М. М. Постников

ТЕОРЕМА ФЕРМА

М. М. Постников

ТЕОРЕМА ФЕРМА

•

Введение в теорию алгебраических чисел

ИЗДАТЕЛЬСТВО «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
Москва 1978

517.1
П63
УДК 511.52

АННОТАЦИЯ

Книга является введением в теорию алгебраических чисел. Основные понятия и идеи этой теории изложены в ней в связи с теоремой Ферма. Читатель должен видеть, что их появление не случайно, а диктуется логикой решения конкретной задачи. Одна из целей книги — убедить читателя в глубине и сложности проблематики, связанной с теоремой Ферма, и в полной бесперспективности поисков ее элементарного доказательства.

Изложение в книге ведется концентрически, с тем чтобы читатель, даже с минимальной подготовкой (например, школьник), мог усвоить основные идеи.

Книга предназначена школьникам старших классов (в ее первых главах), студентам, учителям и всем любителям математики. Она может быть интересна и более квалифицированным читателям, которые хотят познакомиться с теорией алгебраических чисел в ее классическом аспекте.

Михаил Михайлович Постников

ТЕОРЕМА ФЕРМА

●

ВВЕДЕНИЕ В ТЕОРИЮ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

М., 1978 г., 128 стр.

Редакторы *В. Л. Попов, В. В. Донченко*
Технический редактор *Е. В. Морозова* Корректор *Н. Д. Дорохова*

ИБ № 11184

Сдано в набор 27.07.77. Подписано к печати 2.01.78. Бумага 84×108$^{1}/_{32}$ тип. № 3. Физ. печ. л. 4. Условн. печ. л. 6,72. Уч.-изд. л. 6,03, Тираж 50 000 экз. Цена книги 20 коп. Заказ № 702.

Издательство «Наука». Главная редакция физико-математической литературы 117071. Москва. В-71, Ленинский проспект, 15

Ордена Трудового Красного Знамени Ленинградская типография № 2 имени Евгении Соколовой Союзполиграфпрома при Государственном комитете Совета Министров СССР по делам издательств, полиграфии и книжной торговли. 198052, Ленинград, Л-52, Измайловский проспект, 29.

П $\frac{20203-018}{053(02)-78}$ 75-78

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Теория алгебраических чисел является одним из красивейших созданий математики XIX века. Основные ее идеи легли в основу современной общей алгебры и тем самым оказали стимулирующее влияние на развитие всей математики. В последнее время наблюдается и обратный процесс: конструкции и методы современной абстрактной математики интенсивно вторгаются в прежде запретную для них область теории чисел, быстро меняющей поэтому свое лицо. Это новейшее развитие теории вполне удовлетворительно отражено в литературе, в том числе и учебной: достаточно назвать две недавно переведенные у нас книги Вейля и Ленга. Более классическое направление нашло отражение в книге З. И. Боревича и И. Р. Шафаревича «Теория чисел», в 1972 г. вышедшей вторым изданием. Однако книга Боревича и Шафаревича представляет собой обстоятельный (можно сказать даже — энциклопедический) учебник, предназначенный, в первую очередь, для студентов и аспирантов, специализирующихся по теории алгебраических чисел. Поэтому эта книга для первоначального ознакомления с основными идеями и положениями теории малопригодна. К тому же она требует от читателя достаточно солидной математической подготовки.

Как ни странно, но на русском языке отсутствуют книги, предназначенные для не очень искушенного читателя, желающего лишь познакомиться с главнейшими идеями теории алгебраических чисел. Заполнить в определенной мере этот пробел имеет целью предлагаемая небольшая книжка. Она посвящена не всей теории алгебраических чисел, а только одному ее разделу — теории делимости целых алгебраических

чисел. Однако читатель, изучивший ее, сможет уже увереннее ориентироваться и в более трудных вопросах.

При последовательном чтении книги читатель будет встречаться со все более и более сложным материалом. Однако книга составлена так, что на каждом этапе сообщается некоторый в достаточной степени законченный комплекс сведений. Таким образом, даже читатель со слабой математической подготовкой (например, школьник) узнает достаточно много, чтобы иметь стимул для дальнейшей работы.

Эта «сверхзадача» определила несколько необычный план изложения, устремленный к тому, чтобы, во-первых, на каждом шагу получилось нечто законченное, а, во-вторых, было ясно, что нужно делать дальше.

Исторически теория делимости целых алгебраических чисел была создана в связи с теоремой Ферма. Поскольку эта мотивация теории сохраняет всю свою силу и сегодня, мы имеем уникальную возможность объединить концептуальный подход с историческим. Изложение начинается с теоремы Ферма, и теория постепенно развертывается с единственной, формально, целью — доказать эту теорему. Очень быстро это делается для некоего класса простых показателей, а все дальнейшее преподносится как постепенная расшифровка этого класса и представление его в удобной алгоритмической форме. К сожалению, заключительные этапы этой расшифровки пришлось изложить без доказательства в обзорном порядке.

Ввиду учебно-элементарного характера книги литературных ссылок в ней, как правило, нет. Однако любой компетентный читатель поймет, сколь многим автор обязан книге Боревича и Шафаревича, особенно в части, непосредственно касающейся теоремы Ферма. Что же касается общей теории (существование теории дивизоров и конечность групп классов), она излагается «в классическом духе» по Дедекинду и Гурвицу.

Автор признателен Д. К. Фадееву, с исключительным вниманием прочитавшему рукопись книги и сделавшему много замечаний, способствовавших улучшению текста. В частности, по его совету был полностью переработан § 6.

История теоремы Ферма

В XVII веке жил один из величайших математиков Пьер Ферма (1608—1665). Он заложил основы аналитической геометрии (одновременно то же сделал Декарт) и нашел общий метод разыскания максимумов и минимумов (впоследствии развившийся в исчисление бесконечно малых). Однако более всего известны результаты Ферма в области теории чисел.

Свои теоретико-числовые результаты Ферма не публиковал. Они известны из его писем, а также из бумаг, оставшихся после его смерти. Как правило, доказательства Ферма до нас не дошли. Эти доказательства были восстановлены последующими математиками, в основном Эйлером.

Некоторые свои утверждения Ферма сопровождал пометкой, что он не располагает удовлетворительным их доказательством. Впоследствии выяснилось, что часть этих утверждений была ошибочна. Например, Ферма ошибался, утверждая, что все числа вида $2^{2^n}+1$ простые; уже при $n=5$, как показал Эйлер, получается составное число.

Однако во всех случаях, когда Ферма определенно утверждал, что он доказал то или иное утверждение, впоследствии удавалось это утверждение доказать.

Замечательным исключением является так называемая «Большая теорема Ферма» (она же «Великая» или «Последняя»), утверждающая, что не существует отличных от нуля целых чисел x, y и z, для которых имеет место равенство

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

где $n > 2$. (Общеизвестно, что при $n = 2$ такие числа существуют, например, 3, 4, 5.)

В бумагах Ферма было найдено доказательство этой теоремы при $n = 4$ (любопытно, что это единственное полное доказательство теоретико-числового результата, сохранившееся от Ферма). Относительно же общего случая любого $n > 2$ Ферма лишь написал (на полях «Арифметики» Диофанта), что он нашел «поистине замечательное доказательство» этого факта, но «поля слишком малы, чтобы его уместить».

Несмотря на усилия многих математиков (в «Истории теории чисел» Диксона прореферировано более трехсот (!) работ на эту тему), это доказательство найдено не было, и можно сомневаться, существовало ли оно вообще.

Более того, как мы увидим ниже, кроме показателя 4, нет ни одного показателя n, для которого теорему Ферма удалось бы доказать элементарными средствами.

Этим объясняется, почему в настоящее время все специалисты твердо уверены в невозможности доказать теорему Ферма элементарными методами.

В 1908 г. немецкий любитель математики Вольфскель завещал 100 000 марок тому, кто докажет теорему Ферма. Немедленно сотни и тысячи людей, движимых одним лишь стремлением к наживе, стали бомбардировать научные общества и журналы своими рукописями, якобы содержащими доказательство теоремы Ферма. Только в Гёттингенское математическое общество за первые три года после объявления завещания Вольфскеля пришло более тысячи (!) решений.

Рассказывают, что то ли в Гёттинген, то ли в нашу Академию наук однажды поступила следующая телеграмма: «Решил проблему Ферма двт икс степени эн плюс игрек степени эн не равно зет степени эн тчк доказательство двт переносим игрек степени эн правую часть тчк подробности письмом тчк». Неизвестно, так это или не так, но эта история хорошо отражает как ажиотаж, возникший вокруг теоремы Ферма, так и уровень предлагаемых «доказательств».

В период инфляции после первой мировой войны премия Вольфскеля обесценилась, и ныне «ферматисты» (так называют математики лиц, пытающихся явно с негодными средствами атаковать теорему Ферма) ни на какое финансовое вознаграждение рассчитывать не могут. Поток «ферматистских доказательств» после этого, естественно, сильно ослаб, но, к сожалению, не прекратился. В научные математические центры постоянно продолжает течь струйка писем, авторы которых мечтают во что бы то ни стало прославиться, хотя и не имеют на это никаких объективных оснований. Часто они с негодованием заявляют, что гонятся вовсе не за личной славой, а хотят прославить свою страну и принести пользу науке. На самом же деле это в лучшем случае — печальное заблуждение.

Значение теоремы Ферма для математики в том, что при попытках ее доказательства были, как мы увидим, выкованы новые мощные средства, приведшие к созданию обширного отдела математики — так называемой «теории алгебраических чисел». Тот факт, что до сих пор теорема Ферма не доказана, по-видимому, означает необходимость в еще более мощных и утонченных методах. Элементарное же доказательство теоремы Ферма (или, более общо, доказательство, не вводящее новых идей и остающееся в рамках уже известных методов), хотя и закроет проблему, но большого значения для математики иметь заведомо не будет.

Следует со всей решительностью предостеречь читателя от попытки искать элементарное доказательство теоремы Ферма. Можно быть уверенным, что это будет лишь ненужная потеря труда и времени. Во всяком случае, ни издательство, ни автор этой книги ни в какую переписку по поводу теоремы Ферма вступать не будут.

Одна из целей настоящей книги — показать, с какими трудными и глубокими вопросами теории чисел соприкасается теорема Ферма, и тем самым обескуражить каждого, кто подумывал взяться за эту теорему и пополнить ряды ферматистов (раз вступившие на эту стезю уже, как правило, недоступны никаким доводам).

Быть может, стоит в связи с этим заметить, что пытаться «вслепую» искать контрпример к теореме Ферма также безнадежно. Еще в 1856 г. Грюнерт заметил, что натуральные числа x, y, z, удовлетворяющие соотношению

$$x^n + y^n = z^n$$

(если такие числа существуют), должны удовлетворять неравенствам

$$x > n, \quad y > n, \quad z > n.$$

Действительно, пусть $z = x + a$, где $a \geqslant 1$. Тогда

$$x^n + y^n = x^n + nx^{n-1}a + \ldots + nxa^{n-1} + a^n$$

и потому $y^n > nx^{n-1}a > nx^{n-1}$. Аналогично доказывается, что $x^n > ny^{n-1}$. Следовательно,

$$(y^n)^n > n^n x^{n(n-1)} > n^n n^{n-1} (y^{n-1})^{n-1}.$$

т. е. $y^{2n-1} > n^{2n-1}$ и, значит, $y > n$. По симметрии, $x > n$ и потому $z > n$. ■ [1]).

К настоящему времени теорема Ферма доказана для всех показателей $n < 100\,000$ (см. ниже). Поэтому в опровергающем ее примере мы должны были бы иметь дело с числами, превосходящими $10^{500\,000}$.

Как уже говорилось, *элементарного доказательства теоремы Ферма нет ни для одного показателя* $n \neq 4$. Даже в случае $n = 3$, который был рассмотрен Эйлером в 1768 г., оказались необходимыми соображения, использующие числа вида

$$a + b\sqrt{-3}, \tag{1}$$

где a, b — целые числа. Такого рода методы были полностью чужды Ферма, и он их заведомо использовать не мог.

Собственно говоря, доказательство Эйлера было дефектным, поскольку он без всякого обоснования перенес на числа вида (1) рассуждения, эксплуатировавшиеся до него лишь в области целых чисел. Например, он пользовался для чисел (1) простейшими фактами теории делимости, никак это не оправдывая.

Первым, кто построил арифметику чисел (1) и, тем самым, подвел под рассуждения Эйлера надежный фундамент, был, по-видимому, Гаусс.

---

[1]) Знаком ■ мы отмечаем конец доказательства.

Доказательство теоремы Ферма для случая $n = 5$ предложили в 1825 г. почти одновременно Лежен Дирихле и Лежандр. Свое доказательство Дирихле опубликовал в 1828 г. Оно было очень сложным. В 1912 г. его упростил Племель.

Для следующего простого показателя $n = 7$ теорема Ферма была доказана лишь в 1839 г. Ламе. Доказательство Ламе было почти сразу же существенно усовершенствовано и упрощено Лебегом.

В 1847 году Ламе объявил, что ему удалось найти доказательство теоремы Ферма для всех простых показателей $n \geqslant 3$. Метод Ламе представлял собой весьма далекое развитие идей Эйлера и основывался на арифметических свойствах чисел вида

$$a_0 + a_1\zeta + \ldots + a_{n-2}\zeta^{n-2}, \tag{2}$$

где $a_0, a_1, \ldots, a_{n-2}$ — целые числа, а

$$\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

— первообразный корень n-й степени из 1.

Однако сразу же Лиувилль обнаружил в рассуждениях Ламе серьезный пробел, заключающийся в том, что Ламе без доказательства предполагал, что числа вида (2), подобно обыкновенным целым числам, единственным образом разлагаются в произведение простых (далее неразложимых) чисел. Ламе был вынужден признать свою ошибку.

Пока во Франции происходили эти события, в Германии молодой математик Куммер упорно занимался теоремой Ферма. Сперва он полагал, что ему удалось найти полное доказательство этой теоремы, и в 1843 г. он представил Дирихле соответствующий мемуар. Доказательство также использовало числа вида (2), и, подобно Ламе, Куммер предполагал, что эти числа единственным образом разлагаются на простые множители. Дирихле немедленно указал Куммеру, что этот факт требует доказательства, и Куммер забрал свой манускрипт обратно.

Вскоре Куммер уже знал, что теорема о единственности разложения на простые множители для чисел вида (2) неверна и искать ее доказательство

бессмысленно. В этой ситуации он нашел замечательный выход, который прославил его и породил целый ряд разделов современной алгебры. Этот выход состоял в том, что Куммер добавил к числам (2) еще некие новые, несуществующие числа, которые он назвал «идеальными» и для которых свойство единственности разложения на простые множители восстанавливается.

Например, легко можно показать (сделайте это!), что в области чисел вида

$$a + b\sqrt{-5}, \tag{3}$$

где a и b — целые числа, число 21 двумя различными способами разлагается в произведение простых множителей:

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

Хотя числа вида (3) и не являются числами вида (2) ни при каком n (для чисел (2) аналогичный пример возможен только при $n \geqslant 23$), но идея Куммера к ним применима. Таким образом, следует добавить к числам (3) некие идеальные числа A, B, C, D и считать, что

$$3 = AB, \quad 7 = CD, \quad 1 + 2\sqrt{-5} = AC, \quad 1 - 2\sqrt{-5} = BD.$$

Ясно, что тогда единственность разложения числа 21 на простые (уже идеальные) множители будет восстановлена.

Конечно, «идеальность» новых чисел привела к своим трудностям, но с ними оказалось легче сладить. Уже в 1847 году Куммер опубликовал статью, в которой он доказал теорему Ферма для всех простых показателей $n = l$, удовлетворяющих неким условиям (А) и (В). В это время он думал (как доказывает его письмо к Лиувиллю), что эти условия выполнены для всех простых чисел, но вскоре он пришел к заключению, что, по-видимому, имеются исключения (например, число 37). Рассуждения Куммера были упрощены в 1894 г. Гильбертом.

Конечно, этот результат Куммера заставлял желать большего, поскольку он не давал пока ни одного конкретного простого показателя l, для которого справедлива теорема Ферма. Тем не менее, это было замечательное продвижение, и в этой книге мы его подробно обсудим и докажем.

Весьма искусным, тонким и очень трудным анализом арифметики чисел (2) Куммер к 1851 году добился серьезных усовершенствований своих результатов

1847 года. Ему удалось доказать, что условие (B) вытекает из условия (A) (это — так называемая «лемма Куммера»; см. ниже § 6) и потому излишне. Он существенно упростил условие (A) и придал ему легко проверяемую форму. Это условие в первоначальной формулировке состояло в требовании, чтобы простое число l не делило некоторого трудно определяемого числа h. Куммер разложил число h на два множителя:

$$h = h_1 h_2;$$

нашел явные (хотя и довольно сложные) формулы для h_1 и h_2; показал, что число h тогда и только тогда делится на l, когда на l делится число h_1 (так называемый *первый множитель*), и, основываясь на этом, весьма изящными теоретико-числовыми рассуждениями доказал, что условие (A) выполнено тогда и только тогда, когда простое число l не делит числителей первых $l-3$ членов ряда, состоящего из так называемых *чисел Бернулли* (в их несократимом представлении). Такие простые числа Куммер назвал *регулярными*.

Числа Бернулли — это рациональные числа

$$B_1 = \frac{1}{6}, \quad B_2 = \frac{1}{30}, \quad B_3 = 0, \ldots,$$

которые могут быть вполне автоматически вычислены друг за другом по очень простым правилам (см. § 12). Поэтому условие Куммера проверяется для каждого l без особого труда.

В частности, оказывается, что *среди простых чисел* $l < 100$ *нерегулярны только числа* 37, 59 *и* 67.

Это было замечательным завершением исследований 1847 г., но, к сожалению, доказательства этих результатов слишком сложны, чтобы их можно было здесь изложить. Мы лишь постараемся в § 12 хотя бы показать, почему в условии регулярности возникают числа Бернулли.

Куммер всю жизнь думал, что регулярных чисел бесконечно много, и эту уверенность разделяли с ним многие математики. Однако до сих пор этот факт не доказан.

Более того, в 1915 году Иенсен очень просто доказал, что напротив, *имеется бесконечно много нерегулярных простых чисел*.

После 1851 г. Куммер обратился к исследованию нерегулярных простых чисел и пытался доказать для них теорему Ферма. В очень трудной работе 1858 года он доказал теорему Ферма для некоторого класса нерегулярных простых показателей, включающего показатели 37, 59 и 67. Тем самым теорема Ферма оказалась доказанной для всех простых показателей $l < 100$. Правда, позднее (в первой четверти XX века) Мертенс и Вандивер обнаружили в рассуждениях Куммера неточности, но они оказались вполне исправимыми.

Специальное, более простое, доказательство теоремы Ферма для показателя $l = 37$ в 1893 г. дал Мириманов.

Около 1850 г. Французская академия наук учредила награду в 3 тыс. франков за доказательство теоремы Ферма. Присуждение несколько раз откладывалось, пока, наконец, в 1857 г. премия не была присуждена Куммеру (который, кстати сказать, даже не был вначале среди претендентов).

После Куммера серьезных сдвигов в доказательстве теоремы Ферма не произошло до 1929 года, когда Вандивер доказал, что *теорема Ферма справедлива для простого показателя l, если*

1) *второй множитель h_2 числа h не делится на l;*
2) *числители $l-3$ чисел Бернулли*

$$B_{2l}, \quad B_{4l}, \quad \ldots, \quad B_{2l\,(l-3)}$$

не делятся на l[3].

Проверка условия 2) для современных ЭВМ труда не составляет. Что же касается условия 1), то до сих пор неизвестно ни одного простого числа l, для которого оно не выполнено, хотя были проверены все простые числа $l < 100\,000$. Для этих чисел условие 2) теоремы Вандивера тоже оказалось выполненным. Таким образом, *теорема Ферма справедлива для всех простых показателей $l < 100\,000$.*

Уже Эйлеру было известно, что при исследовании уравнения

$$x^l + y^l = z^l, \quad l \text{ простое} \geqslant 3, \tag{4}$$

необходимо различать случай, когда ни одно из чисел x, y, z не делится на l, от случая, когда хотя бы одно из этих чисел делится на l.

Допуская определенную небрежность речи, принято называть утверждение, что уравнение (4) не может быть удовлетворено не делящимися на l числами, первым случаем теоремы Ферма, а утверждение, что уравнение (2) не может быть удовлетворено числами, одно из которых делится на l,— вторым случаем теоремы Ферма.

Оказывается, что, в отличие от общего случая теоремы Ферма, ее первый случай допускает для многих l элементарное доказательство. Подход к этому доказательству был нащупан еще в начале XIX века известной Софи Жермен (1776—1831), первой женщиной-математиком нового времени. В частности, она доказала, что *для простого числа l справедлив первый случай теоремы Ферма, если число $2l+1$ также является простым числом.*

Однако надежды, которые возбудила Жермен, не оправдались, и на предложенном ей пути найти полное доказательство хотя бы первого случая теоремы Ферма не удалось.

Жермен не опубликовала своих результатов, а сообщила их в письме известному французскому математику Лежандру. В 1823 г. Лежандр выпустил в свет обширный мемуар по теореме Ферма, в котором он изложил теоремы Жермен и вывел из них ряд следствий. В частности, он показал, что *первый случай теоремы Ферма справедлив для простого показателя l, если хотя бы одно из пяти чисел*

$$4l+1, \quad 8l+1, \quad 10l+1, \quad 14l+1, \quad 16l+1$$

является простым числом. Тем самым первый случай теоремы Ферма оказался доказанным для всех простых показателей <197. Для показателя 197 теорема Лежандра ответа не дает.

После Лежандра многие математики пытались улучшить его результаты. По-видимому, окончательную (далее существенно не улучшаемую элементарными методами) теорему получил в 1893 г. немецкий математик Вендт.

Для любого $m \geqslant 1$ Вендт ввел некое целое число D_m и, используя общую технику Жермен, показал, что *первый случай теоремы Ферма справедлив для простого показателя l, если существует такое $m \geqslant 1$, что*

1) *число $p = 2ml + 1$ является простым числом, не делящим числа D_m;*

2) *число $l^{2m} - 1$ не делится на p.*

Число D_m допускает три равносильных определения:

а)
$$D_m = (-1)^m \prod_{j=1}^{2m-1} [(1 + \zeta^j)^{2m} - 1],$$

где $\zeta = \cos \frac{\pi}{m} + i \sin \frac{\pi}{m}$;

б) D_m является определителем матрицы

$$\begin{Vmatrix} \binom{2m}{1} & \binom{2m}{2} & \cdots & \binom{2m}{2m-1} & \binom{2m}{2m} \\ \binom{2m}{2} & \binom{2m}{3} & \cdots & \binom{2m}{2m} & \binom{2m}{1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \binom{2m}{2m} & \binom{2m}{1} & \cdots & \binom{2m}{2m-2} & \binom{2m}{2m-1} \end{Vmatrix};$$

в) D_m представляет собой так называемый результант многочленов $x^{2m} - 1$ и $(x + 1)^{2m} - 1$.

Отметим, что, несмотря на усилия не одного десятка математиков, среди которых были чрезвычайно остроумные и изобретательные люди, не удалось найти *никаких других* элементарных и вместе с тем достаточно общих подходов к доказательству теоремы Ферма или хотя бы ее первого случая. (Впрочем, общность результатов Жермен до сих пор до конца не выяснена. Например, неизвестно, существует ли бесконечное число простых показателей l, к которым они применимы.)

Неэлементарные методы к первому случаю теоремы Ферма привлек Куммер. В упоминавшейся выше

работе 1858 г. он доказал, что *первый случай теоремы Ферма справедлив для простого показателя l, если на l не делится числитель хотя бы одного из двух чисел Бернулли B_{l-3} и B_{l-5}.*

В 1905 г. Мириманов обобщил этот результат, показав, что *достаточно, чтобы l не делило числителя хотя бы одного из четырех чисел Бернулли B_{l-3}, B_{l-5}, B_{l-7} и B_{l-9}.* Это покрывает все $l < 257$.

Используя метод Мириманова, Виферих в 1909 г. доказал, что *первый случай теоремы Ферма справедлив для всех простых показателей l, для которых $2^{l-1} - 1$ не делится на l^2.* Этот результат произвел сенсацию. О его силе можно судить, например, по тому, что для простых чисел $\leqslant 200\,183$ он не дает ответа только для двух чисел 1093 и 3511.

Доказательство Вифериха было впоследствии упрощено Мириманом и Фробениусом, которые также показали, что в условии Вифериха основание 2 можно заменить основанием 3 (так что первый случай теоремы Ферма оказывается справедливым для любого простого показателя l, для которого хотя бы одно из чисел $2^{l-1} - 1$ или $3^{l-1} - 1$ не делится на l^2).

В 1912 г. Фуртвенглер, обратившись к очень сильным средствам (к так называемому *закону взаимности Эйзенштейна*), доказал критерии Вифериха и Мириманова — Фробениуса буквально в несколько строк. Эта работа послужила началом целой серии исследований, авторы которых, опираясь на самые новейшие достижения теории чисел (например, так называемую *теорию полей классов*), смогли к 1941 году доказать, что в критерии Вифериха основание 2 можно заменить произвольным простым числом $p \leqslant 43$. Это позволило проверить, что *первый случай теоремы Ферма справедлив для всех показателей $l < 253\,747\,889$.*

В 1934 г. Вандивер доказал, что *для простого показателя l справедлив первый случай теоремы Ферма, если второй множитель h_2 не делится на l.* Эта теорема интересна тем, что, как уже говорилось, до сих пор неизвестно ни одного простого показателя l, который бы этому условию не удовлетворял. Однако тот факт, что l не делит h_2, проверен пока только для $l < 100\,000$.

§ 1. Теорема Жермен

Как же можно подойти к доказательству теоремы Ферма?

В первую очередь, здесь следует заметить, что если тройка (x, y, z) целых чисел удовлетворяет уравнению

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

(случай $n = 2$ мы пока не исключаем), то ему будет удовлетворять и любая тройка вида $(\lambda x, \lambda y, \lambda z)$, где λ — произвольное целое число. Обратно, если тройка $(\lambda x, \lambda y, \lambda z)$ является решением уравнения (1), то решением будет и тройка (x, y, z). Поэтому, чтобы найти все решения уравнения (1) (состоящие из отличных от нуля чисел), достаточно найти решения (x, y, z), для которых числа x, y, z взаимно просты (не имеют общего множителя, отличного от единицы), а чтобы доказать, что уравнение (1) неразрешимо в целых числах, достаточно привести к противоречию предположение о существовании решения (x, y, z), состоящего из взаимно простых чисел.

Более того, ясно, что если в каком-нибудь решении (x, y, z) уравнения (1) два из чисел x, y, z имеют общий множитель $\lambda \neq \pm 1$, то третье число также будет делиться на λ. Поэтому мы можем ограничиться лишь решениями, состоящими из попарно взаимно простых чисел. Такие решения мы будем называть *примитивными*.

Далее, ясно, что если теорема Ферма верна для показателя n, то она автоматически верна и для любого показателя an, кратного n, потому что, если уравнение

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

имеет целочисленное решение (x, y, z), то уравнение (1) будет иметь целочисленное решение (x^a, y^a, z^a). Поэтому теорему Ферма достаточно доказать для $n=4$ (это сделал, как было уже сказано, сам Ферма) и для $n = l$, где l — произвольное *простое* число $\geqslant 3$.

Фундаментальную роль во всех рассуждениях, связанных с теоремой Ферма, играет следующая очевидная лемма:

Лемма. *Пусть a, b и c — такие натуральные (целые положительные) числа, что*

1) *имеет место равенство*

$$ab = c^n;$$

2) *числа a и b взаимно просты.*

Тогда существуют такие натуральные числа x и y, что

$$a = x^n, \quad b = y^n.$$

Короче говоря, *если произведение двух взаимно простых натуральных чисел является n-й степенью, то каждый из сомножителей также будет n-й степенью.*

Если n нечетно, то эта лемма справедлива, очевидно, для любых отличных от нуля целых (положительных или отрицательных) чисел a, b и c.

Приведем для полноты доказательство леммы. Пусть

$$a = p_1^{k_1} \dots p_s^{k_s}, \quad b = q_1^{l_1} \dots q_t^{l_t}$$

— разложения чисел a и b в произведение простых чисел. Здесь $k_1 \geqslant 1, \dots, k_s \geqslant 1$ и $p_1, \dots, p_s$ — различные простые числа. Аналогично, $l_1 \geqslant 1, \dots, l_t \geqslant 1$ и $q_1, \dots, q_t$ — различные простые числа. При этом, так как числа a и b, по условию, взаимно просты, то ни одно из чисел $p_1, \dots, p_s$ не равно ни одному из чисел $q_1, \dots, q_t$. Следовательно, формула

$$c^n = p_1^{k_1} \dots p_s^{k_s} q_1^{l_1} \dots q_t^{l_t} \tag{2}$$

дает разложение чисел $c^n = ab$ в произведение степеней различных простых чисел. Но известно (это так называемая основная теорема арифметики), что разложение натурального числа в произведение степеней различных простых чисел единственно (с точностью до порядка множителей). Поэтому разложение (2) должно совпадать с разложением, которое получается, когда мы возьмем разложение числа c и возведем его в n-ю степень. Это доказывает, что все показатели $k_1, \dots, k_s, l_1, \dots, l_t$ делятся на n. Поэтому и a, и b является n-й степенью.

Мы привели это доказательство (безусловно, известное читателю) в основном для того, чтобы подчеркнуть роль, которую играет в нем основная теорема арифметики.

Для любого примитивного решения (x, y, z) уравнения

$$x^l + y^l = z^l, \quad l \text{ простое } \geqslant 3, \tag{3}$$

число z^l будет произведением целых чисел

$$a = x + y$$

и

$$(4) \qquad b = \frac{x^l + y^l}{x + y} = \frac{(a-y)^l + y^l}{a} =$$

$$= a^{l-1} - \binom{l}{1} a^{l-2}y + \ldots + (-1)^k \binom{l}{k} a^{l-k-1}y^k + \ldots$$

$$\ldots + \binom{l}{l-1} y^{l-1},$$

где

$$\binom{l}{k} = \frac{l!}{k!\,(l-k)!}$$

— так называемые биномиальные коэффициенты (часто обозначаемые также символом C_l^k).

Из равенства (4) следует, что любой общий простой делитель p чисел a и b делит число

$$\binom{l}{l-1} y^{l-1} = ly^{l-1},$$

и потому, если $p \neq l$, то и число y. Но если p делит a и y, то p делит $x = a - y$, что невозможно, ибо, по условию, числа x и y взаимно просты. Если теперь z не делится на l, то l не делит $z^l = ab$, а значит, ни a, ни b. Таким образом, в этом случае числа a и b взаимно просты и потому, согласно лемме (в которой положено $c = z$ и $n = l$), существуют такие целые числа u и v, что

$$x + y = u^l, \quad \frac{x^l + y^l}{x + y} = v^l, \quad z = uv.$$

Заметив теперь, что уравнение (3) может быть переписано в виде

$$x^l + y^l + (-z)^l = 0$$

и, следовательно, что числа x, y, $-z$ играют в нем вполне симметричные роли, мы получим, что аналогичные формулы должны иметь место для тройки $(y, -z, x)$ и для тройки $(-z, x, y)$. Этим доказано, что *для любых взаимно простых и не делящихся на l целых чисел x, y, z, удовлетворяющих уравнению*

$$x^l + y^l = z^l, \quad l \text{ — нечетное простое число},$$

существуют такие пары целых чисел (u, v), (u_1, v_1) *и* (u_2, v_2), *состоящие из взаимно простых чисел, что*

$$
\begin{aligned}
&x+y=u^l, \quad \frac{x^l+y^l}{x+y}=v^l, \quad z=uv,\\
&z-y=u_1^l, \quad \frac{z^l-y^l}{z-y}=v_1^l, \quad x=u_1v_1,\\
&z-x=u_2^l, \quad \frac{z^l-x^l}{z-x}=v_2^l, \quad y=u_2v_2.
\end{aligned}
\tag{5}
$$

Эти формулы известны как формулы Абеля, хотя их знала еще Жермен, а опубликованы они впервые были Лежандром.

Аналогичные (но более сложные) формулы могут быть выведены и в случае, когда одно из чисел x, y, z делится на l. Однако за полтораста лет интенсивных исследований эти формулы никакой реальной пользы не принесли, и поэтому мы их выписывать здесь не будем.

Исследование теоретико-числовых проблем, связанных с делимостью чисел, существенно облегчается удобными обозначениями, предложенными Гауссом.

Пусть n — произвольное натуральное число. Согласно Гауссу, целые числа a и b называются *сравнимыми по модулю* n, если их разность $a-b$ делится на n. В этом случае пишут

$$a \equiv b \bmod n.$$

Ясно, что отношение сравнимости является отношением эквивалентности, и потому множество Z всех целых чисел распадается на классы сравнимых между собой чисел. Множество всех этих классов мы будем обозначать символом Z/n.

Сравнения, подобно равенствам, можно складывать и умножать. Их можно также сокращать на общий множитель, если только этот множитель взаимно прост с n. На языке современной алгебры это означает, что множество Z/n всех классов сравнимых чисел является кольцом (ассоциативным, коммутативным и обладающим единицей), причем классы, состоящие из чисел, взаимно простых с n, не являются в этом кольце делителями нуля.

Более того, легко видеть, что эти классы в кольце Z/n даже обратимы, т. е. для любого числа a, взаимно простого с n, существует такое число b («обратное по модулю n для a»), что

$$ab \equiv 1 \bmod n. \tag{6}$$

Действительно, так как числа a и n взаимно просты, то по известной теореме элементарной теории чисел (которую, кстати сказать, мы докажем в § 4), существуют такие целые числа x и y, что

$$nx+ay=1.$$

Но ясно, что это равенство в точности равносильно сравнению (6) с $b = y$.

В частности, мы видим, что если $n = l$, где l — простое число, то все отличные от нуля элементы кольца Z/l обратимы, т. е. *это кольцо является полем.*

Иными словами, *множество Z^*/l всех отличных от нуля элементов кольца Z/l является группой по умножению.*

С другой стороны, ясно, что любое число сравнимо по модулю l с одним и только одним из чисел

$$0, 1, 2, \ldots, l-1, \tag{7}$$

откуда следует, что поле Z/l содержит l элементов, а группа Z^*/l содержит $l-1$ элементов, т. е. порядок этой группы равен $l-1$.

