ЧЕТВЕРТАЯ ГЛАВА

ТЕОРИЯ ЧИСЕЛ

Возрождение теории чисел

В XVII в. вместе с интересом к точным наукам воскресает и интерес к теории чисел. Особенно он возрос после издания в 1621 г. литератором и любителем математики Клодом-Гаспаром Баше де Мезириаком (1581—1638) греческого текста «Арифметики» Диофанта с латинским переводом и комментариями. Во Франции образовалась группа ученых, занимавшихся задачами теории чисел. В нее входили Пьер Ферма, сотрудник монетного двора Бернар Френикль де Бесси (1605—1675), лионский учитель математики Жак де Билли (1602—1679), Мерсенн, отчасти Декарт и Блез Паскаль. Эти люди жили в различных городах Франции, и некоторые даже никогда не видели друг друга. Зато они вели оживленную переписку как непосредственно друг с другом, так и через Мерсенна (ср. стр. 17). Впоследствии в эту переписку были втянуты ученые Англии — Валлис, Броункер и Голландии — Гюйгенс, Схоотен. Когда Мерсенн скончался, его функции посредника между учеными занял друг Ферма Пьер де Каркави (ум. 1684), любитель математики и королевский библиотекарь, один из организаторов Парижской академии наук.

Однако из всей этой плеяды ученых одному только Пьеру Ферма удалось выделить из хаоса многочисленных задач и частных вопросов, сразу же возникающих перед исследователем при изучении свойств целых чисел, те основные проблемы, которые стали центральными для всей классической теории чисел. Ему же принадлежит открытие замечательного метода для доказательства теоретико-числовых предложений — так называемого метода бесконечного спуска. Поэтому Ферма по праву может считаться основоположником алгебраической теории чисел.

Пьер Ферма

Уроженец юга Франции, Пьер Ферма (1601—1665) провел большую часть жизни в Тулузе, где состоял советником местного парламента (т. е. высшего суда). Он получил юридическое образование, был прекрасным знатоком древних и современных ему языков: латыни, древнегреческого, испанского, итальянского, писал изящные стихи по-французски, по-испански и по-латыни. Греческий он знал настолько хорошо, что делал поправки ко многим ученым переводам и мог бы прославиться как знаток эллинизма. Изучение в подлинниках Евклида, Архимеда, Аполлония, Паппа и Диофанта, вероятно, послужило толчком для занятий Ферма

Пьер Ферма
(с гравюры Фр. де Пуалли, помещенной в издании Диофанта 1670 г.
с замечаниями Ферма)

математикой. Именно здесь и проявился с полной силой его гений. Ферма был чрезвычайно разносторонним математиком: он существенно развил методы определения площадей и объемов, создал новый метод касательных и экстремумов, наряду с Декартом явился создателем аналитической геометрии, вместе с Паскалем заложил основы теории вероятностей. Как и большинство ученых того времени, Ферма не ограничивался исследованиями по «чистой» математике. Он занимался оптикой, и ему принадлежит носящий его имя принцип минимума, которому следует луч света при прохождении через неоднородную среду.

Одной из любимых областей математики была для Ферма теория чисел, которой он занялся, по-видимому, в середине 30-х годов и которой посвящены наиболее вдохновенные строки его писем. «Арифметика,— писал он,— имеет свою собственную область. теорию целых чисел, эта теория была лишь слегка затронута Евклидом и не была достаточно раз-

Титульный лист латинского издания Диофанта с комментариями Баше де Мезириака и замечаниями Ферма (Тулуза, 1670)

DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.

CVM COMMENTARIIS C. G. BACHETI V. C.
& obseruationibus D. P. de FERMAT Senatoris Tolosani.

Accessit Doctrinæ Analyticæ inuentum nouum, collectum
ex varijs eiusdem D. de FERMAT Epistolis.

TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Iesu.
M. DC LXX.

работана его последователями (если только она не содержалась в тех книгах Диофанта, которых нас лишило разрушительное действие времени); арифметики, следовательно, должны ее развить или возобновить»[1].

