МАТЕМАТИЧЕСКАЯ
ЛОГИКА
И ОСНОВАНИЯ
МАТЕМАТИКИ

Ю.В.МАТИЯСЕВИЧ

ДЕСЯТАЯ ПРОБЛЕМА ГИЛЬБЕРТА

Москва
Издательская фирма
«Физико-математическая литература»
ВО «Наука»
1 9 9 3

ПРЕДИСЛОВИЕ

На Втором Международном конгрессе математиков в Париже Давид Гильберт [1900] сделал свой знаменитый доклад «Математические проблемы», содержащий 23 проблемы или, точнее, 23 группы родственных проблем, которые 19-й век оставлял в наследие 20-му. Проблема под номером десять была посвящена диофантовым уравнениям.

10. ЗАДАЧА О РАЗРЕШИМОСТИ ДИОФАНТОВА УРАВНЕНИЯ.

> Пусть задано диофантово уравнение с произвольными неизвестными и целыми рациональными числовыми коэффициентами. *Указать способ, при помощи которого возможно после конечного числа операций установить, разрешимо ли это уравнение в целых рациональных числах.*

Под «способом», который предлагает найти Д. Гильберт, в настоящее время подразумевают «алгоритм». В начале века, когда проблемы формулировались, ещё не было математически строго общего понятия алгоритма. Отсутствие такого понятия не могло само по себе служить препятствием к положительному решению 10-й проблемы Гильберта, поскольку про конкретные алгоритмы всегда было ясно, что они действительно дают требуемый общий способ решения соответствующих проблем.

В 30-е годы в работах К. Гёделя, А. Чёрча, А. М. Тьюринга и других логиков было выработано строгое общее понятие алгоритма, которое дало принципиальную возможность устанавливать алгоритмическую неразрешимость, т. е. доказывать невозможность алгоритма с требуемыми свойствами. Тогда же были найдены первые примеры алгоритмически неразрешимых проблем, сначала в самой математической логике, а затем и в других разделах математики.

Таким образом, теория алгоритмов создала необходимые предпосылки для попыток доказать неразрешимость 10-й проблемы Гильберта. Первые работы в этом направлении были опубликованы в начале 50-х годов, а в 1970 году исследования завершились «отрицательным решением» 10-й проблемы Гильберта.

В случае 10-й проблемы Гильберта, как и в случае других проблем, долго ожидавших своего решения, не меньшее, а пожалуй, большее значение имеет математический аппарат, развитый для решения проблемы и находящий затем другие приложения, порой неожиданные. Основной технический результат, полученный при доказательстве неразрешимости 10-й проблемы Гильберта — это теорема о совпадении класса *диофантовых множеств* и класса *перечислимых множеств*. В качестве одного из следствий этой теоремы, формулировка которого не содержит специальных терминов, приведем следующее: *можно явно указать полином от многих переменных с целыми коэффициентами такой, что множество всех его положительных значений, принимаемых при целочисленных значениях переменных, есть в точности множество всех простых чисел.*

Настоящая книга посвящена алгоритмической неразрешимости 10-й проблемы Гильберта и родственным вопросам; многочисленные частичные результаты, полученные в направлении положительного решения 10-й проблемы Гильберта, здесь почти не рассматриваются.

Отрицательное решение 10-й проблемы Гильберта излагали (с разной степенью детализации) многие авторы, в частности: Азра [1971], Белл и Маховер [1977]. Гермес [1972, 1978], Девис [1973a, 1974]. Захаров [1970, 1986], Капланский [1977], Манин [1973, 1977], Маргенштерн [1981]. Матиясевич [1972a], Мияйлович, Маркович и Дошен [1986], Руохонен [1972, 1980], Саломаа [1985], Смориньский [1987], Сусман [1971], Такахаши [1974], Фенстад [1971], Хавел [1973], Хиросе [1973].

Одной из отличительных особенностей настоящей книги является то. что она. помимо собственно отрицательного решения 10-й проблемы Гильберта, содержит ряд приложений разработанной для этого решения техники; приложения эти в настоящее время разбросаны, в основном, по журнальным публикациям. За два десятилетия, прошедшие со времени решения проблемы, были получены многообразные упрощения и модификации первоначального доказательства. Настоящая книга также содержит ряд новых, ранее не публиковавшихся доказательств.

