С.А. Степанов

Арифметика алгебраических кривых

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
С11

С.А. Степанов
С11 Арифметика алгебраических кривых / С.А. Степанов – М.: Книга по Требованию, 2021. – 368 с.

ISBN 978-5-458-44791-1

ISBN 978-5-458-44791-1

ПРЕДИСЛОВИЕ

Данная книга основана на курсе лекций, прочитанном автором весной 1989 г. в Тата институте фундаментальных исследований (Бомбей), и посвящена наиболее изученному разделу диофантова анализа — теории уравнений с двумя неизвестными.

Проблематика теории диофантовых уравнений обманчиво проста и состоит (при классическом понимании) в отыскании рациональных или целочисленных решений неопределенных полиномиальных уравнений с целыми коэффициентами. Что касается вопроса о роли теории диофантовых уравнений в математике, то ответ на него (в значительной степени предугаданный еще К. Ф. Гауссом в его знаменитом изречении о королевском статусе теории чисел) удалось получить лишь в наши дни, после создания формализованной теории доказательств и теории алгоритмов. Он оказался необычайно эффектным: к теории диофантовых уравнений сводится в некотором смысле слова «почти вся» математика (см. [81 d]).

Указанная универсальность диофантовых уравнений требует, естественно, для их изучения огромного арсенала понятий и методов. В настоящее время этот арсенал достаточно солиден и включает в себя не только классические методы арифметики, геометрии чисел и анализа, но и современные методы алгебраической геометрии, математической логики и теории диофантовых приближений.

Еще сравнительно недавно (см. Диксон [44]) совокупность исследованных к тому времени диофантовых уравнений можно было уподобить многочисленным островам Полинезии и Микронезии, разбросанным по бесконечному простору Тихого океана. Многие из этих уравнений стали знаменитыми (вроде острова Гуам — первого клочка суши, открытого в Океании экспедицией Магеллана, и одновременно, по неведомому стечению обстоятельств, величественнейшей вершины затонувшего горного хребта, вознесшейся над прилегающей к ней Марианской впадиной на целую милю выше, чем Джомолунгма над уровнем моря); некоторые до сих пор сохранили налет экзотичности (вроде острова Таити); другие снискали печальную славу (подобно аттолу Бикини), и, наконец, очень многие диофантовы уравнения весьма специального вида в настоящее время почти полностью забыты (подобно многочисленным необитаемым островам).

Последние десятилетия ознаменовались созданием достаточно общих методов, применимых к широким классам диофантовых уравнений. Доказательство гипотезы Морделла о конечности числа рациональных точек на кривой рода $g > 1$ (Фалтингс [125])

и более ранние результаты о числе точек кривых над конечными полями (см. гл. I, V) привели к созданию сравнительно законченной теории диофантовых уравнений с двумя неизвестными. Значительный прогресс достигнут (см. гл. III) и при исследовании вопроса о структуре множества рациональных точек в исключительном случае кривых рода 1 (эллиптических кривых), а также в вопросе об эффективном перечислении множества целых точек на кривых достаточно общего вида (см. гл. VI). Развитие кругового метода Харди — Литтлвуда открыло возможность для установления целочисленной разрешимости ряда диофантовых уравнений с достаточно большим числом неизвестных. Обобщение метода Туэ на многомерный случай (В. Шмидт [146a]) позволило изучить структуру множества целочисленных решений широкого класса норменных уравнений с произвольным числом неизвестных. Наконец, отрицательное решение 10-й проблемы Гильберта (Ю. В. Матиясевич [82a]) привело к уяснению причин тех трудностей, которые связаны с изучением диофантовых уравнений, и значительно расширило наши представления о роли диофантовых уравнений в математике.

Первоначально автор предполагал нарисовать по возможности широкую картину современного состояния теории диофантовых уравнений, дать представление о всем спектре используемых в ней методов и, в то же время, продемонстрировать их внутреннее единство. Объем книги не позволил, однако, изложить аналитические аспекты теории и, в частности, результаты, полученные с помощью кругового метода Харди — Литтлвуда и методами теории диофантовых приближений. С этими аспектами читатель может познакомиться по книгам И. М. Виноградова [27 c], Р. Вона [28] и В. Шмидта [146 i]. Поэтому было решено ограничиться рассмотрением арифметических, алгебро-геометрических и логических аспектов вопроса. Но и после этого материал оказался слишком обширным. Поэтому значительную его часть пришлось изложить в виде задач (которых в книге более двухсот пятидесяти). Задачи рассчитаны на активно работающего читателя. Некоторые из них (отмеченные звездочкой) — весьма трудные и требуют для своего решения значительных творческих усилий. Как правило, такие задачи снабжены подробными указаниями, а наиболее сложные из них — еще и ссылками на источники.