Но из элементарной теории групп известно, что, возведя любой элемент конечной группы в степень, равную порядку группы, мы получим единицу группы. Применительно к группе Z^*/l это означает, что

$$a^{l-1} \equiv 1 \bmod l \tag{8}$$

для любого целого числа a, не делящегося на l. Это утверждение называется малой теоремой Ферма.

Умножив сравнение (8) на a, мы получим сравнение

$$a^l \equiv a \bmod l. \tag{9}$$

Ясно, что это сравнение выполнено и при $a \equiv 0 \bmod l$. Таким образом, *сравнение* (9) *имеет место для любых целых чисел a.* Это — малая теорема Ферма в формулировке Эйлера.

На более алгебраическом языке сравнение (9) означает, что *каждый элемент поля Z/l является корнем многочлена $x^l - x$.*

Доказать сравнение (9) можно, и не обращаясь к теории групп, например, следующим образом.

Из того, что простое число l делит $l!$ и при $0 < k < l$ не делит $k!(l-k)!$, следует, что все биномиальные коэффициенты

$$\binom{l}{k} = \frac{l!}{k!\,(l-k)!}, \qquad 0 < k < l,$$

делятся на l. Поэтому

$$(x_1 + x_2)^l \equiv x_1^l + x_2^l \bmod l$$

для любых (целых) x_1 и x_2.

Очевидной индукцией отсюда вытекает аналогичная формула для любого числа слагаемых:

$$(x_1 + x_2 + \ldots + x_n)^l \equiv x_1^l + x_2^l + \ldots + x_n^l \bmod l. \tag{10}$$

Положив в этой формуле $x_1 = \ldots = x_n = 1$, мы и получим (9) (при $a = n$). ■

Теперь мы можем непосредственно приступить к изложению исследований Жермен.

Пусть (x, y, z) — примитивное решение уравнения (3), состоящее из чисел, не делящихся на l. Рассмотрим произвольное простое число p, сравнимое с единицей по модулю l, т. е. имеющее вид

$$p = 2ml + 1,$$

где m — некоторое целое число. Предположим, что ни одно из чисел x, y, z не делится на p. Поскольку $x \not\equiv 0 \bmod p$, существует такое целое число x', что

$$xx' \equiv 1 \bmod p.$$

Умножив на $(x')^l$ равенство (3) и перейдя к сравнениям, мы получим, что $1 + (yx')^l \equiv (zx')^l \bmod p$, т. е. что

$$1 + a^l \equiv b^l \bmod p,$$

где $a = yx'$, $b = zx'$ не делятся на p.

Целое число ξ мы будем называть *l-й степенью по модулю p*, если существует такое число $a \not\equiv 0 \bmod p$, что

$$\xi \equiv a^l \bmod p.$$

Кроме того, две l-е степени ξ и η мы будем называть *соседними по модулю p*, если

$$\xi - \eta \equiv \pm 1 \bmod p.$$

В этой терминологии доказанное выше сравнение означает, что, *если ни одно из чисел x, y, z не делится на p, то существуют соседние l-е степени по модулю p.*

Предположим теперь, что одно (и, в силу примитивности, только одно) из чисел x, y, z делится на p. Для определенности будем считать, что на p делится число z. Тогда одно (и только одно) из фигурирующих в формуле Абеля $z = uv$ (см. (5)) взаимно простых чисел u и v будет делиться на p.

Пусть на p делится v. Тогда u на p не делится, и потому существует такое число u', что

$$uu' \equiv 1 \bmod p.$$

С другой стороны, из формул Абеля (5) следует, что

$$2z = u^l + u_1^l + u_2^l.$$

Поэтому

$$u^l + u_1^l \equiv (-u_2)^l \bmod p$$

и, значит,

$$1 + (u_1 u')^l \equiv (-u_2 u')^l \bmod p.$$

Таким образом, *если* $u \not\equiv 0 \bmod p$, *то также существуют соседние* l*-е степени по модулю* p.

Пусть, наконец, на p делится u. Тогда в соотношении (4) (где, напомним, $b = v^l$, $a = u^l$) все слагаемые правой части, кроме последнего $\binom{l}{l-1} y^{l-1} = ly^{l-1}$, будут делиться на p, и, следовательно, будет иметь место сравнение

$$v^l \equiv ly^{l-1} \bmod p.$$

Но по тем же формулам Абеля

$$y = z - u_1^l,$$

т. е.

$$y \equiv (-u_1)^l \bmod p.$$

Следовательно,

$$v^l \equiv l(-u_1)^{l(l-1)} \bmod p$$

и потому

$$l \equiv (vu_1')^l \bmod p,$$

где u_1' — такое число, что

$$u_1^{l-1} u_1' \equiv 1 \bmod p$$

(ясно, что u_1, а значит, и u_1^{l-1} не делится на p).

Этим доказано, что *при* $u \equiv 0 \bmod p$ *число* l *является* l*-й степенью по модулю* p.

Тем самым доказана следующая теорема:

Теорема Софи Жермен. *Пусть для простого числа* $l \geqslant 3$ *существует такое целое число* m, *что*

1) *число* $p = 2ml + 1$ *является простым числом*;

2) *среди* l*-х степеней по модулю* p *нет соседних*;

3) *число* l *не является* l*-й степенью по модулю* p.

Тогда для показателя l *справедлив первый случай теоремы Ферма.*

Для проверки в конкретных ситуациях условий 2) и 3) этой теоремы полезно иметь в виду, что *любая l-я степень ξ по модулю $p = 2ml + 1$ удовлетворяет сравнению*

$$\xi^{2m} \equiv 1 \bmod p. \tag{11}$$

Действительно, если $\xi = a^l \bmod p$, где $a \not\equiv 0 \bmod p$, то по малой теореме Ферма

$$\xi^{2m} \equiv a^{2ml} \equiv a^{p-1} \equiv 1 \bmod p. \quad \blacksquare$$

Задача. Докажите, что и обратно, любое решение ξ сравнения (11) является l-й степенью по модулю p.

Легко видеть, что для любого простого числа p существует только два не сравнимых числа ξ, удовлетворяющих сравнению

$$\xi^2 \equiv 1 \bmod p,$$

а именно, числа 1 и $-1 \equiv p - 1 \bmod p$.

Тот факт, что числа 1 и $p-1$ удовлетворяют этому сравнению, очевиден, а то, что других корней это сравнение не имеет, проще всего доказывается ссылкой на теорему алгебры о том, что в произвольном поле многочлен степени n не может иметь более n корней. (Можно также воспользоваться тем, что число $\xi^2 - 1 = (\xi - 1)(\xi + 1)$ тогда и только тогда делится на простое число p, когда $\xi - 1$ или $\xi + 1$ делятся на p.)

Так как числа 1 и $p-1$ не являются, очевидно, соседними l-ми степенями по модулю $p = 2l + 1$, этим доказано, что при $m = 1$ условие 2) теоремы Жермен автоматически выполнено.

Поскольку число $l^2 - 1 = (l + 1)(l - 1)$ не может делиться на простое число $2l+1 > l + 1$, то при $m=1$ условие 3) также выполнено.

Таким образом, *если показатель l (являющийся простым нечетным числом) обладает тем свойством, что число $2l + 1$ также является простым числом, то для l справедлив первый случай теоремы Ферма.*

Как уже было сказано на стр. 15, это следствие выведено самой Жермен. Многие авторы именно его называют теоремой Жермен.

Аналогичным образом из общей теоремы Жермен может быть выведена сформулированная на стр. 15 теорема Лежандра.

Мы сделаем это только для $m = 2$, поскольку с увеличением m рассуждения стремительно усложняются.

Пусть при $m = 2$ условие 1) теоремы Жермен выполнено, т. е. число $p = 4l + 1$ является простым числом.

Проверим, что условие 2) этой теоремы также будет выполнено. Согласно сделанному выше замечанию, для этого достаточно доказать, что среди корней сравнения

$$\xi^4 \equiv 1 \bmod p \tag{12}$$

нет соседних.

Так как $\xi^4 - 1 = (\xi^2 + 1)(\xi^2 - 1)$, то корнями сравнения (12) будут корни сравнения

$$\xi^2 \equiv 1 \bmod p$$

и сравнения

$$\xi^2 \equiv -1 \bmod p.$$

Первое сравнение имеет, как мы знаем, корни 1 и $-1 \equiv p - 1$. Что же касается второго сравнения, то a priori возможны два случая: либо оно не имеет корней, либо обладает точно двумя корнями ξ_0 и $-\xi_0 \equiv p - \xi_0$.

В первом случае сравнение (12) имеет корни 1 и $p - 1$, заведомо не соседние. Таким образом, условие 2) теоремы Жермен в этом случае выполнено.

Во втором случае (кстати сказать, как можно без труда показать, единственно на самом деле реализующемся) сравнение (12) имеет четыре корня

$$1 \quad p - 1, \quad \xi_0, \quad p - \xi_0.$$

Соседними два из этих корней могут быть только при $\xi_0 = \pm 2$ или при $\xi_0 = \pm(p-1)/2 = \pm 2l$. Если $\xi_0 = \pm 2$, то $2^2 + 1 = 5$ делится на $p = 4l + 1$, что при $l > 1$ невозможно. Аналогично, если $\xi_0 = \pm 2l$, то $(2l)^2 + 1 = (4l + 1)l - (l - 1)$ делится на $p = 4l + 1$, т. е. $l - 1$ делится на $4l + 1$, что при $l > 1$ также невозможно. Следовательно, условие 2) теоремы Жермен выполнено и в этом случае.

Обратимся теперь к условию 3). Если оно не выполнено, то $l^4 \equiv 1 \bmod p$. Но поскольку при $p = 4l + 1$ имеет место сравнение $4l \equiv -1 \bmod p$, а потому и сравнение $(4l)^4 \equiv 1 \bmod p$, отсюда следует, что

$$4^4 \equiv 1 \bmod p,$$

т. е. что $4^4 - 1 = 255 = 3 \cdot 5 \cdot 17$ делится на p. Так как мы уже знаем, что $p \neq 5$, это возможно только при $p = 17$. Но уравнение $17 = 4l + 1$ имеет непростое решение $l = 4$, и потому этот случай также невозможен. Следовательно, условие 3) должно быть выполнено. ■

Теорема Вендта (см. стр. 16) также сводится к теореме Жермен. Следует лишь доказать, что если простое число $p = 2ml + 1$ не делит число Вендта D_m, то условие 2) теоремы Жермен выполнено.

Это доказательство мы оставляем читателю в качестве несложного упражнения.

§ 2. Теорема Ферма для показателя 4

Случай $n = 4$ — это единственный случай теоремы Ферма, допускающий вполне элементарное доказательство. Как мы уже говорили, это доказательство было придумано еще самим Ферма. Оно использует формулы общего решения уравнения

$$x^2 + y^2 = z^2, \tag{1}$$

которые были известны еще индусам. Мы начнем с того, что докажем эти формулы.

Как мы знаем, достаточно искать примитивные решения уравнения (1). Ясно, что если (x, y, z) — решение, то (y, x, z) также будет решением. С другой стороны, для любого решения (x, y, z) хотя бы одно из чисел x или y четно. Действительно, если x и y нечетны, то $x^2 + y^2$ имеет вид $4k + 2$ и потому не может быть равно квадрату z^2 никакого целого числа (ибо каждый квадрат z^2 имеет либо вид $4k$ либо вид $4k + 1$). Кроме того, очевидно, что вместе с решением (x, y, z) и $(\pm x, \pm y, \pm z)$ также будет решением.

Из этих замечаний непосредственно следует, что нам достаточно найти лишь состоящие из положительных чисел примитивные решения (x, y, z) уравнения (1), для которых число x четно.

Лемма. *Для любых взаимно простых положительных целых чисел m и $n < m$ разной четности формулы*

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

доставляют состоящее из положительных целых чисел примитивное решение уравнения (1) *с четным x. Обратно, любое состоящее из положительных чисел примитивное решение (x, y, z) уравнения* (1), *для которого x четно, выражается формулами* (2), *где m и $n < m$ — взаимно простые числа разной четности.*

Доказательство. Тождество

$$(2mn)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2$$

показывает, что числа (2) (очевидно, положительные) составляют решение, для которого x четно. Если эти

числа имеют общий множитель $\lambda \geqslant 2$, то λ будет делить и числа

$$2m^2 = (m^2 + n^2) + (m^2 - n^2),$$
$$2n^2 = (m^2 + n^2) - (m^2 - n^2).$$

Значит, $\lambda = 2$, ибо, по условию, m и n взаимно просты. Но если $\lambda = 2$, то число $y = m^2 - n^2$ четно, и, следовательно, числа m^2 и n^2 одновременно либо четны, либо нечетны, что невозможно, ибо по условию числа m и n имеют разную четность. Это доказывает, что решение (2) примитивно.

Обратно, путь (x, y, z) — произвольное состоящее из положительных чисел примитивное решение с четным $x = 2a$. Так как числа y и z нечетны, то числа $z + y$ и $z - y$ четны. Пусть

$$z + y = 2b, \quad z - y = 2c,$$

где числа b и c, очевидно, положительны.

Каждый общий делитель λ чисел b и c делит $z = b + c$ и $y = b - c$. Поэтому $\lambda = \pm 1$, так что числа b и c взаимно просты. С другой стороны,

$$4a^2 = x^2 = z^2 - y^2 = 4bc,$$

т. е.

$$a^2 = bc.$$

Следовательно, согласно лемме из § 1 (примененной к случаю $n = 2$), существуют такие (очевидно, взаимно простые и разной четности) положительные числа m и n, что

$$b = m^2, \quad c = n^2.$$

Тогда $a^2 = m^2n^2$, т. е. $a = mn$ и

$$x = 2a = 2mn, \quad y = b - c = m^2 - n^2,$$
$$z = b + c = m^2 + n^2.$$

Для завершения доказательства остается заметить, что $n < m$. ■

Теперь мы можем перейти к доказательству теоремы Ферма при $n = 4$. Мы докажем даже более общее утверждение:

Предложение 1. *Уравнение*

$$x^4 + y^4 = z^2 \tag{3}$$

не имеет решений в целых отличных от нуля числах.

Доказательство. Предположим, что решение уравнения (3) в целых отличных от нуля числах существует. Ясно, что, не теряя общности, мы можем считать, что оно состоит из попарно взаимно простых положительных чисел. Так как в любом множестве натуральных чисел существует наименьшее число, то среди всех таких решений существует решение (x, y, z) с наименьшим z. Рассмотрим это решение более внимательно.

Так же, как для решений уравнения (1), немедленно доказывается, что одно из чисел x и y должно быть четным. Мы будем предполагать, что четно число x. Ясно, что это предположение общности не ограничивает.

Так как

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

и так как числа x^2, y^2, z положительны и взаимно просты, а число x^2 четно, то, согласно лемме, существуют такие взаимно простые числа m и $n < m$ разной четности, что

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

Если $m = 2k$ и $n = 2l + 1$, то

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

что невозможно, ибо, как выше мы уже отмечали, любой нечетный квадрат должен иметь вид $4k + 1$. Следовательно, число m нечетно, а число n четно.

Пусть $n = 2q$. Тогда $x^2 = 4mq$ и потому

$$mq = \left(\frac{x}{2}\right)^2.$$

Поскольку числа m и q взаимно просты, отсюда вытекает, что

$$m = z_1^2, \quad q = t^2,$$

где z_1 и t — некоторые целые (очевидно, взаимно простые) положительные числа.

В частности, мы видим, что

$$y^2 = (z_1^2)^2 - (2t^2)^2,$$

т. е. что

$$(2t^2)^2 + y^2 = (z_1^2)^2.$$

Так как числа t и z_1 взаимно просты, к этому равенству снова применима доказанная выше лемма. Следовательно, существуют такие положительные взаимно простые числа a и $b < a$ различной четности, что

$$2t^2 = 2ab, \quad \text{т. е.} \quad t^2 = ab,$$
$$y^2 = a^2 - b^2,$$
$$z_1^2 = a^2 + b^2.$$

Так как a и b взаимно просты, из первого равенства вытекает (по лемме из § 1), что существуют целые числа x_1 и y_1, для которых

$$a = x_1^2, \quad b = y_1^2.$$

Поэтому третье равенство может быть переписано следующим образом:

$$x_1^4 + y_1^4 = z_1^2.$$

Это означает, что числа x_1, y_1, z_1 составляют (очевидно, примитивное) решение уравнения (3), состоящее из положительных чисел. Поэтому в силу выбора решения (x, y, z) должно иметь место неравенство

$$z_1 \geqslant z,$$

а потому и неравенство

$$z_1^2 \geqslant z,$$

т. е. абсурдное неравенство

$$m \geqslant m^2 + n^2.$$

Таким образом, предположение о существовании у уравнения (3) целочисленных решений приводит к противоречию. Следовательно, это уравнение не имеет решений в целых отличных от нуля числах. ■

§ 3. Теорема Ферма для показателя 3

Как уже говорилось, теорема Ферма при $l = 3$ впервые была доказана Эйлером в 1768 году. Мы воспроизведем сейчас это доказательство Эйлера.

Эйлер основывается на следующей лемме.

Лемма. *Если взаимно простые целые числа a и b обладают тем свойством, что число $a^2 + 3b^2$ является кубом целого числа, то существуют такие целые числа s и t, что*

$$a = s(s^2 - 9t^2), \qquad b = 3t(s^2 - t^2).$$

Покажем сначала, как из этой леммы вытекает теорема Ферма.

Предположим, что при $l = 3$ теорема Ферма неверна, т. е. что существуют такие целые отличные от нуля числа x, y и z, что

$$x^3 + y^3 = z^3. \tag{1}$$

Как мы знаем, числа x, y и z мы можем считать попарно взаимно простыми. Поэтому, в частности, только одно из них может быть четным. С другой стороны, ясно, что все три числа нечетными быть не могут (сумма или разность двух нечетных чисел четна). Следовательно, одно и только одно из чисел x, y, z четно.

Без ограничения общности мы можем считать, что четно число x. Действительно, если четно y, то достаточно переименовать x и y, а если четно z, то достаточно переименовать x и z и изменить знаки (ибо $(-z)^3 + y^3 = (-x)^3$).

Среди всех троек (x, y, z) целых чисел, удовлетворяющих уравнению (1) и таких, что x четно, мы выберем тройку, для которой $|x|$ имеет наименьшее возможное значение. Такая «минимальная» тройка существует, ибо в любом непустом множестве целых положительных чисел существует наименьшее число.

Так как y и z нечетны, то числа

$$p = \frac{z+y}{2} \quad \text{и} \quad q = \frac{z-y}{2}$$

целые. Так как

$$z = p + q, \qquad y = p - q, \tag{2}$$

то одно из чисел p и q четно, а другое нечетно. Кроме того, эти числа, очевидно, взаимно просты.

Согласно (1) и (2)

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

Полагая здесь $x = 2u$, мы получим, что

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

Так как p и q — числа разной четности, то число $q^2 + 3p^2$ нечетно. Поэтому из (3) следует, что q делится на 4 (и, значит, q четно, а p нечетно).

Согласно доказанной в § 1 лемме, произведение двух взаимно простых чисел тогда и только тогда является кубом, когда каждое из них является кубом. С другой стороны, числа $q/4$ и $q^2 + 3p^2$ тогда и только тогда взаимно просты, когда взаимно просты числа q и $3p^2 = (q^2 + 3p^2) - q^2$, что имеет место (в силу взаимной простоты чисел p и q) тогда и только тогда, когда q не делится на 3. Поэтому, если мы предположим, что q не делится на 3, то из (3) будет следовать, что числа $q/4$ и $q^2 + 3p^2$ являются кубами.

Но, согласно лемме, если $q^2 + 3p^2$ — куб, то

$$q = s(s^2 - 9t^2), \qquad p = 3t(s^2 - t^2),$$

где s и t — некоторые целые числа. Так как p нечетно, то из равенства $p = 3t(s^2 - t^2)$ следует, что t нечетно, а s четно. Кроме того, так как p и q взаимно просты, то t и s также взаимно просты.

Так как число $q/4$ — куб, то число $2q = 8 \cdot q/4$ — также куб. Это доказывает, что число

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

тоже является кубом.

Числа $2s$, $s - 3t$ и $s + 3t$ взаимно просты. Действительно, если $2s$ и $s \pm 3t$ имеют общий простой множитель λ, то $\lambda \neq 2$, ибо число $s \pm 3t$ нечетно. Следовательно, λ делит s и $\pm 3t = (s \pm 3t) - s$. Но, так как t и s взаимно просты, это возможно только при $\lambda = 3$. Аналогично, если числа $s + 3t$ и $s - 3t$ имеют общий простой множитель λ, то, во-первых, $\lambda \neq 2$, ибо оба эти числа нечетны, а, во-вторых, числа

$2s = (s + 3t) + (s - 3t)$ и $6t = (s + 3t) - (s - 3t)$ делятся на λ, что опять возможно только при $\lambda = 3$. Таким образом, в обоих случаях число s, а, значит, и число q делится, вопреки предположению, на $\lambda = 3$.

Так как произведение взаимно простых чисел $2s$, $s - 3t$ и $s + 3t$ является кубом, то, следовательно, кубом будет и каждое из них. Это означает, что существуют такие целые числа x_1, y_1 и z_1, что

$$x_1^3 = 2s,$$
$$y_1^3 = -(s + 3t),$$
$$z_1^3 = s - 3t,$$

и, следовательно,

$$x_1^3 + y_1^3 = z_1^3.$$

Таким образом, исходя из тройки (x, y, z), мы получили новую тройку (x_1, y_1, z_1), также удовлетворяющую уравнению (1) и обладающую тем свойством, что ее первое число x_1 четно.

Так как $x^3 = 2q(q^2 + 3p^2)$, то $|q| < \frac{|x^3|}{2}$, а так как $q = s(s^2 - 9t^2)$, то $|s| \leqslant |q|$. Следовательно,

$$|x_1^3| = 2|s| < |x^3|$$

и потому $|x_1| < |x|$, что противоречит свойству минимальности тройки (x, y, z). Полученное противоречие доказывает, что число q должно делиться на 3, т. е. должно иметь место равенство

$$q = 3r,$$

где r — некоторое целое число (делящееся на 4). Тогда (см. (3))

$$u^3 = \frac{3}{4} r(9r^2 + 3p^2) = \frac{9}{4} r(3r^2 + p^2). \tag{4}$$

Если целые числа $\frac{9}{4}r$ и $3r^2 + p^2$ имеют общий простой множитель λ, то $\lambda \neq 3$, так как в противном случае число p делится на 3 и, значит, не взаимно просто с q. Но если $\lambda \neq 3$, то λ делит r

и $p^2=(3r^2+p^2)-3r^2$, а значит, q и p, что невозможно. Следовательно, числа $\frac{9}{4}r$ и $3r^2+p^2$ взаимно просты.

Поэтому из (4) следует, что оба эти числа являются кубами и потому, согласно лемме (примененной к числу p^2+3r^2), имеют место равенства

$$p=s(s^2-9t^2), \quad r=3t(s^2-t^2), \tag{5}$$

где s и t — некоторые (очевидно, взаимно простые) целые числа. При этом ясно, что число t четно (ибо r четно), а число s, следовательно, нечетно.

Кроме того, мы видим, что (целое) число

$$\frac{8}{27}\cdot\frac{9}{4}r=\frac{2}{3}r=2t(s^2-t^2)=2t(s+t)(s-t)$$

является кубом.

Так как числа s и t взаимно просты и имеют разную четность, то числа $2t$, $s+t$ и $s-t$ попарно взаимно просты. Поэтому каждое из них является кубом, так что существуют такие целые числа x_1, y_1 и z_1, что

$$x_1^3=2t,$$
$$y_1^3=s-t,$$
$$z_1^3=s+t.$$

Но тогда

$$x_1^3+y_1^3=z_1^3$$

и

$$|x_1^3|=2|t|\leqslant\frac{2}{3}|r|=\frac{2}{9}|q|<2|q|<|x^3|,$$

т. е. $|x_1|<|x|$.

Таким образом, и в этом случае мы приходим в противоречие с минимальностью тройки (x, y, z). ■

§ 4. Арифметика кольца D_3

Итак, для завершения доказательства теоремы Ферма при $l=3$ нам осталось лишь доказать сформулированную выше лемму.

Эйлер доказывает эту лемму, замечая, что [1])

$$a^2+3b^2=(a+b\sqrt{-3})(a-b\sqrt{-3}).$$

Потом он пишет, что, поскольку левая часть является по условию кубом, то и оба множителя правой части должны быть кубами. В частности,

$$a+b\sqrt{-3}=(s+t\sqrt{-3})^3,$$

где s и t — некоторые целые числа. Возводя в куб, мы получаем, что

$$a+b\sqrt{-3}=s^3-9st^2+(3s^2t-3t^3)\sqrt{-3}$$

и, следовательно, что

$$a=s^3-9st^2=s(s^2-9t^2),$$
$$b=3s^2t-3t^3=3t(s^2-t^2). \quad \blacksquare$$

Нельзя не отдать должное остроумию и смелости Эйлера, бесстрашно перешедшего от целых чисел к числам вида $a+b\sqrt{-3}$. Но, конечно, чтобы сделать его доказательство безупречным, надо предварительно построить арифметику таких чисел. В частности, поскольку утверждение о произведениях, являющихся кубами, существенно зависит, как мы знаем, от основной теоремы арифметики, нужно для чисел вида $a+b\sqrt{-3}$ доказать аналог этой теоремы (мы не говорим уже о том, что требует доказательства «взаимная простота» чисел $a+b\sqrt{-3}$ и $a-b\sqrt{-3}$).

Однако оказывается, что *для чисел вида* $a+b\sqrt{-3}$ *основная теорема арифметики неверна*: единственности разложения на «простые» (далее неразложимые) множители нет. Например,

$$4=2\cdot 2=(1+\sqrt{-3})(1-\sqrt{-3})$$

и, вместе с тем, числа 2 и $1\pm\sqrt{-3}$ неразложимы.

Доказательство. Имеем

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

[1]) Здесь и далее под $\sqrt{-3}$ понимается корень уравнения $x^2+3=0$, лежащий в верхней полуплоскости.

Поэтому, если

$$2=(a+b\sqrt{-3})(c+d\sqrt{-3}),$$

то

$$\begin{cases} ac-3bd=2, \\ ad+bc=0 \end{cases}$$

Можно непосредственно доказать, что эти уравнения не имеют решений в целых числах, но лучше поступить по-другому, заметив, что они не меняются при одновременном изменении знака у b и d. Поэтому

$$2=(a-b\sqrt{-3})(c-d\sqrt{-3})$$

и значит,

$$2\cdot 2=(a+b\sqrt{-3})(a-b\sqrt{-3})\cdot(c+d\sqrt{-3})(c-d\sqrt{-3}),$$

т. е.

$$4=(a^2+3b^2)(c^2+3d^2). \tag{1}$$

Аналогично, если

$$1+\sqrt{-3}=(a+b\sqrt{-3})(c+d\sqrt{-3}),$$

то

$$1-\sqrt{-3}=(a-b\sqrt{-3})(c-d\sqrt{-3}),$$

и потому мы снова получаем уравнение (1).

Поскольку в этом уравнении участвуют только натуральные числа, то либо один из множителей правой части равен 4, а другой 1, т. е., скажем,

$$a^2+3b^2=4,$$
$$c^2+3d^2=1,$$

либо оба они равны 2, т. е.

$$a^2+3b^2=2,$$
$$c^2+3d^2=2$$

Но ясно, что уравнение вида $a^2+3b^2=2$ не имеет решения в целых числах. Поэтому второй случай невозможен. Что же касается первого, то уравнение

$$a^2+3b^2=4$$

удовлетворяется только при $a=\pm 1$, $b=\pm 1$ и $a=\pm 2$, $b=0$, а уравнение

$$c^2+3d^2=1$$

— только при $c=\pm 1$, $d=0$.

Это доказывает неразложимость как числа 2, так и чисел $1\pm\sqrt{-3}$. ■

Тем не менее, рассуждение Эйлера можно спасти, если чуть глубже вникнуть в предмет.

Поставим вопрос, закономерно ли у Эйлера появились числа вида $a+b\sqrt{-3}$, или это было случайным эффектом, обязанным изобретательности Эйлера?

Если вообще прибегать к каким-нибудь нецелым числам, то в первую очередь следует, конечно, привлечь числа, участвующие в разложении левой части уравнения Ферма на линейные множители. Такое разложение имеет вид

$$x^3+y^3=(x+y)(x+\zeta y)(x+\bar{\zeta}y),$$

где ζ и $\bar{\zeta}$ — комплексные числа, являющиеся вместе с 1 корнями уравнения

$$x^3=1. \tag{2}$$

Это соображение подсказывает, что естественной областью, в которой следует рассматривать уравнение Ферма при $l=3$, являются числа вида

$$a+b\zeta+c\bar{\zeta}, \tag{3}$$

где a, b и c — целые числа.

Но легко видеть, что вместе с числом ζ корнем уравнения (2) будет и число ζ^2, ибо

$$(\zeta^2)^3=(\zeta^3)^2=1^2=1.$$

Поэтому $\zeta^2=\bar{\zeta}$, и, значит, число (3) мы можем записывать в виде

$$a+b\zeta+c\zeta^2. \tag{3'}$$

Более того, число ζ (вместе с числом $\bar{\zeta}=\zeta^2$) является корнем уравнения

$$\frac{x^3-1}{x-1}=x^2+x^2+1=0,$$

откуда следует, что

$$\zeta^2=-1-\zeta. \tag{4}$$

Поэтому любое число вида (3') имеет вид

$$A+B\zeta, \tag{5}$$

где $A=a-c$, $B=b-c$.

Итак, мы видим, что нам следует ввести в рассмотрение множество всех чисел вида (5), где A и

B — произвольные целые числа. Это множество мы будем обозначать символом D_3.

Ясно, что сумма и разность чисел из D_3 является числом из D_3. Более того, произведение любых двух чисел из D_3 также будет числом из D_3, поскольку появляющийся после перемножения член с ζ^2 мы можем преобразовать с помощью соотношения (4). (Таким образом, $(A + B\zeta)(A_1 + B_1\zeta) = (AA_1 - BB_1) + (AB_1 + BA_1 - BB_1)\zeta$.)

На языке современной алгебры все это означает, что D_3 *является кольцом* (числовым).

Для удобства вычислений целесообразно рассматривать также числа вида (5) с произвольными рациональными A и B. Множество таких чисел мы обозначим через K_3.

Ясно, что сумма, разность и произведение чисел из K_3 также будет числом из K_3. Однако теперь и частное любых двух чисел из K_3 будет числом из K_3. Действительно, любое число вида $\frac{C + D\zeta}{A + B\zeta}$, где, конечно, $A + B\zeta \neq 0$, мы можем преобразовать следующим образом (в элементарной алгебре это называется «освобождением знаменателя от иррациональности»):

$$\frac{C + D\zeta}{A + B\zeta} = \frac{(C + D\zeta)(A + B\bar{\zeta})}{(A + B\zeta)(A + B\bar{\zeta})} = \frac{(C + D\zeta)(A + B\zeta^2)}{A^2 + AB(\zeta + \bar{\zeta}) + B^2\zeta\bar{\zeta}} =$$

$$= \frac{CA + DA\zeta + CB\zeta^2 + DB\zeta^3}{A^2 - AB + B^2} =$$

$$= \frac{CA + DB - CB}{A^2 - AB + B^2} + \frac{DA - CB}{A^2 - AB + B^2}\zeta.$$

Все это означает, что K_3 *является полем*. Оно называется 3-*круговым полем* (это название возникло из-за тесной связи корней уравнения (2) с задачей деления круга на 3 части). Числа из D_3 называются, естественно, *целыми числами поля* K_3; соответственно этому, D_3 называется *кольцом целых чисел* поля K_3. Оно содержит все обычные целые числа (они получаются при $B = 0$).

Заметим, что запись числа из D_3 (или из K_3) в форме (5) *единственна*. Действительно, если

$$A + B\zeta = A_1 + B_1\zeta$$

и $B \neq B_1$, то

$$\zeta = -\frac{A - A_1}{B - B_1},$$

что невозможно, ибо ζ не является вещественным и, тем более, рациональным числом. Следовательно, $B = B_1$ и потому $A = A_1$. ■

Выше при вычислении частного в K_3 мы фактически ввели для любого числа

$$\alpha = A + B\zeta \in K_3$$

число

$$N\alpha = \alpha\bar{\alpha} = A^2 - AB + B^2 = \frac{(2A - B)^2 + 3B^2}{4}.$$

Это неотрицательное рациональное число (целое, когда $\alpha \in D_3$) называется *нормой* числа α. Оно равно нулю только при $\alpha = 0$.

Замечательное свойство нормы состоит в том, что *норма произведения равна произведению норм*:

$$N(\alpha\beta) = N\alpha \cdot N\beta, \quad \alpha, \beta \in K_3. \tag{6}$$

Действительно,

$$N(\alpha\beta) = \alpha\beta \cdot \overline{\alpha\beta} = \alpha\beta \cdot \bar{\alpha}\bar{\beta} = \alpha\bar{\alpha} \cdot \beta\bar{\beta} = N\alpha \cdot N\beta. \quad ■$$

В раскрытом виде соотношение (6) имеет вид

$$(AA_1 - BB_1)^2 - (AA_1 - BB_1)(AB_1 + BA_1 - BB_1) + (AB_1 + BA_1 - BB_1)^2 = (A^2 - AB + B^2)(A_1^2 - A_1B_1 + B_1^2)$$

Оно является простейшим примером алгебраических тождеств, возникающих из соотношений вида (6) для других полей алгебраических чисел.

