математическая
логика
и основания
математики

Ю.В.МАТИЯСЕВИЧ

ДЕСЯТАЯ ПРОБЛЕМА ГИЛЬБЕРТА

Москва
Издательская фирма
«Физико-математическая литература»
ВО «Наука»
1993

ББК 22.12
М34
УДК 510.5

Матиясевич Ю.В. Десятая проблема Гильберта. М.: Физматлит. 1993.— 224 с.—ISBN 5-02-014326-X.

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.

Рецензент
доктор физико-математических наук С.И.Адян

$М\frac{1602020000-003}{053(02)-93}$ КБ-40-1-92

© Физматлит, 1993

ISBN 5-02-014326-X

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 прило-

жения, 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 [1973а, 1974], Захаров [1970, 1986], Капланский [1977], Манин [1973, 1977], Маргенштерн [1981], Матиясевич [1972а], Мияйлович, Маркович и Дошен [1986], Руохонен [1972, 1980], Саломаа [1985], Сморинский [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, посвящённой 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 *сведéния* данной массовой проблемы к другой массовой проблеме, решение которой ужé известно. Мы не будем давать формального определения сведéния, поскольку общая теория сводимости нам не потребуется, а в конкретных случаях сведéния 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 сведéние 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 сведéний 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

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

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

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

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

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

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 $y_1,\ldots,y_l$) 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 урав-

нение 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 $x_1, \ldots, x_m$, $y_1, \ldots, y_l$. 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

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

Затем введём 14 новых переменных и получим эквивалентную систему

$$\begin{gathered} p_1 = 4x, \quad p_2 = p_1x, \quad p_3 = p_2x, \quad p_4 = p_3y; \\ q_1 = 5z; \\ r_1 = 2x, \quad r_2 = r_1x, \quad r_3 = r_2z, \quad r_4 = r_3z, \quad r_5 = r_4z; \\ s_1 = 3y, \quad s_2 = s_1y; \\ t_1 = p_4 + q_1, \quad u_1 = r_5 + s_2, \quad t_1 = 1u_1. \end{gathered} \tag{9}$$

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 неотрицатель-

ными 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

$$\begin{gathered} D(x_1,\ldots,x_m)=0, \\ x_1=y_{1,1}^2+y_{1,2}^2+y_{1,3}^2+y_{1,4}^2, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x_m=y_{m,1}^2+y_{m,2}^2+y_{m,3}^2+y_{m,4}^2. \end{gathered} \tag{3}$$

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

$$D(\chi_1,\ldots,\chi_m)=0 \tag{5}$$

— произвольное диофантово уравнение, и мы интересуемся его решениями в целых числах $\chi_1,\ldots,\chi_m$. 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

$$\begin{gathered}\chi_1=x_1-y_1,\\ \cdots\cdots\cdots\\ \chi_m=x_m-y_m\end{gathered} \tag{7}$$

уравнения (5) в целых числах $\chi_1,\ldots,\chi_m$. С другой стороны, для любого решения $\chi_1,\ldots,\chi_m$ 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 сведéние — 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 диофантóвых уравнений в теории чисел рассматриваются также *семейства диофантовых уравнений*. Под семейством диофантовых уравнений мы понимаем равенство вида

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

где D — полином с целыми коэффициентами относительно всех переменных $a_1,\ldots,a_n$, $x_1,\ldots,x_m$, которые разбиты на две части: *параметры* $a_1,\ldots,a_n$ и *неизвестные* $x_1,\ldots,x_m$. При фиксировании значений параметров получаются конкретные диофантовы уравнения, составляющие семейство. Семейство диофантовых уравнений *не* является бесконечной системой уравнений, поскольку не предполагается, что неизвестные должны удовлетворять всем уравнениям сразу, как это имеет место в случае систем уравнений. Семейства уравнений называют также *пара-*

метрическими уравнениями. У параметрических диофантовых уравнений мы будем различать *степень уравнения относительно всех неизвестных* и *степень относительно всех переменных*.

При разном выборе значений параметров получаются, вообще говоря, как уравнения, имеющие решения, так и уравнения, решений не имеющие. Параметрическое диофантово уравнение (1) определяет некоторое множество $\mathfrak{M}$, состоящее из всех таких наборов значений параметров $a_1,\ldots,a_n$, для которых существуют значения неизвестных $x_1,\ldots,x_m$, удовлетворяющие (1):

$$\langle a_1,\ldots,a_n\rangle\in\mathfrak{M} \iff \exists x_1\ldots x_m[D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0]. \qquad (2)$$

Число n при этом называется *размерностью* множества $\mathfrak{M}$, а эквивалентность (2) — его *диофантовым представлением*; допуская некоторую вольность речи, можно называть диофантовым представлением не только (2), но и (1). Множества, имеющие диофантовы представления, называют, аналогично уравнениям, *диофантовыми множествами*. Понятно, что каждое диофантово множество имеет бесконечно много диофантовых представлений.

Диофантовы множества будут основными объектами изучения в этой книге. При этом если в теории чисел исходным объектом обычно является некоторое семейство диофантовых уравнений и требуется описать в каких-то других терминах соответствующее диофантово множество, то у нас обычно будет обратная постановка задачи: *дано некоторое множество, состоящее из n-ок натуральных чисел; требуется узнать, является ли это множество диофантовым, и если является, то найти для него какое-либо диофантово представление*. Иногда диофантовость множества тривиальна, например, очевидна диофантовость множества всех чётных чисел. В других случаях установление диофантовости оказывается технически трудным и вовсе не очевидным, примером здесь может служить множество всех простых чисел, диофантовость которого будет установлена в § 3.4.

Кроме установления диофантовости или недиофантовости конкретных множеств, можно поставить вопрос о характеризации всего класса диофантовых множеств в каких-то других терминах. Такая характеризация будет дана в главе 5, что и позволит получить отрицательное решение 10-й проблемы Гильберта.

В этой главе мы установим простейшие свойства диофантовых множеств и укажем ряд примеров диофантовых множеств, важных для дальнейшего.

Нетрудно понять, что *объединение двух диофантовых множеств одинаковой размерности также диофантово*. Действительно, если

$$D_1(a_1,\ldots,a_n,x_1,\ldots,x_{m_1})=0 \qquad (3)$$

и

$$D_2(a_1,\ldots,a_n,x_1,\ldots,x_{m_2})=0 \qquad (4)$$

— диофантовы представления двух множеств, то

$$D_1(a_1,\ldots,a_n,x_1,\ldots,x_{m_1})\times D_2(a_1,\ldots,a_n,x_1,\ldots,x_{m_2})=0 \qquad (5)$$

— диофантово представление их объединения.

Пересечение двух диофантовых множеств одинаковой размерности также диофантово, а именно, определяется уравнением

$$D_1^2(a_1,\ldots,a_n,x_1,\ldots,x_{m_1})+D_2^2(a_1,\ldots,a_n,y_1,\ldots,y_{m_2})=0. \qquad (6)$$

Обратите внимание на то, что мы не просто воспользовались техникой § 1.2 для объединения уравнений (3) и (4) в одно уравнение, а предварительно изменили неизвестные в уравнении (4).

Дополнение диофантова множества n-ок натуральных чисел (до множества всех n-ок натуральных чисел) может не быть диофантовым, но этот факт далеко не тривиален и будет установлен только в § 4.6.

В определении диофантова представления (2) на вид входящего в него диофантова уравнения никаких ограничений не накладывалось. Из § 1.2 мы знаем, что можно было бы ограничиться уравнениями четвёртой степени. В дальнейшем нам потребуется другая возможность специализировать вид уравнений в диофантовых представлениях множеств натуральных чисел (т. е. в случае $n=1$). А именно, нетрудно понять, что уравнение

$$D(a,x_1,\ldots,x_m)=0 \qquad (7)$$

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

$$(x_0+1)(1-D^2(x_0,\ldots,x_m))-1=a \qquad (8)$$

имеет решение в неизвестных $x_0,\ldots,x_m$. Действительно, из любого решения уравнения (7) можно получить решение уравнения (8), полагая дополнительно $x_0=a$; с другой стороны, в любом решении уравнения сомножитель $1-D^2(x_0,\ldots,x_m)$ должен быть положительным, что возможно, лишь если $D(x_1,\ldots,x_m)=0$, а в таком случае из (8) следует, что $x_0=a$ и, значит, равенство (7) также выполнено.

Таким образом, *множество натуральных чисел является диофантовым тогда и только тогда, когда оно является множеством всех натуральных значений, принимаемых некоторым полиномом с целыми коэффициентами при натуральных значениях переменных.*

§ 1.5. Логическая терминология

Весь материал настоящей книги мог бы быть изложен в терминах диофантовых множеств, операций пересечения и объединения множеств и отношения принадлежности числа множеству.

Тем не менее часто вместо языка множеств удобнее использовать ему эквивалентный, по существу, язык свойств и отношений между числами. Например, вместо того, чтобы говорить о принадлежности к диофантову множеству чётных чисел, можно говорить о диофантовости свойства *быть чётным числом*. Аналогично, вместо того, чтобы говорить, скажем, о диофантовом множестве с представлением

$$(a_1 - a_2)^2 = x+1, \tag{1}$$

можно говорить о диофантовости отношения $\neq$.

Формально мы говорим, что свойство $\mathcal{P}$ натуральных чисел является *диофантовым свойством*, если диофантовым является множество всех чисел, обладающих свойством $\mathcal{P}$; соответственно эквивалентность вида

$$\mathcal{P}(a) \Leftrightarrow \exists x_1 \ldots x_m [D(a, x_1, \ldots, x_m) = 0] \tag{2}$$

называется *диофантовым представлением свойства* $\mathcal{P}$. Аналогично, отношение $\mathcal{R}$ между n натуральными числами называется *диофантовым отношением*, если диофантовым является множество всех n-ок натуральных чисел, находящихся в отношении $\mathcal{R}$; соответственно эквивалентность вида

$$\mathcal{R}(a_1, \ldots, a_n) \Leftrightarrow \exists x_1 \ldots x_m [D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0] \tag{3}$$

называется *диофантовым представлением отношения* $\mathcal{R}$.

Объединению множеств в этой терминологии соответствует построение нового свойства или отношения с помощью логической операции «ИЛИ» (дизъюнкции). Иными словами, если $\mathcal{R}_1$ и $\mathcal{R}_2$ — два диофантовых отношения (или свойства), то отношение (свойство) $\mathcal{R}$ такое, что для всех $a_1, \ldots, a_n$

$$\mathcal{R}(a_1, \ldots, a_n) \Leftrightarrow \mathcal{R}_1(a_1, \ldots, a_n) \vee \mathcal{R}_2(a_1, \ldots, a_n), \tag{4}$$

также является диофантовым. Формально для обоснования диофантовости $\mathcal{R}$ мы должны были бы взять какие-то диофантовы представления (4.3) и (4.4) отношений $\mathcal{R}_1$ и $\mathcal{R}_2$ и построить из них диофантово представление (4.5) отношения $\mathcal{R}$. Обычно этот шаг будет опускаться, и для обоснования диофантовости $\mathcal{R}$ мы будем ограничиваться получением эквивалентности типа (4), считая её обобщенным диофантовым представлением отношения $\mathcal{R}$, если диофантовость $\mathcal{R}_1$ и $\mathcal{R}_2$ была установлена ранее.

Аналогично, пересечению множеств соответствует логическая операция «И» (конъюнкция), и эквивалентность типа

$$\mathcal{R}(a_1, \ldots, a_n) \Leftrightarrow \mathcal{R}_1(a_1, \ldots, a_n) \,\&\, \mathcal{R}_2(a_1, \ldots, a_n) \tag{5}$$

также будет рассматриваться как обобщённое диофантово представление отношения $\mathcal{R}$, если диофантовость $\mathcal{R}_1$ и $\mathcal{R}_2$ уже была установлена.

Понятно, что по этому пути мы можем пойти и дальше, считая обобщённым диофантовым представлением множества, свойства или отношения любую формулу, построенную из параметрических диофантовых уравнений с использованием в произвольном порядке дизъюнкции, конъюнкции и квантора существования. Примеры таких формул будут приведены в следующем параграфе. При необходимости все такие представления могут быть приведены к каноническому виду (4.2), (2) или (3).

Ещё одно средство, облегчающее установление диофантовости, состоит в введении понятия *диофантовой функции* как функции, график которой является диофантовым множеством. Соответственно *диофантовым представлением функции* F будет эквивалентность типа

$$a = F(b_1,\dots,b_n) \Leftrightarrow \exists x_1\dots x_m[D(a,b_1,\dots,b_n,x_1,\dots,x_m)=0], \tag{6}$$

где D — полином с целыми коэффициентами. Мы можем теперь рассматривать наравне с диофантовыми уравнениями и уравнения вида

$$P(\mathrm{t}_1,\dots,\mathrm{t}_k)=0, \tag{7}$$

где P — полином с целыми коэффициентами, а $\mathrm{t}_1,\dots,\mathrm{t}_k$ — *диофантовы термы*, т. е. выражения, построенные по обычным правилам из конкретных натуральных чисел, переменных, знаков "+", "−", "×" и символов диофантовых функций. Подобно переходу от (2.7) к (2.9), уравнение (7) может быть преобразовано (ценой введения новых неизвестных) в эквивалентную систему, состоящую из уравнений типов (2.5) и (2.6) и типа

$$\alpha = F(\beta_1,\dots,\beta_n), \tag{8}$$

где F — диофантова функция, а α и $\beta_1,\dots,\beta_n$ — переменные или конкретные натуральные числа. Каждое уравнение типа (8) можно затем заменить на копию уравнения из (6), подставив α вместо a, $\beta_1,\dots,\beta_n$ вместо $b_1,\dots,b_n$ и новые, ещё не использованные переменные вместо $x_1,\dots,x_m$. Полученная система может быть затем свернута в одно уравнение, эквивалентное (7).

Аналогично мы можем разрешить использовать произвольные диофантовы термы в качестве аргументов диофантовых отношений в обобщенных диофантовых представлениях. Действительно, если $\mathcal{R}$ — некоторое диофантово отношение, то утверждение

$$\mathcal{R}(\mathrm{t}_1,\dots,\mathrm{t}_n) \tag{9}$$

эквивалентно утверждению

$$\exists t_1\dots t_n[\mathcal{R}(t_1,\dots,t_n)\,\&\,t_1=\mathrm{t}_1\,\&\ \dots\ \&\,t_n=\mathrm{t}_n]. \tag{10}$$

Первый конъюнктивный член в (10) можно заменить на копию уравнения из (3), а остальные преобразовать так же, как (7).

Диофантова функция может быть определена не при всех значениях аргументов. Добавляя уравнение (8), мы налагаем требование определённости F для $\beta_1,\ldots,\beta_n$. По этой причине, например, формула

$$F(a_1,\ldots,a_n)=0 \vee F(a_1,\ldots,a_n)\neq 0 \tag{11}$$

не является обобщённым диофантовым представлением тождественно истинного отношения, если F не является всюду определённой функцией.