По некоторым вопросам книга пересекается с «Основами диофантовой геометрии» С. Ленга [70 h]. Но в отличие от последней она не предполагает у читателя столь солидной математической подготовки и, в частности, знания современных методов алгебраической геометрии.

Предварительный текст книги был просмотрен А. Н. Паршиным и С. Ф. Сопруновым (гл. VI, VII). Автор выражает им благодарность за ряд полезных советов и замечаний.

ВВЕДЕНИЕ

В наиболее общей формулировке задача о решении диофантовых (неопределенных) уравнений состоит в отыскании множества $X(k_0)$ всех решений $(x_1, \ldots, x_n) \in k_0^n$ системы полиномиальных уравнений

$$f_i(x_1, \ldots, x_n) = 0, \quad 1 \leqslant i \leqslant m, \tag{1}$$

с коэффициентами из некоторого поля k_0 и в определении алгебраической структуры множества $X(k_0)$.

В классической постановке, восходящей к Диофанту Александрийскому [45], коэффициенты многочленов f_i являются целыми числами, и задача заключается в отыскании всех рациональных решений системы (1) (см. также [140, с. 171; 9]).

В арифметических вопросах, связанных с диофантовыми уравнениями, возникает необходимость в нахождении множества $X(\mathbb{Z})$ всех целочисленных решений системы (1), или, в более общей постановке, множества $X(\mathbb{Z}_{k_0})$ всех наборов $(x_1, \ldots, x_n)$ с компонентами из кольца целых чисел $\mathbb{Z}_{k_0}$ поля k_0, удовлетворяющих этой системе. Пример уравнения

$$y^2 = x^3 - 2,$$

имеющего бесконечное число рациональных решений и лишь два целочисленных решения $(x, y) = (3, \pm 5)$, показывает (см. задачи 1, 2 из § 2 гл. III), что вопрос о целочисленных решениях часто существенно отличается от вопроса о рациональных решениях и требует для своего исследования особых приемов и методов.

На всех этапах своего многовекового развития теория диофантовых уравнений оказывала определяющее влияние на формирование науки нового времени. Становление теории относится к I — III векам н. э. и характеризуется решительным отказом от прежних геометрических традиций греческих математиков и поворотом к арифметико-алгебраическому направлению. Перед средневековой Европой достижения античной математики в указанном направлении неожиданно предстали шестью книгами «Арифметики» Диофанта [45], случайно обнаруженными в 1571 г. в библиотеке Ватикана.

Следующий этап в развитии теории диофантовых уравнений тесно связан с именем Ф. Виета — родоначальника буквенного исчисления, и с именами создателей теории чисел — П. Ферма, Л. Эйлера, Ж. Л. Лагранжа и А. Лежандра, разработавших локальные методы изучения диофантовых уравнений на основе теории сравнений (см. [23 h]). Достижения этих выдающихся уче-

ных были подытожены К. Ф. Гауссом в его знаменитой книге «Disquisitiones arithmeticae [30 a], опубликованной в 1801 г. (см. также [30 c]).

Начало XIX века ознаменовалось открытием тесных взаимосвязей между теорией диофантовых уравнений и другими областями математики — алгеброй, геометрией и анализом. Подтверждением тому служат исследования Ж. Л. Лежандра, К. Ф. Гаусса, Л. Дирихле, Ш. Эрмита по теории квадратичных форм, завершившиеся созданием арифметики квадратичных полей и заложившие основы группового подхода в математике; работы Э. Куммера по изучению уравнения Ферма $x^n + y^n = z^n$, приведшие его к созданию арифметики круговых полей и увенчавшиеся разработкой теории дивизоров для полей алгебраических чисел (Р. Дедекинд, Е. И. Золотарев, Л. Кронекер); наконец, результаты К. Якоби по применению теорем Л. Эйлера и Н. Абеля о сложении эллиптических и абелевых интегралов к сложению рациональных точек на алгебраических кривых, заложившие основы арифметики абелевых многообразий. При этом была обнаружена глубокая аналогия между полями алгебраических чисел и полями алгебраических функций, приведшая, с одной стороны, к созданию арифметической теории функциональных полей и, с другой стороны, к введению в арифметику p-адических чисел (К. Гензель), играющих в числовых полях роль рядов Пюизе для алгебраических функций. Тем самым были заложены основы коммутативной алгебры и современной алгебраической геометрии.