Числа из K_3 (и D_3) можно записать в более явной форме, заметив, что квадратное уравнение

$$x^2 + x + 1 = 0$$

имеет корни

$$\frac{-1 \pm \sqrt{-3}}{2}.$$

Любой из этих корней можно принять за ζ. Для определенности мы положим

$$\zeta = \frac{-1 + \sqrt{-3}}{2}.$$

Тогда

$$A + B\zeta = \frac{(2A - B) + B\sqrt{-3}}{2}.$$

Таким образом, получается, что числа из K_3 имеют вид $a + b\sqrt{-3}$, где a и b — рациональные числа, а числа из D_3 (целые числа из K_3) — вид

$$\frac{p + q\sqrt{-3}}{2}, \tag{7}$$

где p и q — целые числа одинаковой четности.

В частности, при p и q четных мы получаем числа Эйлера

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

Таким образом, ограничение только такими числами с общей точки зрения ничем не оправдано, и поэтому можно надеяться, что при переходе к более естественно возникающим числам (7) все наши трудности исчезнут. Оказывается, что это и на самом деле так.

Чтобы избежать кустарности в исследовании этой проблематики, целесообразно ввести простейшие основные понятия арифметики в кольцах. Хотя сейчас нам нужно только кольцо D_3, а в дальнейшем понадобятся лишь его непосредственные обобщения D_l, $l \geqslant 3$, мы дадим определения этих понятий в их естественной общности. Читатель, безразличный к эстетическим сторонам теории и не желающий вникать в абстрактные определения, может пока игнорировать несколько следующих строк и во всем дальнейшем понимать под D кольцо D_3.

Мы будем считать известным понятие кольца (коммутативного, ассоциативного и с единицей 1). Напомним, что такое кольцо называется *целым кольцом* (традиционное название — «область целостности»), если оно не имеет делителей нуля, т. е. произведение любых его двух отличных от нуля элементов отлично от нуля. *В дальнейшем под кольцом мы будем всегда иметь в виду целое кольцо.*

Основное свойство целых колец, которым мы будем постоянно пользоваться, состоит в том, что в них

(и только в них) справедливо *правило сокращения*, т. е. из равенства $\alpha\beta = \alpha\gamma$, где $\alpha \neq 0$, следует, что $\beta = \gamma$.

Элемент ε кольца D называется *единицей* (или *обратимым элементом*; последний термин используется теперь все чаще, а употребление термина «единица» постепенно сходит на нет), если существует такой элемент $\varepsilon^{-1} \in D$, что

$$\varepsilon\varepsilon^{-1} = 1.$$

Ясно, что произведение и частное двух единиц также является единицей.

Пример 1. Кольцо $\mathbb{Z}$ целых чисел имеет две единицы $+1$ и -1.

Пример 2. Элемент $\varepsilon \in D$ называется *корнем из единицы степени n*, если

$$\varepsilon^n = 1.$$

Ясно, что каждый корень из единицы (содержащийся в D) будет единицей кольца D (для которой $\varepsilon^{-1} = \varepsilon^{n-1}$).

Пример 3. Найдем единицы кольца D_3. Оказывается, что *число $\alpha \in D_3$ тогда и только тогда является единицей, когда $N\alpha = 1$.*

Действительно, если $\alpha\alpha^{-1} = 1$, то

$$N\alpha \cdot N\alpha^{-1} = N(\alpha\alpha^{-1}) = N1 = 1,$$

и потому $N\alpha = 1$. Обратно, если $N\alpha = 1$, т. е. $\alpha\bar{\alpha} = 1$, то α является единицей (с $\alpha^{-1} = \bar{\alpha}$). ■

Так как для числа $\alpha = A + B\zeta$ норма $N\alpha$ выражается формулой

$$N\alpha = A^2 - AB + B^2 = \frac{(2A - B)^2 + 3B^2}{4},$$

то $N\alpha = 1$ тогда и только тогда, когда либо $B = 0$ и $A = \pm 1$, либо $B = \pm 1$ и $(2A - B)^2 = 1$, т. е. $A = B = \pm 1$ или $A = 0$, $B = \pm 1$. Таким образом, *кольцо D_3 имеет шесть единиц*:

$$+1, \quad +\zeta, \quad 1 + \zeta = -\zeta^2,$$
$$-1, \quad -\zeta, \quad -1 - \zeta = \zeta^2.$$

Все они являются корнями из единицы степени 6. При

этом каждая единица является степенью единицы

$$1+\zeta=\frac{1+\sqrt{-3}}{2}$$

(первообразного корня из единицы степени 6). Именно,

$$(1+\zeta)^1=1+\zeta, \quad (1+\zeta)^2=\zeta, \quad (1+\zeta)^3=-1,$$
$$(1+\zeta)^4=-1-\zeta, \quad (1+\zeta)^5=-\zeta, \quad (1+\zeta)^6=1.$$

Пусть D^* — множество $D\setminus\{0\}$ всех отличных от нуля элементов кольца D.

Два элемента $\alpha, \beta \in D^*$ называются *ассоциированными* (обозначение $\alpha \sim \beta$), если существует такая единица ε, что $\beta = \varepsilon\alpha$. Очевидно, что отношение ассоциированности является отношением эквивалентности и потому множество D^* распадается на классы ассоциированных элементов.

Пусть $D' \subset D^*$ — множество всех отличных от нуля элементов кольца D, не являющихся единицами.

Элемент $\alpha \in D'$ называется *разложимым*, если существуют такие элементы $\beta, \gamma \in D'$, что $\alpha = \beta\gamma$. Неразложимый элемент $\alpha \in D'$ называется также *простым элементом*.

Функция $\alpha \mapsto \|\alpha\|$, определенная на D^* и принимающая значения в множестве $\mathbb{N}$ целых положительных чисел, называется *псевдонормой*, если из того, что $\alpha \in D^*$ делится на $\beta \in D^*$ (т. е. $\alpha = \beta\gamma$, где $\gamma \in D$), следует, что $\|\alpha\| \geqslant \|\beta\|$.

Если γ — единица, то $\beta = \alpha\gamma^{-1}$, где $\gamma^{-1} \in D$, и потому $\|\beta\| \geqslant \|\alpha\|$. Следовательно, *если элементы α и β ассоциированы, то* $\|\alpha\| = \|\beta\|$. Если обратное тоже верно, т. е. если $\|\alpha\| > \|\beta\|$, когда α делится на β, но частное γ не является единицей, то псевдонорма называется *строгой*.

Примером строгой псевдонормы является, очевидно, норма в D_3.

Предложение 1. *Если в кольце D существует строгая псевдонорма, то любой элемент $\alpha \in D'$ разлагается в произведение простых элементов, т. е.*

$$\alpha = \pi_1\pi_2 \ldots \pi_k, \tag{8}$$

где $\pi_1, \pi_2, \ldots, \pi_k$ — простые элементы.

Доказательство. Значения псевдонормы на элементах $\alpha \in D'$ являются целыми положительными числами. Поэтому среди них существует наименьшее. Пусть p_0 — это наименьшее значение. Ясно, что любой элемент $\alpha \in D'$, для которого $\|\alpha\| = p_0$, будет простым. Поэтому разложение (8) для него имеет место (с $k = 1$ и $\pi_1 = \alpha$). Пусть теперь $p > p_0$ и пусть существование разложения (8) доказано для всех элементов $\alpha \in D'$ с $\|\alpha\| < p$. Рассмотрим произвольный элемент $\alpha \in D'$, для которого $\|\alpha\| = p$. Если α прост, то доказывать нечего. Пусть $\alpha = \alpha_1\alpha_2$, где α_1, $\alpha_2 \in D'$. Тогда $\|\alpha_1\| < \|\alpha\| = p$ и $\|\alpha_2\| < \|\alpha\| = p$. Поэтому для элементов α_1 и α_2 существуют разложения (8). Перемножив их, мы и получим разложение элемента α. Тем самым предложение 1 по индукции полностью доказано. ■

Вообще говоря, разложение (8) не единственно. Например, можно менять порядок простых множителей и заменять их на ассоциированные (с тем, конечно, чтобы произведение всех дополнительных множителей-единиц было равно 1). Назовем два разложения

$$\alpha = \pi_1 \dots \pi_r \quad \text{и} \quad \alpha = \pi'_1 \dots \pi'_s$$

элемента $\alpha \in D'$ в произведение простых множителей *ассоциированными*, если $r = s$ и, после возможной перенумерации, элемент π'_i для каждого $i = 1, \dots, r$ ассоциирован с элементом π_i. Если любой элемент $\alpha \in D'$ разлагается в произведение простых элементов и если каждые два таких разложения ассоциированы, то говорят, что *в кольце D выполнена основная теорема арифметики*, или (допуская определенную неточность) что D является *кольцом с однозначным разложением на множители*.

В таком кольце имеют смысл все основные понятия теории делимости целых чисел, и их свойства аналогичны свойствам, известным из элементарной арифметики.

Например, по аналогии с натуральными числами назовем элементы кольца D *взаимно простыми*, если у них нет общих простых множителей. Тогда то же рассуждение, что и для натуральных чисел (см. лемму в § 1) покажет, что *если в кольце D выполнена*

основная теорема арифметики, то взаимно простые элементы α *и* β *являются с точностью до единиц* n*-ми степенями, когда* n*-й степенью является их произведение* $\alpha\beta$.

Элемент $\delta \in D^*$ называется *наибольшим общим делителем* элементов $\alpha, \beta \in D^*$, если он делит эти элементы и делится на любой другой общий делитель элементов α и β. Ясно, что наибольший общий делитель однозначно определен с точностью до ассоциированности. Однако, вообще говоря, для элементов произвольного кольца он может и не существовать. В кольце же с однозначным разложением на множители наибольший общий делитель существует, очевидно, для любых элементов α и β. Чтобы его найти, следует разложить эти элементы в произведение простых множителей и отобрать в обоих разложениях одинаковые (ассоциированные) множители. Если таких множителей нет (т. е. элементы α и β взаимно просты), — в частности, так будет, если хотя бы один из элементов α и β является единицей, — то наибольшим общим делителем является элемент 1 (а также произвольная единица).

Из основной теоремы арифметики непосредственно вытекает также следующее утверждение:

(*) *Если простой элемент* π *делит произведение* $\alpha\beta$, *то он делит либо* α, *либо* β.

Легко видеть, что и обратно, *если в кольце* D *любой элемент* $\alpha \in D'$ *разлагается в произведение простых элементов* (например, если в D есть строгая псевдонорма) *и если* D *обладает свойством* (*), *то в* D *имеет место основная теорема арифметики.*

Действительно, если

$$\pi_1 \dots \pi_r = \pi_1' \dots \pi_s',$$

где $\pi_1, \dots, \pi_r, \pi_1', \dots, \pi_s'$ — простые элементы, то π_1 делит произведение $\pi_1' \dots \pi_s'$. Поэтому π_1 делит хотя бы один из сомножителей (это получается из (*) посредством очевидной индукции). Мы можем считать, что π_1 делит π_1', т. е. что $\pi_1' = \pi_1 \varepsilon_1$, где, поскольку элемент π_1' также прост, элемент ε_1 является единицей. Сократив на π_1, мы получим, таким образом, что $\pi_2 \dots \pi_r = \varepsilon_1 \pi_2' \dots \pi_s'$. Аналогично доказывается, что π_2 (после соответ-

ствующей перенумерации) делит π_2' и (после сокращения π_2) что π_3 делит π_3' и т. д. После r шагов мы получим, во-первых, что $r \leqslant s$, а во-вторых, что при $r < s$ имеет место равенство вида

$$1 = \varepsilon_1 \dots \varepsilon_r \pi_{r+1}' \dots \pi_s'.$$

Поскольку это равенство невозможно (элементы $\pi_{r+1}', \dots, \pi_s'$ единицами, по условию, не являются), этим доказано, что $r = s$ и что для любого $i = 1, \dots, r$ элемент π_i' ассоциирован с элементом π_i. ■

Известно (мы покажем это ниже), что в кольце целых чисел наибольший общий делитель d любых двух чисел a и b может быть представлен в виде

$$ax + by = d, \tag{9}$$

где x и y — целые числа (т. е., иначе говоря, уравнение (9) всегда имеет решение в целых числах). Оказывается, что аналогичное свойство для произвольных колец не вытекает из основной теоремы арифметики. Поэтому приходится вводить еще один класс колец.

Кольцо D называется *кольцом главных идеалов* (происхождение этого названия станет ясным в § 11), если для любых элементов $\alpha, \beta \in D^*$

а) существует их наибольший общий делитель δ;

б) можно найти такие элементы $x, y \in D$, что

$$\alpha x + \beta y = \delta.$$

Легко видеть, что *любое кольцо главных идеалов обладает свойством* (*).

Действительно, если π не делит α, то π и α взаимно просты, и потому существуют такие элементы $x, y \in D$, что $\alpha x + \pi y = 1$. Умножив это равенство на β, мы получим, что

$$\beta = (\alpha\beta)\, x + \pi\, (y\beta).$$

Оба слагаемых справа делятся на π. Поэтому на π делится и элемент β. ■

Говорят, что в кольце D с псевдонормой имеет место *алгоритм деления с остатком* (такое кольцо называется также *евклидовым кольцом*), если для любых элементов $\alpha, \beta \in D^*$ существуют такие элементы γ и ρ, что $\alpha = \beta\gamma + \rho$, причем либо $\rho = 0$, либо $\|\rho\| < \|\beta\|$.

Интересно, что *в евклидовом кольце псевдонорма обязательно является строгой.* Действительно, если $\alpha = \beta\gamma$ и $\|\alpha\| = \|\beta\|$, то, разделив с остатком β на α,

мы получим равенство вида

$$\beta = \alpha\delta + \rho,$$

где $\delta \in D$, и либо $\rho = 0$, либо $\|\rho\| < \|\alpha\|$. Но $\rho = \beta(1 - \gamma\delta)$, и потому при $\rho \neq 0$ имеет место неравенство $\|\rho\| \geqslant \|\beta\| = \|\alpha\|$. Следовательно, $\rho = 0$ и потому $\beta = (\beta\gamma)\delta$, т. е. $\gamma\delta = 1$. ■

С другой стороны, *любое евклидово кольцо является кольцом главных идеалов* (и, следовательно, обладает свойством (*)). Действительно, для любых элементов $\alpha, \beta \in D^*$ в множестве всех отличных от нуля элементов вида

$$\alpha x + \beta y, \qquad x, y \in D, \tag{10}$$

существуют элементы с наименьшей псевдонормой. Пусть $\delta = \alpha x_0 + \beta y_0$ — один из таких элементов. Все будет доказано, если мы покажем, что δ является наибольшим общим делителем элементов α и β. Но ясно, что δ делится на любой общий делитель элементов α и β. Поэтому нужно только доказать, что δ делит α и β. Докажем, что δ делит α (для β доказательство аналогично).

Пусть $\alpha = \delta\gamma + \rho$, где либо $\rho = 0$, либо $\|\rho\| < \|\delta\|$. Тогда

$$\rho = \alpha - \delta\gamma = \alpha - (\alpha x_0 + \beta y_0)\gamma = \alpha(1 - x_0\gamma) + \beta(-y_0\gamma),$$

так что ρ также имеет вид (10). Следовательно, неравенство $\|\rho\| < \|\delta\|$ невозможно, и, значит, $\rho = 0$. ■

Сопоставляя все доказанное, мы видим, что справедливо следующее предложение:

Предложение 2. *Любое евклидово кольцо является кольцом главных идеалов, в котором выполнена основная теорема арифметики.*

Заметим, что существуют кольца, в которых выполнена основная теорема арифметики, но которые не допускают алгоритма деления с остатком (ни по отношению ни к какой псевдонорме).

Таким кольцом является, например, кольцо всех чисел вида

$$\frac{a + b\sqrt{-19}}{2},$$

где a и b — целые числа одинаковой четности, но доказать это не так-то просто.

Как мы уже говорили, чтобы подвести прочную базу под доказательство Эйлера, достаточно доказать, что в кольце D_3 выполнена основная теорема арифметики. Согласно предложению 2 для этого достаточно доказать следующее предложение:

Предложение 3. *По отношению к норме в кольце D_3 имеет место алгоритм деления с остатком.*

Доказательство. Нужно доказать, что для любых элементов α и $\beta \neq 0$ кольца D_3 существуют такие элементы γ и ρ, что $\alpha = \beta\gamma + \rho$ и $N\rho < N\beta$.

Лемма. *Для любого числа $\xi \in K_3$ существует такое число $\gamma \in D_3$, что*

$$N(\xi - \gamma) \leqslant \frac{3}{4}.$$

Предложение 3 из этой леммы следует непосредственно. Действительно, применив лемму к числу $\xi = \frac{\alpha}{\beta}$ и положив $\rho = \alpha - \beta\gamma$, мы немедленно получим, что $\alpha = \beta\gamma + \rho$ и что

$$N\rho = N(\alpha - \beta\gamma) = N\beta \cdot N(\xi - \gamma) \leqslant \frac{3}{4} N\beta < N\beta. \quad \blacksquare$$

Таким образом, нам нужно лишь доказать лемму.

Доказательство леммы. Пусть

$$\xi = A + B\zeta,$$

и пусть a и b — такие целые числа, что

$$|A - a| \leqslant \frac{1}{2}, \quad |B - b| \leqslant \frac{1}{2}.$$

Тогда для числа

$$\gamma = a + b\zeta \in D_3$$

мы получаем

$$N(\xi - \gamma) = (A - a)^2 - (A - a)(B - b) + (B - b)^2 \leqslant$$
$$\leqslant |A - a|^2 + |A - a| \cdot |B - b| + |B - b|^2 \leqslant$$
$$\leqslant \left(\frac{1}{2}\right)^2 + \frac{1}{2} \cdot \frac{1}{2} + \left(\frac{1}{2}\right)^2 = \frac{3}{4}. \quad \blacksquare$$

Следствие. *В кольце D_3 выполнена основная теорема арифметики.*

Существование двух разложений

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

этому не противоречит, так как в D_3 числа 2 и $1 + \sqrt{-3}$ ассоциированы (число $\frac{1 + \sqrt{-3}}{2}$ принадлежит D_3 и является в D_3 единицей).

Теперь для завершения доказательства Эйлера осталось лишь заполнить в нем два незначительных пробела.

Во-первых, надо доказать, что для взаимно простых целых чисел a и b элементы $a + b\sqrt{-3}$ и $a - b\sqrt{-3}$ кольца D_3 также взаимно просты. Но это легко. Действительно, если эти элементы делятся на элемент $\gamma \in D_3$, то на γ будут делиться и элементы

$$2a = (a + b\sqrt{-3}) + (a - b\sqrt{-3}),$$
$$2b\sqrt{-3} = (a + b\sqrt{-3}) - (a - b\sqrt{-3}).$$

Перейдя к нормам, мы получаем, что число $N\gamma$ будет делить числа $N(2a) = 4a^2$ и $N\gamma = 12b^2$. Поскольку числа a и b по условию взаимно просты, отсюда следует, что (целое положительное) число $N\gamma$ делит число 4.

Если $N\gamma = 4$, то $N\left(\frac{\gamma}{2}\right) = 1$, т. е. $\gamma = 2\varepsilon$, где ε — единица. Таким образом, в этом случае с точностью до ассоциированности имеется единственное решение $\gamma = 2$. Но это решение нам не годится, потому что число $a + b\sqrt{-3}$ тогда и только тогда делится в D_3 на 2, когда оба числа a и b делятся на 2.

Случай $N\gamma = 2$ вообще невозможен, ибо уравнение $x^2 - xy + y^2 = 2$ не имеет целочисленных решений.

Таким образом, обязательно $N\gamma = 1$, т. е. γ является единицей. Следовательно, элементы $a + b\sqrt{-3}$ и $a - b\sqrt{-3}$ взаимно просты. ■

Второй пробел, которого не было у Эйлера, но который возник, когда мы перешли к кольцу D_3, состоит в том, что в равенстве

$$a + b\sqrt{-3} = (s + t\sqrt{-3})^3 \tag{11}$$

числа s и t могут, вообще говоря, оказаться нецелыми,

поскольку, как мы знаем, числа из D_3 имеют вид

$$\frac{p+q\sqrt{-3}}{2}, \tag{12}$$

где p и q — целые числа одинаковой четности.

Чтобы преодолеть эту трудность, мы заметим, что если число (12) записать в форме $A+B\zeta$, то будут иметь место равенства

$$p=2A-B, \quad q=B.$$

Поэтому числа p и q тогда и только тогда четны (и, значит, число (12) имеет нужный нам вид $s+t\sqrt{-3}$, где s и t целые), когда четно число B. Но формулы

$$(A+B\zeta)\zeta=-B+(A-B)\zeta, \quad (A+B\zeta)\zeta^2=(B-A)-A\zeta$$

показывают, что хотя бы у одного из трех ассоциированных чисел $A+B\zeta$, $(A+B\zeta)\zeta$, $(A+B\zeta)\zeta^2$ коэффициент при ζ четен. Следовательно, умножив в равенстве (11) число $s+t\sqrt{-3}$ на ζ или на ζ^2 (отчего равенство, очевидно, не нарушится), мы всегда сможем добиться, чтобы числа s и t стали целыми.

Тем самым лемма Эйлера полностью доказана, и вместе с ней наконец-то доказана и теорема Ферма для показателя 3. ■

Приложение. Об арифметике многочленов

Пусть K — произвольное поле и $K[x]$ — кольцо многочленов от одной переменной над полем K (т. е. с коэффициентами из K). Из элементарной алгебры известно, что для многочленов имеет место алгоритм деления с остатком (с псевдонормой — степенью многочлена). Следовательно, *в кольце $K[x]$ выполнена основная теорема арифметики.*

При этом единицами кольца $K[x]$ являются, очевидно, лишь многочлены нулевой степени, т. е. отличные от нуля элементы поля K.

Простые элементы кольца $K[x]$ называются, обыкновенно, *неприводимыми многочленами.* Таким образом, можно сказать, что любой многочлен разлагается в произведение неприводимых многочленов и с

точностью до постоянных множителей это разложение единственно.

Более того, являясь евклидовым кольцом, *кольцо $K[x]$ является также кольцом главных идеалов.* Поэтому, в частности, для любых взаимно простых многочленов $f(x)$ и $g(x)$ существуют такие многочлены $u(x)$ и $v(x)$, что

$$f(x)u(x)+g(x)v(x)=1.$$

Следовательно, ни при одном значении x многочлены $f(x)$ и $g(x)$ не могут одновременно обращаться в нуль. Этим доказано, что *многочлены, имеющие общий корень, не взаимно просты.*

Поскольку неприводимый многочлен взаимно прост с каждым многочленом меньшей степени, отсюда, в частности, вытекает, что *никакой корень неприводимого многочлена не может быть корнем многочлена меньшей степени.*

§ 5. Поле K_l и кольцо D_l

Единственный известный к настоящему времени общий метод доказательства теоремы Ферма для любых простых $l \geqslant 3$ (к сожалению, увенчивающийся успехом не для всех l) восходит, как уже говорилось, к Куммеру и основывается на дальнейшем развитии и обобщении идей Эйлера. Естественно, что основную роль в нем играет некое поле K_l, аналогичное полю K_3. Поэтому мы начнем с описания и изучения этого поля.

Рассмотрим многочлен

$$x^l-1 \tag{1}$$

или, лучше, многочлен

$$\varphi(x)=x^{l-1}+x^{l-2}+\ \dots\ +x+1, \tag{2}$$

получающийся из многочлена (1) делением на $x-1$. Корни многочлена (1) выражаются формулой

$$\cos\frac{2\pi k}{l}+i\sin\frac{2\pi k}{l}, \tag{3}$$

где $k=0,\ 1,\ \dots,\ l-1$. На плоскости комплексных чисел эти корни изображаются вершинами правиль-

ного l-угольника, вписанного в единичную окружность. На этом основании многочлен (1), а также многочлен (2) называется *многочленом деления круга на l частей.*

Замечательный факт (оправдывающий переход от многочлена (1) к многочлену (2)) состоит в том, что *многочлен* (2) *неприводим* (над полем $\mathbb{Q}$ рациональных чисел).

Доказательство этого утверждения мы проведем в ряд этапов.

1. Ясно, что достаточно доказать неприводимость многочлена

$$p(y)=\frac{(y+1)^l-1}{y}=$$
$$=y^{l-1}+\binom{l}{1}y^{l-2}+\ \dots\ +\binom{l}{l-2}y+\binom{l}{l-1},$$

получающегося из многочлена (2) подстановкой $x=y+1$.

2. Как мы уже отмечали, *все биномиальные коэффициенты*

$$\binom{l}{k}=\frac{l!}{k!\,(l-k)!},\qquad k=1,\ \dots,\ l-1, \tag{4}$$

делятся на l.

3. Предположим, что многочлен $p(y)$ приводим, т. е. что существуют такие многочлены $a(y)$ и $b(y)$ с рациональными коэффициентами, имеющие положительные степени (и, значит, не являющиеся единицами кольца многочленов $\mathbb{Q}[y]$), что $p(y)=a(y)\,b(y)$. Вообще говоря, многочлены $a(y)$ и $b(y)$ определены только с точностью до ассоциированности (каждый из этих многочленов можно умножить на произвольное отличное от нуля рациональное число, одновременно разделив другой многочлен на то же число). Пользуясь этим, мы можем сделать все коэффициенты, скажем, многочлена $a(y)$ взаимно простыми (в совокупности) целыми числами, а его старший коэффициент положительным. Это однозначно определит многочлен $a(y)$, а потому и многочлен $b(y)$.

4. Приведя коэффициенты многочлена $b(y)$ к общему знаменателю, мы можем записать этот

многочлен в виде

$$b(y)=\frac{b_0}{N}y^s+\frac{b_1}{N}y^{s-1}+\ \dots\ +\frac{b_s}{N},$$

где b_0, b_1, ..., b_s и $N>0$ — целые числа, причем ни один простой делитель числа N не делит всех чисел $b_0, b_1, \dots, b_s$. По условию

$$a(y)=a_0y^r+a_1y^{r-1}+\ \dots\ +a_r,$$

где a_0, a_1, ..., a_r — целые взаимно простые в совокупности числа и $r=l-1-s$. Поэтому для коэффициентов $\binom{l}{k}$ многочлена $p(y)$ будут иметь место равенства

$$\begin{aligned}
&\binom{l}{0}=1=\frac{a_0b_0}{N},\\
&\binom{l}{1}=l=\frac{a_0b_1+a_1b_0}{N},\\
&\dots\dots\dots\dots\dots\dots\dots\dots\\
&\binom{l}{k}=\frac{a_0b_k+a_1b_{k-1}+\ \dots\ +a_kb_0}{N},\\
&\dots\dots\dots\dots\dots\dots\dots\dots\\
&\binom{l}{l-1}=l=\frac{a_rb_s}{N}
\end{aligned}\tag{5}$$

(условно считается, что $a_i=0$ при $i>r$ и $b_j=0$ при $j>s$). Это, в частности, показывает, что *все числа*

$$a_0b_k+a_1b_{k-1}+\ \dots\ +a_kb_0,\quad k=0,\ 1,\ \dots,\ l-1,\tag{6}$$

делятся на N.

5. Предполагая, что $N>1$, рассмотрим произвольный простой делитель p числа N. Так как коэффициенты a_0, ..., a_r по условию взаимно просты, среди них существуют коэффициенты, не делящиеся на p. Пусть a_{i_0} — первый такой коэффициент (так что либо $i_0=0$, либо все коэффициенты a_0, ..., a_{i_0-1} делятся на p). Аналогично, так как, по условию, p не делит всех коэффициентов b_0, ..., b_s, то существует коэффициент b_{j_0}, не делящийся на p и такой, что при $j_0\geqslant 1$ все коэффициенты b_0, ..., b_{j_0-1} делятся на p.

Рассмотрим теперь число (6) при $k=i_0+j_0$. Это число содержит слагаемое $a_{i_0}b_{i_0}$, не делящееся на p.

Все же остальные слагаемые (имеющие вид $a_i b_j$, где либо $i < i_0$, либо $j < j_0$), очевидно, делятся на p. Поэтому рассматривавшееся число не делится на p, а значит, и на N.

Поскольку это противоречит результату этапа 4, тем самым доказано, что $N = 1$, т. е. что *все коэффициенты многочлена* $b(y)$ (при наложенных условиях на многочлен $a(y)$) *являются взаимно простыми в совокупности целыми числами.*

В частности, *числа* (6) *являются коэффициентами* $\binom{l}{k}$ *многочлена* $p(y)$.

6. Так как все коэффициенты многочлена $a(y)$ (и, по доказанному, многочлена $b(y)$) являются взаимно простыми целыми числами, то среди них существуют коэффициенты, не делящиеся на простое число l. Пусть a_{i_0} — обладающий этим свойством коэффициент многочлена $a(y)$ с наибольшим номером, а b_{j_0} — аналогичный коэффициент многочлена $b(y)$.

Поскольку $a_r b_s = l$, то либо $i_0 < r$, либо $j_0 < s$. Пусть, для определенности, $i_0 < r$, так что $a_r = \pm l$, а $b_s = \pm 1$. Тогда число $\binom{l}{i_0 + s}$ будет коэффициентом многочлена $p(y)$, и, значит, для него будет иметь место формула

$$\binom{l}{i_0 + s} = a_{i_0} b_s + a_{i_0+1} b_{s-1} + \ldots + a_r b_{s-(r-i_0)}.$$

Но все члены этой формулы, кроме первого члена $a_{i_0} b_s = \pm a_{i_0}$, делятся на l (потому что на l делятся числа $a_{i_0+1}, \ldots, a_r$), а член $a_{i_0} b_s$ на l не делится. Поэтому и вся сумма $\binom{l}{i_0 + s}$ на l не делится, что противоречит этапу 2.

Таким образом, предположив, что многочлен $p(y)$ приводим, мы пришли к противоречию. Следовательно, этот многочлен неприводим. ■

Заметим, что по ходу дела мы фактически доказали две общие теоремы, первая из которых утверждает разложимость приводимого над $\mathbb{Q}$ многочлена с целыми коэффициентами на множители с целыми коэффициентами (эта теорема известна как лемма Гаусса), а вторая утверждает неприводимость (над $\mathbb{Q}$) многочлена с целыми коэффициентами, если его старший

коэффициент не делится на некоторое простое число l, все остальные коэффициенты делятся на l, но свободный член не делится на l^2 (это так называемый критерий Эйзенштейна).

Пусть теперь ζ — произвольный фиксированный корень многочлена (2). Для определенности можно считать, что

$$\zeta = \cos\frac{2\pi}{l} + i\sin\frac{2\pi}{l},$$

но на самом деле этот выбор не имеет никакого значения (при l простом!) и в дальнейшем не используется.

Более того, явные выражения (3) корней многочленов (1) и (2) нам по существу также не нужны. Достаточно знать, что ζ представляет собой комплексное число, удовлетворяющее соотношению

$$\zeta^{l-1} = -1 - \zeta - \ldots - \zeta^{l-2}, \tag{7}$$

равносильному утверждению, что ζ является корнем многочлена (2). Только этим его свойством мы и будем пользоваться.

По аналогии со случаем $l = 3$ мы введем в рассмотрение множество K_l всевозможных чисел вида

$$\alpha = a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2}, \tag{8}$$

где $a_0, a_1, \ldots, a_{l-2}$ — произвольные рациональные числа.

Легко видеть, что *представление каждого числа* $\alpha \in K_l$ *в виде* (8) *единственно.*

Действительно, если это не так, то будет иметь место равенство вида

$$a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2} = 0,$$

где не все числа $a_0, a_1, \ldots, a_{l-2}$ отличны от нуля. Другими словами, число ζ будет корнем некоторого многочлена с рациональными коэффициентами степени, меньшей $l - 1$, что невозможно, ибо многочлен (2) неприводим.

Так как, согласно (7), имеет место равенство

$$1 = -\zeta - \zeta^2 - \ldots - \zeta^{l-1},$$

то любой элемент $\alpha \in K_l$ может быть (очевидно, единственным

образом) представлен в виде

$$\alpha = b_1\zeta + b_2\zeta^2 + \ldots + b_{l-1}\zeta^{l-1},$$

где $b_1, b_2, \ldots, b_{l-1}$ — рациональные числа (целые, если числа $a_0, \ldots, a_{l-2}$ были целыми).

Такое представление иногда бывает полезно.

Ясно, что сумма двух чисел вида (8) снова будет числом вида (8). То же самое верно, конечно, и по отношению к произведению, поскольку появляющиеся после перемножения высокие (с показателями, бо́льшими, чем $l-2$) степени числа ζ можно выразить через более низкие степени с помощью соотношения (7). Это означает, что K_l представляет собой кольцо. Более того, оказывается, что K_l *является полем*, т. е. что частное любых двух чисел вида (8) снова представляет собой число того же вида.

Действительно, равенство (8) означает, что число $\alpha \in K_l$ является значением $f(\zeta)$ при $x = \zeta$ многочлена

$$f(x) = a_0 + a_1x + \ldots + a_{l-2}x^{l-2}$$

(отличного от нуля при $\alpha \neq 0$). Поскольку степень этого многочлена меньше степени $l-1$ многочлена деления круга $\varphi(x)$, а последний многочлен неприводим, то многочлены $f(x)$ и $\varphi(x)$ взаимно просты. Поэтому существуют такие многочлены $u(x)$ и $v(x)$, что

$$f(x)u(x) + \varphi(x)v(x) = 1.$$

Полагая здесь $x = \zeta$ и учитывая, что $\varphi(\zeta) = 0$, мы получаем, что

$$f(\zeta)u(\zeta) = 1,$$

т. е. что

$$\frac{1}{\alpha} = u(\zeta) \in K_l.$$

Таким образом, в кольце K_l каждый элемент $\alpha \neq 0$ обратим. Следовательно, K_l является полем. ■

Обратим внимание, что при $l = 3$ мы тот факт, что K_l является полем, доказывали на основе совсем других соображений. Для того чтобы перенести эти соображения на случай любого l, нам понадобятся некоторые предварительные рассмотрения.

Корень ζ является лишь одним из $l-1$ корней

(9) $$\zeta^{(1)} = \zeta, \ \zeta^{(2)}, \ \zeta^{(3)}, \ \ldots, \ \zeta^{(l-1)}$$

многочлена (2). Оказывается, что все эти корни очень просто выражаются через корень ζ.