Отметим, что в отличие от диофантовых представлений, обобщённые диофантовы представления не являются строгим математическим понятием, поскольку отражают не только объективные качества множеств, свойств, отношений и функций, но и тот зависящий от нас порядок, в котором мы устанавливаем их диофантовость. Например, мы можем сначала установить диофантовость свойства *быть чётным числом*:

$$\mathbf{Even}(a) \Leftrightarrow \exists x[2x=a], \tag{12}$$

а затем указать обобщённое диофантово представление для свойства *быть нечётным числом*:

$$\mathbf{Odd}(a) \Leftrightarrow \mathbf{Even}(a+1), \tag{13}$$

или, наоборот, сначала дать прямое доказательство диофантовости **Odd** на основе представления

$$\mathbf{Odd}(a) \Leftrightarrow \exists x[2x+1=a], \tag{14}$$

а затем уже установить диофантовость **Even** с помощью обобщённого диофантова представления

$$\mathbf{Even}(a) \Leftrightarrow \mathbf{Odd}(a+1). \tag{15}$$

Мы не можем, однако, *одновременно* рассматривать оба представления (13) и (15) как обобщённые диофантовы.

§ 1.6. Простейшие примеры диофантовых множеств, свойств, отношений и функций

Диофантовость отношения $\neq$ была продемонстрирована представлением (5.1). Аналогично устанавливается диофантовость неравенств $\leq$ и $<$:

$$a\leq b \Leftrightarrow \exists x[a+x=b], \tag{1}$$

$$a<b \Leftrightarrow \exists x[a+x+1=b]. \tag{2}$$

Диофантовость отношения делимости

$$a\,|\,b \Leftrightarrow \exists x[ax=b] \tag{3}$$

позволяет дать следующее обобщённое диофантово представление функции $\mathbf{rem}(b,c)$ — *остаток от деления* b *на* c:

$$a=\mathbf{rem}(b,c) \Leftrightarrow a<c \;\&\; c\,|\,b-a. \tag{4}$$

В § 2.2 нам потребуется функция **arem**, дающая минимальную абсолютную величину вычета по модулю:

$$\mathbf{arem}(b,c) \equiv \pm b(\mathbf{mod}\ c)\ \&\ 0 \le \mathbf{arem}(b,c) \le c/2. \tag{5}$$

Эта функция также диофантова, ибо

$$a = \mathbf{arem}(b,c) \iff 2a \le c\ \&\ [c \mid b-a \vee c \mid b+a]. \tag{6}$$

Нам потребуется также диофантовость отношения неделимости:

$$a \nmid b \iff \mathbf{rem}(b,a) > 0. \tag{7}$$

Обратите внимание, что введённое так отношение $\nmid$ не является отрицанием отношения делимости $\mid$, ибо согласно (3) и (7) оба отношения ложны, если $a = 0$ и $b > 0$. Этот «недостаток» можно было бы легко устранить, но на самом деле мы будем использовать отношение $\nmid$ только в таких случаях, когда первый аргумент заведомо отличен от нуля.

Установив диофантовость **rem**, мы можем дать обобщённое диофантово представление функции $b\ \mathbf{div}\ c$ — *целая часть от деления b на c*:

$$a = b\ \mathbf{div}\ c \iff ac + \mathbf{rem}(b,c) = b \tag{8}$$

и обобщённое диофантово представление трёхместного отношения сравнимости по положительному модулю:

$$a \equiv b(\mathbf{mod}\ c) \iff \mathbf{rem}(a,c) = \mathbf{rem}(b,c). \tag{9}$$

Известно, что $\mathbf{GCD}(b,c)$ — *наибольший общий делитель положительных целых чисел b и c* — представим в виде $bx-cy$; ясно также, что любое число такого вида делится на $\mathbf{GCD}(b,c)$, откуда получаем следующее обобщённое диофантово представление функции **GCD**:

$$a = \mathbf{GCD}(b,c) \iff bc > 0\ \&\ a \mid b\ \&\ a \mid c\ \&\ \exists xy[a = bx-cy]. \tag{10}$$

Наконец, диофантовость **GCD** позволяет установить диофантовость функции $\mathbf{LCM}(b,c)$ — *наименьшее общее кратное положительных чисел b и c*:

$$a = \mathbf{LCM}(b,c) \iff bc = a\mathbf{GCD}(b,c). \tag{11}$$

Упражнения

1.1. В § 1.3 установлена эквивалентность двух массовых проблем, касающихся решений диофантовых уравнений в целых числах и в натуральных числах. Покажите, что им эквивалентна аналогичная проблема, касающаяся решений в положительных целых числах.

1.2. Переход от уравнения (3.2) к системе (3.3) приводит к пятикратному увеличению количества неизвестных. Неизвестные $x_1, \ldots, x_m$ можно устранить, используя их явные выражения через $y_{1,1}, \ldots, y_{m,4}$, что даст

только четырёхкратный рост количества неизвестных. Предложите другие способы, дающие ещё меньшее возрастание количества неизвестных.

1.3. Переход от уравнения (3.5) к уравнению (3.6) приводит к двукратному увеличению количества неизвестных. Покажите, что вопрос о разрешимости (3.5) в целых числах можно свести к вопросу о разрешимости в натуральных числах некоторого диофантова уравнения также с m неизвестными.

1.4. Уравнение (4.7) эквивалентно уравнению (4.8) только при нашем соглашении о том, что параметр a и неизвестные — натуральные числа. Покажите, что множество натуральных чисел является диофантовым тогда и только тогда, когда оно является множеством всех натуральных значений, принимаемых некоторым полиномом с целыми коэффициентами при *целочисленных* значениях переменных.

1.5. Легко видеть, что любое конечное множество является диофантовым, но никакое конечное множество, содержащее более одного элемента, не представимо как множество *всех* значений, принимаемых полиномом с целыми коэффициентами при натуральных (или целочисленных) значениях неизвестных. В качестве менее тривиального примера покажите, что в таком виде не представимо никакое более чем одночленное множество, состоящее только из простых чисел, даже если считать простыми числа -2, -3, $-5, \ldots$ (диофантовость множества всех простых чисел будет установлена в § 3.4).

1.6. Согласно предыдущему упражнению полином, стоящий в левой части в (4.8), имеет в общем случае в качестве своих значений не только элементы множества, задаваемого уравнением (4.7), но и еще какие-то отрицательные числа. Покажите, что для любого диофантова множества $\mathfrak{M}$ натуральных чисел можно найти полином с целыми коэффициентами, множество *всех* значений которого есть объединение множества $\mathfrak{M}$ и множества всех отрицательных чисел (переменные могут быть как целочисленными, так и натуральными).

1.7. Покажите, что для любого диофантова множества $\mathfrak{M}$ существуют полиномы P и Q с целыми коэффициентами такие, что множество $\mathfrak{M}$ есть в точности множество *всех целочисленных* значений, принимаемых дробью

$$\frac{P(x_0, \ldots, x_m)}{Q(x_0, \ldots, x_m)}$$

при натуральных значениях переменных.

1.8. Специальная форма диофантовых представлений одномерных множеств из § 1.4 допускает различные обобщения на многомерный случай. Покажите, что:

а) каждое n-мерное диофантово множество $\mathfrak{M}$ имеет представление вида

$$D(x_1, \ldots, x_m) = A(a_1, \ldots, a_n),$$

где A и D — полиномы с целыми коэффициентами;

б) для $\mathfrak{M}$ можно также указать полиномы $D_1, \ldots, D_n$ с целыми коэффициентами, такие, что $\langle a_1, \ldots, a_n \rangle \in \mathfrak{M}$ тогда и только тогда, когда разрешима

система

$$D_1(x_1,\ldots,x_m)=a_1,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$D_n(x_1,\ldots,x_m)=a_n.$$

1.9. Покажите, что каждая диофантова функция имеет представление вида

$$a=F(b_1,\ldots,b_n) \iff \exists x_0\ldots x_m[a=E(b_1,\ldots,b_n,x_0,\ldots,x_m)],$$

где E — полином с целыми коэффициентами.

1.10. Установите диофантовость:

а) множества всех составных чисел;

б) множества всех чисел, не являющихся степенью числа 2;

в) множества всех чисел, не являющихся полными квадратами.

1.11. В качестве менее тривиального примера установите диофантовость двухместного отношения *число a не является степенью числа b.*

1.12. Покажите, что для любого положительного алгебраического числа χ двухместное отношение *быть числителем и знаменателем подходящей дроби к χ* является диофантовым.

1.13. Будем называть *тригонометрическими диофантовыми уравнениями* уравнения вида

$$R(x_1,\ldots,x_m,T_1(\pi P_1(x_1,\ldots,x_m)/Q_1(x_1,\ldots,x_m)),\ldots$$
$$\ldots,T_l(\pi P_l(x_1,\ldots,x_m)/Q_l(x_1,\ldots,x_m))=0,$$

где $P_1,\ldots,P_l$, $Q_1,\ldots,Q_l$, R — полиномы с целыми коэффициентами, а $T_1,\ldots,T_l$ — тригонометрические функции. Покажите, что проблема распознавания наличия решений у тригонометрических диофантовых уравнений сводится к 10-й проблеме Гильберта.

1.14. Покажите, что если $R(x_1,\ldots,x_m)$ — полином степени k с *вещественными* коэффициентами, который при натуральных значениях $x_1,\ldots,x_m$ принимает только целочисленные значения, то

$$R(x_1,\ldots,x_m)=P\left(\binom{x_1}{1},\ldots,\binom{x_1}{k},\ldots,\binom{x_m}{1},\ldots,\binom{x_m}{k}\right),$$

где P — полином с целыми коэффициентами.

1.15. Как было сказано в § 1.4, дополнение диофантова множества в общем случае может быть не диофантовым. В качестве *специального* случая установите диофантовость дополнения любого диофантова множества, определяемого диофантовым уравнением с одной неизвестной.

Нерешённые проблемы

1.1. Может ли каждое диофантово множество быть задано диофантовым уравнением третьей степени относительно всех переменных? Относительно неизвестных?

1.2. Сводится ли 10-я проблема Гильберта к её аналогу для уравнений 3-й степени?

1.3. Является ли аналог 10-й проблемы Гильберта для уравнений 3-й степени также алгоритмически неразрешимым?

Комментарии

Дошедшие до нас труды Диофанта изданы [1974] в переводе на русский язык с комментариями.

Десятая проблема является единственной массовой проблемой среди 23 проблем Гильберта.

Специалисты по теории чисел не проявляли особого интереса к обратной постановке задачи — нахождению по множеству, свойству или отношению его диофантова представления или доказательству невозможности этого. Такая постановка задачи более характерна для исследований по математической логике. В «Автобиографии Джулии Робинсон» (см. публикацию Рид [1986]), говорится, что в 1948 году А. Тарский ставил задачу доказать, что множество всех степеней числа 2 не является диофантовым. Эта задача послужила Дж. Робинсон [1952] отправной точкой для систематического исследования диофантовости конкретных множеств. В это же время М. Девис [1953] предпринял анализ всего класса диофантовых множеств, показав, в частности, допустимость использования дизъюнкции и конъюнкции и недопустимость использования отрицания. В этой работе также была установлена эквивалентность 10-й проблемы Гильберта её аналогу для решений в натуральных числах. К этому же периоду начальных исследований по 10-й проблеме Гильберта относится и работа Майхила [1953].

Специальные формы представлений одномерных диофантовых множеств из § 1.4 и из упражнений 1.4, 1.6, 1.7 были предложены в работе Патнама [1960].

Сведение произвольного диофантова уравнения к уравнению четвёртой степени было указано в работе Скулема [1934]. В работе Бриттона [1979] рассматривается сведение произвольных диофантовых уравнений к системам диофантовых уравнений второй степени, имеющих специальный вид.

Вопрос об алгоритмической разрешимости уравнений 3-й степени был сформулирован в обзоре Девиса, Матиясевича и Робинсон [1975]. Приведённые здесь три открытые проблемы, очевидно, тесно связаны друг с другом, а именно, положительный ответ в первой проблеме влечёт положительный ответ во второй, что, в свою очередь, влечёт положительный ответ в третьей проблеме. Тем не менее эти три проблемы не эквивалентны друг другу — a priori может оказаться, что для первой ответ отрицателен, а для третьей — положителен. Укажем, что для аналогов этих трёх проблем, касающихся разрешимости в целых числах диофантовых уравнений второй степени, отрицательный ответ следует из работы Зигеля [1972].

Глава 2

ДИОФАНТОВОСТЬ ВОЗВЕДЕНИЯ В СТЕПЕНЬ

Цель настоящей главы — установить диофантовость функции двух аргументов b^c. Установление диофантовости возведения в степень является технически трудным (и при первом чтении § 2.1–2.4 могут быть пропущены), но оно открывает простой путь к доказательству диофантовости многих других интересных и важных функций и отношений. В частности, в § 3.4 будет установлена диофантовость множества простых чисел.

§ 2.1. Специальные рекуррентные последовательности второго порядка

Как уже было сказано, цель настоящей главы — установление диофантовости функции b^c. В другой терминологии это звучит как установление диофантовости множества троек

$$\{\langle a,b,c\rangle \mid a = b^c\}. \tag{1}$$

Из диофантовости множества (1) следует диофантовость множества пар

$$\{\langle a,b\rangle \mid \exists n[a = b^n]\}. \tag{2}$$

Справедливо и обратное (см. упражнение 2.2), но и установление диофантовости множества (2) является трудным.

Множество всех степеней данного числа b — это множество всех членов рекуррентной последовательности первого порядка

$$\beta_b(0) = 1, \quad \beta_b(n+1) = b\beta_b(n). \tag{3}$$

Существенную роль в доказательстве диофантовости (1) будут играть рекуррентные последовательности второго порядка

$$\alpha_b(0) = 0, \quad \alpha_b(1) = 1, \quad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n), \tag{4}$$

где $b \geq 2$. В качестве первого шага в этом параграфе мы установим диофантовость множества пар

$$\{\langle a,b\rangle \mid b \geq 2 \,\&\, \exists n[a = \alpha_b(n)]\}. \tag{5}$$

Как это ни странно, сделать это гораздо легче, чем установить диофантовость, казалось бы, более простого и естественного множества (2).