Естественно, что для понимания отрицательного решения 10-й проблемы Гильберта требуются знания как по теории чисел, так и по математической логике. Стремясь сделать книгу доступной для более широкой аудитории, в особенности, для начинающих математиков, автор старался ограничиться минимальными требованиями к математической подготовке читателя. В частности, у него не предполагается специальных знаний по теории алгоритмов, все необходимые понятия вводятся в книге, которая, тем самым, может служить для первоначального знакомства с этим увлекательным предметом (конечно, эта книга не может служить для систематического изучения даже основ теории алгоритмов). Немногочисленные требуемые сведения по теории чисел, выходящие за рамки общематематической подготовки, приведены в *приложениях* в конце книги.

Книга снабжена многочисленными *упражнениями* различной сложности — от совершенно элементарных до составляющих предмет небольшого исследования. Цель упражнений — ознакомить читателя с многообразными результатами, не приводя их доказательств. Вопрос о том, что следует отнести к основному содержанию книги, излагаемому с полным доказательством, а что — к упражнениям, естественно, решался субъективно. В упражнения попадали, в частности, результаты, которые требовали специальных знаний или имели громоздкие доказательства, результаты, далекие, по-видимому, от окончательных или представляющие ограниченный интерес. Упражнения снабжены указаниями к решению и/или отсылкой к литературному источнику.

Помимо упражнений в книгу включены немногочисленные открытые вопросы и нерешённые проблемы. Деление опять-таки субъективное. Открытый вопрос, возможно, не закрыт до сих пор лишь из-за того, что никто серьёзно над ним не задумывался, и ответ на открытый вопрос, быть может, окажется малополезным. С другой стороны, нерешённые проблемы, приведённые в книге, привлекали многих серьёзных исследователей, и, возможно, решение этих проблем потребует десятилетий.

Каждая глава завершается комментариями, в которых излагается история получения соответствующих результатов. Это представляется необходимым, поскольку логический порядок изложения материала, использованный в книге, часто не соответствует хронологическому порядку получения соответствующих результатов.

Список литературы содержит все основные публикации, нацеленные на получение отрицательного решения 10-й проблемы Гильберта, и большинство публикаций, использующих разработанную для этого технику. Автор будет признателен за указания на относящиеся к этой тематике работы, не вошедшие в этот список.

Нумерация формул в каждом параграфе своя. При ссылке на выделенную формулу из другого параграфа к номеру формулы добавляется номер параграфа, например, формула (5.3) — это формула (3) из пятого параграфа той же главы. Аналогично, формула (2.4.6) — это формула (6) из § 2.4, т. е. четвёртого параграфа главы 2.

Книгу не обязательно читать последовательно. Её можно условно разбить на две части. Первая часть, в которой даётся решение 10-й проблемы Гильберта, состоит из глав 1-5. Приведённая ниже диаграмма показывает зависимость друг от друга параграфов первой части: чтение каждого параграфа предполагает знакомство с теми параграфами, которые на диаграмме расположены не ниже и не правее него.

					§ 5.1		
					§ 5.2		
§ 1.1							
§ 1.2							
§ 1.3							
§ 1.4							
§ 1.5				§ 3.1	§ 5.3	§ 5.4	
	§ 1.6	§ 2.1					
		§ 2.2					
		§ 2.3					
		§ 2.4					
		§ 2.5					
§ 3.1	§ 3.2	§ 3.3	§ 3.4				
			§ 3.5	§ 3.6	§ 5.5		
§ 4.1							
§ 4.2		§ 4.3	§ 4.4				
			§ 4.5				
			§ 4.6			§ 5.6	
						§ 5.7	

Аналогично, следующая диаграмма показывает зависимость параграфов второй части, посвященной приложениям, от параграфов первой части.