Действительно, вместе с ζ уравнению $x^l = 1$ удовлетворяют, очевидно, и все числа вида ζ^k, где k — произвольное целое число, причем $\zeta^{k_1} = \zeta^{k_2}$ тогда и только тогда, когда $k_1 \equiv k_2 \bmod l$. Это показывает, что при соответствующей нумерации корней (9) будут иметь место равенства

$$(10) \quad \zeta^{(1)} = \zeta,\ \zeta^{(2)} = \zeta^2,\ \zeta^{(3)} = \zeta^3,\ \ldots,\ \zeta^{(l-1)} = \zeta^{l-1}.$$

В частности, мы видим, что *все корни* (9) *принадлежат полю* K_l.

Поэтому, если в выражение (8) вместо $\zeta = \zeta^{(1)}$ подставить произвольный корень $\zeta^{(k)}$, $k = 1, 2, \ldots, l-1$, то снова получится число из поля K_l. Мы обозначим это число символом $\alpha^{(k)}$. Таким образом, по определению,

$$\alpha^{(k)} = a_0 + a_1\zeta^{(k)} + a_2(\zeta^{(k)})^2 + \ldots + a_{l-2}(\zeta^{(k)})^{l-2} = \\ = a_0 + a_1\zeta^k + a_2\zeta^{2k} + \ldots + a_{l-2}\zeta^{(l-2)k}.$$

Рассмотрим теперь произведение

$$N\alpha = \alpha^{(1)}\alpha^{(2)} \ldots \alpha^{(l-1)}.$$

Это произведение является многочленом от $\zeta^{(1)}, \ldots, \zeta^{(l-1)}$, коэффициенты которого представляют собой многочлены от $a_0, a_1, \ldots, a_{l-2}$ с целыми коэффициентами. Любая перестановка чисел $\zeta^{(1)}, \ldots, \zeta^{(l-1)}$ вызывает такую же перестановку чисел $\alpha^{(1)}, \ldots, \alpha^{(l-1)}$ и, следовательно, не меняет $N\alpha$. Это означает, что $N\alpha$ представляет собой симметрический многочлен от $\zeta^{(1)}, \ldots, \zeta^{(l-1)}$. Но известно (см., например, книгу В. Г. Болтянского, Н. Я. Виленкина, Симметрия в алгебре, «Наука», М., 1967), что любой симметрический многочлен F является многочленом $G(\sigma_1, \ldots, \sigma_{l-1})$ от так называемых элементарных симметрических многочленов $\sigma_1, \ldots, \sigma_{l-1}$, причем коэффициенты многочлена G выражаются через коэффициенты многочлена F посредством действий сложения, вычитания и умножения, т. е. в нашем случае (при $F = N\alpha$) по-прежнему являются многочленами от $a_0, a_1, \ldots, a_{l-2}$ с целыми коэффициентами. Эти элементарные симметрические многочлены

имеют вид

$$\sigma_1 = \zeta^{(1)} + \zeta^{(2)} + \ldots + \zeta^{(l-1)},$$
$$\sigma_2 = \zeta^{(1)}\zeta^{(2)} + \ldots + \zeta^{(l-2)}\zeta^{(l-1)},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\sigma_{l-1} = \zeta^{(1)}\zeta^{(2)} \ldots \zeta^{(l-1)},$$

и, согласно формулам Вьета, примененным к многочлену (2), равны $(-1)^k$. Этим доказано, что число

$$N\alpha = G(-1, 1, \ldots)$$

представляет собой многочлен от $a_0, a_1, \ldots, a_{l-2}$ с целыми коэффициентами и потому является рациональным числом (целым, когда все числа $a_0, a_1, \ldots, a_{l-2}$ целые).

Изложенное рассуждение имеет общий характер и дословно применимо не только к $N\alpha$, но и к произвольному симметрическому многочлену от $\alpha^{(1)}, \ldots, \alpha^{(l-1)}$ с целыми коэффициентами, например, к коэффициентам многочлена

$$(x - \alpha^{(1)}) \ldots (x - \alpha^{(l-1)}).$$

Таким образом, мы, в частности, видим, что *для любого элемента* $\alpha = a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2} \in K_l$ *коэффициенты многочлена* $(x - \alpha^{(1)}) \ldots (x - \alpha^{(l-1)})$ *являются рациональными числами* (целыми, если все числа $a_0, a_1, \ldots, a_{l-2}$ целые).

Рациональное число $N\alpha$ называется *нормой* элемента $\alpha \in K_l$. Оно обладает следующими свойствами:

1) $N\alpha \geqslant 0$, причем $N\alpha = 0$ тогда и только тогда, когда $\alpha = 0$;

2) для любых чисел $\alpha, \beta \in K_l$ имеет место равенство

$$N(\alpha\beta) = N\alpha \cdot N\beta; \tag{11}$$

3) если число $\alpha \in K_l$ рационально (т. е. $a_1 = \ldots = a_{l-2} = 0$ и, значит, $\alpha = a_0$), то

$$N\alpha = a_0^{l-1}.$$

Эти свойства очевидны (ср. со случаем $l = 3$), за исключением, возможно, неравенства $N\alpha \geqslant 0$, для доказательства которого надо вспомнить, что числа (9) (являясь невещественными корнями уравнения с вещественными коэффициентами) попарно комплексно сопряжены. (Например, можно считать, что $\zeta^{(l-k)} = \overline{\zeta^{(k)}}$; см. формулу (10).) Поэтому числа $\alpha^{(1)}, \ldots, \alpha^{(l-1)}$ также

попарно комплексно сопряжены (скажем, $\alpha^{(l-k)} = \overline{\alpha^{(k)}}$) и, значит, $N\alpha \geqslant 0$ (при указанной нумерации корней имеет место формула $N\alpha = |\alpha_1|^2 \dots |\alpha_s|^2$, где $s = \frac{l-1}{2}$).

С помощью нормы доказательство того, что K_l является полем, сводится, как и при $l = 3$, к тривиальной выкладке:

$$\frac{\beta}{\alpha} = \frac{\beta\alpha^{(2)}\alpha^{(3)} \dots \alpha^{(l-1)}}{\alpha^{(1)}\alpha^{(2)} \dots \alpha^{(l-1)}} = \frac{\beta\alpha^{(2)}\alpha^{(3)} \dots \alpha^{(l-1)}}{N\alpha} \in K_l.$$

Число (8) поля K_l называется *целым*, если все коэффициенты $a_0, a_1, \dots, a_{l-2}$ являются целыми рациональными числами (принадлежат кольцу $\mathbb{Z}$). Как уже отмечалось, норма $N\alpha$ целого числа α является (неотрицательным) целым рациональным числом. Все целые числа поля K_l составляют, очевидно, кольцо. Мы будем обозначать это кольцо символом D_l.

Так же, как и в случае $l = 3$, *число $\alpha \in D_l$ тогда и только тогда является единицей кольца D_l, когда* $N\alpha = 1$.

Действительно, если $\alpha\alpha^{-1} = 1$, то $N\alpha \cdot N\alpha^{-1} = 1$ и потому $N\alpha = 1$. Обратно, если $N\alpha = 1$, то $\alpha\alpha^{-1} = 1$, где $\alpha^{-1} = \alpha^{(2)} \dots \alpha^{(l-1)}$. ■

Отсюда (и из (11)) следует, что функция $\alpha \mapsto N\alpha$ является (на D_l^*) строгой псевдонормой. Поэтому (см. § 4, предложение 1) *в кольце D_l любой не являющийся единицей элемент разлагается в произведение простых элементов.*

Однако, как показывают примеры, кольцо D_l, вообще говоря, не является кольцом с однозначным разложением на множители.

Например, можно показать, что кольцо D_{23} не будет кольцом с однозначным разложением на множители. Напротив, в кольцах D_l с $l < 23$ разложение на множители однозначно.

Задача. Изучите кольцо D_5. Найдите его единицы. Покажите, что кольцо D_5 евклидово и потому является кольцом с однозначным разложением на множители.

Аналогичное исследование колец D_l при $5 < l < 23$ является уже очень трудной задачей.

Так как числа $\zeta^{(1)} = \zeta$, $\zeta^{(2)} = \zeta^2$, $\dots$, $\zeta^{(l-1)} = \zeta^{l-1}$ являются корнями многочлена (2), то

$$x^{l-1} + \dots + 1 = (x - \zeta)(x - \zeta^2) \dots (x - \zeta^{l-1}).$$

Полагая здесь $x=1$, мы получим, что

$$l=(1-\zeta)(1-\zeta^2)\dots(1-\zeta^{l-1}), \tag{12}$$

т. е. что $l=\lambda^{(1)}\dots\lambda^{(l-1)}$, где $\lambda=1-\zeta$. Это означает, что

$$N\lambda=l, \qquad \lambda=1-\zeta. \tag{13}$$

Отсюда следует, что *число* $\lambda=1-\zeta$ *является простым элементом кольца* D_l. Действительно, если $\lambda=\alpha\beta$, то $l=N\lambda=N\alpha\cdot N\beta$ и потому либо $N\alpha=1$, либо $N\beta=1$. ■

Кроме того, *если целое рациональное число* a *делится в кольце* D_l *на* λ, *то оно делится и на* l. Действительно, переходя в равенстве $a=\lambda\alpha$ к нормам, мы получим, что $a^{l-1}=l\cdot N\alpha$, где $N\alpha$ — целое рациональное число. Таким образом, l делит a^{l-1}, а значит, и a. ■

Роль ζ может играть любой корень $\zeta^{(k)}=\zeta^k$. Поэтому аналог равенства (13) справедлив для любого k:

$$N(1-\zeta^k)=l, \qquad k=1,\dots,l-1.$$

Другое доказательство:

$$N(1-\zeta^k)=\prod_{s=1}^{l-1}(1-\zeta^{sk})=\prod_{s=1}^{l-1}(1-\zeta^s)=N(1-\zeta)=l,$$

ибо числа k, $2k$, ..., $(l-1)k$ с точностью до порядка и слагаемых, кратных l, совпадают с числами 1, 2, ..., $l-1$. ■

Но

$$1-\zeta^k=(1-\zeta)\varepsilon_k, \quad \text{где} \quad \varepsilon_k=1+\zeta+\dots+\zeta^{k-1},$$

откуда следует, что

$$N(1-\zeta^k)=N(1-\zeta)\cdot N\varepsilon_k,$$

т. е. что $l=l\cdot N\varepsilon_k$. Следовательно, $N\varepsilon_k=1$, так что число ε_k является единицей и, значит, *число* $1-\zeta^k$, $k=1,\dots,l-1$, *ассоциировано с числом* $\lambda=1-\zeta$.

В силу (12), это означает, что *в кольце* D_l *имеет место равенство*

$$l=\varepsilon\lambda^{l-1}, \tag{14}$$

где ε — некоторая единица.

Таким образом, с точностью до ассоциированности число l в кольце D_l является $l-1$-й степенью простого элемента $\lambda = 1 - \zeta$.

Для дальнейшего полезно иметь в виду, что любой элемент $\alpha \in D_l$ может быть, очевидно, записан в виде линейной комбинации степеней элемента λ:

$$\alpha = b_0 + b_1\lambda + \ldots + b_{l-2}\lambda^{l-2}. \tag{15}$$

Перенося на случай кольца D_l обозначения Гаусса (см. § 1), будем писать $\alpha \equiv \beta \bmod \lambda$, где $\alpha, \beta \in D_l$, если разность $\alpha - \beta$ делится на λ. Так же как и для целых рациональных чисел, эти сравнения в отношении действий сложения и умножения ведут себя, как обыкновенные равенства (их можно складывать, перемножать и, в частности, возводить в степень с натуральным показателем).

Из формулы (15) немедленно вытекает теперь, что *для любого $\alpha \in D_l$ существует такое целое рациональное число b_0, что*

$$\alpha \equiv b_0 \bmod \lambda. \tag{16}$$

§ 6. Единицы кольца D_l

Доказательство Куммера основывается на довольно тонком изучении структуры группы единиц кольца D_l. Нам понадобится четыре утверждения об этой группе, три из которых мы докажем, а четвертое, к сожалению, будем вынуждены оставить без доказательства.

В первую очередь, мы найдем все элементы кольца D_l, являющиеся корнями из единицы. Примером такого элемента служит число ζ, являющееся, по построению, корнем из единицы степени l. Другой пример доставляет нам число $-\zeta$, являющееся, очевидно, корнем из единицы степени $2l$. Всевозможные степени числа $-\zeta$ (имеющие, как легко показать, вид $\pm\zeta^a$, где $a = 0, 1, \ldots, l-1$) также являются корнями из единицы степени $2l$ (и, очевидно, исчерпывают все такие корни). Оказывается, что это все корни из единицы, содержащиеся в кольце D_l.

Предложение 1. *Любой корень из единицы, содержащийся в кольце D_l, является корнем степени $2l$ и, значит, может быть представлен в виде*

$$\pm\zeta^a, \quad a=0,\ 1,\ \ldots,\ l-1.$$

Доказательство. Нам надо показать, что если в кольце D_l имеет место равенство $\alpha^N=1$ с целым положительным показателем N, причем $\alpha^{N_1}\neq 1$ ни для одного положительного $N_1<N$, то N делит $2l$, т. е. не делится ни на l^2, ни на 4, ни на произвольное простое число $p\neq l$.

Пусть $N=l^2n$. Рассмотрим число $\beta=\alpha^n$. Как мы знаем (см. формулу (16) § 5), существует такое целое рациональное число b_0, что

$$\beta\equiv b_0 \bmod \lambda.$$

Это означает, что $\beta=b_0+\lambda\gamma$, где $\gamma\in D_l$. Но тогда по уже известному нам свойству биномиальных коэффициентов $\beta^l\equiv b_0^l+(\lambda\gamma)^l \bmod l$, и потому (см. формулу (14) § 5)

$$\beta^l\equiv c_0 \bmod l,$$

где $c_0=b_0^l$.

С другой стороны, ясно, что $\beta^l\neq 1$, но $(\beta^l)^l=1$, т. е. β^l является отличным от 1 корнем степени l из единицы. Но все такие корни содержатся, по построению, в D_l и имеют вид ζ^a, где $0<a\leqslant l-1$. Этим доказано, что $\beta^l=\zeta^a$ при некотором a, $0<a\leqslant l-1$.

Таким образом, мы видим, что в кольце D^l имеет место сравнение вида

$$\zeta^a\equiv c_0 \bmod l,$$

где $0<a\leqslant l-1$ и $c_0\in\mathbb{Z}$. Но это невозможно, так как элемент вида $\frac{\zeta^a-c_0}{l}$ не может принадлежать D_l. Следовательно, равенство $N=l^2n$ невозможно, т. е. N не делится на l^2.

Пусть $N=4n$ или $N=pn$, где p — простое нечетное число, отличное от l. Снова рассмотрим число $\beta=\alpha^n$. Ясно, что $\beta=\pm i$ при $N=4n$, т. е. $\beta^2=-1$, и $\beta^p=1$ при $N=pn$. В обоих случаях

$$\beta^p\equiv 1 \bmod p,$$

т. е.

$$\beta^p \equiv -\zeta - \zeta^2 - \ \dots\ - \zeta^{l-1} \bmod p, \tag{1}$$

где $p = 2$ при $N = 4n$.

Представим число β в виде

$$\beta = b_1\zeta + b_2\zeta^2 + \ \dots\ + b_{l-1}\zeta^{l-1}.$$

Тогда по известному свойству полиномиальных коэффициентов

$$\beta^p \equiv b_1^p\zeta^p + b_2^p\zeta^{2p} + \ \dots\ + b_{l-1}^p\zeta^{(l-1)p} \bmod p,$$

т. е. (мы применяем здесь теорему Эйлера)

$$\beta^p \equiv b_1\zeta^p + b_2\zeta^{2p} + \ \dots\ + b_{l-1}\zeta^{(l-1)p} \bmod p.$$

Но ясно, что при любом простом $p \geqslant 2$, отличном от l, числа $\zeta^p, \zeta^{2p}, \dots, \zeta^{(l-1)p}$ с точностью до порядка совпадают с числами $\zeta, \zeta^2, \dots, \zeta^{l-1}$, откуда, ввиду сравнения (1) (и единственности разложения элементов кольца D_l по степеням $\zeta, \zeta^2, \dots, \zeta^{l-1}$), вытекает, что

$$b_1 \equiv b_2 \equiv \ \dots\ \equiv b_{l-1} \equiv -1 \bmod p.$$

Следовательно,

$$\beta \equiv -\zeta - \zeta^2 - \ \dots\ - \zeta^{l-1} \bmod p,$$

т. е.

$$\beta \equiv 1 \bmod p.$$

Это означает, что элемент β может быть представлен в виде $\beta = 1 + p^k\gamma$, где $k \geqslant 1$ и $\gamma \in D_l$ не делится на p. Отсюда, пользуясь формулой бинома Ньютона и учитывая, что $2k + 1 \geqslant k + 2$ при $k \geqslant 1$, мы немедленно получаем, что

$$\beta^p \equiv 1 + p^{k+1}\gamma \bmod p^{k+2}.$$

Если теперь $p > 2$ (т. е. мы имеем дело со случаем $N = pn$), то $\beta^p = 1$ и, следовательно,

$$p^{k+1}\gamma \equiv 0 \bmod p^{k+2},$$

т. е. $\gamma \equiv 0 \bmod p$, что противоречит выбору γ. Таким образом, предположение, что N делится на p, приводит к противоречию.

Если же $p = 2$ (т. е. мы имеем дело со случаем $N = 4n$), то $\beta^p = -1$ и, следовательно,

$$0 \equiv 2 + 2^{k+1}\gamma \bmod 2^{k+2}, \text{ т. е. } 2^k\gamma \equiv 1 \bmod 2^{k+1},$$

что явно невозможно. Таким образом, N не может делиться и на 4. ■

Замечание. В формулировке предложения 1 слова «в кольце D_l» можно заменить словами «в поле K_l», ибо можно показать, что любой корень из единицы, содержащийся в поле K_l, автоматически будет принадлежать кольцу D_l (см. ниже § 12). В дальнейшем это замечание использоваться не будет.

Каждый корень из единицы $\alpha \in D_l$ обладает, очевидно, тем свойством, что $|\alpha^{(k)}| = 1$ для любого $k = 1, \ldots, l-1$ (ибо $(\alpha^{(k)})^{2l} = 1$). Оказывается, что верно и обратное.

Предложение 2. *Если для элемента $\alpha \in D_l$ имеют место равенства*

$$|\alpha^{(k)}| = 1, \quad k = 1, \ldots, l-1, \tag{2}$$

то α является корнем из единицы.

Доказательство. Пусть A_l — множество всех элементов $\alpha \in D_l$, удовлетворяющих условию (2).

Для произвольного элемента $\alpha \in A_l$ рассмотрим многочлен

$$(x - \alpha^{(1)}) \ldots (x - \alpha^{(l-1)}) = x^{l-1} + c_1 x^{l-2} + \ldots + c_{l-1}, \tag{3}$$

корнем которого является число $\alpha = \alpha^{(1)}$. Ясно, что абсолютная величина $|c_k|$ каждого коэффициента c_k, $k = 1, \ldots, l-1$, этого многочлена не превосходит соответствующего коэффициента многочлена

$$(x + |\alpha^{(1)}|) \ldots (x + |\alpha^{(l-1)}|) = (x+1)^{l-1},$$

т. е. не превосходит $\binom{l-1}{k}$.

Но в § 5 было показано (для любого $\alpha \in D_l$), что многочлен (3) имеет целые коэффициенты. Поскольку целых чисел c_k, удовлетворяющих неравенствам

$$|c_k| \leqslant \binom{l-1}{k}, \quad k = 1, \ldots, l-1,$$

существует (при данном l) только конечное число, этим доказано, что множество многочленов вида (3) (для всевозможных $\alpha \in A_l$) конечно. Так как конечное число многочленов данной степени имеет только конечное число корней и так как любой элемент

$\alpha \in A_l$ является корнем соответствующего многочлена (3), отсюда вытекает, что множество A_l конечно.

С другой стороны, ясно, что если $\alpha \in A_l$, то $\alpha^n \in A_l$ для каждого $n \in Z$. Поэтому, ввиду конечности A_l, для любого $\alpha \in A_l$ существуют такие различные показатели m и n, что $\alpha^m = \alpha^n$. Но тогда $\alpha^{n-m} = 1$, т. е. α является корнем из единицы. ■

Несмотря на то, что все корни многочлена (2) из § 5 являются комплексными (невещественными) числами, в поле K_l (и в кольце D_l) имеется достаточно много вещественных чисел.

В частности, оказывается, что единицами вида $\pm\zeta^a$ и вещественными единицами исчерпываются, по существу, все единицы кольца D_l.

Предложение 3. *Любая единица кольца D_l имеет вид*

$$\pm \zeta^a \varepsilon_0,$$

где ε_0 — вещественная единица.

Доказательство. Пусть

$$\varepsilon = a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2}$$

— произвольная единица кольца D_l. Так как $\bar{\zeta} = \zeta^{-1} = \zeta^{l-1}$, то комплексно сопряженное число

$$\bar{\varepsilon} = a_0 + a_1\bar{\zeta} + \ldots + a_{l-2}\bar{\zeta}^{l-2}$$

лежит в D_l и является, очевидно, единицей. Поэтому единицей будет и число

$$\mu = \frac{\bar{\varepsilon}}{\varepsilon} \in D_l.$$

Эта единица обладает, очевидно, тем свойством, что $|\mu| = 1$.

Более того, для любого $k = 1, \ldots, l-1$ число

$$\varepsilon^{(k)} = a_0 + a_1\zeta^{(k)} + \ldots + a_{l-2}(\zeta^{(k)})^{l-2}$$

также является единицей, причем

$$\mu^{(k)} = \frac{\bar{\varepsilon}^{(k)}}{\varepsilon^{(k)}}.$$

Поэтому $|\mu^{(k)}| = 1$ для любого $k = 1, 2, \ldots, l-1$.

Следовательно, согласно предложению 2, число μ является корнем из единицы. Поскольку, согласно предложению 1, любой корень из единицы имеет вид $\pm\zeta^c$, тем самым доказано, что существует такое целое число $c \geqslant 0$, что

$$\bar{\varepsilon} = \pm\zeta^c\varepsilon.$$

Согласно сказанному в конце § 5, существует такое целое рациональное число b_0, что

$$\varepsilon \equiv b_0 \bmod \lambda.$$

При этом, так как $\bar{\lambda} \equiv 0 \bmod \lambda$, то также

$$\bar{\varepsilon} \equiv b_0 \bmod \lambda.$$

Поэтому, если

$$\bar{\varepsilon} = -\zeta^c\varepsilon,$$

то

$$b_0 \equiv -b_0 \bmod \lambda,$$

ибо $\zeta \equiv 1 \bmod \lambda$. Следовательно,

$$2b_0 \equiv 0 \bmod \lambda,$$

т. е. $2b_0$ делится на λ. Но мы знаем (см. § 5), что если целое рациональное число делится в кольце D_l на λ, то оно делится и на l. Следовательно, $2b_0$, а значит, и b_0 делится на l. В частности, b_0 делится на λ и, значит, ε делится на λ, что невозможно (ибо $N\varepsilon = 1$ не делится на $N\lambda = l$).

Полученное противоречие показывает, что

$$\bar{\varepsilon} = \zeta^c\varepsilon.$$

Мы положим

$$\varepsilon_0 = \zeta^{-sc}\varepsilon, \quad \text{где} \quad s = \frac{l-1}{2}.$$

Тогда

$$\varepsilon = \zeta^a\varepsilon_0, \quad \text{где} \quad a = sc,$$

причем (напомним, что $\bar{\zeta} = \zeta^{-1}$)

$$\bar{\varepsilon}_0 = \bar{\zeta}^{-sc}\bar{\varepsilon} = \zeta^{sc}\zeta^c\varepsilon = \zeta^{(s+1)c}\varepsilon = \zeta^{(l-s)c}\varepsilon = \zeta^{-sc}\varepsilon = \varepsilon_0. \quad \blacksquare$$

Для исследования первого случая теоремы Ферма методом Эйлера — Куммера, к которому мы перейдем в следующем параграфе, нам достаточно предложе-

ния 3. Однако для более трудного второго случая нам будет нужно еще одно свойство единиц кольца D_l, имеющее место, когда простое число l регулярно (см. стр. 13). Это свойство выражается так называемой «леммой Куммера», которая дает достаточные условия того, чтобы некоторая единица кольца D_l была l-й степенью другой единицы.

Лемма Куммера. *Если простое число l регулярно, то каждая единица ε кольца D_l, для которой существует такое целое рациональное число e, что*

$$\varepsilon \equiv e \bmod l,$$

является l-й степенью некоторой другой единицы $\eta \in D_l$:

$$\varepsilon = \eta^l.$$

Мы не будем даже пытаться доказывать эту лемму. Формально ее утверждение можно включить в определение регулярного числа (именно так первоначально и поступил Куммер).

§ 7. Первый случай теоремы Ферма

Чтобы выпукло показать трудности, возникающие при попытках доказать теорему Ферма, мы разобьем доказательство Куммера первого случая теоремы Ферма (для регулярных показателей) на два этапа. В этом параграфе мы выведем теорему из некоего вспомогательного утверждения, а в следующих параграфах обсудим пути его доказательства.

Вспомогательное утверждение. *Если*

$$x^l + y^l = z^l, \quad l \geqslant 3, \tag{1}$$

где x, y, z — взаимно простые целые рациональные числа, не делящиеся на простое число l, то в кольце D_l имеет место равенство

$$x + \zeta y = \varepsilon \alpha^l, \tag{2}$$

где $\alpha \in D_l$, а ε — единица кольца D_l.

Ввиду этого утверждения, чтобы в первом случае теоремы Ферма прийти к противоречию, достаточно показать, что равенство (2) в кольце D_l возможно (при выполнении равенства (1)) только тогда, когда

хотя бы одно из чисел x, y и z делится на l. При этом мы можем считать, что $l \geqslant 5$, поскольку при $l = 3$ теорема Ферма нами уже доказана.

Как мы знаем (см. § 1),

$$(3) \qquad (x_1 + \ldots + x_n)^l \equiv x_1^l + \ldots + x_n^l \bmod l$$

для любых $x_1, \ldots, x_n$.

Лемма. *Если*

$$x + \zeta y = \varepsilon \alpha^l,$$

где x, y — целые рациональные числа, $\alpha \in D_l$ и ε — единица кольца D_l, то при $l \geqslant 5$ либо x или y делятся на l, либо $x \equiv y \bmod l$.

Доказательство. Пусть

$$\alpha = b_0 + b_1\lambda + \ldots + b_{l-2}\lambda^{l-2},$$

где $b_0, b_1, \ldots, b_{l-2}$ — целые рациональные числа (см. § 5, формула (15)). Тогда, согласно формуле (3),

$$\alpha^l \equiv b_0^l + b_1^l\lambda^l + \ldots + b_{l-2}^l\lambda^{l(l-2)} \bmod l,$$

откуда, ввиду формулы (14) § 5, вытекает, что

$$\alpha^l \equiv b_0^l \bmod l.$$

Следовательно, ввиду малой теоремы Ферма,

$$\alpha^l \equiv b_0 \bmod l.$$

Согласно предложению 4 § 6, единица ε имеет вид

$$\varepsilon = \zeta^a \varepsilon_0,$$

где ε_0 — вещественная единица. Следовательно, полагая

$$\eta = b_0\varepsilon_0,$$

мы получим, что

$$x + \zeta y \equiv \zeta^a \eta \bmod l,$$

т. е. что

$$\zeta^{-a}(x + \zeta y) \equiv \eta \bmod l.$$

Заметим теперь, что если $\alpha \equiv \beta \bmod l$, т. е. $\alpha = \beta + l\gamma$, где $\gamma \in D_l$, то $\bar{\alpha} = \bar{\beta} + l\bar{\gamma}$, где $\bar{\gamma} \in D_l$, и по-

тому $\bar{\alpha} \equiv \bar{\beta} \bmod l$. В частности,

$$\overline{\zeta^{-a}(x+\zeta y)} \equiv \bar{\eta} \bmod l.$$

Но число η вещественно ($\bar{\eta} = \eta$), а $\bar{\zeta} = \zeta^{-1}$. Следовательно,

$$\zeta^a (x + \zeta^{-1} y) \equiv \eta \bmod l,$$

и, значит,

$$\zeta^a (x + \zeta^{-1} y) \equiv \zeta^{-a} (x + \zeta y) \bmod l,$$

т. е.

$$x\zeta^a + y\zeta^{a-1} - x\zeta^{-a} - y\zeta^{1-a} \equiv 0 \bmod l.$$

Обозначая символом $\langle k \rangle$ неотрицательный остаток от деления целого числа k на l (вычет числа k), мы можем это соотношение переписать в следующем виде:

$$x\zeta^{\langle a \rangle} + y\zeta^{\langle a-1 \rangle} - x\zeta^{\langle -a \rangle} - y\zeta^{\langle 1-a \rangle} \equiv 0 \bmod l. \tag{4}$$

Ясно, что число $a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2}$ кольца D_l тогда и только тогда делится на l, когда все его коэффициенты $a_0, a_1, \ldots, a_{l-2}$ делятся на l. Поэтому, если показатели в (4) все различны и отличны от $l-1$, то сравнение (4) возможно только тогда, когда числа x и y делятся на l. Таким образом, в этом случае все доказано.

Пусть среди показателей в (4) имеется число $l-1$. Это возможно тогда и только тогда, когда

$$\langle a \rangle = 0,\ 1,\ 2,\ l-1,$$

и соответственно

$$\begin{aligned} \langle a-1 \rangle &= l-1, \quad 0, \quad 1, \quad l-2, \\ \langle -a \rangle &= \quad 0, \quad l-1, \quad l-2, \quad 1, \\ \langle 1-a \rangle &= \quad 1, \quad 0, \quad l-1, \quad 2. \end{aligned}$$

Так как, по условию, $l \geqslant 5$, то в каждом из этих четырех случаев только один из показателей в (4) равен $l-1$. Член с этим показателем мы должны преобразовать по формуле

$$\zeta^{l-1} = -1 - \zeta - \ldots - \zeta^{l-2}.$$

После такого преобразования этот член заменится суммой одночленов $1, \zeta, \ldots, \zeta^{l-2}$ с коэффициентами $\pm x$ или $\pm y$. Так как число $l-1$ этих одночленов не меньше четырех (ибо $l \geqslant 5$), то при приведении подобных членов хотя бы один из них не сократится с остальными тремя членами левой части сравнения (4). (Например, если $\langle -a \rangle = l-1$, то заведомо останется слагаемое $x\zeta$.) Поскольку в результате приведения подобных членов в левой части сравнения (4) получается число кольца D_l, записанное в нормальной форме $a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2}$, коэффициент при этом оставшемся одночлене должен делиться на l.

Таким образом, и в этом случае либо x, либо y делится на l.

Пусть все показатели в (4) меньше $l-1$, но пусть среди них есть равные. Поскольку равенства $\langle a \rangle = \langle a-1 \rangle$ и $\langle -a \rangle = \langle 1-a \rangle$, очевидно, вообще невозможны (соседние числа не могут давать при делении на l одинаковых остатков), нам следует рассмотреть только четыре случая

$$\langle a \rangle = \langle -a \rangle, \qquad \langle a \rangle = \langle 1-a \rangle,$$
$$\langle a-1 \rangle = \langle 1-a \rangle, \quad \langle a-1 \rangle = \langle -a \rangle,$$

т. е. случаи

$$a \equiv -a \bmod l, \qquad a \equiv 1-a \bmod l,$$
$$a-1 \equiv 1-a \bmod l, \quad a-1 \equiv -a \bmod l.$$

В первом случае $2a \equiv 0 \bmod l$, т. е. $2a = Al$, где A — целое число (очевидно, четное). Поэтому

$$a-1 = (l-1) + \left(\frac{A}{2} - 1\right) l$$

и, следовательно, $\langle a-1 \rangle = l-1$, что, по условию, невозможно.

Аналогично, во втором случае $2a \equiv 2 \bmod l$, т. е. $2a = 2 + Al$, где A — целое (очевидно, четное) число. Поэтому

$$-a = (l-1) - \left(\frac{A}{2} + 1\right) l$$

и, следовательно, мы снова получаем невозможное равенство $\langle -a \rangle = l-1$.

В третьем же и четвертом случаях $2a \equiv 1 \bmod l$, т. е. $2a = 1 + Al$, где A — целое число (очевидно, нечетное).

Поэтому

$$a = \frac{l+1}{2} + \frac{A-1}{2} l$$

и, следовательно, $\langle a \rangle = \frac{l+1}{2}$, а значит,

$$\langle a - 1 \rangle = \langle -a \rangle = \frac{l-1}{2}$$

и

$$\langle 1 - a \rangle = \langle a \rangle = \frac{l+1}{2}.$$

Таким образом, в этих случаях сравнение (4) приобретает вид

$$(5) \qquad (x-y)\zeta^{\frac{l+1}{2}} + (y-x)\zeta^{\frac{l-1}{2}} \equiv 0 \bmod l.$$

Поскольку левая часть сравнения (5) имеет нормальный вид (показатели $\frac{l+1}{2}$ и $\frac{l-1}{2}$ различны и меньше числа $l-1$), из него следует, что $x-y$ делится на l, т. е. что

$$x \equiv y \bmod l.$$

Тем самым лемма полностью доказана. ■

Из этой леммы и Вспомогательного утверждения вытекает, что если

$$(6) \qquad x^l + y^l = z^l,$$

где числа x, y, z взаимно просты и не делятся на l, то $x \equiv y \bmod l$. Но вместе с равенством (6) имеет место и равенство

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

Поэтому то же рассуждение показывает, что $x \equiv -z \bmod l$.

Следовательно,

$$x + y - z \equiv 3x \bmod l.$$

С другой стороны, из равенства (6) в силу малой теоремы Ферма вытекает, что

$$z \equiv x + y \bmod l.$$

Следовательно,

$$3x \equiv 0 \bmod l,$$

что невозможно, поскольку $l > 3$, а x не делится на l.

Итак, предположив, что для не делящихся на l взаимно простых чисел x, y, z имеет место соотношение (6), мы, используя Вспомогательное утверждение, получили противоречие.