Соотношение второго порядка (4) можно переписать в виде соотношения первого порядка между матрицами

$$A_b(n)=\begin{pmatrix}\alpha_b(n+1) & -\alpha_b(n)\\ \alpha_b(n) & -\alpha_b(n-1)\end{pmatrix}, \tag{6}$$

где $\alpha_b(-1)=-1$. А именно,

$$A_b(0)=E,\quad A_b(n+1)=A_b(n)\Xi_b, \tag{7}$$

где

$$E=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\qquad \Xi_b=\begin{pmatrix}b & -1\\ 1 & 0\end{pmatrix}. \tag{8}$$

Отсюда немедленно получаем, что

$$A_b(n)=\Xi_b^n, \tag{9}$$

и, следовательно,

$$\det(A_b(n))=1, \tag{10}$$

т. е.

$$\alpha_b^2(n)-\alpha_b(n+1)\alpha_b(n-1)=\alpha_b^2(n+1)-b\alpha_b(n+1)\alpha_b(n)+\alpha_b^2(n)=$$

$$=\alpha_b^2(n)-b\alpha_b(n)\alpha_b(n-1)+\alpha_b^2(n-1)=1. \tag{11}$$

Оказывается, что соотношение (11) является характеристическим для последовательности (4), а именно, *если*

$$x^2-bxy+y^2=1, \tag{12}$$

то либо

$$x=\alpha_b(m+1),\quad y=\alpha_b(m), \tag{13}$$

либо

$$x=\alpha_b(m),\quad y=\alpha_b(m+1) \tag{14}$$

для некоторого m. Чтобы различить, какой из двух случаев, (13) *или* (14), имеет место, достаточно заметить, что из (4) по индукции легко доказывается, что

$$0=\alpha_b(0)<\alpha_b(1)<\ldots<\alpha_b(n)<\alpha_b(n+1)<\ldots \tag{15}$$

Покажем, что *из* (12) *и неравенства*

$$y<x \tag{16}$$

следует существование некоторого m, *для которого выполнено* (13). Доказательство проведём индукцией по y. Если $y=0$, то, очевидно, $x=1$, т. е. (13) выполнено при $m=0$. Если же $y>0$, то согласно (12) и (16)

$$x=by+(1-y^2)/x\le by, \tag{17}$$

$$x=by+1/x-y^2/x>by-y. \tag{18}$$

Положим $x_1 = y$, $y_1 = by-x$, тогда

$$x_1^2-bx_1y_1+y_1^2 = y^2-by(by-x)+(by-x)^2 = x^2-bxy+y^2 = 1, \tag{19}$$

согласно (18) $y_1 < x_1$ и по индукционному предположению

$$x_1 = \alpha_b(m_1+1), \quad y_1 = \alpha_b(m_1) \tag{20}$$

для некоторого m_1; следовательно, для $m = m_1+1$

$$x = bx_1-y_1 = \alpha_b(m+1), \quad y = x_1 = \alpha_b(m). \tag{21}$$

Итак, мы доказали, что *множество* (5) *задаётся формулой*

$$b \geq 2 \,\&\, \exists x[x^2-abx+a^2 = 1]. \tag{22}$$

§ 2.2. Диофантовость специальных рекуррентных последовательностей (основные идеи)

Наша ближайшая цель — установить диофантовость множества троек

$$\{\langle a,b,c\rangle \mid b \geq 4 \,\&\, a = \alpha_b(c)\}. \tag{1}$$

В этом параграфе будут обрисованы основные идеи, а формальное доказательство будет проведено в следующем параграфе.

Множество (1) удобно представлять себе как объединение членов последовательностей

$$\langle \alpha_b(0), b, 0\rangle, \ldots, \langle \alpha_b(n), b, n\rangle, \ldots \tag{2}$$

при $b = 4, 5, \ldots$ По индукции из определения (1.4) легко вывести, что

$$\alpha_2(n) = n, \tag{3}$$

и потому при $b = 2$ последовательность (2) является очень простой:

$$\langle 0, 2, 0\rangle, \ldots, \langle n, 2, n\rangle, \ldots \tag{4}$$

В интересующих нас случаях $b \geq 4$ и $\alpha_b(n)$ не может быть определено столь просто, как $\alpha_2(n)$ в (3). Тем не менее для $b > 2$ имеется некоторый слабый аналог (3), а именно, из (1.4) по индукции легко получить, что

$$\alpha_{b_1}(n) \equiv \alpha_{b_2}(n) (\mathbf{mod}\ q) \tag{5}$$

при условии, что

$$b_1 \equiv b_2 (\mathbf{mod}\ q). \tag{6}$$

В частности,

$$\alpha_b(n) \equiv \alpha_2(n) = n (\mathbf{mod}\ b-2), \tag{7}$$

и потому первые $b-2$ члена последовательности (2) совпадают с

первыми b-2 членами последовательности

$$\langle\alpha_b(0), b, \mathbf{rem}(\alpha_b(0), b\text{-}2)\rangle, \ldots, \langle\alpha_b(n), b, \mathbf{rem}(\alpha_b(n), b\text{-}2)\rangle, \ldots \tag{8}$$

«Преимущество» последовательности (8) по сравнению с (2) состоит в том, что здесь n входит только в качестве аргумента α, и потому диофантовость множества, состоящего из всех троек последовательности (8), легко следует из диофантовости (1.5) и диофантовости функции **rem**. «Недостаток» же состоит в том, что (8) и (2) совпадают лишь на небольшом начальном отрезке.

Воспользовавшись (5), мы можем построить другую последовательность, которая имеет то же «преимущество», но лишена упомянутого «недостатка». А именно, пусть

$$w \equiv b(\mathbf{mod}\ v), \tag{9}$$

$$w \equiv 2(\mathbf{mod}\ u), \tag{10}$$

$$v > 2\alpha_b(k), \tag{11}$$

$$u > 2k, \tag{12}$$

тогда первые k членов последовательности (2) совпадают с первыми k членами последовательности

$$\langle\mathbf{arem}(\alpha_w(0), v), b, \mathbf{arem}(\alpha_w(0), u)\rangle, \ldots$$

$$\ldots, \langle\mathbf{arem}(\alpha_w(n), v), b, \mathbf{arem}(\alpha_w(n), u\rangle, \ldots \tag{13}$$

(роль замены функции **rem** на введённую в § 1.6 функцию **arem** станет ясна позднее).

Таким образом, объединение всех последовательностей вида (13), получающихся при различных значениях u, v и w, удовлетворяющих условиям (9)-(10), содержит все тройки из последовательности (2), но может, вообще говоря, содержать и тройки, не входящие в (2). Для избавления от этих «лишних» троек мы, во-первых, наложим на v и u, наряду с (9)-(10), дополнительные ограничения и, во-вторых, исключим из (13) те тройки, которые не удовлетворяют неравенству

$$2\mathbf{arem}(\alpha_w(n), v) < u. \tag{14}$$

Чтобы понять характер требуемых дополнительных ограничений на v и u, укажем, что из рекуррентных соотношений (1.4) легко получить, что для любого положительного v последовательность

$$\alpha_b(0), \ldots, \alpha_b(n), \ldots \tag{15}$$

является чисто периодической **modulo** v. При специальном выборе v длина периода и его структура легко определяются. А

именно, пусть

$$v = \alpha_b(m+1)-\alpha_b(m-1), \tag{16}$$

тогда

$$\alpha_b(m+1) \equiv \alpha_b(m-1)(\mathbf{mod}\ v). \tag{17}$$

Рекуррентное соотношение (1.4) можно переписать в виде

$$\alpha_b(n-2) = b\alpha_b(n-1)-\alpha_b(n), \tag{18}$$

и потому

$$\alpha_b(m+2) = b\alpha_b(m+1)-\alpha_b(m) \equiv b\alpha_b(m-1)-\alpha_b(m) = \alpha_b(m-2)(\mathbf{mod}\ v), \tag{19}$$

$$\begin{gathered} \alpha_b(m+3) \equiv \alpha_b(m-3)(\mathbf{mod}\ v), \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \alpha_b(2m-1) \equiv \alpha_b(1)(\mathbf{mod}\ v), \\ \alpha_b(2m) \equiv \alpha_b(0)(\mathbf{mod}\ v). \end{gathered} \tag{20}$$

Далее имеем:

$$\alpha_b(2m) \equiv \alpha_b(0) = 0 = -\alpha_b(0)(\mathbf{mod}\ v), \tag{21}$$

$$\alpha_b(2m+1) = b\alpha_b(2m)-\alpha_b(2m-1) \equiv -\alpha_b(1)(\mathbf{mod}\ v), \tag{22}$$

и, следовательно,

$$\alpha_b(2m+n) \equiv -\alpha_b(n)(\mathbf{mod}\ v). \tag{23}$$

Таким образом, при выбранном v последовательность (15) **modulo** v имеет период, состоящий из $4m$ членов:

$$\begin{gathered} 0,\ 1,\ldots,\ \alpha_b(m-1),\ \alpha_b(m),\ \alpha_b(m-1),\ldots,\ 1, \\ 0,-1,\ldots,-\alpha_b(m-1),-\alpha_b(m),-\alpha_b(m-1),\ldots,-1. \end{gathered} \tag{24}$$

Согласно (9) тот же период **modulo** v имеет и последовательность

$$\alpha_w(0),\ldots,\alpha_w(n),\ldots \tag{25}$$

Последовательность же

$$\mathbf{arem}(\alpha_w(0),v),\ldots,\mathbf{arem}(\alpha_w(n),v),\ldots \tag{26}$$

имеет период, состоящий из $2m$ членов

$$0,1,\ldots,\alpha_b(m-1),\alpha_b(m),\alpha_b(m-1),\ldots,1, \tag{27}$$

ибо согласно (1.15) $v = \alpha_b(m+1)-\alpha_b(m-1) = b\alpha_b(m)-2\alpha_b(m-1) \geq 2\alpha_b(m)$ при $b \geq 4$.

Согласно (10) и (7) последовательность (25) **modulo** u имеет период, состоящий из u членов:

$$0,1,\ldots,u-1. \tag{28}$$

Очень существенным для дальнейшего является то, что мы будем

выбирать u так, чтобы

$$u \mid m. \tag{29}$$

В этом случае длина периода последовательности (26) будет кратна длине периода последовательности

$$\mathbf{arem}(\alpha_w(0), u), \ldots, \mathbf{arem}(\alpha_w(n), u), \ldots \tag{30}$$

и поэтому последовательность (13) будет иметь почти симметричный период длины $2m$. Таким образом, все «лишние» тройки в (13) появляются уже среди первых $m+1$ членов этой последовательности. Условие (14) для этих первых троек можно переписать как

$$2\alpha_b(n) < u, \tag{31}$$

откуда следует, что

$$2n < u, \tag{32}$$

ибо согласно (1.15)

$$n \le \alpha_b(n). \tag{33}$$

Из (32) следует, что

$$\mathbf{arem}(\alpha_b(n), u) = \mathbf{arem}(n, u) = n, \tag{34}$$

т. е. условие (14) действительно исключает все «лишние» тройки.

На пути реализации описанного выше плана осталась одна трудность — как записать диофантовым образом пару условий (16) и (29), не имея ещё в своём распоряжении диофантовости функции α? Здесь нам поможет следующее её свойство:

$$\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow \alpha_b(k) \mid m. \tag{35}$$

Мы положим

$$u = \alpha_b(k) \tag{36}$$

и заменим (29) на более сильное условие

$$u^2 \mid \alpha_b(m). \tag{37}$$

§ 2.3. Диофантовость специальных рекуррентных последовательностей (доказательство)

Мы начнём с доказательства импликации (2.35). Пусть b, k и m таковы, что

$$\alpha_b{}^2(k) \mid \alpha_b(m). \tag{1}$$

Вспомним, что $\alpha_b(k)$ и $\alpha_b(m)$ являются элементами матриц $A_b(k)$ и $A_b(m)$, определённых в (1.6) и удовлетворяющих (1.9). Пусть

$$m = n + kl, \quad 0 \le n < k. \tag{2}$$

Имеем:

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} = A_b(m) = \Xi_b^m = \Xi_b^{n+kl} = \Xi_b^n(\Xi_b^k)^l =$$

$$= A_b(n)A_b^l(k) = \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \begin{pmatrix} \alpha_b(k+1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^l. \qquad (3)$$

Переходя к сравнению **modulo** $\alpha_b(k)$, получаем:

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \equiv$$

$$\equiv \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \begin{pmatrix} \alpha_b(k+1) & 0 \\ 0 & -\alpha_b(k-1) \end{pmatrix}^l (\mathbf{mod}\ \alpha_b(k)), \qquad (4)$$

откуда

$$\alpha_b(m) \equiv \alpha_b(n)\alpha_b^l(k+1)(\mathbf{mod}\ \alpha_b(k)). \qquad (5)$$

Согласно (1.11) $\alpha_b(k)$ и $\alpha_b(k+1)$ взаимно просты, поэтому из (1) и (5) следует, что

$$\alpha_b(k) \mid \alpha_b(n). \qquad (6)$$

Из (2) и (1.15) следует, что $\alpha_b(n) < \alpha_b(k)$, поэтому (6) возможно, лишь если $n = 0$, т. е. $m = kl$. Далее имеем:

$$A_b(m) = A_b^l(k) = [\alpha_b(k)\Xi_b - \alpha_b(k-1)E]^l =$$

$$= \sum_{i=0}^{l} (-1)^{l-i} \binom{l}{i} \alpha_b^i(k)\alpha_b^{l-i}(k-1)\Xi_b^i. \qquad (7)$$

Переходя здесь от равенства к сравнению **modulo** $\alpha_b^2(k)$, мы можем опустить в сумме все слагаемые, кроме двух первых:

$$A_b(m) = \begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \equiv$$

$$\equiv (-1)^l \alpha_b^l(k-1)E + (-1)^{l-1} l \alpha_b(k)\alpha_b^{l-1}(k-1)\Xi_b (\mathbf{mod}\ \alpha_b^2(k)), \qquad (8)$$

откуда

$$\alpha_b(m) \equiv (-1)^{l-1} l \alpha_b(k)\alpha_b^{l-1}(k-1)(\mathbf{mod}\ \alpha_b^2(k)). \qquad (9)$$

Отсюда и из (1) следует, что

$$\alpha_b(k) \mid l\alpha_b^{l-1}(k-1), \qquad (10)$$

и, поскольку согласно (1.11) $\alpha_b(k)$ и $\alpha_b(k-1)$ взаимно просты, то

$$\alpha_b(k) \mid l. \qquad (11)$$

Импликация (2.35) доказана.