§ 2.1	§ 2.4	§ 3.4	§ 5.4	§ 5.5	§ 5.7	§ 7.1	§ 7.2
§ 7.3	§ 6.4	§ 6.2		§ 6.1	§ 9.1	§ 9.2	§ 9.3
§ 7.4		§ 6.3			§ 10.1	§ 10.2	

Между собой параграфы второй части связаны слабо. В § 6.1-6.3 приведены три разных способа для достижения одной и той же цели; достаточно знать любой из них для чтения § 6.4-6.6 и § 9.1. Аналогично, в § 4.5 и § 6.5 приведены две разные конструкции универсальных уравнений, и знакомства с любой из них достаточно для чтения § 6.6 и § 8.1. Чтение § 8.2 предполагает знакомство с § 7.2, которое в свою очередь предполагает знание § 6.2-6.3; в § 9.4 используются результаты § 9.2, а в § 10.1 — результаты § 6.6.

Глава 1
ОСНОВНЫЕ ПОНЯТИЯ

В этой главе будет введено основное понятие, изучаемое в данной книге, — понятие диофантова множества, и будут установлены его простейшие свойства.

§ 1.1. Разрешимость диофантовых уравнений как массовая проблема

Напомним, что диофантовыми уравнениями называют уравнения вида

$$D(x_1, \ldots, x_m) = 0, \tag{1}$$

где D — полином с целыми коэффициентами. Наряду с (1)) диофантово уравнение может быть записано в более общем виде

$$D_L(x_1, \ldots, x_m) = D_R(x_1, \ldots, x_m), \tag{2}$$

где D_L и D_R также являются полиномами с целыми коэффициентами. Говоря о «произвольном диофантовом уравнении», мы будем иметь в виду уравнение типа (1), поскольку уравнение типа (2) легко приводится к виду (1) перенесением всех членов в левую часть. С другой стороны, выписывая конкретные уравнения, мы часто будем использовать запись вида (2), если она легче для восприятия. Другое преимущество более общей записи вида (2), которым мы будем пользоваться, состоит в том, что, записывая уравнение в виде (2), мы можем потребовать, чтобы D_L и D_R были полиномами с неотрицательными коэффициентами.

Поскольку диофантовы уравнения, как правило, имеют много неизвестных, следует различать *степень уравнения* (1) *относительно данной неизвестной* x_i и *(полную) степень уравнения* (1), под которой мы будем подразумевать максимальную суммарную (по всем неизвестным) степень одночленов, составляющих полином D.

Существенной характеристикой диофантовых уравнений является не только их вид (1), но и множество допустимых значений неизвестных. Гильберт в 10-й проблеме говорит о решениях в *целых рациональных числах*. В этой книге мы будем говорить просто о *целых числах*, поскольку *целые алгебраические числа* в ней почти не будут рассматриваться. (Вопросы о разрешимости диофантовых уравнений в других типах неизвестных рассматриваются в § 1.3, 7.3, 7.4.)

Десятая проблема Гильберта является примером *массовой проблемы*. Массовая проблема — это проблема, состоящая из счётного множества *индивидуальных проблем*, на каждую из которых надо дать конкретный ответ «ДА» или «НЕТ». Эти индивидуальные проблемы мы будем называть *подпроблемами* соответствующей массовой проблемы. Каждая индивидуальная проблема специфицируется конечным объёмом информации (в случае 10-й проблемы Гильберта такой информацией является полином D из (1)). Суть массовой проблемы состоит в том, что требуется найти единый метод, пригодный для получения ответа на любую из её индивидуальных подпроблем. Со времени Диофанта специалисты по теории чисел нашли решения огромного количества диофантовых уравнений и установили отсутствие решений у массы других уравнений, однако при этом для разных классов уравнений или даже отдельных уравнений приходилось изобретать свой особый метод. Д. Гильберт в 10-й проблеме предлагал найти *универсальный метод* для распознавания разрешимости диофантовых уравнений.

Решение массовой проблемы может быть либо прямым — посредством указания процедуры нахождения ответа для каждой индивидуальной подпроблемы, либо косвенным — путем сведения данной массовой проблемы к другой массовой проблеме, решение которой

уже известно. Мы не будем давать формального определения сведения, поскольку общая теория сводимости нам не потребуется, а в конкретных случаях сведения одной массовой проблемы к другой из контекста будет ясно, что имеется в виду.