Тем самым доказано, что *первый случай теоремы Ферма имеет место для всех l, для которых верно Вспомогательное утверждение.*

Поскольку

$$x^l + y^l = (x + y)(x + \zeta y) \ldots (x + \zeta^{l-1} y),$$

равенство

$$x^l + y^l = z^l \tag{7}$$

может быть переписано в следующем виде:

$$(x + y)(x + \zeta y) \ldots (x + \zeta^{l-1} y) = z^l. \tag{8}$$

Если

А) все множители в левой части равенства (8) взаимно просты;

Б) в кольце D_l справедлива основная теорема арифметики,

то каждый из множителей в (8) с точностью до ассоциированности будет l-й степенью (ибо, согласно (8), их произведение является l-й степенью). Другими словами, в кольце D_l найдется такой элемент α и такая единица ε, что, скажем,

$$x + \zeta y = \varepsilon \alpha^l.$$

Этим доказано Вспомогательное утверждение из § 7, с точностью, конечно, до двух больших «если». Впрочем, первое «если» легко доказывается:

Предложение 1. *Если целые рациональные числа x и y взаимно просты, а их сумма $x + y$ не делится на l, то все числа*

$$x + y,\ x + \zeta y,\ \ldots,\ x + \zeta^{l-1} y \tag{9}$$

попарно взаимно просты (в кольце D_l).

Доказательство. Пусть в D_l существует простой множитель π, делящий два из чисел (9), скажем, числа $x+\zeta^m y$ и $x+\zeta^n y$, где $0 \leqslant m, n \leqslant l-1$ и $m \neq n$.

Так как

$$-\zeta^{n-m}(x+\zeta^m y)+(x+\zeta^n y)=(1-\zeta^{n-m})x,$$
$$\zeta^{-m}(x+\zeta^m y)-\zeta^{-m}(x+\zeta^n y)=(1-\zeta^{n-m})y$$

и так как $1-\zeta^{n-m} \sim 1-\zeta$ (см. § 5), то π делит числа $(1-\zeta)x$ и $(1-\zeta)y$.

Так как целые числа x и y взаимно просты, существуют такие целые числа a и b, что $xa+yb=1$. Поэтому π делит число

$$(1-\zeta)xa+(1-\zeta)yb=1-\zeta,$$

а значит, и число $l \sim (1-\zeta)^{l-1}$.

Поскольку число π делит число $1-\zeta$, оно делит и число $1-\zeta^m \sim 1-\zeta$. Поэтому π делит и число

$$x+y=x+\zeta^m y+(1-\zeta^m)y.$$

Но, по условию, числа l и $x+y$ взаимно просты. Поэтому существуют такие числа u и v, что

$$lu+(x+y)v=1.$$

Это показывает, что π делит 1.

Полученное противоречие доказывает, что любые два из чисел (9) взаимно просты. ■

Предложение 1 немедленно обеспечивает выполнение условия А), так как в равенстве (1) числа x и y, по условию, взаимно просты, а число z, в силу малой теоремы Ферма сравнимое по модулю l с числом $x+y$, не делится по условию на l.

Что же касается условия Б), то, как мы знаем, оно выполнено только для некоторых l. Следовательно, мы пока вынуждены ограничиться только этими l.

Резюмируя, мы видим, что метод Эйлера пока позволил нам доказать теорему Ферма в следующей форме:

Теорема 1. *Пусть $l \geqslant 3$ — такое простое число, что в кольце D_l справедлива основная теорема ариф-*

метики. Тогда если для целых рациональных чисел x, y, z имеет место равенство

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

то хотя бы одно из этих чисел делится на l.

Можно показать (см. § 12), что условиям этой теоремы удовлетворяют простые числа

(10) $$l = 3, 5, 7, 11, 13, 17, 19.$$

В пределах первой сотни других простых чисел, удовлетворяющих условиям теоремы 1, нет.

Подчеркнем, однако, что проверка того, что для чисел (10) в кольце D_l справедлива основная теорема арифметики, является при $l > 5$ совсем не простой задачей. Таким образом, утверждать, что для чисел (10) нами доказан первый случай теоремы Ферма, мы, собственно говоря, права пока не имеем.

§ 8. Теория дивизоров

Как же дело обстоит с Вспомогательным утверждением, когда разложение на простые множители в кольце D_l не однозначно? Оказывается, что его все же можно доказать и в этом случае (по крайней мере, для некоторых l). Идея, принадлежащая Куммеру, состоит, как уже говорилось, в том, чтобы восстановить в D_l однозначность разложения на простые множители, добавив некоторые новые «идеальные» числа. Эта мысль Куммера преобразовала всю теорию алгебраических чисел и в руках Дедекинда, Кронекера и Золотарева привела к созданию совершенно новых концепций, оказавших глубокое влияние на все отделы современной математики.

Идеальные числа Куммера называются теперь «дивизорами». Абстрактно, ситуацию с ними можно описать следующим образом.

Предположим, что нам задано некоторое множество $\mathscr{D}$, в котором определено коммутативное и ассоциативное умножение, обладающее единицей (в абстрактной алгебре такие множества называются *коммутативными моноидами*). Элементы моноида $\mathscr{D}$ мы

будем обозначать малыми готическими буквами. В частности, единицу моноида $\mathscr{D}$ мы будем обозначать символом $\mathfrak{e}$.

Говорят, что элемент $\mathfrak{a} \in \mathscr{D}$ *делит* элемент $\mathfrak{c} \in \mathscr{D}$, если существует такой элемент $\mathfrak{b} \in \mathscr{D}$, что $\mathfrak{c} = \mathfrak{ab}$. Элемент $\mathfrak{p} \neq \mathfrak{e}$ называется *простым*, если он делится только на себя и на единицу $\mathfrak{e}$. Моноид $\mathscr{D}$ называется *свободным* (коммутативным) моноидом (или моноидом *с однозначным разложением на простые множители*), если каждый элемент $\mathfrak{a} \in \mathscr{D}$ может быть представлен в виде произведения простых элементов

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r, \quad r \geqslant 0,$$

и такое разложение с точностью до порядка множителей единственно (при $r = 0$ произведение считается равным $\mathfrak{e}$). Таким образом, в свободном моноиде нет никаких обратимых элементов («единиц»), кроме «настоящей» единицы $\mathfrak{e}$.

Примером свободного моноида является множество $\mathbb{N}$ натуральных чисел по отношению к умножению.

В свободном моноиде для любых элементов существует, очевидно, единственный *наибольший общий делитель* и единственное *наименьшее общее кратное*. Если наибольший общий делитель равен $\mathfrak{e}$, то элементы называются *взаимно простыми*.

Ясно, что в произвольном свободном моноиде сохраняются известные свойства делимости в свободном моноиде натуральных чисел. Например, если $\mathfrak{ab}$ делится на $\mathfrak{c}$ и $\mathfrak{a}$ взаимно просто с $\mathfrak{c}$, то $\mathfrak{b}$ делится на $\mathfrak{c}$. Если $\mathfrak{a}$ и $\mathfrak{b}$ взаимно просты и $\mathfrak{ab} = \mathfrak{r}^n$, то существуют такие элементы $\mathfrak{a}_1$ и $\mathfrak{b}_1$, что $\mathfrak{a} = \mathfrak{a}_1^n$ и $\mathfrak{b} = \mathfrak{b}_1^n$, и т. д.

Для произвольного кольца D множество D^* всех его отличных от нуля элементов является, очевидно, моноидом (приведите пример кольца, для которого этот моноид свободен). Предположим, что задано некоторое отображение этого моноида в свободный моноид $\mathscr{D}$. Обозначая образ элемента $\alpha \in D^*$ символом (α), мы потребуем, чтобы для любых элементов $\alpha, \beta \in D^*$ было выполнено равенство

$$(\alpha\beta) = (\alpha)(\beta),$$

т. е. чтобы отображение $\alpha \longmapsto (\alpha)$ было *гомоморфизмом*

моноидов. Тогда, если α делится на β в D, то (α) будет делиться на (β) в $\mathscr{D}$. Мы потребуем, чтобы было верно и обратное:

Аксиома 1. *Элемент* $\alpha \in D^*$ *тогда и только тогда делится на элемент* $\beta \in D^*$, *когда элемент* $(\alpha) \in \mathscr{D}$ *делится на элемент* $(\beta) \in \mathscr{D}$.

В частности, отсюда следует, что $(\alpha) = (\beta)$ тогда и только тогда, когда элементы α и β ассоциированы. Единицы ε кольца D характеризуются поэтому равенством $(\varepsilon) = \mathfrak{e}$.

Если элемент $\mathfrak{a}$ делит элемент (α), то мы будем говорить, что $\mathfrak{a}$ *делит* α. Совокупность всех элементов $\alpha \in D^*$, делящихся на элемент $\mathfrak{a} \in \mathscr{D}$, плюс элемент $0 \in D$ (который мы, таким образом, по определению, считаем делящимся на любой элемент $\mathfrak{a} \in \mathscr{D}$), мы обозначим символом $[\mathfrak{a}]$. Естественно потребовать, чтобы сумма и разность элементов кольца D, делящихся на элемент $\mathfrak{a} \in \mathscr{D}$, также делилась на $\mathfrak{a}$.

Аксиома 2. *Если* $\alpha, \beta \in [\mathfrak{a}]$, *то* $\alpha \pm \beta \in [\mathfrak{a}]$.

Наконец, потребуем, чтобы в $\mathscr{D}$ не было «лишних» элементов, т. е. чтобы любые два элемента из $\mathscr{D}$ отличались по их свойствам делимости по отношению к элементам кольца D.

Аксиома 3. *Если* $[\mathfrak{a}] = [\mathfrak{b}]$, *то* $\mathfrak{a} = \mathfrak{b}$.

Если для кольца D задан свободный коммутативный моноид $\mathscr{D}$ и гомоморфизм $\alpha \mapsto (\alpha)$, удовлетворяющий аксиомам 1—3, то говорят, что в D задана *теория дивизоров.* Элементы моноида $\mathscr{D}$ называются при этом *дивизорами,* а дивизоры вида (α), где $\alpha \in D$, — *главными дивизорами.* Единица $\mathfrak{e}$ моноида $\mathscr{D}$ называется *единичным дивизором.*

Заметим, что в этом определении ни существование, ни единственность теории дивизоров не предполагается. Впрочем, можно без труда доказать, что в некотором естественном смысле теория дивизоров для данного кольца D может существовать только одна. Этот факт нам не понадобится, и мы его доказывать не будем (см. З. И. Боревич, И. Р. Шафаревич, Теория чисел, М., 1972, гл. III, § 2, п. 2).

Напротив, существование теории дивизоров накладывает на кольцо D очень сильные ограничения.

В общем виде мы этим вопросом заниматься не будем, поскольку это увело бы нас далеко в сторону.

Легко видеть, однако, что *кольцо D, в котором выполнена основная теорема арифметики, обладает теорией дивизоров, причем в этой теории все дивизоры будут главными.*

Действительно, пусть $\mathscr{D}$ — множество классов ассоциированных элементов множества D^* (см. § 4). Обозначая класс, содержащий элемент α, символом (α) и полагая $(\alpha)(\beta)=(\alpha\beta)$, мы, как непосредственно проверяется, корректно определим в множестве $\mathscr{D}$ умножение, относительно которого оно будет свободным коммутативным моноидом. Отображение $\alpha\longmapsto(\alpha)$ будет при этом гомоморфизмом, удовлетворяющим аксиомам 1—3. При этом дивизор (α) будет прост тогда и только тогда, когда прост элемент α. ■

Обратно, *если для кольца D существует теория дивизоров, в которой все дивизоры главные, то в D выполнена основная теорема арифметики.*

Действительно, достаточно заметить, что в таком кольце дивизор (π) прост тогда и только тогда, когда прост элемент π (если $\pi=\pi_1\pi_2$, то $(\pi)=(\pi_1)(\pi_2)$, а если $(\pi)=(\pi_1)(\pi_2)$, то π ассоциирован с произведением $\pi_1\pi_2$; обратим внимание, что здесь существенно использовано предположение, что все дивизоры главные), и потому разложение каждого дивизора (α) в произведение простых дивизоров даст разложение элемента α в произведение простых элементов, причем с точностью до ассоциированности это разложение будет единственно. ■

Таким образом, чем больше неглавных дивизоров, тем дальше свойства делимости элементов кольца D (обладающего теорией дивизоров) отличаются от стандартных свойств делимости натуральных чисел. Чтобы придать этому высказыванию точный смысл, назовем два дивизора $\mathfrak{a}$ и $\mathfrak{b}$ *эквивалентными* (обозначение $\mathfrak{a}\sim\mathfrak{b}$), если они отличаются только на главные дивизоры, т. е. существуют такие элементы $\alpha,\beta\in D^*$, что

$$(\alpha)\mathfrak{a}=(\beta)\mathfrak{b}.$$

Ясно, что это отношение действительно является отношением эквивалентности (оно рефлексивно,

симметрично и транзитивно), и потому моноид $\mathscr{D}$ распадается на классы $\{\mathfrak{a}\}$ эквивалентных между собой дивизоров. Очевидно, далее, что формула $\{\mathfrak{a}\}\{\mathfrak{b}\} = \{\mathfrak{ab}\}$ корректно определяет умножение классов дивизоров. Это умножение ассоциативно и коммутативно, так что относительно него множество $\mathscr{H}$ всех классов дивизоров является моноидом. Этот моноид (точнее, число его элементов) и измеряет отклонение арифметики в D от арифметики натуральных чисел.

Заметим, что любой главный дивизор эквивалентен, очевидно, единичному дивизору, т. е. его класс является единицей моноида $\mathscr{H}$. Верно и обратное: если $\mathfrak{a} \sim \mathfrak{e}$, т. е. $(\alpha)\mathfrak{a} = (\beta)$, то, согласно аксиоме 1, существует такой элемент γ, что $\alpha\gamma = \beta$, и, значит, $(\alpha)(\gamma) = (\beta)$, т. е. $\mathfrak{a} = (\gamma)$. Таким образом, *дивизор тогда и только тогда эквивалентен единичному дивизору, когда он является главным дивизором*:

$$\mathfrak{a} \sim \mathfrak{e} \Leftrightarrow \mathfrak{a} = (\alpha).$$

В случае, когда моноид $\mathscr{H}$ конечен, число его элементов, т. е. число классов дивизоров кольца D, мы будем обозначать символом h. Согласно доказанному выше, *в кольце D тогда и только тогда выполнена основная теорема арифметики, когда моноид $\mathscr{H}$ состоит только из одного элемента, т. е. число h определено и равно 1.*

Мы наложим на рассматриваемую теорию дивизоров следующие две дополнительные аксиомы:

Аксиома 4. *Моноид $\mathscr{H}$ является (абелевой) группой, т. е. каждый его элемент обратим.*

Аксиома 5. *В группе $\mathscr{H}$ нет элементов порядка l.*

В последней аксиоме, как и всюду у нас, под l понимается данное фиксированное простое число.

Из аксиом 4 и 5 вытекает, что *если* $\mathfrak{a}^l \sim \mathfrak{b}^l$, *то* $\mathfrak{a} \sim \mathfrak{b}$. Действительно, эквивалентность $\mathfrak{a}^l \sim \mathfrak{b}^l$ означает, что для классов имеет место равенство $\{\mathfrak{a}\}^l = \{\mathfrak{b}\}^l$, т. е. (поскольку $\mathscr{H}$ — группа) равенство $(\{\mathfrak{a}\}\{\mathfrak{b}\}^{-1})^l = \{\mathfrak{e}\}$. Но так как в группе $\mathscr{H}$ нет элементов порядка l, последнее равенство возможно

только тогда, когда $\{\mathfrak{a}\}\{\mathfrak{b}\}^{-1} = \{\mathfrak{e}\}$, т. е. когда $\{\mathfrak{a}\} = \{\mathfrak{b}\}$ и, значит, $\mathfrak{a} \sim \mathfrak{b}$. ■

Заметим, что если группа $\mathcal{H}$ конечна, то *аксиома 5 равносильна требованию, чтобы простое число l не делило числа классов h* (порядка группы $\mathcal{H}$).

Вернемся теперь к теореме Ферма.

Будем называть простое число l *регулярным*, если кольцо D_l обладает теорией дивизоров, удовлетворяющей аксиомам 4—5. Обратим внимание, что в аксиоме 5 фигурирует то же число l, что и в конструкции кольца D_l.

Предложение 1. *Для каждого регулярного простого числа l Вспомогательное утверждение из* § 7 *верно.*

Доказательство. Если

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

то

$$(x + y)(x + \zeta y) \ldots (x + \zeta^{l-1} y) = z^l.$$

Перейдем в этом равенстве к дивизорам. Легко видеть, что доказательство предложения 1 из § 7 дословно сохранится, если под π понимать не простой элемент, а простой дивизор. Следовательно, все главные дивизоры вида $(x + \zeta^m y)$, $0 \leqslant m \leqslant l - 1$, попарно взаимно просты. Поэтому из того, что произведение этих дивизоров является l-й степенью (оно равно дивизору $(z)^l$), следует, что каждый из них будет l-й степенью. Таким образом, в частности, существует такой дивизор $\mathfrak{a} \in \mathcal{D}$, что

$$(x + \zeta y) = \mathfrak{a}^l.$$

Это равенство означает, что $\mathfrak{a}^l \sim \mathfrak{e}$, откуда, как мы знаем, следует, что $\mathfrak{a} \sim \mathfrak{e}$, т. е. что $\mathfrak{a} = (\alpha)$ для некоторого элемента $\alpha \in D_l$. Таким образом,

$$(x + \zeta y) = (\alpha^l),$$

и потому числа $x + \zeta y$ и α^l ассоциированы, т. е. существует такая единица $\varepsilon \in D_l$, что

$$x + \zeta y = \varepsilon \alpha^l. \quad ■$$

Тем самым, согласно § 7, для регулярных простых чисел доказан первый случай теоремы Ферма:

Теорема. *Если простое число $l \geqslant 3$ регулярно, то равенство*

$$x^l + y^l = z^l$$

для целых рациональных чисел x, y и z возможно только тогда, когда хотя бы одно из этих чисел делится на l.

Конечно, эту теорему следует дополнить исследованием, какие простые числа регулярны и как про данное простое число узнать, регулярно оно или нет. Без этого теорема 3 никакой реальной ценности, естественно, не имеет. Но мы пока отложим выяснение этого вопроса и займемся вторым случаем теоремы Ферма.

§ 9. Второй случай теоремы Ферма

В этом параграфе мы докажем, что для регулярных простых показателей l справедлив и второй случай теоремы Ферма, т. е. что равенство

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

невозможно и тогда, когда одно из (не равных нулю) чисел x, y, z делится на l.

Поскольку числа x, y, z предполагаются попарно взаимно простыми, только одно из них может делиться на l. Мы будем предполагать, что на l *делится число* z, что общности не ограничивает, поскольку если на l делится, например, y, то достаточно равенство (1) переписать в виде

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

Пусть $z = l^k z_0$, где z_0 не делится на l, а $k \geqslant 1$. Поскольку в кольце D_l имеет место равенство

$$l = \varepsilon_0 \lambda^{l-1}, \qquad \lambda = 1 - \zeta,$$

где ε_0 — некоторая единица (см. § 5, формула (14)), мы можем переписать равенство (1) в следующем виде (обозначив z_0 снова через z и положив $m = k(l-1)$):

$$x^l + y^l = \varepsilon \lambda^{lm} z^l, \tag{2}$$

где ε — единица. Здесь числа x, y, z взаимно просты

с l, а значит (рассматриваемые как элементы кольца D_l), и с λ.

Мы докажем, что равенство типа (2) невозможно даже тогда, когда под x, y, z мы будем понимать *произвольные числа кольца D_l, взаимно простые с λ* (и потому не равные нулю). Другими словами, мы докажем, что второй случай теоремы Ферма (для регулярных l) справедлив и в кольце D_l.

Заметим, что первый случай теоремы Ферма (и значит, полная теорема Ферма) также справедлив в кольце D_l. Для доказательства достаточно несколько усложнить рассуждения предыдущих двух параграфов.

В отличие от первого случая, мы не можем доказать второй случай только для целых рациональных чисел: необходимо доказывать более сильное утверждение, относящееся к числам из D_l. (Такого рода ситуация типична для индуктивных доказательств; часто индукция проходит только тогда, когда мы в достаточной мере усилим доказываемое утверждение.)

В доказательстве мы будем существенно пользоваться тем, что *главный дивизор* $\mathfrak{l} = (\lambda)$, *где* $\lambda = 1-\zeta$, *является простым дивизором.* Мы докажем этот факт позже (в приложении к § 10), а пока, чтобы не прерывать изложения, примем его без доказательства.

Число α кольца D_l мы назовем *полупервичным* (у нас нет здесь возможности объяснить происхождение этого термина), если, во-первых, оно не делится на $\mathfrak{l}$ (т. е. на λ) и, во-вторых, существует такое целое рациональное число b_0 (автоматически отличное от нуля), что разность $\alpha - b_0$ делится на $\mathfrak{l}^2$ (т. е. $\alpha \equiv b_0 \bmod \lambda^2$).

Другими словами, число α полупервично, если в его разложении (15) из § 5 число b_0 не делится на l, а $b_1 = 0$.

Легко видеть, что *для любого числа $\alpha \in D_l$, не делящегося на $\mathfrak{l}$, существует такое целое рациональное число a, что произведение $\zeta^a\alpha$ полупервично.*

Действительно, согласно формуле (15) § 5,

$$\alpha \equiv b_0 + b_1\lambda \bmod \lambda^2,$$

где, по условию, $b_0 \not\equiv 0 \bmod l$. Пусть a_0 — такое целое рациональное число, что $a_0 b_0 \equiv 1 \bmod l$, и пусть $a = a_0 b_1$.

Так как

$$\zeta^a = (1-\lambda)^a \equiv 1 - a\lambda \bmod \lambda^2,$$

то

$$\zeta^a\alpha \equiv (1-a\lambda)(b_0 + b_1\lambda) \equiv b_0 + (b_1 - ab_0)\lambda \bmod \lambda^2.$$

Но, по построению, $b_1 - ab_0 = b_1(1 - a_0b_0)$ делится на l, а, значит, и на λ.

Следовательно, $\zeta^a\alpha \equiv b_0 \bmod \lambda^2$. ■

Поскольку $\zeta^l = 1$, равенство (2) не меняется при умножении чисел x, y и z на любые степени числа ζ. Поэтому, без ограничения общности, мы можем считать, что *все числа x, y и z в равенстве* (2) *полупервичны*. Заметим, что при этой редукции показатель m не меняется.

После этих предварительных замечаний мы можем непосредственно перейти к доказательству невозможности равенства типа (2).

Предполагая, что равенства типа (2) существуют, выберем среди них то, у которого показатель m наименьший (а числа x, y, z полупервичны и, напомним, взаимно просты с l). Чтобы не вводить новых обозначений, будем считать, что этим равенством является (2).

Заметим, что теперь m уже не имеет, вообще говоря, вида $k(l-1)$. Однако, тем не менее, справедлива следующая лемма:

Лемма 1. *Показатель m больше единицы*:

$$m > 1.$$

Доказательство. Перепишем равенство (2), разложив левую часть на множители:

$$(3) \qquad (x+y)(x+\zeta y)\ \ldots\ (x+\zeta^{l-1}y) = \varepsilon\lambda^{lm}z^l.$$

Так как дивизор $\mathfrak{l} = (\lambda)$ прост, то хотя бы один из множителей слева должен делиться на $\mathfrak{l}$. Но так как все эти множители сравнимы друг с другом по модулю λ (ибо $(x+\zeta^a y) - (x+\zeta^b y) = \zeta^a(1-\zeta^{b-a})y$ делится на $\lambda = 1-\zeta$), то на $\mathfrak{l}$ делится каждый из них. В частности, на $\mathfrak{l}$ делится $x+y$.

Поскольку числа x и y полупервичны, существует такое целое рациональное число a, что

$$x + y \equiv a \bmod \lambda^2$$

(число $x+y$ не полупервично, потому что оно делится на λ). Это сравнение показывает, что целое рациональное число a делится на λ. Но тогда оно делится на l, т. е. на λ^{l-1}. Значит, оно заведомо делится на λ^2, а потому на λ^2 делится и число $x+y$.

Таким образом, в равенстве (3) все множители слева делятся на λ, а первый из них делится даже на λ^2. Следовательно, левая часть этого равенства делится на λ^{l+1}. Поэтому на λ^{l+1} делится и правая часть. Так как z взаимно просто с λ, это возможно только тогда, когда $m>1$. ■

Произведенное исследование делимости на λ множителей левой части равенства (3) можно уточнить:

Лемма 2. *Числа*

$$x+\zeta y,\ \ldots,\ x+\zeta^{l-1}y, \tag{4}$$

делясь на λ, *не делятся на* λ^2. *Число*

$$x+y$$

делится на $\lambda^{l(m-1)+1}$, *но не делится на* $\lambda^{l(m-1)+2}$.

Доказательство. Достаточно, очевидно, доказать, что ни одно из чисел (4) не делится на λ^2. Пусть, например, число $x+\zeta^k y$ делится на λ^2. Тогда на λ^2 будет делиться число

$$(1-\zeta^k)\,y=(x+y)-(x+\zeta^k y),$$

а значит, и число $1-\zeta^k$, что невозможно, ибо, как мы знаем, число $1-\zeta^k$ ассоциировано с $\lambda=1-\zeta$. ■

Пусть теперь $\mathfrak{m}$ — наибольший общий делитель главных дивизоров (x) и (y). Так как x и y не делятся на $\mathfrak{l}=(\lambda)$, то и $\mathfrak{m}$ не делится на $\mathfrak{l}$. Поэтому, согласно лемме 2, дивизоры вида $(x+\zeta^k y)$, $k\neq 0$, делятся на $\mathfrak{lm}$, а дивизор $(x+y)$ — даже на $\mathfrak{l}^{l(m-1)+1}\mathfrak{m}$. Пусть

$$(x+y)=\mathfrak{l}^{l(m-1)+1}\mathfrak{m}\mathfrak{c}_0,$$

$$(x+\zeta^k y)=\mathfrak{lm}\mathfrak{c}_k,\qquad k=1,\ \ldots\ ,l-1. \tag{5}$$

Согласно лемме 2, ни один из дивизоров $\mathfrak{c}_0, \mathfrak{c}_1, \ldots, \mathfrak{c}_{l-1}$ не делится на $\mathfrak{l}$.

Лемма 3. *Дивизоры* $\mathfrak{c}_0, \mathfrak{c}_1, \ldots, \mathfrak{c}_{l-1}$ *попарно взаимно просты.*

Доказательство. Пусть, например, дивизоры $\mathfrak{c}_i$ и $\mathfrak{c}_k$, $0 \leqslant i < k \leqslant l-1$, имеют общий делитель $\mathfrak{p}$. Тогда числа $x+\zeta^i y$ и $x+\zeta^k y$ делятся на $\mathfrak{l}\mathfrak{m}\mathfrak{p}$ и потому числа

$$(x+\zeta^k y)\,\zeta^i - (x+\zeta^i y)\,\zeta^k = \zeta^i(1-\zeta^{k-i})\,x,$$
$$-(x+\zeta^k y) + (x+\zeta^i y) = \zeta^i(1-\zeta^{k-i})\,y$$

также делятся на $\mathfrak{l}\mathfrak{m}\mathfrak{p}$. Поскольку множитель $\zeta^i(1-\zeta^{k-i})$ ассоциирован с $\lambda = 1-\zeta$, отсюда следует, что числа x и y делятся на $\mathfrak{m}\mathfrak{p}$, что противоречит определению наибольшего общего делителя. ■

Перейдя в (3) к дивизорам и подставив их выражения (5), мы получим (после сокращения на $\mathfrak{l}^{lm}$) равенство

$$\mathfrak{m}^l \mathfrak{c}_0 \mathfrak{c}_1 \ldots \mathfrak{c}_l = \mathfrak{z}^l,$$

где $\mathfrak{z} = (z)$. Поскольку дивизоры $\mathfrak{c}_0, \mathfrak{c}_1, \ldots, \mathfrak{c}_l$ попарно взаимно просты, это равенство возможно только тогда, когда эти дивизоры являются l-ми степенями, т. е. имеют вид

$$\mathfrak{c}_i = \mathfrak{a}_i^l, \quad i = 0, 1, \ldots, l-1, \tag{6}$$

где $\mathfrak{a}_i$ — некоторые дивизоры (очевидно, не делящиеся на $\mathfrak{l}$).

Лемма 4. *Дивизоры* $\mathfrak{a}_0, \mathfrak{a}_1, \ldots, \mathfrak{a}_{l-1}$ *эквивалентны* (*принадлежат одному классу*).

Доказательство. Подставив в (5) выражения (6), мы получим, что

$$(x+y) = \mathfrak{l}^{l(m-1)+1}\mathfrak{m}\mathfrak{a}_0^l,$$
$$(x+\zeta^k y) = \mathfrak{l}\mathfrak{m}\mathfrak{a}_k^l, \qquad k = 1, \ldots, l-1.$$

Перемножив эти равенства «крест накрест» и сократив на $\mathfrak{m}\mathfrak{l}$, мы получим соотношения

$$(x+y)\,\mathfrak{a}_k^l = (x+\zeta^k y)\,(\mathfrak{l}^{m-1}\mathfrak{a}_0)^l, \quad k = 1, \ldots, l-1, \tag{7}$$

означающие, что $\mathfrak{a}_k^l \sim (\mathfrak{l}^{m-1}\mathfrak{a}_0)^l$. Так как число l регулярно, то отсюда следует, что $\mathfrak{a}_k \sim \mathfrak{l}^{m-1}\mathfrak{a}_0$. Но дивизор $\mathfrak{l} = (\lambda)$ главный и потому $\mathfrak{l}^{m-1}\mathfrak{a}_0 \sim \mathfrak{a}_0$. Таким образом, $\mathfrak{a}_k \sim \mathfrak{a}_0$ для любого $k = 1, \ldots, l-1$. ■

Согласно лемме 4, существуют такие числа $\alpha_k, \beta_k \in D_l$, что

$$(\alpha_k)\mathfrak{a}_0 = (\beta_k)\mathfrak{a}_k, \qquad k = 1, \ldots, l-1. \tag{8}$$

Так как дивизоры $\mathfrak{a}_i$, $i = 0, 1, \ldots, l-1$, не делятся на $\mathfrak{l} = (\lambda)$, то без ограничения общности можно считать, что числа α_k и β_k не делятся на λ.

Умножив равенства (7) на $(\alpha_k\beta_k)^l$ и воспользовавшись соотношением (8), мы получим следующее соотношение между главными дивизорами:

$$(x+y)(\alpha_k)^l = (x+\zeta^k y)(\lambda^{m-1}\beta_k)^l, \qquad k = 1, \ldots, l-1.$$

Но равенство главных дивизоров равносильно равенству соответствующих чисел с точностью до множителя, являющегося единицей. Следовательно,

$$(x+\zeta^k y)\lambda^{l(m-1)}\beta_k^l = (x+y)\varepsilon_k\alpha_k^l, \tag{9}$$

где ε_k — некоторая единица кольца D_l. Это равенство нам понадобится только при $k = 1, 2$.

Лемма 5. *В кольце D_l существуют такие числа x_1, β, z_1, не делящиеся на λ (а значит, отличные от нуля), и такие единицы ε_0 и ε, что*

$$x_1^l + \varepsilon_0\beta^l = \varepsilon\lambda^{l(m-1)}z_1^l. \tag{10}$$

Доказательство. Покажем, что равенство (10) имеет место при

$$x_1 = \alpha_1\beta_2, \quad \beta = \alpha_2\beta_1, \quad z_1 = \beta_1\beta_2,$$

$$\varepsilon_0 = \frac{\varepsilon_2}{\varepsilon_1(1+\zeta)}, \quad \varepsilon = \frac{\zeta}{\varepsilon_1(1+\zeta)}$$

(ясно, что число $1+\zeta$ является единицей).

Так как

$$(x+\zeta y)(1+\zeta) - (x+\zeta^2 y) = (x+y)\zeta,$$

то, умножив это равенство на $\lambda^{l(m-1)}$ и воспользовавшись соотношением (9) при $k = 1, 2$, мы получим, что

$$(x+y)\left(\frac{\alpha_1}{\beta_1}\right)^l \varepsilon_1(1+\zeta) - (x+y)\left(\frac{\alpha_2}{\beta_2}\right)^l \varepsilon_2 = (x+y)\zeta\lambda^{l(m-1)}.$$

Сократив это равенство на $x+y$ и умножив на $(\beta_1\beta_2)^l\varepsilon_1^{-1}(1+\zeta)^{-1}$, мы и получим (10). ■

Теперь мы уже без особого труда можем прийти к противоречию.

Как мы знаем, для числа x_1 существует такое целое рациональное число b_0 (не делящееся на λ, а значит, и на l), что число $x_1 - b_0$ делится на λ. Но тогда число $(x_1 - b_0)^l$ делится на λ^l и потому делится на $l \sim \lambda^{l-1}$. Так как, с другой стороны,

$$(x_1 - b_0)^l \equiv x_1^l - b_0^l \bmod l,$$

этим доказано, что

$$x_1^l \equiv a \bmod l,$$

где $a = b_0^l$.

Аналогично показывается, что существует такое целое рациональное число b, не делящееся на λ, что

$$\beta^l \equiv b \bmod l.$$

С другой стороны, так как $l(m-1) \geqslant l > l-1$ (см. лемму 1), то правая часть соотношения (10) делится на $l \sim \lambda^{l-1}$. Следовательно, на l делится и левая часть. Другими словами,

$$a + \varepsilon_0 b \equiv 0 \bmod l.$$

Но, поскольку b не делится на l, существует такое целое число b', что $bb' \equiv 1 \bmod l$. Поэтому

$$\varepsilon_0 \equiv b'b\varepsilon_0 \equiv -b'a \bmod l.$$

Этим доказано, что единица ε_0 удовлетворяет условиям леммы Куммера из § 6. Следовательно, она является l-й степенью некоторой другой единицы η:

$$\varepsilon_0 = \eta^l.$$

Таким образом, в кольце D_l существуют такие (отличные от нуля) числа x_1, $y_1 = \eta\beta$ и z_1, не делящиеся на λ, и такая единица ε, что

$$x_1^l + y_1^l = \varepsilon\lambda^{l(m-1)} z_1^l.$$

Мы видим, что, отправляясь от равенства (2) с показателем m, мы пришли к такому же равенству с меньшим показателем $m-1$. Поскольку это невозможно (показатель m был выбран наименьшим возможным), тем самым доказано, что равенство (2) невозможно. ■

Резюмируя, мы видим, чт теорема Ферма нами доказана для всех регулярных простых показателей:

Теорема. *Если простое число* $l \geqslant 3$ *регулярно, то ни для каких отличных от нуля целых рациональных чисел* x, y, z *равенство*

$$x^l + y^l = z^l$$

невозможно.