Ферма писал мало и всегда очень сжато, а кроме того, не публиковал свои работы, циркулировавшие при его жизни лишь в рукописях. Некоторые открытия он изложил только в переписке. Свое намерение написать специальное сочинение по теории чисел он не осуществил. Поэтому результаты Ферма по теории чисел дошли до нас в разрозненном виде: некоторые содержатся в его письмах, другие представляют его замечания к задачам Диофанта на полях принадлежавшего ему экземпляра «Арифметики». Только в 1670 г., после смерти Ферма, его старший сын Самюэль выпустил новое издание Диофанта с комментариями Баше и замечаниями Ферма, а позднее собрал сохранившиеся в бумагах отца математические наброски и небольшие трактаты и издал их под названием «Разные математические сочинения» (Varia opera mathematica, Tolosae, 1679). Но и после этого были найдены многие письма и заметки Ферма, не вошедшие в это издание.

Таким образом, теоретико-числовые результаты Ферма дошли до последующих математиков в виде проблем, в подавляющем большинстве случаев без доказательств и указаний на внутренние связи между ними. После смерти Ферма проблемы эти пролежали без движения около семидесяти лет, пока ими не заинтересовался Л. Эйлер. С этого момента началась их новая жизнь. Исследования Эйлера превратили теорию чисел в неотъемлемую составную часть математики.

Перейдем теперь к проблемам Ферма.

Простые числа

Занимаясь арифметикой целых чисел, Ферма обратил внимание на большую роль, которую играют простые числа. По-видимому, он начал искать различные критерии для определения того, будет ли заданное число N простым или составным. Он искал также выражения $F(n)$, которые при любом целом значении n давали бы только простые числа. Ферма полагал, что таким выражением будет

$$F(n) = 2^{2^n} + 1.$$

Действительно, при $n = 0, 1, 2, 3$ и 4 $F(n)$ принимает значения 3, 5, 17, 257, 65537, являющиеся простыми числами. Однако, как показал Эйлер, $F(5) = 2^{32} + 1$ не простое. Что не существует целого многочлена $P(x)$ с целыми коэффициентами, все значения которого при целых x были бы простыми числами, доказали Хр. Гольдбах и Эйлер (ср. т. III, гл. 3).

Простые числа вида $2^{2^n} + 1$ называются теперь простыми числами Ферма. До сих пор неизвестно, существует ли конечное число простых чисел Ферма или их бесконечно много.

Одним из критериев для определения простоты числа послужила так называемая малая теорема Ферма.

---

[1] P. Fermat. Oeuvres, v. II, Parisii, 1894, p. 334.

Малая теорема Ферма

Ферма установил, что для каждого числа a, не делящегося на простое число p, существует такое число f, являющееся делителем $p - 1$, что $a^f - 1$ делится на p. Он сформулировал это предложение сначала для $a = 2$, затем для любого a.

Малая теорема Ферма — одна из самых важных теорем элементарной теории чисел; здесь впервые мы сталкиваемся с частным случаем важнейшего понятия современной алгебры — конечной циклической группой, образованной элементами

$$1,\ a,\ a^2,\ \ldots,\ a^{f-1},$$

которые рассматриваются по модулю p (т. е. два элемента считаются равными, если при делении на p они дают один и тот же остаток). В малой теореме на частном примере установлено одно из основных предложений теории конечных групп: порядок любого элемента конечной группы является делителем порядка группы (ср. т. III, гл. 2).

Квадратичные формы

Ферма впервые поставил вопрос об определении вида простых чисел, представимых некоторой квадратичной формой. Число n называется представимым формой

$$ax^2 + 2bxy + cy^2,$$

если существуют такие целые, взаимно простые x_1, y_1, что

$$n = ax_1^2 + 2bx_1y_1 + cy_1^2.$$

Ферма решил этот вопрос для форм

$$x^2 + y^2,\ x^2 + 2y^2,\ x^2 - 2y^2,\ x^2 + 3y^2 \text{ и } x^2 + xy + y^2.$$

Так, он нашел, что формой $x^2 + y^2$ представимы те и только те простые числа, которые лежат в прогрессии $4n + 1$, причем каждое простое число этой прогрессии представимо в виде суммы двух квадратов единственным образом, например

$$5 = 4 \cdot 1 + 1 = 1^2 + 2^2$$

(этот результат, впрочем, был известен еще Диофанту).

