(\mathrm{mod.}\ p),$$

откуда легко находим:

$$b^p c^p \equiv a^p\,(\mathrm{mod.}\ p^2),$$

а, следовательно, и подавно $(\mathrm{mod.}\ L^p)$; сопоставляя это сравнение со сравнением (35), находим:

$$\varepsilon'(\alpha) \equiv (-c)^p\,(\mathrm{mod.}\ L^p),$$

а значит, и подавно (mod. p); на основании п. 6 предыдущего параграфа отсюда следует, что

$$e'(\alpha) = [e''(\alpha)]^p,$$

где $e''(\alpha)$ — некоторая новая единица той же области. Полагая $\tau_2 e''(\alpha) = \tau_2'$, мы можем поэтому переписать уравнение (34) в виде

$$\tau_1^p + \tau_2^p = \lambda^{p(\mu-1)} e(\alpha) \tau_3^p$$

это же есть уравнение совершенно такого же вида, как исходное уравнение (32), с той только разницей, что число μ заменилось числом $\mu-1$.

Если $\mu - 1$ все еще больше единицы, мы можем таким же путем понизить это число еще на единицу и т. д., покуда не придем к уравнению, в котором $\mu = 1$; так как невозможность такого уравнения уже показана, то мы приходим к противоречию, показывающему, что и второй случай является невозможным. Таким образом полностью доказана теорема Куммера, а стало быть, и Великая теорема Ферма для всех регулярных показателей.

Здесь, разумеется, возникает вопрос о том, какие простые числа будут регулярными и какие нет; для индивидуального простого числа p этот вопрос может быть легко решен с помощью признака, указанного в п. 9 предыдущего параграфа; но нам сейчас естественно спрашивать о другом: много ли регулярных простых чисел, существуют ли нерегулярные и как много их? К сожалению, никаких общих результатов по этому вопросу мы не знаем. Непосредственные вычисления показывают, что среди простых чисел, не превышающих 100, регулярными являются все, за исключением трех, именно чисел 37, 59 и 67; но и для этих трех показателей Куммеру удалось доказать теорему Ферма в специальном, сложном исследовании, которого мы здесь касаться не можем. Таким образом теорема Ферма в настоящее время является доказанной для всех показателей, не превышающих 100, как об этом и было упомянуто выше.

ГОСУДАРСТВЕННОЕ
ТЕХНИКО-ТЕОРЕТИЧЕСКОЕ ИЗДАТЕЛЬСТВО

В СКОРОМ ВРЕМЕНИ ВЫЙДЕТ ИЗ ПЕЧАТИ СБОРНИК

МАТЕМАТИЧЕСКОЕ ПРОСВЕЩЕНИЕ

под редакцией
С. Е. АРШОНА, Р. Н. БОНЧКОВСКОГО и И. И. ЧИСТЯКОВА.

Сборники будут выходить ежемесячно.

Сборники рассчитаны на преподавателей и учащихся средней школы и техникумов, на инженерно-технических работников, интересующихся математикой и на любителей математики.

Сборники будут содержать статьи и заметки по вопросам элементарной и отчасти высшей математики и ее преподавания, отделы задач и упражнений для учащихся, текущей жизни, библиографии и т. д.