Теперь нам остается только исследовать, какие простые числа регулярны, а какие нет, т. е. исследовать объем понятия регулярного простого числа.

Оказывается, что в наше определение регулярного простого числа входят требования, которые выполнены для любого простого l и которые, следовательно, можно исключить. Именно, оказывается, что *каждое кольцо* D_l *допускает теорию дивизоров, в которой выполнена аксиома* 4 *из* § 8.

Это утверждение является частным случаем общей теоремы, относящейся к кольцам целых элементов произвольного поля алгебраических чисел (см. конец § 11). Впервые эта общая теорема была доказана Дедекиндом (тогда как утверждение о кольце D_l — Куммером) и впоследствии неоднократно передоказывалась многими авторами. Мы докажем эту теорему, следуя идеям Дедекинда.

§ 10. Теория идеалов

Пусть D — произвольное кольцо. Непустое подмножество A кольца D называется его *идеалом* (термин предложен Дедекиндом из-за связи с идеальными числами Куммера), если

1) $\alpha \pm \beta \in A$ для любых элементов $\alpha, \beta \in A$;

2) $\alpha\beta \in A$ для любых элементов $\alpha \in A$, $\beta \in D$.

Примером идеала является так называемый *нулевой идеал*, состоящий только из нуля 0 кольца D. В дальнейшем *все идеалы предполагаются ненулевыми.*

Примером ненулевого идеала является само кольцо D.

Этот идеал называется *единичным.* Иногда мы будем его обозначать символом (1).

Последний пример может быть обобщен. Пусть $\alpha \in D$ — произвольный отличный от нуля элемент кольца D. Ясно, что все элементы кольца D, делящиеся на α, составляют идеал. Этот идеал обозначается символом (α) и называется *главным идеалом*, порожденным элементом α. При $\alpha = 1$ (а также при α, являющемся произвольной единицей) мы, очевидно, получаем единичный идеал.

Ясно, что *пересечение любого семейства идеалов также является идеалом*. Поэтому для любого множества $X \subset D$ существует наименьший идеал, содержащий это множество (им является пересечение всех идеалов, содержащих X). Этот идеал обозначается символом (X) и называется идеалом, *порожденным* множеством X.

Легко видеть, что идеал (X) состоит из всех элементов вида $\alpha_1\xi_1 + \ldots + \alpha_n\xi_n$, где $\alpha_1, \ldots, \alpha_n \in D$ и $\xi_1, \ldots, \xi_n \in X$ (докажите!).

Если X состоит из конечного числа элементов $\xi_1, \ldots, \xi_n$, то идеал (X) обозначается символом $(\xi_1, \ldots, \xi_n)$. В частности, при $n = 1$ мы получаем главный идеал (ξ_1).

Кольцо D называется *кольцом главных идеалов*, если в нем любой идеал главный. Поскольку утверждение, что $(\alpha, \beta) = (\delta)$, в точности равносильно тому, что δ является наибольшим общим делителем элементов α, β и имеет вид $\alpha x_0 + \beta y_0$, мы видим, что в случае, когда любой идеал порождается двумя элементами (или хотя бы конечным числом элементов), это понятие кольца главных идеалов совпадает с понятием, введенным в § 4.

В случае, когда кольцо D допускает теорию дивизоров, понятие главного идеала может быть обобщено иным способом. Именно, согласно аксиоме 2 из § 8, для любого дивизора $\mathfrak{a}$ множество $[\mathfrak{a}]$ всех элементов кольца D (включая нуль), делящихся на $\mathfrak{a}$, обладает свойством 1) идеалов. Свойство 2) для него также, очевидно, выполнено. Следовательно, $[\mathfrak{a}]$ является идеалом.

Таким образом, соответствие $\mathfrak{a} \longmapsto [\mathfrak{a}]$ переводит дивизоры в идеалы и обладает, очевидно, тем свойством, что для любого главного дивизора (α) соответствую-

щий идеал $[(\alpha)]$ — это в точности введенный выше главный идеал (α). Это оправдывает обозначение одним и тем же символом главного дивизора и соответствующего главного идеала; при достаточной внимательности это привести к недоразумениям не может.

Согласно аксиоме 3 из § 8, отображение $\mathfrak{a} \longmapsto [\mathfrak{a}]$ моноида дивизоров в множество идеалов инъективно, т. е. различные дивизоры оно переводит в различные идеалы. Это, казалось бы, позволяет отождествить дивизоры с идеалами и, в частности, строить теорию дивизоров, исходя из идеалов. В этом и состоит идея Дедекинда. С его точки зрения, дивизоры и идеалы — это одно и то же.

Однако оказалось, что существуют кольца, допускающие теорию дивизоров, но в которых есть идеалы, не имеющие вида $[\mathfrak{a}]$ (примером является кольцо многочленов от двух переменных и в нем идеал всех многочленов без свободного члена). Таким образом, в этих кольцах «слишком много» идеалов. С другой стороны, имеются кольца, моноид главных идеалов которых не погружается в свободный моноид. В таких кольцах теория дивизоров вообще невозможна.

Поэтому в настоящее время принято строго различать идеалы и дивизоры.

Программа Дедекинда удалась только потому, что в кольцах целых алгебраических чисел идеалы образуют свободный моноид и в этих кольцах нет «лишних» идеалов.

Проводя в жизнь идею Дедекинда, следует, конечно, начать с определения умножения идеалов.

Пусть A и B — два идеала произвольного (пока) кольца D. Рассмотрим множество X всех элементов вида $\alpha\beta$, где $\alpha \in A$, $\beta \in B$. Это множество, вообще говоря, идеалом не является. Мы примем за *произведение* AB идеалов A и B идеал, порожденный множеством X. Согласно сказанному выше, идеал AB состоит из всевозможных элементов вида $\alpha_1\beta_1 + \ldots + \alpha_n\beta_n$, где $\alpha_1, \ldots, \alpha_n \in A$, $\beta_1, \ldots, \beta_n \in B$.

Ясно, что это умножение ассоциативно, коммутативно и обладает единицей (ею служит идеал $(1) = D$). Таким образом, относительно этого умножения

множество $\mathrm{Id}(D)$ *всех* (*ненулевых*) *идеалов кольца* D *является моноидом.*

Легко видеть, что главный идеал, порожденный произведением элементов кольца D, является произведением соответствующих главных идеалов:

$$(\alpha\beta) = (\alpha)(\beta). \tag{1}$$

Это означает, что *отображение* $\alpha \longmapsto (\alpha)$ *моноида* D^* *в моноид* $\mathrm{Id}(D)$ *представляет собой гомоморфизм.*

Если кольцо D допускает теорию дивизоров, то инъективное отображение $\mathfrak{a} \longmapsto [\mathfrak{a}]$ будет обладать тем свойством, что $[\mathfrak{a}][\mathfrak{b}] \subset [\mathfrak{a}\mathfrak{b}]$ для любых дивизоров $\mathfrak{a}$ и $\mathfrak{b}$. Однако утверждать, что оно будет гомоморфизмом моноида $\mathscr{D}$ в моноид $\mathrm{Id}(D)$, т. е. что для любых дивизоров $\mathfrak{a}$ и $\mathfrak{b}$ будет иметь равенство $[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}]$, вообще говоря, нельзя. Это равенство заведомо выполнено только тогда, когда $\mathfrak{a}$ и $\mathfrak{b}$ — главные дивизоры.

Из формулы (1) следует, что если элемент α делит элемент γ, то идеал (α) делит идеал (γ). Обратное также верно: *если* (α) *делит* (γ), *то* α *делит* γ. Действительно, ясно, что любой идеал вида $(\alpha)B$ состоит из всех элементов вида $\alpha\beta$, где $\beta \in B$. Поэтому, если $(\alpha)B = (\gamma)$, то $\alpha\beta_0 = \gamma$, где $\beta_0 \in B$, т. е. γ делится на α. ■

Таким образом, *для отображения* $\alpha \longmapsto (\alpha)$ *выполнена аксиома* I *теории дивизоров.*

Полезно также иметь в виду, что *если* $(\gamma)A = (\gamma)B$, *то* $A = B$ (возможность сокращения на главный идеал). Действительно, равенство $(\gamma)A = (\gamma)B$ означает, что любой элемент вида $\gamma\alpha$, $\alpha \in A$, имеет вид $\gamma\beta$, $\beta \in B$, и обратно. Сокращая на γ, мы получаем, что любой элемент $\alpha \in A$ лежит в B и обратно. ■

По построению $AB \subset A$. Таким образом, если идеал C делится на идеал A, то $C \subset A$. (Обратите внимание, что делящий идеал «больше» делимого идеала.)

Обратное, во всяком случае, верно, когда идеал A главный, т. е. *если* $C \subset (\alpha)$, *то существует такой идеал* B, *что* $C = (\alpha)B$. Действительно, включение $C \subset (\alpha)$ означает, что любой элемент $\gamma \in C$ имеет вид $\alpha\beta$, где $\beta \in D$. Пусть B — множество всех таких элементов $\beta \in D$, что $\alpha\beta \in C$. Непосредственно проверяется, что B — идеал и что $(\alpha)B = C$. ■

Чтобы пойти дальше, необходимо наложить на D определенные условия. Мы не будем пытаться искать минимально необходимые условия, а наложим на D условия, позволяющие наиболее быстро прийти к цели, и вместе с тем не исключающие колец D_l, которые, собственно говоря, нам только и нужны.

В первую очередь мы потребуем, чтобы в D существовало n таких элементов

$$\omega_1, \omega_2, \ldots, \omega_n$$

(где n — некоторое натуральное число), что любой элемент $\alpha \in D$ однозначно представляется в виде

$$\alpha = a_1\omega_1 + a_2\omega_2 + \ldots + a_n\omega_n, \tag{2}$$

где $a_1, a_2, \ldots, a_n$ — целые рациональные числа. На языке теории групп это свойство означает, что аддитивная группа кольца D является *решеткой* (свободной абелевой группой) *ранга n с базисом* $\omega_1, \omega_2, \ldots, \omega_n$. Кольцо D_l обладает этим свойством при $n = l - 1$, и $\omega_1 = 1$, $\omega_2 = \zeta, \ldots, \omega_n = \zeta^{l-2}$.

В теории групп доказывается, что *любая подгруппа A решетки D ранга n является решеткой ранга* $r \leqslant n$.

Изложим для полноты доказательство этого утверждения. Пусть A_k, $k = 1, \ldots, n+1$, — подгруппа группы A, состоящая из элементов (2), для которых $a_1 = \ldots = a_{k-1} = 0$. (Таким образом, $A_1 = A$ и $A_{n+1} = 0$.) Ясно, что для любого $k = 1, \ldots, n$ множество всех коэффициентов a_k элементов из A_k составляет идеал (возможно, нулевой) в кольце целых чисел Z. Но в этом кольце все идеалы главные (ибо имеет место алгоритм деления с остатком), и поэтому существует коэффициент $a_k^{(0)}$, порождающий этот идеал (случай $a_k^{(0)} = 0$ здесь не исключается). Пусть ξ_k — произвольный элемент группы A_k с этим коэффициентом (если $a_k^{(0)} = 0$, то мы положим $\xi_k = 0$).

Покажем, что элементы $\xi_1, \ldots, \xi_n$ порождают группу A, т. е. что любой элемент $\alpha \in A$ имеет вид

$$\alpha = b_1\xi_1 + \ldots + b_n\xi_n, \tag{3}$$

где $b_1, \ldots, b_n$ — целые рациональные числа.

Поскольку $A_{n+1} = 0$, то для элементов из A_{n+1} формула (3) имеет место. Рассуждая по индукции, предположим, что для некоторого $k \leqslant n$ уже доказано, что любой элемент из A_{k+1} имеет вид (3) (с $b_1 = \ldots = b_k = 0$), и покажем, что тогда любой элемент $\alpha \in A_k$ также имеет вид (3) (с $b_1 = \ldots = b_{k-1} = 0$). Ясно, что этим все будет доказано.

Пусть

$$\alpha = a_k\omega_k + \ldots + a_n\omega_n.$$

По построению коэффициент a_k делится на $a_k^{(0)}$ (если $a_k^{(0)} = 0$, то $a_k = 0$ для всех элементов $\alpha \in A_k$), т. е. существует такое целое число b_k, что $a_k = a_k^{(0)} b_k$. Тогда $\alpha - b_k\xi_k \in A_{k+1}$ и потому $\alpha - b_k\xi_k = b_{k+1}\xi_{k+1} + \ldots + b_n\xi_n$. Следовательно, $\alpha = b_k\xi_k + b_{k+1}\xi_{k+1} + \ldots + b_n\xi_n$.

Вообще говоря, среди элементов $\xi_1, \ldots, \xi_n$ могут быть равные нулю. Перенумеровав (если нужно) эти элементы, мы можем считать, что $\xi_1 \neq 0, \ldots, \xi_r \neq 0$ и $\xi_{r+1} = 0, \ldots, \xi_n = 0$. Соответствующим образом перенумеровав элементы базиса $\omega_1, \ldots, \omega_n$, мы при этом можем считать, что для любого $k = 1, \ldots, n$ по-прежнему $\xi_k \in A_k$, т. е. что в выражении элемента ξ_k через базис $\omega_1, \ldots, \omega_n$ коэффициенты при $\omega_1, \ldots, \omega_{k-1}$ равны нулю. Но теперь, кроме того, мы можем утверждать, что при $k = 1, \ldots, r$ коэффициент $a_k^{(0)}$ элемента ξ_k отличен от нуля, ибо, по построению, $a_k^{(0)} = 0$ только при $\xi_k = 0$.

Отсюда следует, что *элементы* $\xi_1, \ldots, \xi_r$ *независимы*, т. е. равенство $a_1\xi_1 + \ldots + a_r\xi_r = 0$, где $a_1, \ldots, a_r$ — целые рациональные числа, имеет место только при $a_1 = 0, \ldots, a_r = 0$. Действительно, в противном случае будет существовать отличное от нуля число a_i с наименьшим i, и тогда в разложении элемента $a_1\xi_1 + \ldots + a_r\xi_r = 0$ по базису $\omega_1, \ldots, \omega_n$ коэффициентом при ω_i будет отличное от нуля число $a_i a_i^{(0)}$, что невозможно.

Этим доказано, что любой элемент $\alpha \in A$ однозначно выражается через $\xi_1, \ldots, \xi_r$, т. е. что A является решеткой с базисом $\xi_1, \ldots, \xi_r$ (и, следовательно, ранга r). ■

Далее, известно, что *ранг n решетки не зависит от выбора базиса и равен максимальному числу независимых элементов решетки.*

Действительно, элементы базиса по определению независимы, а любые $n + 1$ элементов зависимы (ибо любая система n однородных линейных уравнений с $n + 1$ неизвестными с целыми коэффициентами имеет нетривиальное решение, состоящее из целых чисел).

Заметим, что, в отличие от классического случая линейных пространств, *не любые n* независимых элементов решетки составляют ее базис. Для этого необходимо и достаточно, чтобы определитель, составленный из коэффициентов разложений этих элементов по элементам базиса, был равен ± 1 (см. приложение к этому параграфу).

Кроме того, из теории групп известно также, что *для любой подрешетки A ранга n факторгруппа D/A конечна.*

Действительно, при $r = n$ мы имеем в A базис $\xi_1, \ldots, \xi_n$ вида

$$\begin{aligned}
\xi_1 &= a_1^{(0)}\omega_1 + a_1^{(1)}\omega_2 + \ldots + a_1^{(n-1)}\omega_n,\\
\xi_2 &= \qquad a_2^{(0)}\omega_2 + \ldots + a_2^{(n-2)}\omega_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
\xi_n &= \qquad\qquad\qquad\quad a_n^{(0)}\omega_n,
\end{aligned}$$

где $a_1^{(0)} \neq 0, \ldots, a_n^{(0)} \neq 0$, откуда непосредственно следует, что элементы вида

$$a_1\omega_1 + a_2\omega_2 + \ldots + a_n\omega_n,$$

где

$$0 \leqslant a_1 < \left| a_1^{(0)} \right|,\ 0 \leqslant a_2 < \left| a_2^{(0)} \right|, \ldots,\ 0 \leqslant a_n < \left| a_n^{(0)} \right|,$$

составляют полную систему смежных классов группы D по подгруппе A. Следовательно, D/A *является конечной группой порядка* $\left| a_1^{(0)} a_2^{(0)} \ldots a_n^{(0)} \right|$.

Отсюда следует, что *существует только конечное число подгрупп группы D, содержащих подгруппу A.*

Действительно, при естественном гомоморфизме $D \to D/A$ такие подгруппы взаимно однозначно соответствуют всевозможным подгруппам группы D/A, а этих подгрупп конечное число.

Все эти утверждения применимы к произвольному идеалу A кольца D, поскольку, по определению, идеал является, в частности, подгруппой аддитивной группы кольца. Таким образом, во-первых, мы видим, что *любой идеал A является решеткой.*

Во-вторых, так как для любого элемента $\alpha \in A$ элементы $\alpha\omega_1, \ldots, \alpha\omega_n$ идеала A, очевидно, независимы, то *ранг любого идеала кольца D* (рассматриваемого как решетка) *равен n*, т. е. идеал A обладает базисом из n элементов.

Эти элементы, очевидно, порождают идеал A, так что *любой идеал A кольца D порождается конечным числом элементов*, т. е. имеет вид $A = (\alpha_1, \ldots, \alpha_m)$, где $\alpha_1, \ldots, \alpha_m \in D$ (вообще говоря, число m может быть и меньше ранга n).

В-третьих, мы видим, что, поскольку любой делитель идеала A является подгруппой, содержащей A, *для любого идеала кольца D существует только конечное число различных содержащих его идеалов и, в частности, только конечное число различных дели-*

телей. Очевидной индукцией отсюда немедленно вытекает, что *любой идеал кольца D разлагается в произведение простых идеалов* (далее неразложимых).

Кроме того, мы можем теперь доказать, что в некоторых случаях сокращение равенств идеалов возможно и на не главный идеал. Для этого нам потребуется следующая лемма (в которой под «числами» можно понимать элементы произвольного кольца):

Лемма 1. *Пусть*

$$\left\| \begin{matrix} \beta_{11} & \dots & \beta_{1n} \\ \dots & \dots & \dots \\ \beta_{n1} & \dots & \beta_{nn} \end{matrix} \right\| \tag{4}$$

—произвольная матрица и ρ *— некоторое число. Если существуют такие числа* $\xi_1, \dots, \xi_n$, *хотя бы одно из которых отлично от нуля, что имеют место равенства*

$$\begin{aligned} \rho\xi_1 &= \beta_{11}\xi_1 + \dots + \beta_{1n}\xi_n, \\ &\dots\dots\dots\dots \\ \rho\xi_n &= \beta_{n1}\xi_1 + \dots + \beta_{nn}\xi_n, \end{aligned} \tag{5}$$

то число ρ *является корнем уравнения*

$$x^n + \beta_1 x^{n-1} + \dots + \beta_n = 0, \tag{6}$$

коэффициенты $\beta_1, \dots, \beta_n$ *которого выражаются через элементы матрицы* (4) *посредством действий сложения, вычитания и умножения.*

С помощью этой леммы легко доказывается, что *для любых идеалов A и B из равенства*

$$AB = A$$

следует, что $B = (1)$.

Действительно, пусть $\xi_1, \dots, \xi_n$ — базис идеала A. Тогда любой элемент идеала AB может быть, как легко видеть, представлен в виде $\xi_1\beta_1 + \dots + \xi_n\beta_n$, где $\beta_1, \dots, \beta_n \in B$. Поскольку $AB = B$, отсюда следует, что для $\xi_1, \dots, \xi_n$ имеют место равенства вида

$$\begin{aligned} \xi_1 &= \xi_1\beta_{11} + \dots + \xi_n\beta_{1n}, \\ &\dots\dots\dots\dots \\ \xi_n &= \xi_1\beta_{n1} + \dots + \xi_n\beta_{nn}, \end{aligned} \qquad \beta_{ij} \in B,$$

т. е. равенства (4) с $\rho = 1$. Поэтому число $\rho = 1$ является корнем уравнения вида (6), т. е., другими словами, имеет место равенство $1 = -\beta_1 - \dots - \beta_n$,

где $\beta_1, \ldots, \beta_n$ выражаются через элементы β_{ij} идеала B посредством действий сложения, вычитания и умножения и, следовательно, принадлежат этому идеалу. Но тогда и $1 \in B$, т. е. $B = (1)$. ■

Сама же лемма 1 непосредственно вытекает из простейших фактов линейной алгебры. Действительно, равенства (5) означают, что $(\xi_1, \ldots, \xi_n) \neq (0, \ldots 0)$ является решением системы линейных однородных уравнений

$$(\beta_{11} - \rho)\,\xi_1 + \ldots + \beta_{1n}\xi_n = 0,$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$\beta_{n1}\xi_1 + \ldots + (\beta_{nn} - \rho)\,\xi_n = 0.$$

Но из линейной алгебры известно, что если система n линейных однородных уравнений от n неизвестных имеет решение $\neq (0, \ldots, 0)$, то ее определитель равен нулю.

Следовательно,

$$\begin{vmatrix} \beta_{11} - \rho & \ldots & \beta_{1n} \\ \ldots\ldots\ldots & & \\ \beta_{n1} & \ldots & \beta_{nn} - \rho \end{vmatrix} = 0.$$

Раскрыв этот определитель, мы и получим для ρ уравнение вида (6). ■

Чтобы пойти дальше, мы еще больше сузим класс рассматриваемых колец. Именно, мы потребуем, чтобы для кольца D существовало n его инъективных отображений $\alpha \longmapsto \alpha^{(i)}$, $i = 1, \ldots, n$, в поле комплексных чисел $\mathbb{C}$, сохраняющих сложение и умножение (т. е. являющихся *мономорфизмами*) и таких, что для любого $\alpha \in D$ элементарные симметрические многочлены от $\alpha^{(1)}, \ldots, \alpha^{(n)}$ являются целыми рациональными числами (иными словами, требуется, чтобы многочлен $(x - \alpha^{(1)}) \ldots (x - \alpha^{(n)})$ имел целые коэффициенты).

Для кольца D_l такие отображения были построены в § 5.

Для произвольного D мы введем *норму* $N\alpha$ элемента $\alpha \in D$ формулой

$$N\alpha = \alpha^{(1)} \ldots \alpha^{(n)}.$$

Эта норма является целым рациональным числом, но, вообще говоря, уже не обязательно неотрицательным (хотя по-прежнему $N\alpha = 0$ тогда и только тогда, когда $\alpha = 0$). Как и в случае кольца D_l, для любых элементов $\alpha, \beta \in D$ имеет место равенство

$$N(\alpha\beta) = N\alpha \cdot N\beta$$

(ибо, по условию, $(\alpha\beta)^{(i)}=\alpha^{(i)}\beta^{(i)}$ для любого $i=1, \ldots, n$). Кроме того,

$$Na=a^n$$

для любого рационального a.

Удобно (хотя совсем необязательно) «вложить» кольцо D в поле $\mathbb{C}$ посредством отображения $\alpha \longmapsto \alpha^{(1)}$, т. е. считать, что $D \subset \mathbb{C}$ и $\alpha^{(1)}=\alpha$ для любого $\alpha \in D$. (Заметим, что в случае кольца D_l дело обстоит именно так.)

Считая кольцо D вложенным в поле $\mathbb{C}$, мы можем определить *поле отношений* K кольца D просто как наименьшее подполе поля $\mathbb{C}$, содержащее кольцо D, или, иначе, как множество всех чисел из $\mathbb{C}$ вида $\frac{\beta}{\alpha}$, где $\alpha, \beta \in D$ и $\alpha \neq 0$, избегая, тем самым, простой, но несколько кропотливой абстрактной процедуры построения этого поля для кольца D, не вложенного в $\mathbb{C}$.

В случае кольца D_l для любого $i=1, \ldots, n$, где $n=l-1$, было выполнено включение $\alpha^{(i)} \in D$. Теперь это, вообще говоря, не так. Однако легко видеть, что $\alpha^{(2)} \ldots \alpha^{(n)} \in D$ для любого $\alpha \in D$, т. е. что $N\alpha$ *делится на* α *в* D. Действительно, по условию число $\alpha=\alpha^{(1)}$ удовлетворяет уравнению вида

$$\alpha^n+c_1\alpha^{n-1}+ \ldots +c_{n-1}\alpha+c_n=0$$

с целыми коэффициентами, причем $N\alpha=(-1)^n c_n$. Поэтому

$$\frac{N\alpha}{\alpha}=\frac{(-1)^n c_n}{\alpha}=(-1)^{n+1}\frac{\alpha^n+c_1\alpha^{n-1}+ \ldots +c_{n-1}\alpha}{\alpha}=$$

$$=(-1)^{n+1}(\alpha^{n-1}+c_1\alpha^{n-2}+ \ldots +c_{n-1}) \in D. \blacksquare$$

Известным уже нам рассуждением (см. § 5) отсюда выводится, что любой элемент $\xi=\frac{\beta}{\alpha}$ поля K может быть (очевидно, единственным образом) записан в виде

$$\xi=x_1\omega_1+ \ldots +x_n\omega_n, \tag{7}$$

где $x_1, \ldots, x_n$ — рациональные числа (и, конечно, каждое число ξ такого вида лежит в K).

Лемма 2. *Существует такое натуральное число* $T = T(D)$, *зависящее только от кольца* D, *что для каждого элемента* $\xi \in K$ *найдется такой элемент* $\alpha \in D$ *и такое натуральное число* $s < T$, *что*

$$N(s\xi - \alpha) < 1.$$

Доказательство. Выбрав в D базис $\omega_1, \ldots, \omega_n$, мы примем за T произвольное натуральное число, удовлетворяющее неравенствам

$$T > Q^n > \prod_{i=1}^{n} (|\omega_1^{(i)}| + \ldots + |\omega_n^{(i)}|),$$

где Q — некоторое натуральное число.

Ясно, что для любого элемента (7) поля K и любого натурального i можно подобрать такой элемент $\alpha_i \in D$, что для элемента

$$i\xi - \alpha_i = y_1\omega_1 + \ldots + y_n\omega_n \tag{8}$$

будут выполнены неравенства

$$0 \leqslant |y_1| < 1, \ldots, 0 \leqslant |y_n| < 1.$$

Разобьем полуинтервал $[0, 1)$ на Q полуинтервалов вида

$$\left[\frac{j}{Q}, \frac{j+1}{Q}\right), \quad j = 0, \ldots, Q-1. \tag{9}$$

Каждая координата $y_1, \ldots, y_n$ числа (8) лежит в одном из этих интервалов. Поэтому существует всего Q^n возможностей распределения этих координат по полуинтервалам (9). Следовательно, если мы рассмотрим числа (8) для всех i от 0 до Q^n (т. е. всего $Q^n + 1$ чисел), то по крайней мере два числа будут давать одну и ту же комбинацию распределения координат по полуинтервалам (9). Разность этих чисел имеет вид $s\xi - \alpha$, где $s \in \mathbb{N}$, а $\alpha \in D_l$, а ее координаты удовлетворяют неравенствам

$$|y_1| < \frac{1}{Q}, \ldots, |y_n| < \frac{1}{Q}.$$

Поэтому

$$|(s\xi - \alpha)^{(i)}| < \frac{1}{Q}(|\omega_1^{(i)}| + \ldots + |\omega_n^{(i)}|), \quad i = 1, \ldots, n,$$

и, значит,

$$|N(s\xi-\alpha)|<\frac{1}{Q^n}\prod_{i=1}^{n}(|\omega_1^{(i)}|+\ldots+\widehat{|\omega_n^{(i)}|})<1.$$

Для завершения доказательства остается заметить, что натуральное число s, являясь разностью двух натуральных чисел, не превосходящих Q^n, также не превосходит Q^n и, следовательно, меньше T. ■

По аналогии с дивизорами назовем два идеала A и B *эквивалентными*, если существуют такие главные идеалы (α) и (β), что

$$(\alpha)A=(\beta)B.$$

Ясно, что множество всех идеалов распадается на классы эквивалентных идеалов.

Предложение 1. *Для любого кольца D, удовлетворяющего перечисленным выше условиям, число классов идеалов конечно.*

Доказательство. Пусть A — произвольный идеал.

Среди отличных от нуля чисел идеала A существует число α_0, для которого натуральное число $|N\alpha_0|$ имеет наименьшее возможное значение, так что

$$|N\alpha_0|\leqslant|N\alpha|$$

для любого отличного от нуля элемента $\alpha\in A$.

Пусть $\alpha\in A$. Применив лемму 2 к элементу

$$\xi=\frac{\alpha}{\alpha_0}\in K,$$

мы найдем натуральное число $s<T$ и элемент $\gamma\in D$, удовлетворяющие соотношению

$$\left|N\left(s\frac{\alpha}{\alpha_0}-\gamma\right)\right|<1,$$

т. е. соотношению

$$|N(s\alpha-\gamma\alpha_0)|<|N\alpha_0|.$$

Поскольку $s\alpha-\gamma\alpha_0\in A$, это неравенство возможно только при $s\alpha=\gamma\alpha_0$. Этим доказано, что α_0 делит элемент $s\alpha$, а значит, и элемент $S\alpha$, где $S=T!$.

Таким образом, для любого элемента $\alpha \in A$ существует такой элемент $\beta \in D$, что

$$\alpha_0 \beta = S\alpha. \tag{10}$$

Пусть B — множество всех таких β (при всевозможных $\alpha \in A$). Ясно, что если $\beta_1, \beta_2 \in B$, то $\beta_1 \pm \beta_2 \in B$ (если $\alpha_0 \beta_1 = S\alpha_1$ и $\alpha_0 \beta_2 = S\alpha_2$, где $\alpha_1, \alpha_2 \in A$, то $\alpha_0 (\beta_1 \pm \beta_2) = S(\alpha_1 \pm \alpha_2)$, где $\alpha_1 \pm \alpha_2 \in A$). Кроме того, если $\alpha_0 \beta = S\alpha$, то $\alpha_0 (\beta\gamma) = S(\alpha\gamma)$ для любого $\gamma \in D$, и, следовательно, $\beta\gamma \in B$ (ибо $\alpha\gamma \in A$). Этим доказано, что B представляет собой идеал.

Равенство (10) означает теперь, что

$$(\alpha_0) B = (S) A,$$

т. е. что идеал B эквивалентен идеалу A.

Кроме того, так как $\alpha_0 \in A$, то $(S)(\alpha_0) \subset (\alpha_0) B$, т. е. $(S) \subset B$.

Но мы уже знаем, что число идеалов, содержащих данный фиксированный идеал (в нашем случае — идеал (S)), конечно. Таким образом, каждый идеал A эквивалентен идеалу B, принадлежащему некоторому конечному множеству идеалов.

Следовательно, число классов идеалов конечно. ■

Пусть снова A — произвольный (ненулевой) идеал кольца D. Попробуем доказать, что некоторая его степень A^m, $m \geqslant 0$, является главным идеалом.

Так как число неэквивалентных идеалов конечно, должны существовать такие два числа $p > 0$ и $q > 0$, что $A^p \sim A^{p+q}$. По определению, это означает, что существуют такие элементы $\alpha, \beta \in D^*$, что

$$(\alpha) A^p = (\beta) A^{p+q}. \tag{11}$$

Пусть $\xi_1, \ldots, \xi_n$ — базис идеала A^p. Тогда любой элемент идеала $A^{p+q} \subset A^p$ может быть представлен в виде $a_1\xi_1 + \ldots + a_n\xi_n$, где $a_1, \ldots, a_n$ — целые рациональные числа, а значит, любой элемент идеала $(\beta) A^{p+q}$ — в виде $\beta(a_1\xi_1 + \ldots + a_n\xi_n)$. В частности, такое представление будут иметь элементы $\alpha\xi_1, \ldots, \alpha\xi_n \in (\alpha) A^p = (\beta) A^{p+q}$. Таким образом, полагая

$$\rho = \frac{\alpha}{\beta} \in K,$$

мы видим, что справедливы равенства вида

$$\rho\xi_1 = a_{11}\xi_1 + \ldots + a_{1n}\xi_n,$$
$$\ldots\ldots\ldots\ldots$$
$$\rho\xi_n = a_{n1}\xi_1 + \ldots + a_{nn}\xi_n,$$

где a_{ij}, $i, j = 1, \ldots, n$, — целые рациональные числа. Применив к этим равенствам лемму 1, мы получим, что число ρ является корнем некоторого алгебраического уравнения n-й степени

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0 \tag{12}$$

с целыми коэффициентами $a_1, \ldots, a_n$ и равным единице старшим коэффициентом.

Назовем кольцо D *целозамкнутым*, если любой элемент ρ его поля отношений K, удовлетворяющий уравнению вида (12), принадлежит D.

Таким образом, если D целозамкнуто, то $\rho = \frac{\alpha}{\beta} \in D$, т. е. β делит α.

Поэтому равенство (11) мы можем сократить на β и записать в следующем виде:

$$(\rho)\, A^p = A^{p+q}.$$

Пусть теперь $\gamma_1, \ldots, \gamma_n$ — базис идеала A^q. Так как $\gamma_i\xi_j \in A^{p+q} = (\rho) A^p$, где $i, j = 1, \ldots, n$, то при любом $i = 1, \ldots, n$ для числа

$$\rho_i = \frac{\gamma_i}{\rho}$$

имеют место равенства вида

$$\rho_i\xi_1 = a_{11}^{(i)}\xi_1 + \ldots + a_{1n}^{(i)}\xi_n,$$
$$\ldots\ldots\ldots\ldots$$
$$\rho_i\xi_n = a_{n1}^{(i)}\xi_1 + \ldots + a_{nn}^{(i)}\xi_n,$$

откуда, как и выше, следует, что ρ_i является корнем некоторого уравнения вида (12) и, значит (в силу целозамкнутости кольца D), лежит в D. Это означает, что γ_i делится на ρ.