Далее Ферма нашел, что формой $x^2 + 2y^2$ представимы все простые числа вида $8n + 1$ и $8n + 3$ и только они, а формой $x^2 + 3y^2$ и $x^2 + xy + y^2$ — простые числа вида $6n + 1$.

Замечательно, что Ферма рассматривает распределение по прогрессиям только простых чисел, представимых некоторой формой. Именно на этом пути были открыты в дальнейшем те глубокие закономерности, которые охарактеризованы с помощью квадратичного закона взаимности.

Вопрос о нахождении всех чисел, как простых, так и составных, представимых некоторой квадратичной формой, Ферма поставил и решил только для случая формы $x^2 + y^2$. Для составных чисел уже не существует столь же простого закона, характеризующего представимые числа, как в случае простых чисел.

Однако из формулы

$$(x^2 + y^2)(u^2 + v^2) = (xu \pm yv)^2 + (xv \mp yu)^2$$

видно, что произведение двух представимых чисел снова будет представимым числом. Ферма как раз и воспользовался этой формулой, чтобы показать, что множество чисел, представимых формой $x^2 + y^2$, замкнуто по умножению. Тем самым простейшая формула для композиции форм, известная еще Диофанту, была использована для представления чисел. Теория композиции форм была впоследствии развита Эйлером, Лагранжем и особенно Гауссом.

Упомянем еще предложение о представимости любого целого положительного числа суммой не более четырех целых квадратов, впервые высказанное Баше де Мезириаком в комментариях к его изданию «Арифметики» Диофанта 1621 г. В замечании, относящемся к этому месту, Ферма высказал более общую теорему, согласно которой любое натуральное число есть либо n-угольное, либо сумма не более чем n n-угольных чисел, причем утверждал, что располагает ее доказательством. В 1636 г. теорема стала известной в кругу французских математиков. Доказательство свое Ферма не сообщил; он лишь упомянул в одном письме 1654 г. Паскалю, что вывод опирается на представимость простых чисел вида $4n + 1$ суммой двух квадратов. Эта теорема Ферма для $n = 4$ была доказана во второй половине XVIII в. благодаря совместным усилиям Эйлера и Лагранжа, для $n = 3$ — Гауссом (1801) и в общем случае — О. Коши (1813—1815).

Неопределенные уравнения

Баше де Мезириаку и Ферма принадлежит заслуга постановки задачи о решении неопределенных уравнений в целых числах. До них, следуя за Диофантом, европейские математики обычно искали рациональные решения таких уравнений.

Баше де Мезириак, не зная о своих индийских предшественниках (см. т. I, стр. 194), подробно разработал и изложил на числовых примерах способ решения в целых положительных числах линейного уравнения с двумя неизвестными

$$ax - by = 1,$$

где $(a, b) = 1$. Этот вопрос Баше изложил в замечательном сборнике «Приятных и занимательных задач, рассматриваемых в числах» (Problèmes plaisans et delectables qui se font par les nombres, Lyon, 1612), неоднократно переиздававшихся вплоть до наших дней,— в последний раз книга вышла в 1959 г.

Ферма исследовал гораздо более трудную задачу решения в целых положительных числах уравнения с двумя неизвестными второй степени. В своем письме, получившем название «Второго вызова математикам» (февраль 1657), он предложил своим корреспондентам найти общее правило решения уравнения

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

где a — целое неквадратное число. Такое уравнение рассматривали еще математики древней Греции и средневековой Индии (см. т. I, стр. 195). Впоследствии Эйлер по ошибке связал его с именем английского алгебраиста Джона Пелля (1611—1685). Теперь более принято называть уравнение (1), отдавая долг справедливости, уравнением Ферма, что и мы будем делать в дальнейшем.

Проблема решения уравнения Ферма распадается на две: 1) найти наименьшее целочисленное решение x_0, y_0, после чего, 2) зная наименьшее решение, найти все остальные.