Выпишем явно систему диофантовых условий, которая разрешима тогда и только тогда, когда тройка $\langle a,b,c\rangle$ принадлежит множеству (2.1):

$$b \geq 4, \tag{12}$$

$$u^2-but+t^2=1, \tag{13}$$

$$s^2-bsr+r^2=1, \tag{14}$$

$$r<s, \tag{15}$$

$$u^2 \mid s, \tag{16}$$

$$v=bs-2r, \tag{17}$$

$$v \mid w-b, \tag{18}$$

$$u \mid w-2, \tag{19}$$

$$w>2, \tag{20}$$

$$x^2-wxy+y^2=1, \tag{21}$$

$$2a<u, \tag{22}$$

$$a=\mathbf{arem}(x,v), \tag{23}$$

$$c=\mathbf{arem}(x,u). \tag{24}$$

Докажем сначала, что *если условия* (12)–(24) *выполнены, то*

$$a=\alpha_b(c). \tag{25}$$

Как показано в § 2.1, из (12) и (13) следует, что для некоторого k

$$u=\alpha_b(k). \tag{26}$$

Аналогично, из (12), (14) и (15) следует существование положительного m такого, что

$$s=\alpha_b(m), \quad r=\alpha_b(m-1). \tag{27}$$

Согласно (2.35) из (16), (26) и (27) следует, что

$$u \mid m. \tag{28}$$

Согласно (1.4) из (17) и (27) следует, что

$$v=\alpha_b(m+1)-\alpha_b(m-1). \tag{29}$$

Далее, из (20) и (21) следует, что для некоторого n

$$x=\alpha_w(n). \tag{30}$$

Отсюда и из (18), (19) согласно (2.5)–(2.7) получаем, что

$$x \equiv \alpha_b(n)(\mathbf{mod}\ v), \tag{31}$$

$$x \equiv n(\mathbf{mod}\ u). \tag{32}$$

Представим n в виде

$$n=2lm \pm j, \tag{33}$$

где

$$j \le m. \tag{34}$$

Вновь обращаясь к матричному представлению, имеем:

$$A_b(n) = \Xi_b^n = \Xi_b^{2lm \pm j} = [[\Xi_b^m]^2]^l \Xi_b^{\pm j} = [[A_b(m)]^2]^l [A_b(j)]^{\pm 1}, \tag{35}$$

$$A_b(m) = \begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} =$$

$$= -\begin{pmatrix} -\alpha_b(m-1) & \alpha_b(m) \\ -\alpha_b(m) & \alpha_b(m+1) \end{pmatrix} = -[A_b(m)]^{-1} (\mathbf{mod}\ v), \tag{36}$$

$$[A_b(m)]^2 \equiv -E (\mathbf{mod}\ v), \tag{37}$$

$$A_b(n) \equiv \pm [A_b(j)]^{\pm 1} (\mathbf{mod}\ v) \tag{38}$$

(в последней формуле возможны все четыре комбинации знаков "+" и "–"). Возвращаясь от матричного сравнения (38) к поэлементному, получаем, что

$$x \equiv \alpha_b(n) \equiv \pm \alpha_b(j) (\mathbf{mod}\ v). \tag{39}$$

Из (34) согласно (1.15) следует, что

$$2\alpha_b(j) \le 2\alpha_b(m) \le (b-2)\alpha_b(m) < b\alpha_b(m) - 2\alpha_b(m-1) = v, \tag{40}$$

и потому

$$a = \mathbf{arem}(x, v) = \mathbf{arem}(\alpha_b(n), v) = \alpha_b(j). \tag{41}$$

Отсюда и из (22) согласно (2.33) получаем, что

$$2j \le 2\alpha_b(j) = 2a < u. \tag{42}$$

Наконец, из (28), (31), (33) и (42) получаем, что

$$c = \mathbf{arem}(x, u) = \mathbf{arem}(n, u) = j, \tag{43}$$

что вместе с (41) дает требуемое равенство (25).

Докажем теперь, что, наоборот, *если числа* a, b, *и* c *удовлетворяют* (12) *и* (25), *то найдутся числа* s, r, u, t, v, w, *удовлетворяющие* (13)–(24). Предыдущие рассуждения подсказывают, как осуществить такой выбор.

Выберем u согласно (26), где k таково, что выполнено неравенство (22), и u нечётно. Это сделать можно, ибо ввиду (1.15) последовательность $\alpha_b(0), \alpha_b(1), \ldots$ монотонно возрастает, а согласно (1.11) из любых двух её соседних членов по крайней мере один нечётен. Положим

$$t = \alpha_b(k+1), \tag{44}$$

тогда согласно (1.11) равенство (13) будет выполнено.

Выберем r и s согласно (27), где

$$m = uk, \tag{45}$$

тогда ввиду (1.11) будет выполнено равенство (14), а согласно (1.15) — неравенство (15). Согласно (9)

$$s = \alpha_b(uk) \equiv (-1)^{u-1} u \alpha_b(k) \alpha_b^{u-1}(k-1) (\mathbf{mod}\ u^2), \tag{46}$$

и, следовательно, условие (16) также выполнено.

Мы можем найти v, удовлетворяющее (17), ибо в силу (1.15)

$$bs-2r \geq 4\alpha_b(m)-2\alpha_b(m-1) > 2\alpha_b(m). \tag{47}$$

Проверим, что u и v взаимно просты. Пусть $d|u$, $d|v$, тогда по (16) $d|s$ и по (17) $d|2r$, но по выбору u d нечётно, и потому $d|r$ и по (14) $d|1$. Следовательно, по китайской теореме об остатках (см. Приложение 2) мы можем найти w, удовлетворяющее (18), (19) и (20).

Наконец, положим

$$x = \alpha_w(c), \quad y = \alpha_w(c+1), \tag{48}$$

тогда вследствие (1.15), равенство (21) будет выполнено.

Согласно (2.5) из (25), (48) и (18) следует, что

$$x = \alpha_w(c) \equiv \alpha_b(c) = a (\mathbf{mod}\ v). \tag{49}$$

Поскольку из (17), (25) и (47) следует, что

$$v > 2a, \tag{50}$$

то из (49) следует (23).

Согласно (1.7) из (48) следует, что

$$x \equiv c (\mathbf{mod}\ w-2), \tag{51}$$

что вместе с (19) даёт сравнение

$$x \equiv c (\mathbf{mod}\ u). \tag{52}$$

В силу (2.33) из (25) и (22) следует, что

$$2c \leq 2\alpha_b(c) = 2a < u, \tag{53}$$

отсюда и из (52) получаем справедливость (24).

Поскольку все условия (12)–(24) диофантовы, мы установили диофантовость множества (2.1).

§ 2.4. Диофантовость возведения в степень

Прежде чем приступить к установлению диофантовости возведения в степень, мы должны уточнить, что понимать под 0^0. По разным причинам удобно считать, что $0^0 = 1$.

Рекуррентное соотношение (1.4) при больших b близко к (1.3), и $\alpha_b(n)$ растёт примерно как $\beta_b(n) = b^n$. Точные неравенства легко получаются по индукции, а именно,

$$(b-1)^n \leq \alpha_b(n+1) \leq b^n. \tag{1}$$

При фиксированном n относительная погрешность стремится к 1 при $b\to\infty$, но мы хотели бы получить хорошее приближение к b^c при фиксированном b. Поэтому мы введём новую переменную x, которая будет иметь большое значение. Ниже мы проверим, что

$$b^c=\lim_{x\to\infty}\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)}, \tag{2}$$

причём это верно при любых b и c, в том числе при $b=0$. В нашем языке диофантовых уравнений нет операции **lim**, но в данном случае её с успехом заменит функция **div**. А именно, из (1) следует, что

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)}\ge\frac{(bx+3)^c}{x^c}\ge b^c, \tag{3}$$

так что

$$b^c=\alpha_{bx+4}(c+1)\ \mathbf{div}\ \alpha_x(c+1) \tag{4}$$

при большом x. Для того чтобы узнать, какое значение x является достаточно большим, оценим левую часть (3) сверху. Нам придётся отдельно разбирать случаи $b=0$ и $b>0$. При $b=c=0$

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)}=1; \tag{5}$$

при $b=0,\ c>0,\ x>4$

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)}<\frac{4^c}{(x-1)^c}\le 1; \tag{6}$$

при $b>0,\ x>16c$

$$\frac{\alpha_{bx+4}(c+1)}{\alpha_x(c+1)}\le\frac{(bx+4)^c}{(x-1)^c}=\frac{\left(1+\frac{4}{x}\right)^c}{\left(1-\frac{1}{x}\right)^c}b^c\le\frac{b^c}{\left(1-\frac{1}{x}\right)^c\left(1-\frac{4}{x}\right)^c}\le$$

$$\le\frac{b^c}{\left(1-\frac{4}{x}\right)^{2c}}\le\frac{b^c}{1-\frac{8c}{x}}\le b^c\left(1+\frac{16c}{x}\right). \tag{7}$$

Таким образом, (4) справедливо, если

$$x>16(c+1)(b+1)^c, \tag{8}$$

например, если

$$x=16(c+1)\alpha_{b+4}(c+1). \tag{9}$$

Чтобы получить диофантово представление для $a=b^c$, нам осталось исключить из (4) и (9) функцию α. Для этого доста-

точно использовать три копии условий (3.13)–(3.24), условие (3.12) будет, очевидно, выполнено автоматически.

§ 2.5. Экспоненциально диофантовы уравнения

Большую роль в дальнейших главах будут играть *экспоненциально диофантовы уравнения*. Это уравнения вида

$$E_1(x_1, \ldots, x_m) = E_2(x_1, \ldots, x_m), \tag{1}$$

где E_1 и E_2 — выражения, построенные из переменных и конкретных натуральных чисел с помощью сложения, умножения и возведения в степень.

Использование вычитания при построении экспоненциально диофантовых уравнений запрещено для того, чтобы при вычислении не происходил выход из множества натуральных чисел и соответственно не вставал бы вопрос, скажем, о значении

$$(x-y)^{2^{2^{x-y}}} \tag{2}$$

при $x = 1$, $y = 3$. Тем не менее мы иногда будем использовать знак "–" в записи экспоненциально диофантовых уравнений, но только в тех случаях, когда перенесением членов в другую сторону от знака равенства или другими очевидными преобразованиями операция вычитания может быть устранена.

Учитывая это замечание, мы видим, что произвольная система экспоненциально диофантовых уравнений может быть свёрнута в одно уравнение, подобно переходу от (1.2.1) к (1.2.2).

Аналогично диофантовым уравнениям можно рассматривать параметрические экспоненциально диофантовы уравнения и ввести понятия *экспоненциально диофантовых представлений множеств, свойств, отношений* и *функций*. Согласно § 1.5 из установленной в § 2.4 диофантовости возведения в степень следует, что мы можем преобразовать произвольное экспоненциально диофантово уравнение в эквивалентное диофантово уравнение с теми же параметрами ценой увеличения количества неизвестных. Таким образом, класс множеств (свойств, отношений, функций), имеющих экспоненциально диофантово представление, совпадает с классом диофантовых множеств (свойств, отношений, функций соответственно). Интерес к экспоненциально диофантовым представлениям вызван тем, что очень часто они существенно компактнее, чем соответствующие диофантовы представления. Кроме того, экспоненциально диофантовы представления могут обладать дополнительными свойствами, которых пока не удавалось добиться у диофантовых представлений (см., например, § 7.2, § 8.2). По соглашению, принятому в § 1.5, мы будем считать

экспоненциально диофантовы представления обобщёнными диофантовыми представлениями.

В качестве класса уравнений, промежуточного между диофантовыми и экспоненциально диофантовыми, можно выделить *унарные экспоненциально диофантовы уравнения*. Это те экспоненциально диофантовы уравнения, в которых в степень возводятся только константы, а не переменные или более сложные выражения, т. е. вместо двуместной операции возведения в степень b^c используется одна или несколько одноместных операций типа 2^c, 3^c,... Если используется, быть может неоднократно, только одна одноместная операция, скажем 2^c, то говорят соответственно об *унарных экспоненциально диофантовых уравнениях с основанием* 2.

Рассмотрим в качестве примера экспоненциально диофантова уравнения знаменитое уравнение Ферма

$$(p+1)^{s+3}+(q+1)^{s+3}=(r+1)^{s+3}. \tag{3}$$

Оно записано здесь в такой форме для того, чтобы «Великая теорема Ферма» состояла просто в утверждении о неразрешимости уравнения (3) относительно p, q, r, s. Д. Гильберт не включил «Великую теорему Ферма» в свои «Математические проблемы». При каждом фиксированном значении s уравнение (3) является диофантовым относительно p, q и r, но зависимость от s является показательной, и потому «Великая теорема Ферма» в оригинальной формулировке не является и индивидуальной подпроблемой 10-й проблемы Гильберта. Тем не менее установление диофантовости возведения в степень даёт нам возможность построить конкретный полином $\mathbf{F}$ с целыми коэффициентами такой, что уравнение

$$\mathbf{F}(p,q,r,s,x_1,\ldots,x_m)=0 \tag{4}$$

разрешимо относительно $x_1,\ldots,x_m$ тогда и только тогда, когда p, q, r и s удовлетворяют (3), и, следовательно, «Великая теорема Ферма» эквивалентна утверждению о неразрешимости диофантова уравнения (4) как уравнения с $m+4$ неизвестными. Таким образом, хотя мы всё ещё (1990г.) не знаем, верна ли «Великая теорема Ферма», мы можем явно указать эквивалентную ей индивидуальную подпроблему 10-й проблемы Гильберта.

Упражнения

В упражнениях 2.1–2.3, 2.8–2.10 и открытом вопросе 2.1 имеется виду нахождение более простых конструкций, чем те, которые очевидным образом получаются с помощью техники главы 2.

2.1. Установите диофантовость множества

$$\{\langle a_1,b_1,a_2,b_2\rangle \mid \exists n[a_1=b_1^n \& a_2=b_2^n]\}$$

в предположении диофантовости множества (1.2).

2.2. Установите диофантовость множества (2.1) в предположении диофантовости множества (2.2).

2.3. Для любого фиксированного нечётного b дайте прямое доказательство диофантовости множества

$$\{a \mid \exists n[a=b^n]\}$$

в предположении диофантовости его какого-либо бесконечного подмножества.

2.4. Докажите, что при чётном b множество (1.5) задаётся не только формулой (1.22), но и уравнением Пелля

$$z^2-((b/2)^2-1)a^2=1.$$

2.5. Вместо последовательностей (1.4) для установления диофантовости возведения в степень мы могли бы использовать последовательности, определяемые соотношениями

$$\gamma_b(0)=0, \quad \gamma_b(1)=1, \quad \gamma_b(n+2)=b\gamma_b(n+1)+\gamma_b(n),$$

где $b\geq 1$. Установите диофантовость множества

$$\{\langle a,b\rangle \mid b\geq 1 \& \exists n[a=\gamma_b(n)]\},$$

являющегося аналогом множества (1.5).

2.6. В (2.1) неравенство $b\geq 4$ стоит (вместо $b\geq 2$) ради небольшого упрощения (где?) доказательства диофантовости. Это ограничение не было обременительным в (4.4) и (4.9) для достижения основной цели данной главы, но всё же для полноты докажите диофантовость $\alpha_b(c)$ как функции двух аргументов, определённой для всех $b\geq 2$ и всех c.

2.7. Существует ещё одна, чуть менее очевидная, чем (4.4), связь последовательностей α с возведением в степень, а именно:

$$b^n \equiv \alpha_x(n+1)+(b-x)\alpha_x(n)(\mathrm{mod}\ bx-b^2-1)).$$

Докажите это и используйте затем для получения ещё одного диофантова представления множества (1.1).

2.8. В (4.2) было использовано то обстоятельство (выражаемое неравенствами (4.1)), что $\alpha_b(n)$ растёт почти как b^n. На самом деле эти неравенства можно существенно ослабить. Говорят, что двухместное отношение $\mathcal{J}$ *имеет экспоненциальный рост*, если выполнены следующие два условия:

а) для любых u и v из $\mathcal{J}(u,v)$ следует, что $v<u^u$;

б) для любого k существуют u и v такие, что $\mathcal{J}(u,v)$ и $v>u^k$.

Найдите обощённое диофантово представление возведения в степень в предположении диофантовости какого-либо отношения, имеющего экспоненциальный рост.

2.9. Условия упражнения 2.8 можно ослабить ещё больше. Говорят, что двуместное отношение $\mathcal{R}$ *имеет грубо экспоненциальный рост*, если существует число m такое, что

а) для любых u и v из $\mathcal{R}(u,v)$ следует, что

$$v < u^{u^{\cdot^{\cdot^{\cdot^{u}}}}},$$

где башня экспонент имеет высоту m;

б) для любого k существуют u и v такие, что $\mathcal{R}(u,v)$ и $v>u^k$.

Покажите, что возведение в степень не может не быть диофантовым, если диофантовым является какое-либо отношение, имеющее грубо экспоненциальный рост (обратите внимание, что в этом упражнении не требуется указать обобщённое диофантово представление).