Конец XIX — начало XX веков характеризуется интенсивным проникновением в теорию диофантовых уравнений аналитических методов. Наиболее мощными из них являются метод А. Туэ (см. гл. VI), основанный на применении результатов теории диофантовых приближений (приближений вещественных чисел рациональными), и круговой метод Харди — Литтлвуда (см. [131, 28]), восходящий своими корнями к методу производящих функций Л. Эйлера.

Метод А. Туэ получил свое дальнейшее развитие в работах К. Л. Зигеля, установившего на его основе знаменитую теорему о конечности числа целых точек на кривых рода $g \geqslant 1$ (см. гл. VII). Затем результат Зигеля был перенесен К. Малером на случай квазицелых точек с координатами из произвольного конечного расширения поля рациональных чисел $\mathbb{Q}$. Недавно метод А. Туэ был распространен В. Шмидтом [146e] на случай нескольких переменных, что позволило ему получить многомерное обобщение результата Туэ о конечности числа целочисленных решений норменного диофантова уравнения (*уравнения Туэ*)

$$\operatorname{norm}(\alpha x + \beta y) = a$$

степени $m \geqslant 3$.

Круговой метод Харди — Литтлвуда, основу которого составляет процесс поднятия локальных решений системы полиномиальных уравнений с целыми коэффициентами до ее целочисленных решений, плодотворен лишь в случае, когда число переменных много больше максимальной степени входящих в систему уравнений. Этот метод был значительно усовершенствован И. М. Виноградовым (см. [27 с, 28]), и существенно усиленный его оценками тригонометрических сумм Г. Вейля, привел к практически окончательному решению знаменитой проблемы Варинга о представимости всякого достаточно большого целого N ограниченной суммой n-х степеней целых чисел. Наиболее общий результат, полученный круговым методом, принадлежит Бёрчу [14] и состоит в том, что каждая невырожденная в определенном смысле система однородных уравнений с целыми коэффициентами, имеющих одинаковую степень и зависящих от достаточно большого числа переменных, обладает по меньшей мере одним отличным от нуля целочисленным решением (см. также В. Шмидт [146 j]).

Круговой метод Харди — Литтлвуда в определенном смысле сводит вопрос о разрешимости системы диофантовых уравнений в целых числах к вопросу о разрешимости соответствующей системы сравнений по всем простым модулям. Отчасти поэтому в двадцатых годах нашего столетия возродился интерес к алгебраическим сравнениям и их обобщениям — уравнениям над конечными полями. Изучение таких уравнений методами алгебраической геометрии привело к необходимости их дальнейшей арифметизации и завершилось созданием в «Основаниях» А. Вейля [23 с] алгебро-геометрических принципов исследования решений систем диофантовых уравнений над произвольными полями. Полученные им на этом пути результаты о числе рациональных точек алгебраических кривых, определенных над конечными полями, привели к интересным арифметическим следствиям, касающимся оценок рациональных тригонометрических сумм и сумм характеров (см. комментарии к гл. I и II). Лишь недавно результаты А. Вейля удалось доказать элементарно, опираясь исключительно на классические понятия и методы теории чисел (см. гл. I и V).

Тридцатые годы ознаменовались крупными успехами математической логики в направлении формализации математики. Разработка точного понятия алгоритма привела к обнаружению алгоритмически неразрешимых проблем и открыла возможность для решения знаменитой 10-й проблемы Гильберта о существовании финитного способа, позволяющего определить, разрешимо или не разрешимо в целых числах произвольно заданное диофантово уравнение с целыми коэффициентами. Полученный в 1970 г. Ю. В. Матиясевичем [82 а] результат о совпадении диофантовых и перечислимых множеств привел к отрицательному решению

этой проблемы и дал ясное представление о тех трудностях, с которыми связано изучение общих диофантовых уравнений (см. [41, 81d]).