В своем письме Ферма предлагал найти решения при $a = 149, 109, 433$. Эти значения выбраны так, что наименьшее решение соответствующего уравнения Ферма очень велико и его нельзя найти простым подбором. Вероятно, Ферма специально выбрал эти примеры, чтобы узнать, владеют ли его коллеги общим методом для решения первого из указанных нами вопросов. Что касается самого Ферма, то не подлежит сомнению, что он имел общие формулы для решения второго из вышеназванных вопросов. Для случая $a = 2$ он привел соответствующие формулы в письме к Френиклю. По-видимому, он владел и методом нахождения наименьшего решения, однако в его бумагах никаких следов такого приема не осталось.

Ферма придавал уравнению (1) очень большое значение, считая, что оно поясняет путь, по которому должна развиваться наука о числах. Но его современники не поняли значения этого уравнения. По поводу уравнения Ферма разгорелась интересная дискуссия, в которой приняли участие английские математики и которая была издана Валлисом в 1658 г. под названием «Недавняя переписка о некоторых математических вопросах» (Commercium epistolicum de quaestionibus quibusdam mathematicis nuper habitum, Oxoniae). Из этой переписки видно, что английские математики сначала не поняли задачу: Броункер предложил ее решение в рациональных числах, Валлис считал, что требование найти решение в целых числах делает задачу менее общей. После дополнительных разъяснений Ферма, Броункер решил уравнение Ферма при $a = 109$ с помощью разложения $\sqrt{a}$ в непрерывную дробь, но не доказал ни того, что его способом всегда можно найти решение. ни того, что при этом получаются все решения. Впоследствии эффективное решение уравнения Ферма и исчерпывающее его исследование было дано Эйлером и Лагранжем (см. т. III, гл. 3). Наконец, в 1846 г., обобщив результаты Ферма, Эйлера и Лагранжа, Лежен Дирихле построил свою теорию единиц в полях алгебраических чисел.

Ферма рассматривал и более общее неопределенное уравнение второго порядка

$$ax^2 + b = y^2. \qquad (2)$$

Приведя пример неопределенного уравнения

$$2x^2 + 7967 = y^2,$$

он писал: «Я нашел общее правило, чтобы решать такое уравнение, если оно возможно, или чтобы определять его невозможность. И это — во всех случаях и для всех чисел» [1].

---

[1] *P. Fermat.* Oeuvres, v. II, p. 431.

Далее, в примечаниях к Диофанту, приведя пример так называемого двойного равенства

$$2x + 3 = u^2$$
$$3x + 5 = v^2,$$

решение которого, как нетрудно видеть, сводится к решению уравнения вида

$$au^2 - bv^2 = c,$$

он писал: «Баше в комментариях к Диофанту приписывает себе честь нахождения правила для двух частных случаев. Я даю общее правило для всех случаев. И определяю правилами, является ли оно возможным или нет» [1].

Больше никаких указаний на уравнение (2) в работах Ферма нет. Ни одному из его современников решение этого уравнения было не под силу, Эйлер продвинул вперед его исследование, а полностью решил его Лагранж (см. т. III, гл. 3).

Решение неопределенных уравнений в рациональных числах

В этом вопросе Ферма следовал за Диофантом. Еще Виет и Баше де Мезириак обратили внимание на метод, с помощью которого Диофант находил рациональные решения неопределенных уравнений третьего порядка, а применили его для определения рациональных решений уравнений

$$1)\ x^3 + y^3 = a^3 - b^3,$$
$$2)\ x^3 - y^3 = a^3 + b^3,$$
$$3)\ x^3 - y^3 = a^3 - b^3.$$

Одно решение здесь находится очевидным образом, а другие определяются по методу Диофанта (см. т. I, стр. 147—148). Ферма добавил к этим трем уравнениям четвертое

$$4)\ x^3 + y^3 = a^3 + b^3,$$

которое не могли решить его предшественники, так как если, следуя Диофанту, сделать подстановку

$$x = \zeta + a, \qquad y = k\zeta + b,$$

а затем приравнять нулю коэффициент при первой степени ζ, то полученная рациональная точка x, y будет обязательно иметь одну отрицательную координату, т. е. сумма двух кубов представится не суммой, а разностью двух других кубов (это будет решением задачи 2, а не 4). Ферма находит положительные рациональные значения x, y, решая последовательно задачи 2, 3 и, наконец, 1.