2.10. Покажите, что если уравнение

$$9(u^2+7v^2)^2-7(r^2+7s^2)^2=2$$

имеет лишь конечное число решений, то существует диофантово отношение, имеющее экспоненциальный рост.

Открытые вопросы

2.1. Существует ли прямой путь преобразования диофантова отношения грубо экспоненциального роста в диофантово отношение экспоненциального роста?

2.2. Бесконечно ли количество решений у уравнения из упражнения 2.10?

2.3. Линейное рекуррентное соотношение

$$\delta(n+k)=b_{k-1}\delta_{n+k-1}+\ldots+b_0\delta_n$$

k-го порядка может аналогично (2.7) быть преобразовано в соотношение первого порядка между матрицами размера $k\times k$. Если $b_0=\pm 1$, то аналогично (2.10) определители соответствующих матриц будут равны $\pm c$, где c — константа, определяемая значениями $\delta(0),\ldots,\delta(k-1)$. Это условие можно записать аналогично (2.11) в виде некоторого соотношения, связывающего $\delta(n),\ldots,\delta(n+k-1)$. В каком случае это соотношение будет характеристическим, т. е. будет порождать аналогичное (2.12) диофантово уравнение, все решения которого — элементы рассматриваемой последовательности?

Комментарии

Как сказано в комментариях к главе 1, начало систематических исследований класса диофантовых множеств было связано с предположением А. Тарского о том, что множество всех степеней числа 2 диофантовым не является. Не сумев доказать это, Дж. Робинсон стала склоняться к предположению о диофантовости возведения в степень. Ей [1952] удалось найти достаточные условия для диофантовости b^c, состоящие в диофантовости какого-либо отношения, имеющего экспоненциальный рост (см. упражнение 2.8) или хотя бы грубо экспоненциальный рост (см. упражнение 2.9). Отношения, имеющие экспоненциальный рост, получили в литературе также название *предикатов Джулии Робинсон* (см., например, работу Девиса [1963]).

В дальнейшем Дж. Робинсон [1969а] нашла достаточные условия для существования диофантова отношения экспоненциального роста в виде диофан-

товости какого-либо бесконечного множества, состоящего из простых чисел, и в виде диофантовости множества всех степеней числа 2.

Другое достаточное условие, состоящее в единственности тривиального решения $u=r=1$, $v=s=0$ у уравнения из упражнения 2.10, предложено в работе Девиса [1968]. В работе Хермана [1971], однако, было установлено, что это условие не выполняется, а в работе Шенкса [1972] приведено найденное с помощью ЭВМ решение

$$u=525692038369576, \qquad r=2484616164142152,$$
$$v=1556327039191013, \qquad s=1381783865776981.$$

Тем не менее, как было отмечено в обзоре Девиса, Матиясевича и Робинсон [1976], найденное решение не полностью обесценивает идею М. Девиса, поскольку на самом деле достаточно, чтобы рассматриваемое уравнение имело конечное число решений (см. упражнение 2.10).

Хотя эти подходы пока не привели к успеху, интерес к ним не пропал даже тогда, когда диофантовость возведения в степень была установлена другим путём. Это связано с так называемыми однократными диофантовыми представлениями (см. § 7.2 и комментарии к главе 7). Были предложены и другие, более сложно формулируемые условия, из которых следует, в частности, диофантовость возведения в степень (см., например, работы Девиса [1962, 1966], Девиса и Патнама [1958], Матиясевича [1968б]).

Первый пример диофантова отношения с экспоненциальным ростом был опубликован в работе Матиясевича [1970]. В ней установлена диофантовость отношения

$$v=\varphi_{2u},$$

где $\varphi_0, \varphi_1, \ldots$ — последовательность *чисел Фибоначчи*, определяемая соотношениями

$$\varphi_0=0, \quad \varphi_1=1, \quad \varphi_{n+2}=\varphi_n+\varphi_{n-1},$$

и в силу упомянутого выше критерия Дж. Робинсон этого было достаточно для установления диофантовости возведения в степень. Хронологически именно построение примера диофантова отношения с экспоненциальным ростом стало последним шагом в доказательстве алгоритмической неразрешимости 10-й проблемы Гильберта, ибо к тому времени уже была установлена алгоритмическая неразрешимомть экспоненциально диофантовых уравнений (подробнее об этом см. комментарии к главе 5).

Последовательность чисел Фибоначчи является частным случаем (при $b=1$) последовательностей γ_b из упражнения 2.5, родственных нашим последовательностям α_b. Все эти последовательности обладают близкими свойствами, позволяющими установить и их диофантовость, что было показано в работах Чудновского [1970, 1971, 1984], Девиса [1971, 1973а], Косовского [1971], а также С. Коченом (см. работу Девиса [1971]) и К. Шютте (см. работы Дж. Робинсон [1971] или Фенстада [1971]).

В § 2.3 мы добились большего, чем просто построения диофантова отношения с экспоненциальным ростом, как это было сделано в работе Матиясевича [1970]. Система (12)-(24) определяет не двух-, а трёхместное дио-

фантово отношение, и находящиеся в этом отношении числа удовлетворяют двусторонним неравенствам более жёстким, чем требуемые в определении отношения с экспоненциальным ростом. Это открывает чуть более короткий путь (использованный в § 2.4) к установлению диофантовости возведения в степень, чем непосредственное применение критерия Дж. Робинсон. Другой путь, также восходящий к работе Дж. Робинсон [1952], указан в упражнении 2.7. Диофантовы представления функции b^c детально изложены, в частности, в работах Девиса [1971], Косовского [1971], Матиясевича [1971а, 1971б], Матиясевича и Робинсон [1975].

Диофантово уравнение типа (5.4) явно выписано в работе Руохонена [1972]. Маловероятно, чтобы подобный переход от экспоненциально диофантова уравнения Ферма к эквивалентному диофантову уравнению мог бы оказаться полезным для исследований по «Великой теореме Ферма». Подобное сведение скорее может служить неформальным «психологическим» доводом в пользу неразрешимости 10-й проблемы Гильберта — ведь в противном случае «способ», который требовалось найти для её решения, позволял бы, в частности, узнать, верна ли «Великая теорема Ферма».

В работе Чудновского [1971] (ср. [1984]) говорится, что вопрос Девиса о разрешимости уравнения из упражнения 2.10 «сводится к исследованию арифметических свойств последовательности (A_n, B_n) решений уравнения $9x^2-7y^2=2$» и, «исследуя указанные последовательности, можно получить явное диофантово представление $y=2^x$ при $x>C$, где C — некоторая константа. Полученный результат даёт ответ на вопрос М. Дэвиса». Как мы теперь знаем, гипотеза Девиса об отсутствии нетривиальных решений не верна, и остаётся не ясным, имел ли Г. В. Чудновский в виду конечность количества решений или же какой-то иной способ использования последовательности (A_n, B_n). В связи с этим вопрос 2.2 сформулирован как открытый.

Исследование открытого вопроса 2.3, по-видимому, тесно связано с анализом мультипликативной группы единиц поля $\mathbb{Q}(\chi)$, где χ удовлетворяет уравнению

$$\chi^k=b_{k-1}\chi^{k-1}+\ldots+b_0,$$

и для положительного ответа скорее всего необходимо, чтобы $b_0=\pm 1$ и $k\leq 4$, причём в случае $k=4$ необходимо также, чтобы это уравнение не имело вещественных корней, а в случае $k=3$ имело лишь один вещественный корень (ибо по теореме Дирихле только при этих условиях имеется лишь одна основная единица поля).

Глава 3
ДИОФАНТОВО КОДИРОВАНИЕ

Каждое конкретное диофантово уравнение имеет фиксированное количество переменных. Тем не менее с их помощью можно работать с конечными упорядоченными наборами натуральных чисел произвольной длины, которые мы будем по традиции называть *кортежами*. В настоящей главе мы разовьём соответствующую технику.

§ 3.1. Канторова нумерация

Данное Кантором классическое доказательство счётности счётного объединения счётных множеств использует следующее линейное упорядочивание множества всех пар натуральных чисел:

$$\langle 0,0\rangle,\ \langle 0,1\rangle,\ \langle 1,0\rangle,\ \langle 0,2\rangle,\ \langle 1,1\rangle,\ \langle 2,0\rangle,\ \langle 0,3\rangle,\ldots,\langle 3,0\rangle,\ \ldots \tag{1}$$

Очень полезным для нас оказывается то счастливое обстоятельство, что номер пары $\langle a,b\rangle$ в последовательности (1) полиномиально выражается через a и b, а именно, он равен

$$\mathbf{Cantor}(a,b)=((a+b)^2+3a+b)/2 \tag{2}$$

(мы начинаем нумерацию пар в (1) с 0, а не с 1). Соответственно диофантовыми оказываются функции $\mathbf{Elema}(c)$ и $\mathbf{Elemb}(c)$, дающие по номеру пары её первый и второй элементы:

$$a=\mathbf{Elema}(c) \iff \exists y[(a+y)^2+3a+y=2c], \tag{3}$$

$$b=\mathbf{Elemb}(c) \iff \exists x[(x+b)^2+3x+b=2c]. \tag{4}$$

Нумерацию пар легко обобщить на нумерацию троек, четвёрок и т. д., например, можно положить

$$\begin{gathered}\mathbf{Cantor}_1(a_1)=a_1,\\ \mathbf{Cantor}_{n+1}(a_1,\ldots,a_{n+1})=\mathbf{Cantor}_n(a_1,\ldots,a_{n-1},\mathbf{Cantor}(a_n,a_{n+1}))\end{gathered} \tag{5}$$

и называть число $\mathbf{Cantor}_n(a_1,\ldots,a_n)$ *канторовым номером* кортежа $\langle a_1,\ldots,a_n\rangle$. Аналогично (3)–(4), функция $\mathbf{Elem}_{n,m}(c)$, дающая по числу c, рассматриваемому как номер n-ки натураль-

ных чисел, значение её m-й компоненты, будет диофантовой:

$$a = \mathbf{Elem}_{n,m}(c) \Leftrightarrow$$

$$\Leftrightarrow \exists x_1 \ldots x_{m-1} x_{m+1} \ldots x_n [2^{2^n} \mathbf{Cantor}_n(x_1, \ldots, x_{m-1}, a, x_{m+1}, \ldots, x_n) = 2^{2^n} c] \quad (6)$$

(появление множителя 2^{2^n} в (6) связано с тем, что $\mathbf{Cantor}_n$ не является полиномом с целыми коэффициентами).

§ 3.2. Гёделево кодирование

Введённая в предыдущем параграфе нумерация кортежей натуральных чисел обладает одним существенным для наших целей недостатком: обратная функция $\mathbf{Elem}_{n,m}(c)$ является диофантовой функцией одной переменной при любых фиксированных значениях n и m, но не видно пути установить диофантовость $\mathbf{Elem}_{n,m}(c)$ как функции трёх аргументов c, m, n. Для работы с кортежами, длина которых не фиксирована заранее, нам придётся использовать другие методы.

Один из них основан на *китайской теореме об остатках* (см. Приложение 2). Пусть имеется некоторый кортеж

$$\langle a_1, \ldots, a_n \rangle. \quad (1)$$

Выберем числа

$$b_1, \ldots, b_n \quad (2)$$

так, чтобы они были попарно взаимно просты и

$$a_i < b_i, \quad i = 1, \ldots, n. \quad (3)$$

По китайской теореме об остатках мы можем найти число a такое, что

$$a_i \equiv \mathbf{rem}(a, b_i), \quad i = 1, \ldots, n. \quad (4)$$

Таким образом, элементы кортежа (1) однозначно определяются по

$$a, \ b_1, \ldots, b_n. \quad (5)$$

На первый взгляд, мы не получили никакого выигрыша, перейдя от n чисел (1) к $n+1$ числу (5). Смысл этого перехода состоит в том, что, в отличие от (1), выбор чисел (2) находится в значительной степени в нашей власти, и мы легко можем выбрать их так, чтобы они определялись конечным набором чисел. Например, положим

$$b_i = bi + 1, \quad i = 1, \ldots, n, \quad (6)$$

где b кратно $n!$ и столь велико, что выполнены неравенства (3). В этом случае числа b_i и b_j будут взаимно просты

при $i < j$. Действительно, пусть

$$p \mid bi+1, \tag{7}$$

$$p \mid bj+1, \tag{8}$$

тогда, очевидно,

$$\mathbf{GCD}(p,b)=1, \tag{9}$$

$$\mathbf{GCD}(p,n!)=1, \tag{10}$$

но

$$p \mid b(j-i), \tag{11}$$

и потому

$$p \mid j-i, \tag{12}$$

$$p \le j-i < n. \tag{13}$$

Из (10) и (13) следует, что $p=1$, т. е. b_i и b_j взаимно просты.

Таким образом, пара чисел $\langle a,b\rangle$ несёт информацию о каждом элементе кортежа (1), однако не содержит информации о его длине. Мы можем добавить эту информацию совершенно формально, а именно, будем называть тройку $\langle a,b,c\rangle$ *гёделевым кодом* кортежа (1), если $c=n$ и для $i=1,\ldots,n$

$$a_i = \mathbf{GElem}(a,b,i), \tag{14}$$

где **GElem** — диофантова функция, задаваемая представлением

$$e=\mathbf{GElem}(a,b,i) \Leftrightarrow e=\mathbf{rem}(a,bi+1). \tag{15}$$

Естественно, что $\langle a,b,0\rangle$ — код *пустого кортежа*, т. е. кортежа длины нуль, не содержащего ни одного элемента.

Ясно, что при желании мы могли бы назвать гёделевым кодом не тройку $\langle a,b,c\rangle$, а число $\mathbf{Cantor}_3(a,b,c)$ и получить нумерацию кортежей произвольной длины натуральными числами.

Отметим одно существенное отличие гёделевой кодировки от канторовой — один и тот же кортеж имеет бесконечно много гёделевых кодов ввиду произвола в выборе b и последующего произвола в выборе a. Это не важно для дальнейшего, ибо даже при фиксировании одного кода для каждого кортежа мы не могли бы говорить о диофантовой функции, выдающей по числам $a_1,\ldots,a_n$ код кортежа $\langle a_1,\ldots,a_n\rangle$, поскольку диофантова функция может иметь только фиксированное количество натуральных аргументов.

§ 3.3. Позиционное кодирование

Гёделево кодирование позволяет работать с кортежами произвольной длины, при этом элементы кортежа определяются по его коду и номеру элемента с помощью несложной диофантовой функции. Гораздо труднее установить диофантовость других

операций и отношений между кодами, например *конкатенации*, которая по кодам кортежей

$$\langle p_1,\ldots,p_m\rangle \tag{1}$$

и

$$\langle q_1,\ldots,q_n\rangle \tag{2}$$

выдаёт код кортежа

$$\langle p_1,\ldots,p_m,q_1,\ldots,q_n\rangle. \tag{3}$$

Для кодировки, которая будет введена в этом параграфе, мы сумеем установить диофантовость конкатенации и ряда других функций и отношений.