Установление неразрешимости данной массовой проблемы тоже может быть либо прямым, либо косвенным. При косвенном доказательстве мы также сводим одну проблему к другой, но это сведение производится в другую сторону — чтобы установить неразрешимость некоторой массовой проблемы, надо к ней свести другую массовую проблему, неразрешимость которой уже установлена. На протяжении нескольких первых глав книги мы будем сводить к 10-й проблеме Гильберта все более и более сложные проблемы. Эта цепочка сведений должна в конце концов оборваться на проблеме, для которой мы даём прямое доказательство неразрешимости. Чтобы дать такое доказательство, мы должны суметь каким-то образом обозреть все мыслимые способы решения проблемы. Принципиальная возможность сделать это появилась после выработки математически строгого общего понятия алгоритма. Соответствующие определения будут даны в главе 5, где и будет установлена алгоритмическая неразрешимость 10-й проблемы Гильберта.

§ 1.2. Системы диофантовых уравнений

В 10-й проблеме Гильберт спрашивал про способ для установления существования или отсутствия решений лишь у отдельных диофантовых уравнений, хотя сам Диофант рассматривал и системы уравнений. Легко, однако, понять, что положительное решение 10-й проблемы Гильберта давало бы нам также способ узнавать наличие или отсутствие решений и у произвольных систем диофантовых уравнений. Действительно, система из k диофантовых уравнений

$$\begin{aligned} &D_1(x_1,\ldots,x_m)=0\\ &\ldots\ldots\ldots\ldots\ldots\\ &D_k(x_1,\ldots,x_m)=0 \end{aligned} \tag{1}$$

имеет решение в целых $x_1,\ldots,x_m$ тогда и только тогда, когда имеет решение диофантово уравнение

$$D_1^2(x_1,\ldots,x_m)+\cdots+D_k^2(x_1,\ldots,x_m)=0; \tag{2}$$

более того, множества решений у (1) и (2) совпадают. Таким образом, для систем диофантовых уравнений количество уравнений не является такой существенной характеристикой, как в случае систем линейных алгебраических или дифференциальных уравнений.

В дальнейшем мы будем пользоваться и обратной возможностью — преобразованием диофантова уравнения

$$D(x_1,\ldots,x_m)=0; \tag{3}$$

в некоторую систему диофантовых уравнений

$$\begin{aligned} &D_1(x_1,\ldots,x_m,y_1,\ldots,y_l)=0\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ &D_k(x_1,\ldots,x_m,y_1,\ldots,y_l)=0 \end{aligned} \tag{4}$$

имеющую, быть может, дополнительные неизвестные $y_1,\ldots,y_l$. Переход от (3) и (4) не обязательно является обратным преобразованием к переходу от (1) к (2) — если систему

(4) свернуть описанным выше способом в одно диофантово уравнение, то этим уравнением окажется, вообще говоря, отнюдь не исходное уравнение (3). Единственная связь между (3) и (4), которая будет нас интересовать, такова: уравнение (3) должно иметь решение в том и только том случае, когда имеется решение у системы (4). При этом не требуется ни чтобы каждое решение уравнения (3) было продолжимо (посредством выбора значений $y_1, \dots, y_l$) до какого-то решения системы (4), ни чтобы каждое решение системы (4) содержало решение уравнения (3).

Цель перехода от уравнения (3) к эквивалентной по разрешимости системе (4) может состоять в том, чтобы получить систему, в которой каждое отдельное уравнение было бы очень простым. Например, легко понять, что любое диофантово уравнение можно преобразовать в эквивалентную в описанном выше смысле систему, состоящую из уравнений двух типов

$$\alpha = \beta + \gamma \tag{5}$$

и

$$\alpha = \beta\gamma \tag{6}$$

где α, β и γ - конкретные натуральные числа или какие-то из неизвестных $x_1, \dots, x_m$, $y_1, \dots, y_l$. Проиллюстрируем такое преобразование на примере уравнения