---

[1] *P. Fermat.* Oeuvres, v. II, p. 431.

В примечаниях к 12-й задаче IV книги «Арифметики» Диофанта Ферма рассматривает задачу

$$x^4 - y^4 = u^3.$$

Он полагает $x - y = 1$ и после этого легко находит одно из рациональных решений $y = -9/22$, $x = 13/22$. Чтобы найти положительные рациональные решения, Ферма делает подстановку $y = y' - \frac{9}{22}$, $x = x' + \frac{13}{22}$, т. е. осуществляет сдвиг соответствующей кривой. Этот прием Ферма применял многократно, а после его смерти описание метода Диофанта с применением сдвигов для получения положительных решений дал де Билли в «Новом открытии в аналитическом учении» (Doctrinae analyticae inventum novum), составленном по письмам к нему от Ферма и напечатанном в уже упоминавшемся издании Диофанта 1670 г. в качестве введения. Вряд ли Ферма мог не заметить аналогии своего приема с теми преобразованиями, которыми он пользовался в аналитической геометрии. Вероятно, он понимал также связь метода Диофанта со своим методом касательных к алгебраическим кривым. Однако о геометрическом смысле метода нахождения рациональных решений неопределенных уравнений третьего порядка, который заключается в том, что в рациональной точке $P(x_1, y_1)$ алгебраической кривой третьего порядка проводится касательная и ищется другая ее точка пересечения с кривой $Q(x_2, y_2)$, которая также будет рациональной, Ферма не упоминат, как не делал этого впоследствии и Эйлер. Впервые явная геометрическая интерпретация метода появилась в XIX в. в работах Коши, Люка и Пуанкаре.

Метод Диофанта давал возможность находить рациональные решения в том случае, когда одно из таких решений было уже найдено. Вскоре Ферма встретился с такими задачами, которые не имеют рациональных решений. Они особенно привлекли его внимание. Одна из таких проблем, так называемая великая теорема Ферма, сыграла совершенно исключительную роль в истории теории чисел.

Великая теорема Ферма

В замечании к 8-й задаче II книги «Арифметики» Диофанта, в которой требуется разложить заданное квадратное число a^2 в сумму двух квадратов, Ферма высказал следующее утверждение: «Наоборот, невозможно разложить ни куб на два куба, ни биквадрат на два биквадрата, ни, вообще, степень, большую квадрата, на две степени с тем же показателем; я открыл этому поистине чудесное доказательство, которое из-за недостатка места не может поместиться на этих полях» [1]. Это и есть так называемая великая теорема Ферма, которую теперь выражают в такой форме: уравнение

$$x^n + y^n = z^n \qquad \text{при } n > 2 \text{ и } xyz \neq 0$$

неразрешимо в целых (а значит, и в рациональных) числах.

Однако в своих письмах Ферма говорил об этой теореме только для случаев $n = 3$ и $n = 4$. Последний случай был доказан самим Ферма.

[1] *P. Fermat.* Oeuvres, v. II, p. 241.

Это единственное теоретико-числовое доказательство, которое от него дошло. Оно содержится в замечаниях к Диофанту, и в нем доказывается, что не существует прямоугольного треугольника в целых числах, площадь которого была бы квадратом. Из этого предложения следует, что не существует двух биквадратов, сумма которых равнялась бы квадрату, а значит, и биквадрату. Доказательство проводится методом спуска. В 1659 г., за два года до смерти, Ферма описал этот метод в своем письме-завещании, адресованном Каркави, которое известно под названием «Сводка новых результатов в науке о числах». Мы приведем это описание.