Новые коды также будут состоять из трёх чисел a, b, c, и третье будет иметь то же значение, что и в гёделевой нумерации, т. е. равное n — длине кодируемого кортежа

$$\langle a_1,\ldots,a_n\rangle. \tag{4}$$

На b будет теперь налагаться более сильное неравенство

$$b > a_i, \quad i = 1,\ldots,n, \tag{5}$$

а значение a будет определяться равенством

$$a = a_n b^{n-1} + a_{n-1} b^{n-2} + \ldots + a_1 b^0. \tag{6}$$

Иными словами, $a_n,\ldots,a_1$ — это цифры в записи числа a в позиционной системе счисления с основанием b, и потому кортеж (4) однозначно восстанавливается по a, b и c. Тройку $\langle a,b,c\rangle$ будем называть *позиционным кодом* кортежа (4), если $c = n$ и выполнено (5) и (6). Позиционным кодом пустого кортежа будет, очевидно, тройка $\langle 0,b,0\rangle$.

Так же, как в случае гёделевых кодов, один и тот же кортеж имеет бесконечно много позиционных кодов, но, в отличие от гёделевых кодов, не каждая тройка является позиционным кодом какого-либо кортежа. Это не является существенным недостатком, ибо легко установить диофантовость отношения *быть позиционным кодом*:

$$\mathbf{Code}(a,b,c) \Leftrightarrow b \geq 2 \,\&\, a < b^c. \tag{7}$$

В дальнейшем мы будем в основном иметь дело с позиционными кодами, и потому слово «позиционный» будет часто опускаться. Для элементов кода $\langle a,b,c\rangle$ будут использоваться следующие названия: a — *шифр*, b — *основание*, c — *длина*.

Функция $\mathbf{Elem}(a,b,d)$, выдающая по шифру и основанию d-й элемент соответствующего кортежа, является, как легко видеть, диофантовой:

$$e = \mathbf{Elem}(a,b,d) \Leftrightarrow$$

$$\Leftrightarrow \exists xyz[d = z+1 \,\&\, a = xb^d + eb^z + y \,\&\, e < b \,\&\, y < b^z]. \tag{8}$$

Пусть **Concat**$(a,b,c,a_1,b_1,c_1,a_2,b_2,c_2)$ обозначает отношение *тройка* $\langle a,b,c,\rangle$ *является кодом конкатенации кортежей с кодами* $\langle a_1,b_1,c_1\rangle$ *и* $\langle a_2,b_2,c_2\rangle$. Легко видеть, что

$$\mathbf{Concat}(a,b,c,a_1,b,c_1,a_2,b,c_2) \Leftrightarrow$$

$$\Leftrightarrow \mathbf{Code}(a_1,b,c_1)\ \&\ \mathbf{Code}(a_2,b,c_2)\ \&\ a=a_2b^{c_1}+a_1\ \&\ c=c_1+c_2. \qquad (9)$$

Таким образом, при фиксированном основании конкатенация является диофантовой операцией; поскольку мы рассматриваем только натуральнозначные функции, то точнее было бы сказать, что диофантовыми являются две функции, вычисляющие соответственно шифр и длину кода конкатенации двух кортежей. Мы, однако, не будем вводить специальных обозначений для этих функций, а будем использовать запись $\langle a_1,b,c_1\rangle + \langle a_2,b,c_2\rangle$ для обозначения кода по основанию b конкатенации кортежей с кодами $\langle a_1,b,c_1\rangle$ и $\langle a_2,b,c_2\rangle$.

Диофантовость **Concat** в общем случае (т. е. когда основания могут быть различными) будет установлена в § 3.5.

§ 3.4. Диофантовость биномиальных коэффициентов, факториала и простых чисел

В качестве несколько неожиданного следствия развитой в предыдущем параграфе несложной техники позиционного кодирования мы легко получаем диофантовость биномиальных коэффициентов. Для этого достаточно заметить, что кортеж

$$\left\langle \binom{n}{0},\binom{n}{1},\ldots,\binom{n}{n}\right\rangle \qquad (1)$$

имеет своим позиционным кодом тройку $\langle (b+1)^n,b,n+1\rangle$, если b достаточно велико, чтобы быть основанием кода этого кортежа, например, если $b=2^n+1$. Таким образом,

$$c=\binom{n}{m} \Leftrightarrow c=\mathbf{Elem}((2^n+2)^n,2^n+1,m+1). \qquad (2)$$

Как известно, биномиальные коэффициенты легко выражаются через факториалы:

$$\binom{n}{m}=\frac{n!}{m!(n-m)!}. \qquad (3)$$

Отсюда получаем следующую формулу, выражающую факториал через биномиальные коэффициенты и возведение в степень:

$$m!=\frac{n!}{\binom{n}{m}(n-m)!}=\frac{n(n-1)\ldots(n-m+1)}{\binom{n}{m}}=\frac{n^m}{\binom{n}{m}}\left(1-\frac{1}{n}\right)\ldots\left(1-\frac{m-1}{n}\right)=$$

$$=\lim_{n\to\infty}\frac{n^m}{\binom{n}{m}}\left(1-\frac{1}{n}\right)\ldots\left(1-\frac{m-1}{n}\right)=\lim_{n\to\infty}\frac{n^m}{\binom{n}{m}}. \qquad (4)$$

В нашем языке диофантовых уравнений нет операции **lim**, но так же, как в § 2.4, и в данном случае её с успехом заменит функция **div** — из (4) следует, что при достаточно большом n

$$m! = n^m \ \mathbf{div} \ \binom{n}{m}. \tag{5}$$

Нетрудно проверить, что (5) верно уже при $n \geq (m+1)^{m+2}$, так что

$$m! = (m+1)^{m(m+2)} \ \mathbf{div} \ \binom{(m+1)^{m+2}}{m}. \tag{6}$$

Установив диофантовость факториала, мы немедленно получаем диофантовость свойства *быть простым числом*:

$$\mathbf{Prime}(a) \Leftrightarrow a > 1 \ \& \ \mathbf{GCD}(a,(a-1)!) = 1. \tag{7}$$

Напомним, что, как показано в § 1.4, отсюда следует, что *можно найти полином от многих переменных с целыми коэффициентами такой, что множество всех натуральных значений, принимаемых им при натуральных значениях переменных, есть в точности множество всех простых чисел.*

§ 3.5 Сравнение кортежей

Как уже говорилось, один и тот же кортеж имеет бесконечно много кодов, соответствующих разным основаниям — такие коды мы будем называть *эквивалентными*. Основная цель этого параграфа — установить диофантовость эквивалентности кодов, т. е. диофантовость отношения $\mathbf{Equal}(a_1,b_1,c_1,a_2,b_2,c_2)$ — *тройки* $\langle a_1,b_1,c_1\rangle$ *и* $\langle a_2,b_2,c_2\rangle$ *являются кодами одного и того же кортежа*. Кроме того, будет установлена диофантовость поэлементного неравенства, а именно диофантовость отношения

$$\mathbf{NotGreater}(a_1,b_1,a_2,b_1) \Leftrightarrow \forall k[\mathbf{Elem}(a_1,b_1,k) \leq \mathbf{Elem}(a_2,b_2,k)], \tag{1}$$

и диофантовость сравнения элементов кортежа с числом, а именно диофантовость отношения

$$\mathbf{Small}(a,b,c,e) \Leftrightarrow \mathbf{Code}(a,b,c) \ \& \ \forall k[\mathbf{Elem}(a,b,k) \leq e]. \tag{2}$$

Мы также установим диофантовость некоторого вспомогательного шестиместного отношения, которое будет более сильным, чем **Equal**:

$$\mathbf{Eq}(a_1,b_1,c_1,a_2,b_2,c_2) \Rightarrow \mathbf{Equal}(a_1,b_1,c_1,a_2,b_2,c_2). \tag{3}$$

Обратная импликация будет иметь место только при дополнительном ограничении, а именно, b_2 должно быть достаточно большим по отношению к b_1 и c_1 простым числом. В результате отношение **Equal** сможет быть выражено через **Eq** следующим

образом:

$$\mathbf{Equal}(a_1,b_1,c_1,a_2,b_2,c_2) \Leftrightarrow$$
$$\Leftrightarrow \exists xyz[\mathbf{Eq}(a_1,b_1,c_1,x,y,z)\,\&\,\mathbf{Eq}(a_2,b_2,c_2,x,y,z)]. \qquad (4)$$

Мы начнём с установления диофантовости ещё одного вспомогательного отношения

$$\mathbf{PNotGreater}(a_1,a_2,b) \Leftrightarrow \mathbf{Prime}(b)\,\&\,\mathbf{NotGreater}(a_1,b,a_2,b). \qquad (5)$$

Переход к одинаковому и простому основанию позволяет нам воспользоваться теоремой Куммера (см. Приложение 3) и дать этому отношению следующее представление:

$$\mathbf{PNotGreater}(a_1,a_2,b) \Leftrightarrow \mathbf{Prime}(b)\,\&\,b\uparrow\binom{a_2}{a_1}. \qquad (6)$$

Используя **PNotGreater**, мы можем установить диофантовость отношения

$$\mathbf{PSmall}(a,b,c,e) \Leftrightarrow \mathbf{Prime}(b)\,\&\,\mathbf{Small}(a,b,c,e). \qquad (7)$$

Ясно, что

$$\mathbf{PSmall}(a,b,c,e) \Leftrightarrow$$
$$\Leftrightarrow \mathbf{Prime}(b)\,\&\,[e\geq b \vee \mathbf{PNotGreater}(a,\mathbf{Repeat}(e,b,c),b)], \qquad (8)$$

где $\mathbf{Repeat}(p,q,r)=p(q^r-1)/(q-1)$ — шифр по основанию q кортежа $\langle p,\ldots,p\rangle$ длины r (если $p<q$, конечно).

Теперь у нас достаточно средств для решения нашей основной задачи. Пусть мы имеем два основания — «маленькое» b_1 и «большое» b_2 — и код $\langle a_2,b_2,c\rangle$ некоторого кортежа, все элементы которого меньше b_1. Очевидно, что шифр a_1 того же кортежа по основанию b_1 удовлетворяет сравнению

$$a_1 \equiv a_2 (\mathbf{mod}\ b_2-b_1) \qquad (9)$$

и неравенству

$$a < b_1^c, \qquad (10)$$

поэтому если b_2 столь велико, что

$$b_1^c < b_2-b_1, \qquad (11)$$

то a_1 однозначно определяется условиями (9) и (10). Это позволяет нам определить, наконец, отношение **Eq**:

$$\mathbf{Eq}(a_1,b_1,c_1,a_2,b_2,c_2) \Leftrightarrow \mathbf{Code}(a_1,b_1,c_1)\,\&\,c_1=c_2\,\&$$
$$\&\ \mathbf{PSmall}(a_2,b_2,c_2,b_1-1)\,\&\,b_1^{c_1}+b_1<b_2\,\&\,a_1\equiv a_2(\mathbf{mod}\ b_2-b_1). \qquad (12)$$

Легко видеть, что при так определенном **Eq** справедливы импликация (3) и эквивалентность (4), что доказывает диофантовость **Equal**.

Имея теперь в своем распоряжении отношение **Equal**, мы легко можем установить диофантовость отношений **NotGreater** и

Small, переходя к эквивалентным кодам с простым основанием и пользуясь диофантовостью **PNotGreater** и **PSmall**:

$$\mathbf{NotGreater}(a_1,b_1,a_2,b_2) \Leftrightarrow$$
$$\Leftrightarrow \exists x_1x_2yz[\mathbf{Equal}(a_1,b_1,z,x_1,y,z)\ \&\ \mathbf{Equal}(a_2,b_2,z,x_2,y,z)\ \&$$
$$\&\ \mathbf{PNotGreater}(x_1,x_2,y)], \qquad (13)$$

$$\mathbf{Small}(a,b,c,e) \Leftrightarrow \exists xy[\mathbf{Equal}(a,b,c,x,y,c)\ \&\ \mathbf{PSmall}(x,y,c,e)]. \qquad (14)$$

Аналогично мы можем теперь установить диофантовость введённого в § 3.3 9-местного отношения **Concat**:

$$\mathbf{Concat}(a,b,c,a_1,b_1,c_1,a_2,b_2,c_2) \Leftrightarrow$$
$$\Leftrightarrow \exists x_1x_2[\mathbf{Equal}(a_1,b_1,c_1,x_1,b,c_1)\ \&\ \mathbf{Equal}(a_2,b_2,c_2,x_2,b,c_2)\ \&$$
$$\&\ a = x_2b^{c_1}+x_1\ \&\ c = c_1+c_2] \qquad (15)$$

(ср. с (3.9)).

§ 3.6. Расширение функций на кортежи

В этом параграфе мы будем работать с позиционными кодами по некоторому фиксированному основанию b, не меньшему, чем 3. Элементы соответствующих кортежей, очевидно, принадлежат множеству $\mathfrak{N}_b = \{0,1,\ldots,b-1\}$. Пусть F — произвольная функция, определённая на $\mathfrak{N}_b$, значения которой также лежат в $\mathfrak{N}_b$. Такая функция порождает новую двухместную функцию, которую мы будем обозначать через $F[b]$, а именно, если $\langle a,b,c\rangle$ — код кортежа

$$\langle a_1,\ldots,a_c\rangle, \qquad (1)$$

то значение $F[b](a,c)$ по определению равно шифру кортежа

$$\langle F(a_1),\ldots,F(a_c)\rangle \qquad (2)$$

(если a не является шифром по основанию b никакого кортежа длины c, то значение $F[b](a,c)$ не определено). Мы покажем, что *функция $F[b]$ является диофантовой.*

По кортежу (1) можно построить b *характеристических кортежей*

$$\begin{array}{c}\langle h_{0,1},\ldots,h_{0,c}\rangle,\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ \langle h_{b-1,1},\ldots,h_{b-1,c}\rangle,\end{array} \qquad (3)$$

где

$$h_{k,j}=\begin{cases}1, \text{ если } a_j=k,\\ 0 \text{ в противном случае.}\end{cases} \tag{4}$$

Обозначим посредством $h_0,\ldots,h_{b-1}$ шифры кортежей (3). Очевидно, что

$$0\times h_0+1\times h_1+\ldots+(b-1)\times h_{b-1}=a. \tag{5}$$

Кроме того,

$$h_0+\ldots+h_{b-1}=\mathbf{Repeat}(1,b,c) \tag{6}$$

и

$$\mathbf{Ortnorm}_b(h_k,h_l,c),\quad 0\le k<l<b, \tag{7}$$

где $\mathbf{Ortnorm}_b(q_1,q_2,r)$ — отношение ортонормированности: *все элементы кортежей с кодами* $\langle q_1,b,r\rangle$ *и* $\langle q_2,b,r\rangle$ *не превосходят* 1, *причем* 1 *не стоит одновременно на одном и том же месте в обоих кортежах*. Это отношение является диофантовым, ибо

$$\mathbf{Ortnorm}_b(q_1,q_2,r) \Leftrightarrow$$

$$\Leftrightarrow \mathbf{Small}(q_1,b,r,1)\ \&\ \mathbf{Small}(q_2,b,r,1)\ \&\ \mathbf{Small}(q_1+q_2,b,r,1). \tag{8}$$

Легко видеть, что условия (5)–(7) однозначно определяют шифры характеристических кортежей по a, b и c. Эти условия диофантовы, и для завершения доказательства диофантовости $F[b]$ остается увидеть, что шифр кортежа (2) равен

$$F(0)\times h_0+\ldots+F(b-1)\times h_{b-1}. \tag{9}$$

Заметим, что эта техника легко обобщается на случай, когда F — функция m аргументов. В этом случае аргументами $F[b]$ будут длина c и шифры $a_1,\ldots,a_m$ некоторых кортежей

$$\begin{gathered}\langle a_{1,1},\ldots,a_{1,c}\rangle,\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ \langle a_{m,1},\ldots,a_{m,c}\rangle.\end{gathered} \tag{10}$$

Для получения аналога равенства (8) нам потребуются b^m характеристических кортежей, определяемых следующим аналогом (4):

$$h_{k_1,\ldots,k_m,l}=\begin{cases}1, \text{ если } a_{1,l}=k_1,\ \ldots,\ a_{m,l}=k_m,\\ 0 \text{ в противном случае.}\end{cases} \tag{11}$$

Шифры $h_{k_1,\ldots,k_m}$ этих кортежей также удовлетворяют аналогам условий (5)–(7) и определяются ими.