Следовательно, на ρ делятся все числа идеала A^q. Сокращая их на ρ, мы, очевидно, получим некоторый новый идеал B (с базисом $\rho_1, \ldots, \rho_n$). По построению,

$(\rho)B = A^q$ и, значит,

$$(\rho)A^p = (\rho)A^pB.$$

Но мы знаем, что в моноиде идеалов возможно сокращение равенств на главный идеал. Следовательно,

$$A^p = A^pB,$$

откуда, как мы знаем, следует, что $B = (1)$. Поэтому

$$A^q = (\rho).$$

Тем самым нами доказано следующее предложение:

Предложение 2. *Если кольцо D, удовлетворяющее перечисленным выше условиям, кроме того, еще целозамкнуто, то некоторая степень любого идеала является главным идеалом.* ■

Следствие. *Для любого идеала A существует такой идеал A', что произведение AA' является главным идеалом.*

Действительно, достаточно положить $A' = A^{q-1}$.

Отсюда непосредственно вытекает ряд важных выводов.

Например, теперь легко показать, что закон сокращения справедлив для любых идеалов, т. е. *если* $CA = CB$, *то* $A = B$. Действительно, пусть C' — такой идеал, что $C'C = (\gamma)$. Тогда $(\gamma)A = C'(CA) = C'(CB) = (\gamma)B$, и, следовательно, $A = B$. ■

Далее, *если* $C \subset A$, *то* A *делит* C, т. е. существует такой идеал B, что $C = AB$. Действительно, если $C \subset A$, то $CA' \subset AA'$ для любого идеала A'. Если, в частности, идеал AA' главный, то, как мы выше уже доказали, существует такой идеал B, что $CA' = AA'B$. Сокращая на A', мы и получим, что $C = AB$. ■

В частности, отсюда следует, что *любой простой идеал P максимален*, т. е. если $A \supset P$, то $A = (1)$.

Наконец, легко видеть, что *элемент $\alpha \in D$ тогда и только тогда делится на идеал A* (т. е. на A делится идеал (α)), *когда* $\alpha \in A$. Действительно, если (α) делится на A, то $(\alpha) \subset A$ и потому $\alpha \in A$. Обратно, если $\alpha \in A$, то $(\alpha) \subset A$ и, следовательно, по доказанному, (α) делится на A. ■

Последнее утверждение в точности означает, что для моноида идеалов (с отображением $\alpha \longmapsto (\alpha)$) выполнена аксиома 3 теории дивизоров (см. § 8). Аксиома 2 также, очевидно, выполнена (если α и β делятся на A, то $\alpha \in A$, $\beta \in A$ и потому $\alpha \pm \beta \in A$, т. е. $\alpha \pm \beta$ делится на A). Выполнение аксиомы 1 мы выше уже отмечали.

Таким образом, для того чтобы показать, что моноид идеалов $\mathrm{Id}(D)$ вместе с отображением $\alpha \longmapsto (\alpha)$ составляет теорию дивизоров для кольца D, осталось лишь показать, что этот моноид свободен, т. е. что разложение любого идеала в произведение простых идеалов единственно (с точностью до порядка множителей).

Но это теперь также совсем просто.

Сначала докажем, что *для любых двух идеалов A и B существует их наибольший общий делитель*, т. е. идеал, который делит A и B и который делится на любой идеал, делящий идеалы A и B. Легко видеть, что таким идеалом будет идеал $(A \cup B)$, порожденный теоретико-множественным объединением идеалов A и B. Действительно, ясно, что $A \subset (A \cup B)$ и $B \subset (A \cup B)$, т. е. $(A \cup B)$ делит A и B. Если же C делит A и B, т. е. $C \supset A$ и $C \supset B$, то $C \supset A \cup B$ и потому $C \supset (A \cup B)$, т. е. C делит $(A \cup B)$.

Мы будем идеал $(A \cup B)$ обозначать символом (A, B).

Эта конструкция показывает, в частности, что *любой идеал $A = (\alpha_1, \ldots, \alpha_k)$ является наибольшим общим делителем главных идеалов* $(\alpha_1), \ldots, (\alpha_k)$.

Легко видеть, далее, что *для любых трех идеалов A, B и C справедливо равенство*

$$(A, B)C = (AC, BC)$$

(дистрибутивность наибольшего общего делителя по отношению к умножению).

Теперь мы уже можем непосредственно доказать однозначность разложения идеалов в произведение простых идеалов. Для этого, очевидно, достаточно доказать, что *если простой идеал P делит произведение AB, но не делит идеал A, то он делит идеал B* (ср. со свойством (*) в § 4). Но если P не делит A, то $(A, P) \neq P$ и потому $(A, P) = (1)$ (ибо P — про-

стой, а значит, максимальный идеал). Следовательно,

$$B = (1)B = (A, P)B = (AB, PB),$$

и так как P делит AB и PB, то P делит B. ■

Таким образом, нами доказано, что в кольце D идеалы (ненулевые) обладают всеми свойствами, которые мы требуем от дивизоров. Это означает, что справедлива следующая теорема:

Теорема 1. *Если*

а) *аддитивная группа кольца D является решеткой конечного ранга n;*

б) *существуют n мономорфизмов $\alpha \mapsto \alpha^{(i)}$, $i = 1, \ldots, n$, кольца D в поле $\mathbb{C}$, обладающих тем свойством, что для любого $\alpha \in D$ все элементарные симметрические многочлены от $\alpha^{(1)}, \ldots, \alpha^{(n)}$ являются целыми рациональными числами;*

в) *кольцо D целозамкнуто,*

то это кольцо допускает теорию дивизоров.

В этой теории дивизорами являются ненулевые идеалы кольца D, а соответствие $\alpha \mapsto (\alpha)$ относит каждому элементу $\alpha \in D^*$ порожденный им главный идеал.

При этом моноид классов дивизоров (идеалов) является конечной (абелевой) группой.

Последнее утверждение является простой переформулировкой предложения 1 и следствия из предложения 2. Оно означает, что идеалы кольца D удовлетворяют не только аксиомам 1—3 из § 8, но также и аксиоме 4 (усиленной требованием конечности группы $\mathcal{H}$ классов дивизоров).

Так как кольцо D_l тривиальным образом обладает свойствами а) и б), то, если мы докажем, что оно обладает и свойством в), от требований, которые мы в § 8 наложили на регулярные простые числа, останется только аксиома 5. При этом, пользуясь конечностью группы $\mathcal{H}$, мы эту аксиому сможем сформулировать в ослабленной форме, требуя лишь, чтобы число l не делило порядка h группы $\mathcal{H}$. Все это, конечно, будет большим сдвигом в направлении эффективной характеризации регулярных простых чисел.

Мы докажем целозамкнутость кольца D в следующем параграфе, а пока лишь заметим, что условие в) целозамкнутости отличается от условий а) и б) (вообще говоря, не необходимых для существования в кольце D теории дивизоров) тем, что оно абсолютно необходимо. Другими словами, *в нецелозамкнутом кольце D теории дивизоров существовать не может.*

Действительно, если элемент $\xi = \frac{\beta}{\alpha}$ поля отношений K кольца D, обладающего теорией дивизоров, не лежит в D, то существует простой дивизор $\mathfrak{p}$, делящий α в большей степени, чем β, т. е. такой, что если β делится на $\mathfrak{p}^k$ и не делится на $\mathfrak{p}^{k+1}$, то α делится на $\mathfrak{p}^{k+1}$. Поэтому, если $\xi^n + a_1\xi^{n-1} + \ldots + a_n = 0$, где $a_1, \ldots, a_n$ — целые числа, т. е. если

$$\beta^n = -a_1\beta^{n-1}\alpha - \ldots - a_n\alpha^n,$$

то β^n делится на $\mathfrak{p}^{kn+1}$ (ибо $kn + 1 \leqslant (n-s)k + s(k+1)$ для любого $s = 1, \ldots, n$) и потому на $\mathfrak{p}^{kn+1}$ делится каждый одночлен вида $\beta^{n-s}\alpha^s$. Следовательно, β делится на $\mathfrak{p}^i$, где $i > k + \frac{1}{n}$, т. е., вопреки предположению, делится по крайней мере на $\mathfrak{p}^{k+1}$. ■

Таким образом, единственного условия теоремы 1, которое трудно проверить для кольца D_l, избежать нельзя.

Приложение. Норма идеала

В этом приложении мы установим некоторые дополнительные свойства идеалов в кольцах, удовлетворяющих условиям теоремы § 10. Поскольку, согласно этой теореме, идеалы интерпретируются как дивизоры, мы соответственно этому будем теперь обозначать идеалы строчными готическими буквами.

Под D мы всегда будем понимать произвольное кольцо, удовлетворяющее условиям теоремы § 10. Рассматриваемое как идеал (дивизор), оно обозначается знаком (1) или знаком $\mathfrak{e}$.

Пусть $\mathfrak{a}$ — идеал кольца D и пусть $\alpha, \beta \in D$. Мы будем писать $\alpha \equiv \beta \bmod \mathfrak{a}$ и говорить, что α *сравнимо с* β *по модулю* $\mathfrak{a}$, если элемент $\alpha - \beta$ делится на идеал $\mathfrak{a}$. Эти сравнения обладают всеми стандарт-

ными свойствами равенств (их можно складывать, перемножать и т. д., только сокращение обоих членов сравнения на общий множитель не всегда допустимо; для этого нужно, чтобы этот множитель был взаимно прост с $\mathfrak{a}$).

Следующее предложение известно в элементарной теории чисел как «китайская теорема об остатках»:

Предложение 1. *Для любых попарно взаимно простых идеалов*

$$\mathfrak{a}_1, \ldots, \mathfrak{a}_s \tag{1}$$

и любых элементов

$$\alpha_1, \ldots, \alpha_s$$

кольца D существует такой элемент $\xi \in D$, что

$$\xi \equiv \alpha_1 \bmod \mathfrak{a}_1,$$
$$\ldots\ldots$$
$$\xi \equiv \alpha_s \bmod \mathfrak{a}_s.$$

Доказательство. Пусть $\mathfrak{b}_i$, $i = 1, \ldots, s$, — произведение всех идеалов (1), за исключением идеала $\mathfrak{a}_i$. Ясно, что идеалы $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_s$ взаимно просты, т. е.

$$(\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_s) = (1). \tag{2}$$

Равенство (2) означает, что существуют такие элементы

$$\beta_1 \in \mathfrak{b}_1, \quad \beta_2 \in \mathfrak{b}_2, \ldots, \beta_s \in \mathfrak{b}_s,$$

что

$$\beta_1 + \beta_2 + \ldots + \beta_s = 1. \tag{3}$$

По построению каждый идеал $\mathfrak{a}_i$, $i = 1, \ldots, s$, делит все идеалы $\mathfrak{b}_j$, $j \neq i$, а, значит, делит все элементы β_j, $j \neq i$. Поэтому из равенства (3) следует, что

$$\beta_i \equiv 1 \bmod \mathfrak{a}_i, \quad i = 1, \ldots, s.$$

Положим

$$\xi = \alpha_1\beta_1 + \ldots + \alpha_s\beta_s.$$

Так как $\beta_j \equiv 0 \bmod \mathfrak{a}_i$ при $j \neq i$, а $\beta_i \equiv 1 \bmod \mathfrak{a}_i$, то

$$\xi \equiv \alpha_i \bmod \mathfrak{a}_i, \quad i = 1, \ldots, n. \blacksquare$$

Предложение 2. *Для любых идеалов* $\mathfrak{a}$ *и* $\mathfrak{b}$ *существует такой элемент* $\gamma \in D$, *что*

$$(\mathfrak{ab},\ \gamma) = \mathfrak{a}.$$

Доказательство. Пусть

$$\mathfrak{ab} = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_s^{k_s}; \quad k_1 \geqslant 1, \dots, k_s \geqslant 1,$$

где $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ — различные простые идеалы. Тогда

$$\mathfrak{a} = \mathfrak{p}_1^{l_1} \dots \mathfrak{p}_s^{l_s},$$

где

$$0 \leqslant l_1 \leqslant k_1, \dots, 0 \leqslant l_s \leqslant k_s.$$

Так как $\mathfrak{p}_i^{l_i+1} \subset \mathfrak{p}_i^{l_i}$ и $\mathfrak{p}_i^{l_i+1} \neq \mathfrak{p}_i^{l_i}$ (если $\mathfrak{p}_i^{l_i+1} = \mathfrak{p}_i^{l_i}$, то, сократив на $\mathfrak{p}_i^{l_i}$, мы получим невозможное равенство $\mathfrak{p}_i = \mathfrak{e}$; при $l_i = 0$ мы, естественно, полагаем $\mathfrak{p}_i^{l_i} = \mathfrak{e}$), то существует такой элемент $\alpha_i \in D$, что $\alpha_i \in \mathfrak{p}_i^{l_i}$ и $\alpha_i \notin \mathfrak{p}_i^{l_i+1}$, т. е. такой, что $\alpha_i \equiv 0 \bmod \mathfrak{p}_i^{l_i}$ и $\alpha_i \not\equiv 0 \bmod \mathfrak{p}_i^{l_i+1}$.

Поэтому элемент $\gamma \in D$, для которого

$$\gamma \equiv \alpha_i \bmod \mathfrak{p}_i^{l_i+1}, \quad i = 1, \dots, s$$

(такой элемент существует в силу предложения 1), будет обладать тем свойством, что

$$\gamma \equiv 0 \bmod \mathfrak{p}_i^{l_i}, \quad i = 1, \dots, s,$$

и

$$\gamma \not\equiv 0 \bmod \mathfrak{p}_i^{l_i+1}, \quad i = 1, \dots, s.$$

Но тогда ясно, что

$$(\mathfrak{ab},\ \gamma) = \mathfrak{p}_1^{l_1} \dots \mathfrak{p}_s^{l_s} = \mathfrak{a}. \ \blacksquare$$

Следствие. *Любой идеал* $\mathfrak{a}$ *кольца* D *порождается двумя элементами*:

$$\mathfrak{a} = (\alpha,\ \beta).$$

Доказательство. Согласно предложению 2 § 10, существуют такой элемент $\alpha \in D$ и такой идеал $\mathfrak{b}$, что $\mathfrak{ab} = (\alpha)$. Согласно предложению 2, существует такой элемент $\beta \in D$, что $(\mathfrak{ab},\ \beta) = \mathfrak{a}$. $\blacksquare$

Поскольку $\alpha - \beta$ делится на $\mathfrak{a}$ тогда и только тогда, когда $\alpha - \beta \in \mathfrak{a}$, то классы элементов, сравнимых между собой по модулю идеала $\mathfrak{a}$, являются не чем иным, как смежными классами решетки D по ее подрешетке $\mathfrak{a}$ (элементами факторгруппы $D/\mathfrak{a}$). В основном тексте было показано, что число этих классов конечно. Это число обозначается символом $N\mathfrak{a}$ и называется *нормой* идеала $\mathfrak{a}$.

Оказывается, что *норма $N\mathfrak{a}$ произвольного идеала $\mathfrak{a}$ делится на $\mathfrak{a}$*. Действительно, пусть

$$\alpha_1, \ldots, \alpha_N, \quad N = N\mathfrak{a}, \tag{4}$$

— полная система представителей смежных классов кольца D по идеалу $\mathfrak{a}$. (Это означает, что любой элемент кольца D сравним с одним и только одним из элементов (4).) Ясно, что элементы

$$\alpha_1 + 1, \ldots, \alpha_N + 1 \tag{4'}$$

также будут составлять полную систему представителей (если $\alpha_i + 1 \equiv \alpha_j + 1 \bmod \mathfrak{a}$, то $\alpha_i \equiv \alpha_j \bmod \mathfrak{a}$ и, значит, $i = j$; если $\alpha - 1 \equiv \alpha_i \bmod \mathfrak{a}$, то $\alpha \equiv \alpha_i + 1 \bmod \mathfrak{a}$). Это означает, что каждый из элементов (4') сравним по модулю $\mathfrak{a}$ с одним и только одним из элементов (4). Поэтому сумма всех элементов (4') будет сравнима с суммой всех элементов (4), т. е. разность этих сумм будет делиться на $\mathfrak{a}$. Но ясно, что эта разность равна $N = N\mathfrak{a}$. ∎

Переход от одного базиса идеала (или, более общо, произвольной решетки) к другому описывается некоторой целочисленной матрицей. Поскольку возможен обратный переход, эта матрица обратима. Но легко видеть, что определитель обратимой целочисленной матрицы необходимо равен ± 1. Таким образом, матрица перехода от одного базиса идеала к другому имеет определитель ± 1.

Если $\mathfrak{b} \subset \mathfrak{a}$, то базис идеала $\mathfrak{b}$ также выражается через базис идеала $\mathfrak{a}$ посредством некоторой целочисленной матрицы. Ясно (ср. случай линейных пространств), что при изменении базисов эта матрица умножается (справа или слева) на соответствующие матрицы перехода. Поэтому абсолютная величина ее определителя при этом не меняется. Это означает, что

эта абсолютная величина не зависит от выбора базисов и определяется исключительно идеалами $\mathfrak{a}$ и $\mathfrak{b}$. Мы будем обозначать ее символом $[\mathfrak{a} : \mathfrak{b}]$.

Из того, что определитель произведения матриц равен произведению определителей сомножителей, непосредственно вытекает, что *если* $\mathfrak{c} \subset \mathfrak{b} \subset \mathfrak{a}$, *то*

$$[\mathfrak{a} : \mathfrak{c}] = [\mathfrak{a} : \mathfrak{b}] \cdot [\mathfrak{b} : \mathfrak{c}]. \tag{5}$$

Как мы видели выше, для произвольной подрешетки A ранга n решетки D и произвольного базиса решетки D существует базис подрешетки A, связанный с базисом решетки D треугольной матрицей с отличными от нуля диагональными элементами $a_1^{(0)}, \ldots, a_n^{(0)}$. При этом абсолютная величина $|a_1^{(0)} \ldots a_n^{(0)}|$ произведения этих элементов равна порядку факторгруппы D/A.

В случае, когда решеткой D является идеал $\mathfrak{a}$, а под решеткой A — идеал $\mathfrak{b}$, произведение $a_1^{(0)} \ldots a_n^{(0)}$, представляя собой, в силу треугольности матрицы перехода, ее определитель, совпадает (с точностью до знака) с введенным выше числом $[\mathfrak{a} : \mathfrak{b}]$. Таким образом, мы получаем следующую инвариантную характеристику этого числа: *для любых идеалов* $\mathfrak{a}$ *и* $\mathfrak{b} \subset \mathfrak{a}$ *число* $[\mathfrak{a} : \mathfrak{b}]$ *равно порядку факторгруппы* $\mathfrak{a}/\mathfrak{b}$ (здесь, конечно, имеется в виду, что идеалы $\mathfrak{a}$ и $\mathfrak{b}$ рассматриваются как решетки). В соответствии с общей терминологией теории групп мы будем поэтому называть число $[\mathfrak{a} : \mathfrak{b}]$ *индексом* идеала $\mathfrak{b}$ в идеале $\mathfrak{a}$.

В частности, $[(1) : \mathfrak{a}] = N\mathfrak{a}$ для любого идеала $\mathfrak{a}$.

Пусть теперь идеалы $\mathfrak{a}$ и $\mathfrak{b}$ произвольны. Сравнив определения, мы немедленно обнаружим, что их наибольший общий делитель $(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a} \cup \mathfrak{b})$ является не чем иным, как известной из теории групп *суммой* $\mathfrak{a} + \mathfrak{b}$ подгрупп $\mathfrak{a}$ и $\mathfrak{b}$ решетки $D = (1)$. Но в теории групп доказывается, что для любых подгрупп $\mathfrak{a}$ и $\mathfrak{b}$ произвольной группы имеет место изоморфизм

$$(\mathfrak{a} + \mathfrak{b})/\mathfrak{a} \approx \mathfrak{b}/(\mathfrak{a} \cap \mathfrak{b}).$$

Действительно, каждый смежный класс $\beta + (\mathfrak{a} \cap \mathfrak{b})$, $\beta \in \mathfrak{b}$, из $\mathfrak{b}/(\mathfrak{a} \cap \mathfrak{b})$ однозначно определяет смежный класс $\beta + \mathfrak{a}$ из $(\mathfrak{a} + \mathfrak{b})/\mathfrak{a}$. Ясно, что это отображение гомоморфно. При этом, если $\beta + \mathfrak{a} = 0$, т. е. $\beta \in \mathfrak{a}$, то $\beta \in \mathfrak{a} \cap \mathfrak{b}$, т. е. $\beta + (\mathfrak{a} \cap \mathfrak{b}) = 0$. Поскольку любой элемент из $\mathfrak{a} + \mathfrak{b}$ имеет вид $\alpha + \beta$, где $\alpha \in \mathfrak{a}$, $\beta \in \mathfrak{b}$, и, значит, любой смежный класс из $(\mathfrak{a} + \mathfrak{b})/\mathfrak{a}$ — вид $(\alpha + \beta) + \mathfrak{a} =$

$= \beta + \mathfrak{a}$, это доказывает, что отображение $\beta + (\mathfrak{a} \cap \mathfrak{b}) \longmapsto \beta + \mathfrak{a}$ является изоморфизмом.

В силу этого изоморфизма, для любых идеалов $\mathfrak{a}$ и $\mathfrak{b}$ имеет место равенство

$$[(\mathfrak{a}, \mathfrak{b}) : \mathfrak{a}] = [\mathfrak{b} : (\mathfrak{a} \cap \mathfrak{b})]. \tag{6}$$

Интересно, что фигурирующий в этом равенстве идеал $\mathfrak{a} \cap \mathfrak{b}$ имеет четкий мультипликативный смысл: *в моноиде идеалов он является наименьшим общим кратным идеалов* $\mathfrak{a}$ *и* $\mathfrak{b}$: Действительно, $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}$ и $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{b}$, т. е. $\mathfrak{a} \cap \mathfrak{b}$ делится и на $\mathfrak{a}$ и на $\mathfrak{b}$. Если же $\mathfrak{c}$ делится на $\mathfrak{a}$ и на $\mathfrak{b}$, т. е. $\mathfrak{c} \subset \mathfrak{a}$ и $\mathfrak{c} \subset \mathfrak{b}$, то $\mathfrak{c} \subset \mathfrak{a} \cap \mathfrak{b}$, и потому $\mathfrak{c}$ делится на $\mathfrak{a} \cap \mathfrak{b}$.

Поскольку каждый идеал единственным образом разлагается в произведение простых идеалов, то же рассуждение, что и для натуральных чисел, показывает, что *произведение* $\mathfrak{ab}$ *любых идеалов* $\mathfrak{a}$ *и* $\mathfrak{b}$ *равно произведению их наибольшего общего делителя на их наименьшее общее кратное*:

$$\mathfrak{ab} = (\mathfrak{a}, \mathfrak{b}) \cdot (\mathfrak{a} \cap \mathfrak{b}). \tag{7}$$

Теперь без труда можно доказать, что *для любых идеалов* $\mathfrak{a}$ *и* $\mathfrak{b}$ *индекс* $[\mathfrak{a} : \mathfrak{ab}]$ *не зависит от* $\mathfrak{a}$ *и равен норме* $N\mathfrak{b}$ *идеала* $\mathfrak{b}$:

$$N\mathfrak{b} = [\mathfrak{a} : \mathfrak{ab}].$$

Действительно, согласно предложению 4, существует такой элемент $\gamma \in D$, что $(\mathfrak{ab}, \gamma) = \mathfrak{a}$. Следовательно (см. формулу (7)),

$$\mathfrak{a}(\mathfrak{ab} \cap (\gamma)) = (\mathfrak{ab}, (\gamma))(\mathfrak{ab} \cap (\gamma)) = \mathfrak{ab}(\gamma),$$

откуда, сокращая на $\mathfrak{a}$, мы находим, что $\mathfrak{ab} \cap (\gamma) = \mathfrak{b}(\gamma)$. Поэтому (см. формулу (6))

$$[(\gamma) : \mathfrak{b}(\gamma)] = [(\gamma) : (\mathfrak{ab} \cap (\gamma))] = [(\mathfrak{ab}, \gamma) : \mathfrak{ab}] = [\mathfrak{a} : \mathfrak{ab}].$$

Но очевидно (из интерпретации индекса как определителя), что $[(\gamma) : \mathfrak{b}(\gamma)] = [(1) : \mathfrak{b}] = N\mathfrak{b}$. Поэтому

$$N\mathfrak{b} = [\mathfrak{a} : \mathfrak{ab}]. \quad \blacksquare$$

Предложение 3. (Мультипликативность нормы.) *Для любых идеалов* $\mathfrak{a}$ *и* $\mathfrak{b}$ *имеет место равенство*

$$N(\mathfrak{ab}) = N\mathfrak{a} \cdot N\mathfrak{b}.$$

Доказательство. Согласно формуле (5) (примененной к идеалам $\mathfrak{ab}$, $\mathfrak{a}$ и (1)),

$$[(1) : \mathfrak{ab}] = [(1) : \mathfrak{a}] \cdot [\mathfrak{a} : \mathfrak{ab}],$$

т. е.

$$N(\mathfrak{ab}) = N\mathfrak{a} \cdot N\mathfrak{b}. \quad \blacksquare$$

Следствие. *Если норма $N\mathfrak{p}$ идеала $\mathfrak{p}$ является простым числом, то идеал $\mathfrak{p}$ представляет собой простой идеал.*

Доказательство. Достаточно заметить, что $N\mathfrak{a} = 1$ тогда и только тогда, когда $\mathfrak{a} = (1)$. $\blacksquare$

Обратим внимание, что обратное утверждение места не имеет: легко строятся (сделайте это!) примеры простых идеалов $\mathfrak{p}$, норма которых является составным числом.

Задача. Докажите, что норма простого идеала обязательно является степенью простого числа.

Предложение 4. *Для любого элемента $\alpha \in D^*$ имеет место равенство*

$$N(\alpha) = |N\alpha|.$$

Доказательство. Для простоты мы докажем это предложение при дополнительном предположении, что *все числа $\alpha^{(1)}, \ldots, \alpha^{(n)}$ различны.*

Пусть $\omega_1, \ldots, \omega_n$ — базис кольца D и, значит, $\alpha\omega_1, \ldots, \alpha\omega_n$ — базис идеала (α). Пусть, далее,

$$\begin{aligned} \alpha\omega_1 &= a_{11}\omega_1 + \ldots + a_{1n}\omega_n, \\ &\cdots\cdots\cdots\cdots \\ \alpha\omega_n &= a_{n1}\omega_1 + \ldots + a_{nn}\omega_n. \end{aligned} \tag{8}$$

Тогда норма $N(\alpha) = [(1) : (\alpha)]$ равна абсолютной величине определителя

$$\begin{vmatrix} a_{11} & \ldots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \ldots & a_{nn} \end{vmatrix}. \tag{9}$$

С другой стороны, исключая из равенств (8) числа $\omega_1, \ldots, \omega_n$, мы получим (ср. в основном тексте доказательство леммы 1) уравнение

$$\begin{vmatrix} a_{11} - \alpha & \ldots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \ldots & a_{nn} - \alpha \end{vmatrix} = 0, \tag{10}$$

которому удовлетворяет число $\alpha = \alpha^{(1)}$. Применив к (8) отображение $\alpha \to \alpha^{(i)}$, мы немедленно убедимся, что все числа $\alpha^{(i)}$, $i = 1, \ldots, n$, также удовлетворяют уравнению (10). Поскольку степень уравнения (10) равна n, других корней у него нет. Следовательно, произведение $\alpha^{(1)} \ldots \alpha^{(n)}$ является свободным членом этого уравнения, т. е. определителем (9). ■

Следствие. *Если число $N\alpha$ простое, то главный идеал (α) является простым идеалом.*

Так как, согласно формуле (13) § 5, в кольце D_l имеет место равенство

$$N\lambda = l, \qquad \lambda = 1 - \zeta$$

(и все числа $\lambda^{(1)}, \ldots, \lambda^{(l-1)}$, очевидно, различны), то мы получаем, в частности, что *в кольце D_l главный идеал $\mathfrak{l} = (\lambda)$ является простым идеалом.* Этим заполнен пробел в рассуждениях § 9, если мы, конечно, покажем, что к кольцу D_l наша общая теория применима.

Как мы уже знаем, для этого нужно лишь показать, что кольцо D_l целозамкнуто.

§ 11. Целые алгебраические числа

Мы уже неоднократно встречали уравнения вида

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0, \tag{1}$$

где $a_1, \ldots, a_n$ — целые рациональные числа. Корни таких уравнений называются *целыми алгебраическими числами.*

Просто же *алгебраическими числами* (подразумевается, необязательно целыми) называются корни уравнений более общего вида

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n = 0, \tag{2}$$

где также $a_0, a_1, \ldots, a_n$ — целые рациональные числа.

Ясно, что класс алгебраических чисел не изменится, если в уравнении (2) считать коэффициенты $a_0, a_1, \ldots, a_n$ произвольными рациональными числами. Это означает, что алгебраические числа, как мы их определили, являются ни чем иным, как чис-

лами, алгебраическими *над полем* $\mathbb{Q}$ (см., например, М. М. Постников, Теория Галуа, Физматгиз, М., 1963, стр. 11).

Заметим, что аналогичное расширение класса уравнений (1) приводит к уравнениям (2).

Разлагая левую часть уравнения (2) на множители и отбирая множитель, корнем которого является число α, мы получим, что *любое алгебраическое число является корнем некоторого неприводимого многочлена с рациональными коэффициентами.* Без ограничения общности можно считать, что старший коэффициент этого многочлена равен 1.

Пусть α является целым числом, т. е. корнем уравнения (1). По лемме Гаусса (см. § 4) левая часть уравнения (1) разлагается в произведение неприводимых (над полем $\mathbb{Q}$) многочленов с целыми коэффициентами. Так как старшие коэффициенты этих многочленов равны ± 1 (их произведение равно 1), то, следовательно, *неприводимый многочлен* $h(x)$, *корнем которого является целое алгебраическое число* α *и старший коэффициент которого равен* 1, *имеет целые коэффициенты.*

Умножив уравнение (2) на a_0^{n-1}, мы можем переписать его в виде

$$(a_0x)^n + a_1(a_0x)^{n-1} + \ldots + a_na_0^{n-1} = 0.$$

Таким образом, для $y = a_0x$ мы имеем уравнение вида (1). Этим доказано, что *любое алгебраическое число* ξ *может быть представлено в виде*

$$\xi = \frac{\alpha}{a},$$

где α *— целое алгебраическое, а* a *— целое рациональное числа.*

Можно показать, что сумма, разность, произведение и частное двух алгебраических чисел являются алгебраическими числами, т. е., иными словами, что *все алгебраические числа образуют поле.* Концептуальное («в современном духе») доказательство этого факта можно найти, например, в упомянутой выше

«Теории Галуа» на стр. 24. Здесь мы приведем более непосредственное доказательство, требующее зато некоторых вычислений.

Пусть α и β — алгебраические числа. По определению, число α является корнем некоторого уравнения вида (2). Пусть

$$\alpha_1 = \alpha,\ \alpha_2,\ \ldots,\ \alpha_n \tag{3}$$

— все корни этого уравнения. Аналогично, пусть

$$\beta_1 = \beta,\ \beta_2,\ \ldots,\ \beta_m \tag{4}$$

— все корни уравнения

$$b_0 x^m + b_1 x^{m-1} + \ldots + b_m = 0,$$

которому удовлетворяет число β (степень m этого уравнения, вообще говоря, отлична от степени n уравнения, которому удовлетворяет число α).

Рассмотрим многочлен

$$F(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} (x - \alpha_i \beta_j)$$

степени mn. Его коэффициенты являются многочленами с целыми коэффициентами от корней (3) и (4), очевидно, симметрическими, т. е. не меняющимися при любой перестановке этих корней. Поэтому они являются многочленами от соответствующих элементарных симметрических многочленов и, следовательно, согласно формулам Вьета, — многочленами (с целыми коэффициентами) от

$$\frac{a_1}{a_0},\ \ldots,\ \frac{a_m}{a_0},\ \frac{b_1}{b_0},\ \ldots,\ \frac{b_m}{b_0}.$$

Это доказывает, что все коэффициенты многочлена F являются рациональными числами. Значит, все его корни $\alpha_i \beta_j$ и, в частности, корень $\alpha\beta = \alpha_1\beta_1$ являются алгебраическими числами.

Этим наше утверждение доказано в отношении произведения $\alpha\beta$. Для суммы, разности и частного доказательство аналогично. ■

Это доказательство устанавливает также и другой факт, для нас очень важный. Именно, при $a_0 = b_0 = 1$ мы видим, что все коэффициенты многочлена F (старший коэффициент которого по построению

равен единице) будут целыми числами. Ясно, что это заключение сохранится и по отношению к сумме и разности (но не по отношению к частному!). Этим доказано, что сумма, разность и произведение двух целых алгебраических чисел являются целыми алгебраическими числами, т. е. что *все целые алгебраические числа составляют кольцо.*

Однако арифметика этого кольца малоинтересна. Например, в нем совсем нет неразложимых (простых) элементов. Действительно, любое целое алгебраиеское число α может быть разложено, например, по формуле

$$\alpha = \sqrt{\alpha}\,\sqrt{\alpha}$$

(легко видеть, что $\sqrt{\alpha}$ также является целым алгебраическим числом). Поэтому класс всех целых алгебраических чисел следует как-то ограничить.

Подполе K поля комплексных чисел называется полем *конечной степени*, если как линейное пространство над полем $\mathbb{Q}$ оно имеет конечную размерность (которая называется *степенью* поля K).

Заметим, что в общей алгебре поля конечной степени называются «конечными расширениями» поля $\mathbb{Q}$.

Легко видеть, что *каждый элемент поля конечной степени является алгебраическим числом.* Действительно, если степень поля равна n, то для любого его элемента ξ элементы $1, \xi, \ldots, \xi^n$ линейно зависимы (ибо их $n+1$ штук), и, значит, имеет место равенство

$$c_0\xi^n + c_1\xi^{n-1} + \ldots + c_n = 0$$

с рациональными коэффициентами. ■

На этом основании поля конечной степени называются также *полями алгебраических чисел*, хотя этот термин несколько двусмыслен, не предусматривая обязательно конечность степени.