Метод бесконечного спуска

Ферма пишет, что «поскольку обычные методы, находящиеся в книгах, были недостаточны для доказательства столь трудных предложений, то я, наконец, нашел совершенно особый путь для их достижения. Я назвал этот способ доказательства *бесконечным или неопределенным спуском*» (descente infinie ou indéfinie)[1].

Вначале Ферма пользовался этим методом только для доказательства отрицательных предложений, например: «Не существует прямоугольного треугольника в целых числах, площадь которого была бы квадратом». «Доказательство проводится следующим образом: если бы существовал прямоугольный треугольник в целых числах, площадь которого была бы квадратом, то существовал бы другой треугольник, меньший первого, обладающий тем же свойством. Если бы был второй, меньший первого и с тем же свойством, то тем же рассуждением мы получили бы третий, обладающий тем же свойством и меньший второго, наконец, четвертый, пятый и т. д., спускаясь до бесконечности. Но если дано число, то не существует бесконечного множества чисел, меньших, чем оно... Отсюда заключают, что невозможно существование прямоугольного треугольника, площадь которого была бы квадратом» [2].

Далее Ферма говорит, что после долгих размышлений он смог применить свой метод и для доказательства утвердительных предложений, как, например: каждое простое число вида $4n + 1$ представимо суммой двух квадратов. Но для применения метода к доказательству других предложений, например для доказательства того, что каждое число представимо суммой не более четырех квадратов, требуется применение «новых принципов», на которых Ферма подробнее не останавливается. Далее идет перечисление всех теорем, которые Ферма доказал, пользуясь методом спуска. Среди них находится и великая теорема для случая $n = 3$. В конце письма Ферма выражает надежду, что этот метод окажется полезным для последующих математиков и покажет им, что «древние не все знали». К сожалению, это письмо было опубликовано только в 1879 г. Однако Эйлер восстановил метод по отдельным замечаниям Ферма и с успехом применил его к проблемам неопределенного анализа. Ему, в частности, принадлежит и доказательство великой теоремы для $n = 3$ (см. т. III). Напомним, что первая попытка доказать неразложимость куба натурального числа в сумму двух кубов была сделана около 1000 г. на арабском Востоке (см. т. I, стр. 228).

---

[1] *P. Fermat.* Oeuvres, v. II, p. 431.
[2] Там же, p. 431.

Метод спуска вновь начал играть ведущую роль в исследованиях по диофантову анализу А. Пуанкаре и А. Вейля. В настоящее время для применения этого метода вводится понятие высоты, т. е. такого натурального числа, которое определенным образом ставится в соответствие каждому рациональному решению. При этом если удастся доказать, что для каждого рационального решения высоты h найдется другое решение высоты меньше h, то отсюда будут следовать неразрешимость задачи в рациональных числах.

Значение проблем Ферма

Вся последующая алгебраическая теория чисел вплоть до работ Гаусса развивалась, отправляясь от проблем Ферма. Исследовались в основном вопросы представления чисел квадратичными формами и задачи диофантова анализа, в частности неопределенные уравнения второго порядка. В работах Лагранжа, а особенно Гаусса, первый из названных вопросов был преобразован в теорию квадратичных форм, которая по существу являлась первым учением об арифметике квадратичных полей. Этот же вопрос привел Эйлера к открытию квадратичного закона взаимности. Наконец, в XIX в. исследования, связанные с великой теоремой Ферма и законами взаимности, потребовали расширения области арифметики. При изучении биквадратичного закона взаимности Гаусс ввел целые комплексные числа, а попытки доказательства великой теоремы привели к рассмотрению целых чисел в полях деления круга. Центральной проблемой алгебраической теории чисел в XIX в. становится построение арифметики в кольцах алгебраических чисел. Для спасения обычных законов арифметики вводятся идеальные множители (Куммер, Золотарев), идеалы (Дедекинд) и дивизоры (Кронекер). Строится теория колец, модулей и идеалов, появляются локальные и полулокальные кольца. И все эти ветви восходят к проблемам Ферма. Исчерпаны ли они? По-видимому, все проблемы, кроме великой теоремы, уж полностью раскрыты. Но великая теорема в общем виде еще не доказана. Поэтому мы вправе ожидать здесь появления новых идей и методов.