$$4x^3y - 2x^2z^3 - 3y^2x + 5z = 0. \tag{7}$$

Сначала мы избавимся от вычитаний и получим уравнение

$$4x^3y + 5z = 2x^2z^3 + 3y^2x. \tag{8}$$

Затем введём 14 новых переменных и получим эквивалентную систему

$$\begin{gathered} p_1 = 4x, \quad p_2 = p_1x, \quad p_3 = p_2x, \quad p_4 = p_3y; \\ q_1 = 5z; \\ r_1 = 2x, \quad r_2 = r_1x, \quad r_3 = r_2z, \quad r_4 = r_3z, \quad r_5 = r_4z; \\ s_1 = 3y, \quad s_2 = s_1y; \\ t_1 = p_4 + q, \quad u_1 = r_5 + s_2, \quad t_1 = lu_1. \end{gathered} \tag{9}$$

В качестве примера применения этой несложной техники преобразования уравнений посмотрим, что получится, если сначала некоторое диофантово уравнение преобразовать в эквивалентную по разрешимости систему (1), состоящую из уравнений типа (5) и (6), а затем свернуть эту систему в одно уравнение (2). Ясно, что исходное уравнение будет иметь или не иметь решение одновременно с новым уравнением (2); смысл такого двойного преобразования состоит в том, что новое уравнение (2) будет иметь степень 4 независимо от степени исходного уравнения. Таким образом, *для положительного решения 10-й проблемы Гильберта было бы достаточно найти способ узнавать наличие или отсутствие решений у уравнений 4-й степени.*

§ 1.3. Решения в натуральных числах

В 10-й проблеме Гильберт спрашивал про решения диофантовых уравнений в целых числах. Иногда разрешимость уравнения в целых числах очевидна; например, ясно, что уравнение

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

имеет бесконечно много решений вида $x = z$, $y = -1$. В то же время тот факт, что уравнение (1) не имеет решений с неотрицательными x, y и z, весьма нетривиален. Таким образом, для конкретного диофантова уравнения *проблема распознавания наличия целочисленных решений и проблема распознавания наличия неотрицательных целочисленных решений* — это, вообще говоря, две разные массовые проблемы.

С другой стороны, пусть

$$D(x_1, \ldots, x_m) = 0 \tag{2}$$

— произвольное диофантово уравнение, и мы интересуемся наличием у него неотрицательных решений. Рассмотрим систему уравнений

$$\begin{aligned} D(x_1, \ldots, x_m) &= 0, \\ x_1 &= y_{1.1}^2 + y_{1.2}^2 + y_{1.3}^2 + y_{1.4}^2, \\ &\ldots\ldots\ldots\ldots \\ x_m &= y_{m.1}^2 + y_{m.2}^2 + y_{m.3}^2 + y_{m.4}^2. \end{aligned} \tag{3}$$

Понятно, что любое решение этой системы в произвольных целых числах содержит решение уравнения (2) в неотрицательных целых числах. Верно и обратное — для любого решения уравнения (1) в неотрицательных целых числах $x_1, \ldots, x_m$ найдутся целочисленные значения $y_{1.1}, \ldots, y_{m.4}$, дающие решение системы (3), поскольку каждое неотрицательное целое число представимо в виде суммы квадратов четырёх целых чисел (см. Приложение 1). Как мы знаем из § 1.2, система (3) может быть свёрнута в одно уравнение

$$E(x_1, \ldots, x_m, y_{1.1}, \ldots, y_{m.4}) = 0, \tag{4}$$

разрешимое в целых числах тогда и только тогда, когда исходное уравнение (2) разрешимо в неотрицательных целых числах.

Таким образом, мы показали, что *массовая проблема распознавания наличия решений в неотрицательных целых числах сводится к массовой проблеме распознавания наличия решений в целых числах*. Тем самым мы установили, что для доказательства неразрешимости 10-й проблемы Гильберта в её оригинальной постановке достаточно доказать неразрешимость её аналога, касающегося наличия или отсутствия решений в неотрицательных целых числах. По техническим причинам несколько удобнее работать с неотрицательными числами, и в дальнейшем везде, где явно не будет оговорено противное, строчные курсивные латинские буквы будут обозначать неотрицательные целые числа. По традиции, идущей от математической логики, мы будем называть такие числа *натуральными*, считая тем самым 0 натуральным числом.