Подробному исследованию взаимоотношений между конечными и алгебраическими расширениями посвящена гл. I указанной выше «Теории Галуа».

Пусть K — произвольное поле алгебраических чисел (конечной степени). Ясно, что его подмножество

D, состоящее из всех целых чисел поля K, является кольцом. Это кольцо называется *кольцом целых чисел* поля K. Арифметика таких колец и составляет содержание теории целых алгебраических чисел.

Так как (см. выше) любой элемент $\xi \in K$ имеет вид $\xi = \frac{\alpha}{a}$, где α — целое алгебраическое число (и, значит, — элемент кольца D), а a — целое рациональное число (и, значит, — тоже элемент D), то K *является полем отношений кольца* D.

Поскольку кольцо D состоит, по определению, из всех целых чисел поля K, этим доказано, что *кольцо* D *целозамкнуто.*

Вернемся теперь к l-круговому полю K_l и его подкольцу D_l. Поле K_l является, конечно, полем конечной степени (равной $l-1$), и потому к нему применимо все сказанное выше. В частности, его кольцо целых чисел D целозамкнуто. Поэтому для доказательства целозамкнутости кольца D_l достаточно доказать, что $D = D_l$.

Доказательство включения $D_l \subset D$. Достаточно заметить, что любой элемент $\alpha \in D_l$ является корнем многочлена

$$f(x) = (x - \alpha^{(1)}) \ \dots \ (x - \alpha^{(l-1)}) \tag{5}$$

с целыми рациональными коэффициентами, старший коэффициент которого равен 1. ■

Другое доказательство. Пусть $\alpha \in D_l$, т. е.

$$\alpha = a_0 + a_1\zeta + \ \dots \ + a_{l-2}\zeta^{l-2},$$

где $a_0, a_1, \dots, a_{l-2}$ — целые рациональные числа. Умножая это равенство последовательно на $1, \zeta, \dots, \zeta^{l-2}$ и используя соотношение $\zeta^{l-1} = -1 - \dots - \zeta^{l-2}$, мы получим систему равенств

$$\begin{aligned}
\alpha &= a_0 + a_1\zeta + \ \dots \ + a_{l-2}\zeta^{l-2},\\
\alpha\zeta &= a_0^{(1)} + a_1^{(1)}\zeta + \ \dots \ + a_{l-2}^{(1)}\zeta^{l-2},\\
&\dots\dots\dots\dots\dots\dots\\
\alpha\zeta^{l-2} &= a_0^{(l-2)} + a_1^{(l-2)}\zeta + \ \dots \ + a_{l-2}^{(l-2)}\zeta^{l-2},
\end{aligned}$$

коэффициентами $a_i^{(j)}$, $i, j = 0, 1, \dots, l-2$, которых являются целые рациональные числа.

Но тогда, согласно лемме 1 § 10, число α будет корнем уравнения вида

$$x^{l-1} + A_1 x^{l-2} + \ldots + A_{l-1} = 0,$$

где $A_1, \ldots, A_{l-1}$ — целые рациональные числа. Поэтому $\alpha \in D$. ■

Этот метод составления уравнения, которому удовлетворяет α, требует вычислений только с рациональными числами.

Многочлен (5), конечно, определен для любого элемента $\alpha \in K_l$. Его свободный член совпадает с нормой $N\alpha$ числа α. Другой интересный коэффициент — это коэффициент при x^{l-2}. Взятый с обратным знаком, он называется *следом* элемента α и обозначается символом $\mathrm{Tr}\,\alpha$. Согласно первой формуле Вьета,

$$\mathrm{Tr}\,\alpha = \alpha^{(1)} + \ldots + \alpha^{(l-1)}.$$

Отсюда следует, что след обладает свойством линейности, т. е.

$$\mathrm{Tr}\,(\alpha + \beta) = \mathrm{Tr}\,\alpha + \mathrm{Tr}\,\beta,$$

$$\mathrm{Tr}\,(a\alpha) = a\,\mathrm{Tr}\,\alpha$$

для любых чисел $\alpha, \beta \in K_l$ и любого рационального числа $a \in \mathbb{Q}$.

Изучим более внимательно многочлен (5). В следующих ниже леммах

$$\alpha = a_0 + a_1\xi + \ldots + a_{l-2}\xi^{l-2} \tag{6}$$

— произвольное число поля K_l.

Лемма 1. *Если многочлен $g(x)$ с рациональными коэффициентами обладает тем свойством, что $g(\alpha^{(i)}) = 0$ хотя бы для одного $i = 1, \ldots, l-1$, то*

$$g(\alpha^{(i)}) = 0 \quad \textit{для всех} \quad i = 1, \ldots, l-1.$$

Доказательство. Пусть

$$a(x) = a_0 + a_1 x + \ldots + a_{l-2}x^{l-2}.$$

Тогда $\alpha = a(\xi)$ и вообще $\alpha^{(i)} = a(\xi^{(i)})$, $i = 1, \ldots, l-1$.

Рассмотрим многочлен

$$F(x) = g(a(x)).$$

По условию

$$F(\xi^{(i)}) = g(a(\xi^{(i)})) = g(\alpha^{(i)}) = 0$$

хотя бы для одного $i = 1, \ldots, l-1$. Это означает, что многочлен $F(x)$ имеет общий корень с неприводимым многочленом

$$\varphi(x) = x^{l-1} + x^{l-2} + \ldots + 1.$$

Следовательно, $F(x)$ делится на этот многочлен и потому $F(\zeta^{(i)}) = 0$, т. е. $g(\alpha^{(i)}) = 0$ для любого $i = 1, \ldots, l-1$. ■

Лемма 2. *Существует такое целое число q, что*

$$f(x) = h(x)^q,$$

где $f(x)$ — многочлен (5), а $h(x)$ — неприводимый многочлен над полем $\mathbb{Q}$ со старшим коэффициентом 1, корнем которого является алгебраическое число α.

Доказательство. Так как $f(\alpha) = 0$, то $f(x)$ делится на $h(x)$. Пусть $f(x)$ делится на $h(x)^q$, но не делится на $h(x)^{q+1}$, и пусть

$$f(x) = g(x)\,h(x)^q.$$

Если $g(x) \neq \text{const}$, то хотя бы один из корней $\alpha^{(i)}$, $i = 1, \ldots, l-1$, многочлена $f(x)$ обращает $g(x)$ в нуль. Но тогда по лемме 1

$$g(\alpha^{(i)}) = 0 \quad \text{для любого} \quad i = 1, \ldots, l-1$$

и, в частности, $g(\alpha) = g(\alpha^{(1)}) = 0$. Таким образом, многочлен $g(x)$ имеет общий корень с неприводимым многочленом $h(x)$ и, значит, делится на $h(x)$. Поэтому многочлен $f(x)$ делится на $h(x)^{q+1}$. Полученное противоречие доказывает, что $g(x) = \text{const}$, т. е. что $f(x) = h(x)^q$ (ибо старшие коэффициенты многочленов $f(x)$ и $h(x)$ равны 1). ■

Лемма 3. *Если α является целым алгебраическим числом, то все коэффициенты многочлена $f(x)$ представляют собой целые рациональные числа.*

Доказательство. Как мы знаем, неприводимый (над $\mathbb{Q}$) многочлен $h(x)$, корнем которого является α и старший коэффициент которого равен 1, имеет целые коэффициенты. Поэтому многочлен $f(x) = h(x)^q$ также имеет целые коэффициенты. ■

Следствие. *След $\operatorname{Tr}\alpha$ любого целого алгебраического числа $\alpha \in K_l$ является целым рациональным числом.*

Полезно заметить, что изложенные соображения имеют весьма общий характер.

Пусть θ — произвольное целое алгебраическое число. Пусть оно является корнем неприводимого уравнения степени n. Тогда можно показать (ср. § 5), что совокупность K всех чисел вида

$$a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}, \tag{7}$$

где $a_0, a_1, \ldots, a_{n-1}$ — произвольные рациональные числа, является полем (очевидно, степени n). Оно обозначается символом $\mathbb{Q}(\theta)$. Все предыдущие рассуждения, относящиеся к полю K_l, остаются в силе и для любого поля $\mathbb{Q}(\theta)$ (если, конечно, заменить $l-1$ на n и ζ на θ). В частности, след любого целого алгебраического числа из $\mathbb{Q}(\theta)$ будет целым рациональным числом.

Аналогом кольца D_l будет кольцо $\mathbb{Z}[\theta]$ всех чисел вида (7) с целыми $a_0, a_1, \ldots, a_{n-1}$. Доказательство, что все эти числа являются целыми алгебраическими числами, т. е. что имеет место включение $\mathbb{Z}[\theta] \subset D$, где D — кольцо целых чисел поля $K = \mathbb{Q}(\theta)$, также, как легко видеть, полностью сохранится (в обоих вариантах).

Эти замечания особо интересны потому, что *любое поле конечной степени имеет вид* $\mathbb{Q}(\theta)$ (см., например, «Теория Галуа», гл. I, п. 7).

Теперь мы уже можем доказать обратное включение.

Доказательство включения $D_l \supset D$. Надо доказать, что если элемент (6) поля K_l является целым алгебраическим числом, то все его коэффициенты $a_0, a_1, \ldots, a_{l-2}$ будут целыми рациональными числами.

С этой целью вычислим сначала след $\mathrm{Tr}\,\alpha$ числа α (который, согласно следствию из леммы 2, является целым рациональным числом).

Если $\alpha = \zeta^k$, где $k = 1, \ldots, l-1$, то числа $\alpha^{(1)}, \ldots, \alpha^{(l-1)}$ будут с точностью до порядка совпадать с числами $\zeta^{(1)}, \ldots, \zeta^{(l-1)}$ (см. § 5, формула (10)), и, значит, будет иметь место равенство

$$\mathrm{Tr}\,\zeta^k = -1, \quad k = 1, \ldots, l-1$$

(ибо по формуле Вьета сумма корней $\zeta^{(1)} + \ldots + \zeta^{(l-1)}$ многочлена $x^{l-1} + x^{l-2} + \ldots + 1$ равна -1). Если же $k = 0$, то $\mathrm{Tr}\,\zeta^k = l-1$.

Отсюда, в силу линейности следа, вытекает, что след числа (6) выражается формулой

$$\mathrm{Tr}\,\alpha = (l-1)a_0 - a_1 - \ldots - a_{l-2}.$$

Аналогичным способом вычисляется, что для любого $k = 0, \ldots, l-2$

$$\mathrm{Tr}(\zeta^{-k}\alpha - \zeta\alpha) = la_k.$$

Поскольку $\zeta^{-k}\alpha - \zeta\alpha$ является вместе с α целым алгебраическим числом (принадлежит кольцу D), этим доказано, что *все числа* la_k, $k = 0, \ldots, l-2$, *являются целыми рациональными числами.*

Следовательно, $l\alpha \in D_l$ и потому

$$l\alpha = b_0 + b_1\lambda + \ldots + b_{l-2}\lambda^{l-2}, \quad \lambda = 1 - \zeta, \tag{8}$$

где $b_0, b_1, \ldots, b_{l-2}$ — целые числа (см. § 5, формула (15)).

Для завершения доказательства достаточно теперь показать, что все коэффициенты $b_0, b_1, \ldots, b_{l-2}$ делятся на l. Условно полагая $b_{-1} = 0$, проведем индукцию по k от $k = -1$ до $k = l-2$.

Пусть для некоторого k, $0 \leqslant k < l-2$, уже доказано, что все коэффициенты b_s с $s < k$ делятся на l. Тогда в (8) все члены, кроме члена $b_k\lambda^k$, будут делиться на λ^{k+1} (ибо $l \sim \lambda^{l-1}$, см. § 5, формула (14)). Следовательно, и член $b_k\lambda^k$ будет делиться на λ^{k+1}, т. е. целое рациональное число b_k будет делиться на λ. Значит, число b_k делится и на l. ■

Заметим, что это доказательство существенно использует специфику поля K_l. Не удивительно поэтому, что аналог равенства $D_l = D$ в произвольном поле алгебраических чисел $\mathbb{Q}(\theta)$, вообще говоря, неверен, т. е. существуют поля $\mathbb{Q}(\theta)$, в которых имеются целые числа

$$a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}$$

с нецелыми коэффициентами $a_0, a_1, \ldots, a_{n-1}$.

Рассмотрим, например, поле $\mathbb{Q}(\sqrt{-3})$. Из данного в § 4 описания поля K_3 следует, что поле $\mathbb{Q}(\sqrt{-3})$ совпадает с полем K_3, и потому его целые числа имеют вид

$$\frac{a + b\sqrt{-3}}{2},$$

где a и b — целые рациональные числа одинаковой четности.

Однако можно без особого труда доказать (попытайтесь!), что для любого поля K конечной степени n аддитивная группа его кольца D целых элементов

является решеткой ранга n, т. е. существуют такие целые числа $\omega_1, \ldots, \omega_n$, что любое целое число $\alpha \in D$ единственным образом представляется в виде

$$a_1\omega_1 + \ldots + a_n\omega_n,$$

где $a_1, \ldots, a_n$ — целые числа. (Принято говорить, что $\omega_1, \ldots, \omega_n$ составляют *фундаментальный базис* поля K.)

Например, при $K = \mathbb{Q}(\sqrt{-3})$ фундаментальный базис состоит из чисел

$$1, \quad \frac{1+\sqrt{-3}}{2}.$$

Факт наличия фундаментального базиса означает, что кольцо D обладает свойством а) из теоремы 1 § 10. Как мы уже отмечали, оно автоматически обладает свойством в). Кроме того, нетрудно видеть (это мы фактически выше уже доказали), что оно обладает и свойством б). Поэтому *кольцо целых чисел произвольного поля алгебраических чисел обладает теорией дивизоров, причем соответствующая группа классов дивизоров конечна.*

Это утверждение является фундаментом всей теории алгебраических чисел.

§ 12. Регулярные простые числа

Итак, мы доказали, что определение регулярного простого числа можно существенно упростить. Окончательное определение состоит в том, что *простое число l регулярно, если оно не делит числа h классов идеалов кольца D_l.*

В связи с этим определением, в первую очередь, возникает задача о вычислении числа h. Хотелось бы иметь для этого числа явную формулу. Оказывается, что такая формула существует, но доказательство ее далеко выходит за рамки этой книги. Поэтому мы приведем ее без доказательства.

В отличие от всего предыдущего, теперь необходимо точно фиксировать выбор корня ζ многочлена деления круга (ср. § 5). Мы будем считать, что

$$\zeta = \cos\frac{2\pi}{l} + i\sin\frac{2\pi}{l}.$$

Отличные от нуля классы

$$\{1\},\ \{2\},\ \ldots,\ \{l-1\} \tag{1}$$

целых рациональных чисел по простому модулю l образуют, как мы знаем (см. § 1), группу по умножению $\mathbb{Z}^*/l$ порядка $l-1$.

Лемма 1. *Группа $\mathbb{Z}^*/l$ является циклической группой.*

Доказательство. Пусть m — наименьшее общее кратное порядков всех элементов группы $\mathbb{Z}^*/l$. Тогда

$$\{a\}^m = \{1\} \tag{2}$$

для любого $\{a\} \in \mathbb{Z}^*/l$ и m является наименьшим числом, обладающим этим свойством. Поэтому $m \leqslant l-1$, ибо $\{a\}^{l-1} = \{1\}$ для всех $\{a\} \in \mathbb{Z}^*/l$ (поскольку $l-1$ — порядок группы $\mathbb{Z}^*/l$).

Рассмотрим теперь множество $\mathbb{Z}/l$ *всех* классов по модулю l. Это множество является полем, мультипликативной группой которого служит группа $\mathbb{Z}^*/l$. Равенство (2) означает, что уравнение $x^m - 1$ имеет в этом поле $l-1$ различных корней (1). Поскольку степень этого уравнения равна m, это возможно только при $m \geqslant l-1$.

Таким образом, $m = l-1$, откуда непосредственно вытекает (проведите подробно соответствующее рассуждение), что в $\mathbb{Z}^*/l$ существует элемент порядка $l-1$. Но это и означает, что группа $\mathbb{Z}^*/l$ циклична. ■

Числа g, класс $\{g\}$ которых является образующей группы $\mathbb{Z}^*/l$, называются *первообразными корнями по модулю l*. Они характеризуются тем, что наименьшее положительное m, для которого $g^m \equiv 1 \bmod l$, равно $l-1$.

Например, при $l = 5$ первообразным корнем является число 2, а при $l = 7$ — число 3.

Действительно,

$$2^0 \equiv 1 \bmod 5,\quad 2^1 \equiv 2 \bmod 5,\quad 2^2 \equiv 4 \bmod 5,\quad 2^3 \equiv 3 \bmod 5,$$
$$3^0 \equiv 1 \bmod 7,\quad 3^1 \equiv 3 \bmod 7,\quad 3^2 \equiv 2 \bmod 7,$$
$$3^3 \equiv 6 \bmod 7,\quad 3^5 \equiv 5 \bmod 7.$$

Мы раз и навсегда выберем и зафиксируем некоторый первообразный корень g по модулю l. Для любого $k \geqslant 0$ мы символом g_k обозначим число из ряда $1, 2, \ldots, l-1$, обладающее тем свойством, что

$$g^k \equiv g_k \bmod l, \qquad k = 0, 1, \ldots, l-2$$

(наименьший положительный вычет числа g^k). Поскольку g — первообразный корень, все числа $g_0 = 1$, $g_1, \ldots, g_{l-2}$ различны.

Далее, мы положим

$$G(x) = g_0 + g_1 x + \ldots + g_{l-2} x^{l-2},$$

$$\theta = \cos \frac{2\pi}{l-1} + i \sin \frac{2\pi}{l-1}$$

и

$$h_1 = \frac{1}{(2l)^{s-1}} \left| G(\theta)\, G(\theta^3) \ldots G(\theta^{l-2}) \right|,$$

где

$$s = \frac{l-1}{2}.$$

Утверждение 1. *Число h_1 является целым положительным числом.*

Например, пусть $l = 5$. Тогда

$$s = 2, \quad \theta = i, \quad g = 2,$$

$$G(x) = 1 + 2x + 4x^2 + 3x^3$$

и потому

$$G(\theta) = 1 + 2i + 4i^2 + 3i^3 = -3 - i,$$

$$G(\theta^3) = 1 - 2i + 4i^2 - 3i^3 = -3 + i.$$

Следовательно,

$$h_1 = \frac{1}{(2 \cdot 5)^1} \left| (-3 - i)(-3 + i) \right| = \frac{9+1}{10} = 1.$$

Аналогично, если $l = 7$, то

$$s = 3, \quad \theta = \frac{1 + i\sqrt{3}}{2}, \quad g = 3$$

и

$$G(x) = 1 + 3x + 2x^2 + 6x^3 + 4x^4 + 5x^5.$$

Легкое вычисление дает, что

$$\left| G(\theta)\, G(\theta^3)\, G(\theta^5) \right| = 196.$$

Поэтому

$$h_1 = \frac{196}{(2\cdot 7)^2} = 1.$$

Задача 1. Для произвольной числовой последовательности $x_0, x_1, \ldots, x_{2(s-1)}$ обозначим символом $H(x_0, x_1, \ldots, x_{2(s-1)})$ определитель матрицы (x_{ij}), $i, j = 0, 1, \ldots, s-1$, где $x_{ij} = x_{i+j}$. Докажите, что

$$h_1 = \frac{|H(g_s - g_0, g_{s+1} - g_1, \ldots, g_{3s-2} - g_{2s-2})|}{(2l)^{s-1}}.$$

Задача 2. Докажите, что $h_1 = 1$ при $l < 23$ и $h_1 = 3$ при $l = 23$. Докажите также, что $h_1 = 37$ при $l = 37$.

Можно показать (это частный случай трудной теоремы Дирихле об единицах произвольного поля алгебраических чисел), что в кольце D_l существует $s-1$ таких единиц

$$\varepsilon_1, \ldots, \varepsilon_{s-1}$$

(называемых *основными единицами*), что каждая единица ε однозначно представляется в виде

$$\varepsilon = (-\zeta)^a \varepsilon_1^{a_1} \ldots \varepsilon_{s-1}^{a_{s-1}},$$

где $a, a_1, \ldots, a_{s-1}$ — целые числа, причем $0 \leqslant a < 2l$.

В качестве корней $\zeta^{(k)}$, $k = 1, \ldots, l-1$, многочлена деления круга, определяющих отображения $\alpha \mapsto \alpha^{(k)}$ (см. § 5), мы, как всегда, примем числа ζ^k. В силу нашего выбора корня ζ, тогда для любого $\alpha \in K_l$ будут иметь место соотношения

$$\alpha^{(s+1)} = \overline{\alpha^{(s)}}, \quad \alpha^{(s+2)} = \overline{\alpha^{(s-1)}}, \quad \ldots, \quad \alpha^{(l-1)} = \overline{\alpha^{(1)}}.$$

Для набора $\varepsilon_1, \ldots, \varepsilon_{s-1}$ основных единиц мы обозначим через R_0 абсолютную величину определителя

$$\begin{vmatrix} \ln|\varepsilon_1^{(1)}| & \ldots & \ln|\varepsilon_1^{(s-1)}| \\ \ldots\ldots\ldots\ldots & & \\ \ln|\varepsilon_{s-1}^{(1)}| & \ldots & \ln|\varepsilon_{s-1}^{(s-1)}| \end{vmatrix}.$$

Можно показать (это нетрудно), что число R_0 не зависит от выбора основных единиц и определяется поэтому только полем K_l. (Вместо числа R_0 обычно рассматривается число $R = 2^{s-1}R_0$; это — так называемый *регулятор* поля K_l.)

Мы положим

$$h_2 = \frac{1}{R_0} \prod_{k=1}^{s-1} \left| \sum_{j=0}^{s-1} \theta^{2kj} \ln |1 - \zeta^{g_j}| \right|.$$

Утверждение 2. *Число h_2 является целым положительным числом.*

Например, при $l = 5$, т. е. при $s = 2$, в формуле для h_2 имеется лишь один множитель

$$\sum_{j=0}^{1} \theta^{2j} \ln |1 - \zeta^{g_j}| = \ln |1 - \zeta| - \ln |1 - \zeta^2|,$$

отвечающий значению $k = 1$ (напомним, что в рассматриваемом случае $\theta = i$, а $g_0 = 1$, $g_1 = 2$). Поэтому

$$R_0 h_2 = |\ln |1 - \zeta| - \ln |1 - \zeta^2|| = |\ln |1 + \zeta||,$$

где число $1 + \zeta$ является единицей (ибо $N(1 + \zeta) = N(1 - \zeta^2) N(1 - \zeta)^{-1} = 1$; см. § 5).

Так как в рассматриваемом случае $s - 1 = 1$, то система основных единиц состоит только из одной единицы ε_1. Поэтому, во-первых, $R_0 = |\ln |\varepsilon_1||$ и, во-вторых, $1 + \zeta = (-\zeta)^a \varepsilon_1^b$, где a и b — целые числа. Но тогда $|1 + \zeta| = |\varepsilon_1|^b$, и потому

$$h_2 = \left| \frac{\ln |1 + \zeta|}{\ln |\varepsilon_1|} \right| = |b|.$$

Таким образом, при $l = 5$ число h_2 действительно является целым положительным числом.

Утверждение 3. *Число классов дивизоров h кольца K_l равно произведению чисел*

$$h = h_1 h_2.$$

Это и есть явная формула для вычисления числа h. Однако, если ее первый множитель h_1 вычисляется совершенно автоматически, то о втором множителе h_2, в котором участвует регулятор R_0, этого сказать нельзя. Дело в том, что не существует практичного способа (алгоритма) вычисления основных единиц, пригодного для всех колец K_l. Имеющиеся «теоретические» алгоритмы сводятся по существу к перебору и, как правило, даже для не очень больших l требуют

колоссального объема вычислений (справиться с которым могут только самые мощные ЭВМ). Поэтому особый интерес представляет следующее (очень трудно доказываемое) утверждение Куммера:

Утверждение 4. *Число h тогда и только тогда делится на l, когда на l делится число h_1.*

Поэтому для испытания данного простого числа l на регулярность достаточно вычислить число h_1. Например, согласно задаче 2 (см. выше), мы можем теперь утверждать, что простое число 37 не регулярно, а все числа $l \geqslant 23$ регулярны.

Вычисление числа h_1, хотя и вполне автоматическое, в достаточной степени утомительно (читатель, решивший задачу 2, смог в этом убедиться сам). Поэтому целесообразно спросить себя, а нельзя ли узнать, делится ли h_1 на l, не вычисляя h_1? Ответ оказывается утвердительным. Именно, используя тот факт, что фигурирующие в формуле для числа h_1 значения $G(\theta^k)$ многочлена $G(x)$ являются целыми числами $(l-1)$-кругового поля K_{l-1} (поля K_m при m не простом определяются аналогично полю K_l), можно без особого труда доказать, что h_1 *тогда и только тогда делится на* l (т. е. l не является регулярным простым числом), *когда хотя бы при одном* $k = 1, 3, \ldots, l-4$ *целое рациональное число* $G(g^k)$ *делится на* l^2 (при этом предполагается, что первообразный корень g выбран так, чтобы имело место сравнение $g^{l-1} \equiv 1 \bmod l^2$; это всегда можно сделать, варьируя g в его классе $\{g\}$). Читатель уже обладает по существу всеми нужными для доказательства этого утверждения знаниями и при известной изобретательности и настойчивости может его сам доказать. Мы же ограничимся тем, что переформулируем это условие в более удобном виде.

По определению, для любого $j = 0, 1, \ldots, l-2$

$$g_j \equiv g^j \bmod l.$$

Значит, существуют такие целые числа a_j, что

$$g_j \equiv g^j + la_j \bmod l^2.$$

Возведя это сравнение в степень $k+1$, где $k = 1, 3, \ldots, l-4$, мы получим сравнение

$$g_j^{k+1} \equiv g^{j(k+1)} + (k+1)\, g^{jk} l a_j \bmod l^2,$$

откуда вытекает, что

$$g_j^{k+1} \equiv g^{j(k+1)} + (k+1)\, g^{jk} (g_j - g^j) \bmod l^2,$$

т. е. что

$$g_j^{k+1} \equiv (k+1)\, g_j g^{jk} - k g^{j(k+1)} \bmod l^2.$$

Следовательно,

$$\sum_{j=0}^{l-2} g_j^{k+1} \equiv (k+1) \sum_{j=0}^{l-2} g_j g^{jk} - k \sum_{j=0}^{l-2} g^{j(k+1)} \bmod l^2.$$

Но

$$\sum_{j=0}^{l-2} g^{j(k+1)} = \frac{g^{(l-1)(k+1)} - 1}{g^{k+1} - 1} \equiv 0 \bmod l^2,$$

ибо по условию $g^{l-1} \equiv 1 \bmod l^2$, а $g^{k+1} - 1 \not\equiv 0 \bmod l$ при $k+1 \leqslant l-3$. Кроме того, по определению

$$\sum_{j=0}^{l-2} g_j g^{jk} = G(g^k)$$

и

$$\sum_{j=0}^{l-2} g_j^{k+1} = \sum_{n=1}^{l-1} n^{k+1}$$

(числа $g_0, g_1, \ldots, g_{l-2}$ с точностью до порядка совпадают с числами $1, 2, \ldots, l-1$). Обозначая последнюю сумму через $S_{k+1}(l)$, мы получаем, следовательно, сравнение $S_{k+1}(l) \equiv (k+1)\, G(g^k) \bmod l^2$. Поэтому сравнение $G(g^k) \equiv 0 \bmod l^2$ равносильно сравнению $S_{k+1}(l) \equiv 0 \bmod l^2$.

Таким образом, число l тогда и только тогда нерегулярно, когда существует такое $k = 1, 3, \ldots, l-4$, что $S_{k+1}(l)$ делится на l^2.

Иными словами, *число l тогда и только тогда регулярно, когда для любого $k = 2, 4, \ldots, l-3$ число*

$$S_k(l) = 1^k + 2^k + \ldots + (l-1)^k$$

не делится на l^2.

Удобно ввести в рассмотрение более общие суммы

$$S_k(m) = 1^k + 2^k + \ldots + (m-1)^k.$$

Легкой индукцией без труда доказывается, что числа $S_k(m)$ являются значениями при $x = m$ некоторого многочлена $S_k(x)$ степени k с рациональными коэффициентами, старшим коэффициентом $\frac{1}{k+1}$ и свободным членом, равным нулю.

Например,

$$S_1(x) = \frac{(x-1)\,x}{2} = \frac{1}{2}x^2 - \frac{1}{2}x,$$

$$S_2(x) = \frac{(x-1)\,x\,(2x-1)}{6} = \frac{1}{3}x^3 - \frac{1}{2}x^2 + \frac{1}{6}x,$$

$$S_3(x) = \frac{(x-3)^2\,x^2}{4} = \frac{1}{4}x^4 - \frac{1}{2}x^3 + \frac{1}{4}x^2.$$

Пусть

$$(3) \qquad (k+1)\,S_k(x) = x^{k+1} + \binom{k+1}{1} B_1 x^k + \binom{k+1}{2} B_2 x^{k-1} + \ldots + \binom{k+1}{k} B_k x.$$

Оказывается, что числа $B_1, B_2, \ldots$ не зависят от k. Они называются *числами Бернулли.*

Любопытно, что впервые эти числа Бернулли ввел, решая одну задачу из астрономии!

Дело здесь в том, что бесконечная последовательность B_1, B_2, B_3, ... чисел Бернулли появляется при разложении некоторых простых функций в степенные ряды. Например, можно показать, что

$$\operatorname{ctg} x = \frac{1}{x} - \frac{B_2}{2!}2^2x + \frac{B_4}{4!}2^4x^3 - \ldots + (-1)^k \frac{B_{2k}}{(2k)!}2^{2k}x^{2k-1} + \ldots$$

Именно этот ряд и появился у Бернулли в его астрономических исследованиях.

Тот факт, что в ряду для $\operatorname{ctg} x$ участвуют только числа Бернулли с четными индексами, не случаен, ибо, как можно легко показать, все числа Бернулли с нечетными индексами (кроме числа B_1) равны нулю: $B_{2k+1} = 0$ при $k > 0$.

Что же касается чисел Бернулли B_{2k} с четными индексами, то они обладают целым рядом замеча-

тельных свойств. Например, через них выражаются значения знаменитой ζ-функции Римана при целых четных аргументах:

$$\zeta(2k) = (-1)^{k-1} \frac{(2\pi)^{2k}}{2(2k)!} B_{2k}, \qquad k \geqslant 1.$$

Первые числа Бернулли имеют вид:

$$B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42}, \quad B_8 = -\frac{1}{30},$$

$$B_{10} = \frac{5}{66}, \quad B_{12} = -\frac{691}{2730}, \quad B_{14} = \frac{7}{6}, \quad B_{16} = -\frac{3617}{510},$$

$$B_{18} = \frac{43867}{798}, \quad B_{20} = -\frac{174611}{330}.$$

Числители этих чисел довольно быстро растут. Например,

$$B_{34} = \frac{2577867858367}{6}.$$

Пусть

$$B_k = \frac{P_k}{Q_k}$$

— несократимая запись числа B_k.

Можно без особого труда доказать (это частный случай так называемой теоремы Штаудта), что при $m < l-1$ знаменатель Q_m числа B_m не делится на l.

Но, согласно формуле (3), для любого $k \geqslant 1$ имеет место равенство

$$(k+1) S_k(l) = \sum_{m=0}^{k-1} \binom{k+1}{m} B_m l^{k+1-m} + (k+1) B_k l,$$

т. е. равенство

$$(k+1) S_k(l) Q_k = \left[\left(\sum_{m=0}^{k-1} \binom{k+1}{m} B_m l^{k-1-m}\right) Q_k\right] l^2 + (k+1) P_k l.$$

Поэтому при $k < l-1$ число, стоящее в правой части в скобках, является целым числом.

Переходя к сравнениям по модулю l^2 и сокращая на $k+1$, мы получаем отсюда, что

$$S_k(l)\,Q_k \equiv P_k l \bmod l^2.$$

Следовательно, $S_k(l) \not\equiv 0 \bmod l^2$ тогда и только тогда, когда $P_k \not\equiv 0 \bmod l$. Этим доказана

Теорема Куммера. *Простое число l тогда и только тогда регулярно, когда оно не делит числителей чисел Бернулли* $B_2, B_4, B_6, \ldots, B_{l-3}$.

Например (см. выше значения чисел Бернулли),

числитель $P_2 = 1$ не делится на 5;

числители $P_2 = 1$ и $P_4 = -1$ не делятся на 7;

числители $P_2 = 1$, $P_4 = -1$, $P_6 = 1$ и $P_8 = -1$ не делятся на 11;

числители $P_2 = 1$, $P_4 = -1$, $P_6 = 1$, $P_8 = -1$ и $P_{10} = 5$ не делятся на 13;

числители $P_2 = 1$, ..., $P_{10} = 5$, $P_{12} = -691$ и $P_{14} = 7$ не делятся на 17;

числители $P_2 = 1$, ..., $P_{14} = 7$ и $P_{16} = -3617$ не делятся на 19;

числители $P_2 = 1$, ..., $P_{16} = -3617$, $P_{18} = 43\,867$ и $P_{20} = -174\,611$ не делятся на 23.

Следовательно, все эти показатели регулярны. Иными словами, *для показателей* 5, 7, 11, 13, 17, 19 *и* 23 *теорема Ферма справедлива.*

Заметим, что только теперь мы получили в отношении хотя бы некоторых показателей l окончательный ответ. Какой большой путь нам пришлось для этого пройти!

Аналогичное вычисление выявляет, что среди чисел первой сотни не регулярны только числа 37, 59 и 67 (между прочим, при $l = 67$ число h_1 равно $853\,513 = 67 \cdot 12\,739$). Как уже говорилось, специальным рассуждением Куммер доказал теорему Ферма и для этих чисел.

Упомянутая в § 1 теорема Йенсена легко вытекает из теоремы Куммера и некоторых элементарных свойств чисел Бернулли.

Цена 20 коп.