Упражнения

3.1. В большинстве случаев использования полиномов $\mathbf{Cantor}_n$ в этой книге не существенно, что они принимают в качестве своего значения любое натуральное число, и вместо $\mathbf{Cantor}_n$ можно использовать любой полином с рациональными коэффициентами, который принимает каждое своё значение ровно один раз. Покажите, что этим свойством обладает полином

$$a_1+(a_1+a_2)^2+(a_1+a_2+a_3)^3+\ldots+(a_1+\ldots+a_n)^n.$$

3.2. Докажите, что **Cantor** является единственным (с точностью до порядка аргументов) полиномом с рациональными коэффициентами степени не более, чем 4, взаимно однозначно отображающим множество всех пар натуральных чисел на натуральный ряд.

3.3. Установите диофантовость функции трёх аргументов, значение которой равно $\prod_{k\le c}(a+bk)$.

3.4. Найдите унарное экспоненциально диофантово представление для центрального биномиального коэффициента $\binom{2n}{n}$ на основе тождества

$$\frac{1}{\mathbf{sqrt}(1-4X)}=\sum_{n=0}^{\infty}\binom{2n}{n}X^n,$$

справедливого при $|X|<0{,}25$ (**sqrt** — квадратный корень).

3.5. Постройте другое экспоненциально диофантово представление для факториала на основе следующих классических равенств:

$$\sum_{k=0}^{\infty}\frac{\tau^k}{k!}=e^{\tau}=\lim_{y\to\infty}\left(1+\frac{\tau}{y}\right)^y.$$

3.6. Установите диофантовость трёхместного отношения $a/b=|\mathbf{B}_{2c}|$, где $\mathbf{B}_0=1$, $\mathbf{B}_1=-1/2$, $\mathbf{B}_2=1/6,\ldots$ – числа Бернулли.

3.7. Укажите обобщённое диофантово представление свойства **Prime** в предположении диофантовости двухместного отношения

$$\mathbf{Bernoulli}(a,b)\iff\exists n\left[\frac{a}{b}=|\mathbf{B}_n|\right].$$

3.8. Установите диофантовость отрицаний отношений **Code**, **Equal**, **NotGreater** и **Small**.

3.9. Установите диофантовость функций **Mult** и **Add**, которые по элементам кодов $\langle p,q,r\rangle$ и $\langle u,v,w\rangle$ кортежей $\langle p_1,\ldots,p_r\rangle$ и $\langle u_1,\ldots,u_w\rangle$ дают шифры по основанию qv кортежей $\langle p_1v_1,\ldots,p_1v_w,\ \ldots,\ p_rv_1,\ldots,p_rv_w\rangle$ и $\langle p_1+v_1,\ldots,p_1+v_w,\ \ldots,\ p_r+v_1,\ldots,p_r+v_w\rangle$.

3.10. Установите диофантовость функции **Sum**, которая по коду кортежа определяет сумму его элементов.

3.11. Установите диофантовость функции $\mathbf{Less}(a_1,a_2,b)$, значение которой есть шифр по основанию b кортежа $\langle t_1,\ldots,t_c\rangle$, где $t_i=1$, если $\mathbf{Elem}(a_1,b,i)<\mathbf{Elem}(a_2,b,i)$, и $t_i=0$ в противном случае.

3.12. Установите диофантовость функции $\pi(a)$ — *количество простых чисел, не превосходящих* a.

3.13. Постройте полином **Primenth**$(n, x_1, \ldots, x_m)$, который при каждом фиксированном значении n и произвольных значениях $x_1, \ldots, x_m$ принимает только одно положительное значение — n-ое простое число.

3.14. При установлении в § 3.5 диофантовости отношений **Equal**, **NotGreater** и **Small** мы воспользовались установленной в § 3.4 диофантовостью свойства **Prime**. Покажите, что этого можно было избежать, применяя теорему Куммера только для $p=2$.

3.15. Пусть $\delta(0)=a_0, \ldots, \delta(k-1)=a_{k-1}$, $\delta(n+k)=b_{k-1}\delta_{n+k-1}+\ldots+b_0\delta_n$ — произвольная линейная рекуррентная последовательность k-го порядка. Установите диофантовость этой последовательности, рассматривая её как функцию $2k+1$ аргументов $a_0, \ldots, a_{k-1}, b_0, \ldots, b_{k-1}, n$.

3.16. Основное применение техника § 3.6 найдёт в главе 5, где мы будем работать с кодами по фиксированному основанию. Тем не менее некоторые функции несложно диофантово расширять и при переменном основании. Установите диофантовость трёхместной функции **Min** такой, что

$$\forall k[\mathbf{Elem}(\mathbf{Min}(a_1, a_2, b), k)=\mathbf{min}(\mathbf{Elem}(a_1, b, k), \mathbf{Elem}(a_2, b, k))].$$

3.17. Покажите, что если $ad-bc=1$, то матрица $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ представляется как произведение матриц $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, причём единственным образом. Это свойство можно использовать для кодирования кортежей произвольной длины, состоящих только из 0 и 1. Установите диофантовость конкатенации кортежей при таком представлении.

Открытые вопросы

3.1. Имеется ли какой-либо аналог теоремы Куммера (см. Приложение 2) для сложения в позиционной системе счисления, в которой весами разрядов являются числа $\alpha_b(1)$, $\alpha_b(2)$, ... ?

3.2. Согласно теореме Вольстенхольма [1862], при $n>3$

$$\mathbf{Prime}(n) \Rightarrow \binom{2n-1}{n-1} \equiv 1 (\mathbf{mod}\ n^3).$$

Верна ли обратная импликация?

Комментарии

Кодирование кортежей неограниченной длины на основе китайской теоремы об остатках впервые было использовано К. Гёделем в его знаменитой работе [1931]. Там же был предложен ещё один способ кодирования, использующий *основную теорему арифметики*, т. е. единственность разложения на простые множители. К. Гёдель использовал эти кодировки для арифметизации утверждений и потому мог свободно использовать любые кванторы. В диофантовых представлениях используются только кванторы существования, и потому мы более ограничены в выборе кодировок.

Гёделево кодирование сыграло особую роль в исследованиях по 10-й проблеме Гильберта не только из-за простоты диофантова представления функции **GElem**. Использование китайской теоремы об остатках даёт следующую уникальную возможность, не присущую другим кодировкам, для вычисле-

ния значений полиномов. Пусть $P(x_1,\ldots,x_m)$ — полином с натуральными коэффициентами, $\langle a_1,b,c\rangle$, ..., $\langle a_m,b,c\rangle$ — гёделевы коды каких-то кортежей

$$\langle a_{1,1},\ldots,a_{1,c}\rangle,\ldots,\langle a_{m,1},\ldots,a_{m,c}\rangle.$$

Тогда тройка $\langle P(a_1,\ldots,a_m),b,c\rangle$ является гёделевым кодом кортежа

$$\langle P(a_{1,1},\ldots,a_{m,1}),\ldots,P(a_{1,c},\ldots,a_{m,c})\rangle$$

при условии, что b достаточно велико. Это свойство было использовано в работе Девиса, Патнама и Робинсон [1961] для получения существенного прогресса в иссследовании 10-й проблемы Гильберта — установления алгоритмической неразрешимости экспоненциально диофантовых уравнений (подробнее об их работе см. комментарии к главам 5 и 6).

Гёделево кодирование обладает, однако, и рядом недостатков. Хотя диофантово представление для функции **GElem** очень просто, установить же диофантовость других операций над кодами, например конкатенации, довольно трудно. В этом отношении позиционное кодирование «перераспределяет» трудности — для установления диофантовости **Elem** требуется установить диофантовость возведения в степень, но зато когда это сделано, диофантовость других функций и отношений устанавливается сравнительно просто.

До того как была установлена диофантовость возведения в степень, в исследованиях по 10-й проблеме Гильберта была использована позиционная кодировка, в которой весами разрядов были члены рекуррентной последовательности второго порядка (см. работы Матиясевича [1968а, 1968б]).

Вскоре после установления диофантовости возведения в степень позиционная кодировка была использована в работе Матиясевича [1971б] для получения диофантовых представлений линейных рекуррентных последовательностей произвольного порядка (см. упражнение 3.15). Ещё более эффективным средством позиционные кодировки стали после того, как была уяснена роль теоремы Куммера, которую она может играть при построении диофантовых представлений. Впервые эта новая техника была применена в работе Матиясевича [1976].

Экспоненциальная диофантовость биномиальных коэффициентов и факториала была установлена Дж. Робинсон [1952] независимо от общей идеи позиционного кодирования.

Экспоненциально диофантово представление для множества простых чисел также было указано в работе Дж. Робинсон [1952]. Когда в работе Патнама [1960] было замечено, что диофантовы множества — это множества натуральных значений полиномов (см. § 1.4), стало ясно, что установление диофантовости возведения в степень даст возможность строить полиномы, представляющие простые и только простые числа. Это казавшееся тогда малоправдоподобным следствие рассматривалось многими как неформальный довод против диофантовости возведения в степень.

Ввиду важности множества простых чисел ряд работ был посвящен специально диофантовым представлениям этого множества. В частности, многих исследователей интересовал вопрос о том, сколь малым может быть количество переменных в полиноме, представляющем все простые числа и только их.

В работе Матиясевича [1971a] была получена первая оценка сверху в 24 переменные (улучшенная в добавлении к английскому переводу до 21 переменной). Эта оценка была улучшена до 12 переменных в работах Вады [1975] и Джонса, Сато, Вады и Вьенса [1976]. В настоящее время (1990 г.) наименьшее количество — 10 переменных — имеет полином, указанный в работе Матиясевича [1977a]. Этот полином был построен на основе специфических особенностей множества простых чисел. Полином с 10 неизвестными для простых чисел может быть построен также на основе универсальной техники (см. работы Матиясевича [1977], Джонса [19826] и комментарии к главе 8).

Полиномы, которые строятся на основе общей техники, естественно, получаются довольно громоздкими. В то же время используя специфику простых чисел, можно найти полином, занимающий всего несколько строк. В работе Джонса, Сато, Вады и Вьенса [1976] приведён следующий полином:

$$\begin{aligned}(k+2)\{1 &- [wz+h+j-q]^2 - [(gk+2g+k+1)(h+j)+h-z]^2 - [2n+p+q+z-e]^2 - \\ &- [16(k+1)^3(k+2)(n+1)^2+1-f^2]^2 - [e^3(e+2)(a+1)^2+1-o^2]^2 - \\ &- [(a^2-1)y^2+1-x^2]^2 - [16r^2y^4(a^2-1)+1-u^2]^2 - [n+l+v-y]^2 - \\ &- [((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2 - [(a^2-1)l^2+1-m^2]^2 - \\ &- [q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2 - [z+pl(a-p)+t(2ap-p^2-1)-pm]^2 - \\ &- [ai+k+1-l-i]^2 - [p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2\}.\end{aligned}$$

Он содержит 26 переменных (все буквы латинского алфавита!) и множество его *положительных* значений есть в точности множество всех простых чисел. Рассмотрение только положительных значений позволяет вместо (1.4.8) брать представление типа $x_0(1-D^2(x_0,\ldots,x_m))=a$. В итоге получается парадоксальный факт: приведённый выше полином, представляющий только простые числа, сам является произведением двух полиномов!

Имея диофантово представление множества всех простых чисел, легко можно получить диофантовы представления множества всех *простых чисел Мерсенна*, т. е. простых чисел вида 2^n-1, и множества всех *простых чисел Ферма*, т. е. простых чисел вида 2^n+1. Однако для простоты чисел вида $2^n\pm1$ имеются специальные критерии, формулируемые в терминах делимости членов некоторых рекуррентных последовательностей, что позволило Джонсу [1979] дать для этих множеств представления с 7 неизвестными. (В настоящее время известно всего пять простых чисел вида 2^n+1, и весьма правдоподобной считается гипотеза о том, что других таких чисел нет; в таком случае для задания простых чисел Ферма достаточно и полинома с одной переменной.)

Как хорошо известно, простые числа Мерсенна тесно связаны с чётными совершенными числами. В работе Кряучюкаса [1979] приведено диофантово представление множества *всех* совершенных чисел.

Положительный ответ на открытый вопрос 3.2 позволил бы дать сравнительно несложное диофантово представление для множества всех простых чисел (в этой связи см. упражнение 3.4).

Глава 4

УНИВЕРСАЛЬНЫЕ ДИОФАНТОВЫ УРАВНЕНИЯ

В этой главе мы построим *универсальное диофантово уравнение* — решение любого диофантова уравнения может быть сведено к решению этого уравнения при подходящем выборе значений параметров. Универсальное уравнение позволит нам построить диофантово множество с недиофантовым дополнением.

§ 4.1. Основные определения

Универсальное уравнение имеет вид семейства уравнений

$$U(a_1,\ldots,a_n,k_1,\ldots,k_l,y_1,\ldots,y_w)=0, \tag{1}$$

параметры которого подразбиты на две группы: *параметры-элементы* $a_1,\ldots,a_n$ и *параметры-коды* $k_1,\ldots,k_l$. Уравнение (1) называется *универсальным уравнением*, если для любого диофантова уравнения с n параметрами

$$D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0 \tag{2}$$

можно указать такие числа $k_1^D,\ldots,k_l^D$, что уравнение (2) разрешимо относительно $x_1,\ldots,x_m$ в точности при тех же значениях параметров $a_1,\ldots,a_n$, при которых уравнение

$$U(a_1,\ldots,a_n,k_1^D,\ldots,k_l^D,y_1,\ldots,y_w)=0 \tag{3}$$

разрешимо относительно $y_1,\ldots,y_w$.

Пользуясь иной терминологией, можно сказать, что уравнение (3) является другим представлением диофантова множества, задаваемого уравнением (2). Таким образом, каждое универсальное уравнение порождает кодирование диофантовых множеств данной размерности — кортеж $\langle k_1^D,\ldots,k_l^D\rangle$ можно считать *кодом множества*, задаваемого уравнением (2).

На универсальное уравнение (1) можно посмотреть и как на уравнение, в котором все параметры $a_1,\ldots,a_n$, $k_1,\ldots,k_l$ являются параметрами-элементами; при таком взгляде уравнение (1) определяет некоторое диофантово множество $(l+n)$-ок натуральных чисел, которое, естественно, называется *универсальным диофантовым множеством*.