Разработка понятия алгоритма внесла в теорию диофантовых уравнений еще один новый момент — вопрос об эффективном перечислении множества всех решений изучаемого уравнения. Многие из методов теории диофантовых уравнений (в том числе и метод А. Туэ) обладают тем недостатком, что позволяют установить лишь конечность числа целочисленных решений определенного класса уравнений (и даже дать границу для этого числа), но не позволяют указать границу для самих решений. Начиная с шестидесятых годов в теории диофантовых уравнений интенсивно разрабатывается эффективный метод, основанный на использовании нижних оценок для модуля линейных форм от логарифмов алгебраических чисел (см. гл. VI). К настоящему времени этим методом получены эффективные границы для целочисленных решений целого ряда классических диофантовых уравнений, в том числе для уравнения Туэ, уравнения Туэ — Малера, гиперэллиптического уравнения и уравнения Каталана.

В самые последние годы пальма первенства при решении трудных задач теории диофантовых уравнений снова перешла к алгебраической геометрии. Построение этальной топологии и разработка теории этальных когомологий привели П. Делиня к доказательству справедливости «гипотезы Римана» для дзета-функции А. Вейля алгебраических многообразий над конечными полями (см. § 1 гл. V). Дальнейшее развитие теории абелевых многообразий и многообразий модулей кривых увенчалось замечательным результатом Г. Фалтингса, доказавшего знаменитую гипотезу Морделла о конечности числа рациональных точек на кривых рода $g > 1$. Оба результата являются, несомненно, наиболее выдающимися достижениями математики XX в. Однако математический аппарат, используемый для доказательства этих результатов, настолько объемен и сложен, что всякое более или менее доступное их изложение возможно в наши дни лишь на уровне разъяснения исходных идей и освещения основных этапов рассуждений (см. обзор Катца [60b] и дополнение Ю. Г. Зархина, А. Н. Паршина к книге С. Ленга «Основы диофантовой геометрии» [70h].

Первые две главы книги посвящены систематическому изложению теории уравнений над конечными полями, а также приложениям результатов этой теории к оценкам сумм характеров и к вопросу о распределении квадратичных вычетов и невычетов.

Основными результатами третьей, четвертой и пятой глав являются соответственно теорема Морделла о конечности ранга эллиптической кривой над полем рациональных чисел, теорема Римана — Роха для кривых и базирующееся на ее использовании доказательство теоремы А. Вейля о числе рациональных точек абсолютно неприводимой кривой над конечным полем. Теория

алгебраических кривых изложена с арифметической точки зрения, развитой в монографиях Шевалле [145b], Дойринга [46b] и в лекциях Г. И. Перельмутера.

В шестой и седьмой главах книги излагается «нестандартное» доказательство теоремы Зигеля — Малера о конечности числа квазицелых точек кривой рода $g \geqslant 1$ над полем алгебраических чисел.

Для понимания основного текста книги требуется знакомство с теорией Галуа в объеме «Алгебры» С. Ленга [70 d] и с теорией делимости в полях алгебраических чисел в объеме «Теории чисел» З. И. Боревича, И. Р. Шафаревича [19]. Необходимые сведения из алгебраической геометрии, математической логики и теории диофантовых приближений приведены по мере изложения основного материала. Задачи рассчитаны на активно работающего читателя.

В книге использованы следующие обозначения: $\mathbb{Z}$ — кольцо целых чисел, $\mathbb{N}$ — множество неотрицательных целых чисел; $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ — поля рациональных, действительных и комплексных чисел; $\mathbb{Q}_p$ — поле p-адических чисел; $\mathbb{Z}_p$ — кольцо целых p-адических чисел; F_q — конечное поле характеристики $p > 0$; $\log a$ — логарифм числа $a > 0$ по основанию e ($e = 2{,}718281\ldots$ — неперово число). Знак $\subset$ употребляется для обозначения как строгого, так и нестрогого теоретико-множественного включения (в случаях, приводящих к недоразумениям, точный смысл знака $\subset$ оговаривается особо). Остальные обозначения вводятся по ходу изложения материала.