Наши дальнейшие усилия будут направлены на доказательство неразрешимости аналога 10-й проблемы Гильберта для натуральных решений. Мы достигнем этой цели в главе 5, но a priori могло бы оказаться, что этот аналог разрешим, хотя проблема в исходной постановке неразрешима. Проверим, что это не так, т. е. что, ограничивая область изменения неизвестных натуральными числами, мы, в принципе, ничего не теряем.

Пусть

$$D(x_1, \ldots, x_m) = 0 \tag{5}$$

— произвольное диофантово уравнение, и мы интересуемся его решениями в целых числах $x_1, \ldots, x_m$. Рассмотрим уравнение

$$D(x_1 - y_1, \ldots, x_m - y_m) = 0. \tag{6}$$

Ясно, что любое решение уравнения (6) (в натуральных числах $x_1, \ldots, x_m$, $y_1, \ldots, y_m$, по нашему соглашению) порождает решение

$$\begin{aligned} x_1 &= x_1 - y_1 \\ &\cdots\cdots\cdots \\ x_m &= x_m - y_m \end{aligned} \tag{7}$$

уравнения (5) в целых числах $x_1, \ldots, x_m$. С другой стороны, для любого решения $x_1, \ldots, x_m$ уравнения (5) найдутся натуральные числа $x_1, \ldots, x_m$, $y_1, \ldots, y_m$, удовлетворяющие (7) и тем самым образующие решение уравнения (6).

Таким образом, мы осуществили обратное сведение — показали, что *проблема распознавания наличия целочисленных решений сводится к проблеме распознавания наличия натуральных решений*. В результате оказывается, что две эти проблемы эквивалентны как *массовые проблемы*, хотя, как обсуждалось в начале этого параграфа, для конкретного уравнения ответ может зависеть от области допустимых значений неизвестных.

§ 1.4. Диофантовы множества

Наряду с системами диофантовых уравнений в теории чисел рассматриваются также *семейства диофантовых уравнений*. Под семейством диофантовых уравнений мы понимаем равенство вида

$$D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0 \tag{1}$$

ПРИЛОЖЕНИЯ

1. Теорема о четырёх квадратах

УКАЗАНИЯ К УПРАЖНЕНИЯМ

СПИСОК ЛИТЕРАТУРЫ

Адлеман и Мандерс (Adleman L., Manders K.)

[1976] Diophantine complexity // 17th Annual Symp. on Found, of Computer Sci. (Houston, Texas, 1976). - Long Beach, Calif.: IEEE Comput. Soc - P. 81-88.

Адлер (Adler A.)

[1969а] Some recursively unsolvable problems in analysis // Proc. Amer. Math. Soc. - V. 22. N 2. - P. 523-526.

[1969б] Extentions of nonstandard models of number theory // Z. math. Logik Grundl. Math. - Bd 15, N 4. - S. 289-290.

[1969в] Existential formulas in arithmetic // Dissert. Abstrs. - V. 29, N 8. - P. 2962-2963.

[1971] A reduction of homogeneous diophantine problem // J. London Math. Soc. - V. 3. N 3. - P. 446-448.

Азра (Azra J. P.)

[1971] Relations diophantiennes et la solution negative du 10^e probleme de Hilbert // Lect. Notes Math. - V. 244. - P. 11-28.

Оглавление

Описание

Название: Десятая проблема Гильберта
Автор: Матиясевич Ю.В.
Издательство: М: Физматлит. 1993. - 224 с. - ISBN 5-02-014326-X
Рецензент: доктор физико-математических наук С.И. Адян
Аннотация: Дается полное доказательство алгоритмической неразрешимости 10-й проблемы Гильберта, касающейся диофантовых уравнений, вместе с необходимыми сведениями из теории алгоритмов и теории чисел, а также приложения развитой для этого техники к другим массовым проблемам теории чисел, алгебры, анализа, теоретического программирования.

Для математиков, в том числе аспирантов и студентов старших курсов.

Библиогр. 247 назв.