ГЛАВА I

УРАВНЕНИЯ НАД КОНЕЧНЫМИ ПОЛЯМИ

§ 1. Сравнения

Возникновение теории сравнений тесно связано с изучением диофантовых уравнений. Эта связь основана на том простом факте, что если неопределенное уравнение

$$f(x_1, \ldots, x_n) = 0, \tag{1}$$

где f — многочлен с целыми коэффициентами, имеет целочисленное решение $(x_1, \ldots, x_n)$, то соответствующее ему сравнение

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{m} \tag{2}$$

разрешимо для любого модуля m.

Пример 1. Покажем, что целое число вида $4k+3$ нельзя представить суммой двух квадратов целых чисел. Действительно, если бы это было возможно, то было бы разрешимо сравнение

$$x^2 + y^2 \equiv 3 \pmod{4}.$$

Простая проверка показывает, что последнее сравнение не имеет решений, и мы приходим к противоречию.

Во многих случаях оказывается, что локальная разрешимость, т. е. разрешимость сравнения (2) по некоторым модулям m, является также и достаточным условием для разрешимости диофантова уравнения (1).

Пример 2. Справедлива следующая теорема, доказанная Лежандром: *если a, b и c — попарно взаимно простые положительные целые числа, свободные от квадратов, то неопределенное уравнение*

$$ax^2 + by^2 - cz^2 = 0$$

нетривиальным образом разрешимо в целых числах x, y, z тогда и только тогда, когда разрешимы сравнения

$$x^2 - bc \equiv 0 \pmod{a},$$
$$x^2 - ac \equiv 0 \pmod{b},$$
$$x^2 + ab \equiv 0 \pmod{c}.$$

Разрешимость указанных в теореме сравнений можно установить для каждого конкретного набора чисел a, b и c хотя бы простым перебором. Следовательно, теорема Лежандра дает простой

и эффективный критерий разрешимости диофантова уравнения $ax^2 + by^2 - cz^2 = 0$ (доказательство теоремы Лежандра приведено в § 1 гл. III).

1. Основные понятия. Поставим в соответствие каждому целому числу a его остаток $r = a - mq$, $0 \leqslant r \leqslant m-1$, от деления на целое положительное число m. Если двум целым числам a и b соответствует один и тот же остаток r, то они называются *сравнимыми по модулю* m. Для обозначения сравнимости чисел a и b употребляется запись $a \equiv b \pmod m$. Ясно, что $a \equiv b \pmod m$ тогда и только тогда, когда разность $a - b$ делится на m. Если разность $a - b$ не делится на m, то числа a и b называются *несравнимыми по модулю* m; в этом случае употребляется запись $a \not\equiv b \pmod m$.

Подобно обычным равенствам сравнения можно складывать, вычитать и перемножать. Если $a \equiv b \pmod m$ и $c \equiv d \pmod m$, то $a \pm c \equiv b \pm d \pmod m$ и $ac \equiv bd \pmod m$. Действительно, если $a - b = mq$, $c - d = mt$, то $(a-b) \pm (c-d) = (q \pm t)m$. Далее, $(a-b)c = mqc$, так что $ac = bc + mqc$, и $(c-d)b = mtb$, так что $bc = bd + mtb$. Отсюда $ac = bd + (qc + tb)m$ и, значит, $ac \equiv bd \pmod m$. В общем случае сравнения делить нельзя. Действительно, мы имеем $36 \equiv 16 \pmod{10}$, $12 \equiv 2 \pmod{10}$, но $3 \not\equiv 8 \pmod{10}$. Однако обе части сравнения можно сократить на множитель, взаимно простой с модулем.

Отношение сравнимости по модулю m является отношением эквивалентности; оно рефлексивно, так как $a \equiv a \pmod m$, симметрично, поскольку из $a \equiv b \pmod m$ следует $b \equiv a \pmod m$, и транзитивно, так как из $a \equiv b \pmod m$ и $b \equiv c \pmod m$ следует $a \equiv c \pmod m$. Тем самым отношение «$\equiv \pmod m$» разбивает множество всех целых чисел $\mathbb{Z}$ на непересекающиеся классы A, B, C, ..., состоящие из всех сравнимых между собой по модулю m целых чисел. Эти классы называются *классами вычетов по модулю* m. Очевидно, что целые числа $0, 1, \ldots, m-1$ лежат в разных классах вычетов, и так как каждое целое число сравнимо по модулю m с одним из этих чисел, то имеется ровно m классов вычетов по модулю m.

Операции сложения, вычитания и умножения сравнений индуцируют аналогичные операции на множестве классов вычетов. Пусть A и B — два класса вычетов по модулю m. Каковы бы ни были числа $a \in A$ и $b \in B$, их сумма $a + b$ всегда лежит в одном и том же однозначно определенном классе $C = A + B$, который назовем суммой классов A и B. Аналогичным образом определяется разность $A - B$ и произведение AB двух классов вычетов по модулю m. Эти классы образуют относительно сложения абелеву группу порядка m. Нулевым элементом этой группы является класс вычетов, состоящий из всех целых кратных числа m, а обратным к классу A является класс $-A$, состоящий из всех элементов класса A, взятых со знаком минус. Более того, классы

вычетов по модулю $m > 1$ образуют коммутативное кольцо. Единичным элементом служит класс E, содержащий целое число 1. Дистрибутивный закон $A(B + C) = AB + AC$ непосредственно следует из дистрибутивного закона для целых чисел.

Любое число из класса вычетов A по модулю m называется *вычетом по модулю m*. Вычет r, $0 \leqslant r \leqslant m - 1$, равный остатку от его деления на модуль m, называется *наименьшим неотрицательным вычетом*. Взяв из каждого класса вычетов по одному представителю, получим *полную систему вычетов по модулю m*. Таким образом, множество из m целых чисел образует полную систему вычетов по модулю m тогда и только тогда, когда его элементы несравнимы друг с другом по модулю m. Чаще всего в качестве полной системы вычетов употребляются наименьшие неотрицательные вычеты $0, 1, \ldots, m - 1$.

Классы вычетов по модулю m, элементы которых взаимно просты с m, назовем *приведенными классами вычетов*. Взяв из каждого такого класса по одному вычету, получим *приведенную систему вычетов по модулю m*. Приведенную систему вычетов можно составить из чисел полной системы вычетов $0, 1, \ldots, m - 1$, взаимно простых с модулем m. Следовательно, приведенная система вычетов по модулю m состоит из $\varphi(m)$ элементов, где $\varphi(m)$ — *функция Эйлера*, равная количеству неотрицательных целых чисел, меньших m и взаимно простых с m.

Пусть $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ — многочлен с целыми коэффициентами. *Решением сравнения* $f(x) \equiv 0 \pmod m$ назовем всякий класс вычетов $x \equiv x_0 \pmod m$, для которого целое число x_0 удовлетворяет условию $f(x_0) \equiv 0 \pmod m$.

Обозначим (a, b) наибольший общий делитель целых чисел a и b. Если $(a, m) = 1$ и x пробегает приведенную систему вычетов по модулю m, то ax также пробегает приведенную систему вычетов по модулю m. Действительно, чисел ax столько же, сколько и чисел x, т. е. $\varphi(m)$. Далее, числа ax несравнимы между собой по модулю m и взаимно просты с m. Следовательно, сравнение $ax \equiv 1 \pmod m$ имеет единственное решение $x \equiv x_0 \pmod m$ такое, что $(x_0, m) = 1$. Другими словами, если A, X — приведенные классы вычетов и E — класс вычетов, содержащий число 1, то уравнение $AX = E$ разрешимо. Таким образом, каждый приведенный класс обратим и тем самым приведенные классы вычетов по модулю m образуют по умножению абелеву группу порядка $\varphi(m)$, единичным элементом которой является класс E. Далее, если $(a, m) = 1$ и x пробегает приведенную систему вычетов, состоящую из наименьших неотрицательных вычетов $r_1, r_2, \ldots, r_{\varphi(m)}$, то наименьшие неотрицательные вычеты ax состоят из тех же чисел $r_1, r_2, \ldots, r_{\varphi(m)}$. Следовательно,

$$\prod_{j=1}^{\varphi(m)} r_j \equiv \prod_{j=1}^{\varphi(m)} ar_j \pmod m$$