Нетрудно увидеть, что ценой увеличения количества неизвестных любое универсальное уравнение может быть преобразовано в универсальное уравнение с тем же количеством параметров-элементов, но всего с одним параметром-кодом. Действительно, если (1) — универсальное уравнение, то универсальным является и уравнение

$$U^2(a_1,\ldots,a_n,k_1,\ldots,k_l,y_1,\ldots,y_w)+(k-2^l\mathbf{Cantor}_l(k_1,\ldots,k_l))^2=0 \qquad (4)$$

с одним параметром-кодом k и $l+w$ неизвестными $k_1,\ldots,k_l$, $y_1,\ldots,y_w$ (множитель 2^l обеспечивает целочисленность коэффициентов). Кодом множества (2) в кодировке, определяемой уравнением (4), будет, очевидно, число $2^l\mathbf{Cantor}_l(k_1^{\mathrm{D}},\ldots,k_l^{\mathrm{D}})$.

В этой главе будет установлено существование универсальных уравнений для каждого n. При этом, вообще говоря, мог оказаться неизбежным рост w с ростом n. Это, однако, не происходит: *существует константа* $\mathbf{m}$ *такая, что для любого* n *имеется универсальное уравнение* (1) *с* $l=1$ *и* $w=\mathbf{m}$.

Ограничить количество неизвестных в универсальном уравнении помогает опять-таки канторова нумерация. Пусть $\mathbf{m}$ — количество неизвестных в некотором универсальном диофантовом уравнении

$$U_1(a,k,y_1,\ldots,y_{\mathbf{m}})=0, \qquad (5)$$

кодирующем одномерные диофантовы множества. Определим при $n>1$ полином U_n следующим образом:

$$U_n(a_1,\ldots,a_n,k,y_1,\ldots,y_{\mathbf{m}}) = U_1(2^n\mathbf{Cantor}_n(a_1,\ldots,a_n),k,y_1,\ldots,y_{\mathbf{m}}). \qquad (6)$$

Проверим, что уравнение

$$U_n(a_1,\ldots,a_n,k,y_1,\ldots,y_{\mathbf{m}})=0 \qquad (7)$$

является универсальным. Пусть (2) — произвольное диофантово уравнение. Рассмотрим одномерное диофантово множество $\mathfrak{D}$, задаваемое уравнением

$$D^2(z_1,\ldots,z_n,x_1,\ldots,x_m)+(a-2^n\mathbf{Cantor}_n(z_1,\ldots,z_n))^2=0. \qquad (8)$$

В силу универсальности уравнения (5) найдётся такое число $k^{\mathfrak{D}}$ — код множества $\mathfrak{D}$, что уравнение

$$U_1(a,k^{\mathfrak{D}},y_1,\ldots,y_{\mathbf{m}})=0 \qquad (9)$$

также определяет множество $\mathfrak{D}$. Остается заметить, что согласно определению (6) уравнение

$$U_n(a_1,\ldots,a_n,k^{\mathfrak{D}},y_1,\ldots,y_{\mathbf{m}})=0 \qquad (10)$$

разрешимо или не разрешимо одновременно с уравнением (2), так что в качестве требуемого в определении универсальности числа k^{D} можно взять $k^{\mathfrak{D}}$.

§ 4.2. Кодировка уравнений

Как было показано в предыдущем параграфе, нам достаточно найти универсальное диофантово уравнение (1.1) при $n=1$. Мы начнём с построения универсального диофантова уравнения с шестью параметрами-кодами b, c_L, c_R, d, e, f, а именно, укажем полином U такой, что, каково бы ни было диофантово уравнение

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

найдутся такие числа b^D, c_L^D, c_R^D, d^D, e^D, f^D что уравнение (1) разрешимо или неразрешимо для тех же значений параметра a, что и уравнение

$$U(a, b^D, c_L^D, c_R^D, d^D, e^D, f^D, y_7, \ldots, y_m) = 0. \tag{2}$$

Поскольку на протяжении этой главы мы будем иметь дело только с одним «произвольным» диофантовым уравнением (1), для упрощения записи индекс D у параметров будет в дальнейшем опускаться.

Из определения универсальности следует только, что по шестёрке $\langle b, c_L, c_R, d, e, f\rangle$ можно определить лишь множество, задаваемое уравнением (1). В нашей же конструкции по этой шестёрке можно будет определить и само уравнение (1), и потому мы будем называть её также *расширенным кодом уравнения* (1).

Расширенный код должен, очевидно, содержать информацию о количестве переменных и степени полинома D, а также о его коэффициентах. Первые две характеристики будут представлены явно, а именно, e будет равно m, т. е. количеству неизвестных в уравнении (1), а d может быть любым числом, превосходящим степень полинома D относительно всех переменных (не ограничивая общности, мы будем считать, что эта степень больше 0). Кроме того, значение f будет определяться равенством

$$f = 2^{d^1} + \ldots + 2^{d^e}. \tag{3}$$

Тройку $\langle d, e, f\rangle$ будем называть *форматом уравнения* (1). Понятно, что информация, содержащаяся в f, избыточна. Более того, отношение **Format**(d, e, f), определяемое равенством (3), является диофантовым (см. упражнение 4.3), но мы не будем использовать этот факт.

В предыдущей главе мы ввели разные способы кодирования кортежей *натуральных* чисел, но коэффициенты полинома D в общем случае — *целые* числа. По этой причине мы сначала представим полином D в виде разности двух полиномов с натураль-

ными коэффициентами:

$$D(x_0,\ldots,x_m)=C_L(x_0,\ldots,x_m)-C_R(x_0,\ldots,x_m), \tag{4}$$

$$C_L(x_0,\ldots,x_m)=\sum_{i_0+\ldots+i_m<d} c_{L,i_0,\ldots,i_m}x_0^{i_0}\ldots x_m^{i_m}, \tag{5}$$

$$C_R(x_0,\ldots,x_m)=\sum_{i_0+\ldots+i_m<d} c_{R,i_0,\ldots,i_m}x_0^{i_0}\ldots x_m^{i_m}. \tag{6}$$

Числа c_L и c_R будут шифрами по основанию b некоторых кортежей, несущих информацию о коэффициентах полиномов C_L и C_R соответственно. Поскольку в дальнейшем мы будем одинаково работать с c_L, C_L и c_R, C_R, индексы L и R будут обычно опускаться.

Чтобы определить c, мы должны сначала каким-то образом линейно расположить коэффициенты $c_{i_0,\ldots,i_m}$. Кроме того, по причине, которая станет ясной позднее, мы умножим $c_{i_0,\ldots,i_m}$ на подходящие множители. А именно, определим *шифр с полинома C по основанию b* равенством

$$c=\sum_{i_0+\ldots+i_m<d} i_0!\ldots i_m!(d-i_0-\ldots-i_m)!c_{i_0,\ldots,i_m}b^{d^{m+1}-i_0d^0-\ldots-i_md^m}. \tag{7}$$

Пятёрку чисел $\langle b,c,d,e,f\rangle$ мы будем называть *кодом полинома C* при дополнительном условии

$$b>d!\max\{c_{i_0,\ldots,i_m}\} \tag{8}$$

(это неравенство гарантирует однозначное восстановление коэффициентов $c_{i_0,\ldots,i_m}$ по b, c и d). Наконец, шестёрка $\langle b,c_L,c_R,d,e,f\rangle$ будет *расширенным кодом уравнения* (1), если пятёрки $\langle b,c_L,d,e,f\rangle$ и $\langle b,c_R,d,e,f\rangle$ — коды полиномов C_L и C_R.

Мы не стали устанавливать диофантовость отношения **Format** и не будем устанавливать диофантовость шестиместного отношения **ECode**(b,c_L,c_R,d,e,f) — *быть расширенным кодом некоторого уравнения*. Универсальное уравнение

$$U(a,b,c_L,c_R,d,e,f,y_7,\ldots,y_m)=0, \tag{9}$$

которое мы построим, будет обладать следующим свойством:

$$\begin{aligned}&\mathbf{ECode}(b,c_L,c_R,d,e,f)\Rightarrow\\ &\Rightarrow\forall a[\exists y_7,\ldots,y_m[U(a,b,c_L,c_R,d,e,f,y_7,\ldots,y_m)=0]\Leftrightarrow\\ &\Leftrightarrow\exists x_1,\ldots,x_m[D_{b,c_L,c_R,d,e,f}(a,x_1,\ldots,x_m)=0]],\end{aligned} \tag{10}$$

где

$$D_{b,c_L,c_R,d,e,f}(a,x_1,\ldots,x_m)=0 \tag{11}$$

— уравнение, расширенным кодом которого является $\langle b,c_L,c_R,d,e,f\rangle$. Вопрос о разрешимости или неразрешимости (9) в случае, когда шестёрка $\langle b,c_L,c_R,d,e,f\rangle$ не является расширенным кодом никакого уравнения, нас интересовать не будет.

§ 4.3. Кодировка потенциальных решений

В предыдущем параграфе мы ввели понятие формата уравнения

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

как тройки чисел $\langle d,e,f\rangle$ специального вида. В этом параграфе мы введём новую кодировку кортежей натуральных чисел $\langle x_1,\ldots,x_m\rangle$, связанную с рассмотрением их как потенциальных решений уравнения (1). Эта кодировка решений будет состоять из пяти чисел d, e, f, g, h, первые три из которых образуют формат уравнения (1). Число g должно превосходить числа 1, $x_1,\ldots,x_m$, а h определяется равенством

$$h=x_1g^{d^1}+x_2g^{d^2}+\ldots+x_mg^{d^m}. \tag{2}$$

Иными словами, $\langle h,g,d^m+1\rangle$ — это позиционый код кортежа

$$\langle 0,\ldots,0,x_1,0,\ldots,0,x_2,\ \ldots\ ,0,\ldots,0,x_m\rangle, \tag{3}$$

в котором элементы кортежа $\langle x_1,\ldots,x_m\rangle$ «разбавлены» нулями; роль этих дополнительных нулей прояснится в следующем параграфе.

В § 4.2 мы не стали устанавливать диофантовость отношения **Format** и сейчас не будем устанавливать диофантовость отношения **SCode**(d,e,f,g,h) — *быть кодом некоторого потенциального решения*. Вместо этого мы легко установим диофантовость некоторого другого отношения **SCod**, совпадающего с **SCode** при условии, что $\langle d,e,f\rangle$ — формат некоторого уравнения:

$$\mathbf{Format}(d,e,f) \Rightarrow [\mathbf{SCod}(d,e,f,g,h) \Leftrightarrow \mathbf{SCode}(d,e,f,g,h)]. \tag{4}$$

Отношение **SCod** вводится из следующих соображений: если $\langle d,e,f\rangle$ — формат некоторого уравнения, то $\langle f,2,d^e+1\rangle$ — это позиционный код кортежа

$$\langle 0,\ldots,0,1,0,\ldots,0,1,\ \ldots\ ,0,\ldots,0,1\rangle, \tag{5}$$

в котором единицы стоят на тех же самых местах, на которых в (3) стоят $x_1,\ldots,x_m$. С помощью **Equal** мы можем определить t — шифр того же кортежа (5), но по основанию g. В этом случае

$(g-1)t$ будет шифром по основанию g кортежа

$$\langle 0,\ldots,0,g-1,0,\ldots,0,g-1,\ \ldots\ ,\ 0,\ldots,0,g-1\rangle, \tag{6}$$

и остаётся воспользоваться отношением **NotGreater**.

Итак, мы определяем **SCod** посредством

$$\mathbf{SCod}(d,e,f,g,h) \Leftrightarrow$$

$$\Leftrightarrow \exists t\,[\mathbf{Equal}(f,2,d^e+1,t,g,d^e+1)\ \&\ \mathbf{NotGreater}(h,(g-1)t,g)]. \tag{7}$$

Легко видеть, что свойство (4) при таком определении **SCod** выполнено.

§ 4.4. Вычисление значений полиномов

Пусть у нас есть расширенный код $\langle b,c_L,c_R,d,e,f\rangle$ некоторого уравнения

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

и код $\langle d,e,f,g,h\rangle$ его потенциального решения $x_1,\ldots,x_m$. Мы хотим установить, является ли $\langle d,e,f,g,h\rangle$ кодом фактического решения уравнения (1) при заданном значении параметра a. Один очевидный путь — это восстановить по коду уравнения коэффициенты полинома, восстановить по коду решения значения неизвестных и проверить равенство (1). Существует и другой путь, не требующий декодирования. Благодаря нашему выбору кодировок имеется возможность вычислить значение полинома C прямо по его коду $\langle b,c,d,e,f\rangle$, коду потенциального решения $\langle d,e,f,g,h\rangle$ и параметру a.

Пусть w — большое число (точное неравенство будет выписано ниже). С помощью **Equal** мы можем перейти от кодов с основаниями b и g к новым кодам $\langle w,s,d,e,f\rangle$ и $\langle d,e,f,w,t\rangle$ того же полинома C и того же потенциального решения. Рассмотрим число

$$(1+aw+t)^{d-1}=(1+aw^{d^0}+x_1w^{d^1}+\ldots+x_mw^{d^m})^{d-1}=$$

$$=\sum_{i_0+\ldots+i_m<d}\binom{d-1}{i_0\ldots i_m}a^{i_0}x_1^{i_1}\ldots x_m^{i_m}w^{i_0d^0+\ldots+i_md^m}. \tag{2}$$

Заметим, что в этой сумме все показатели степени у w различны, поэтому, если w достаточно велико, то (2) является шифром по основанию w некоторого кортежа, содержащего все одночлены, составляющие C, но с другими коэффициентами. Чтобы «подправить» коэффициенты, умножим (2) на

$$s=\sum_{i_0+\ldots+i_m<d} i_0!\ldots i_m!(d-1-i_0-\ldots-i_m)!c_{i_0\ldots i_m}w^{d^{m+1}-i_0d^0-\ldots-i_md^m} \tag{3}$$

и сгруппируем вместе члены с одинаковыми степенями w:

$$(1+aw+t)^{d-1}s = \sum_{k=0}^{2d^{m+1}-1} C_k w^k. \tag{4}$$

Здесь C_k — некоторые выражения, содержащие $c_{i_0\ldots i_m}$, a, $x_1,\ldots,x_m$. Нетрудно видеть, что

$$C_{d^{e+1}} =$$

$$= \sum_{i_0+\ldots+i_m<d} \binom{d-1}{i_0\ldots i_m} i_0!\ldots i_m!(d-1-i_0-\ldots-i_m)!c_{i_0\ldots i_m} a^{i_0} x_1^{i_1}\ldots x_m^{i_m} =$$

$$= (d-1)!C(a,x_1,\ldots,x_m). \tag{5}$$

Таким образом, если w превосходит $C_0,\ldots,C_{2d^{m+1}-1}$, то

$$C(a,x_1,\ldots,x_m) = \mathbf{Elem}((1+aw+t)^{d-1}s, w, d^{e+1}+1)/(d-1)!. \tag{6}$$

Остаётся найти какую-либо явную нижнюю границу для w, гарантирующую справедливость (6). Нетрудно проверить, что для этого достаточно потребовать, чтобы

$$w > (1+a+h)^{d-1}c. \tag{7}$$

Определим теперь девятиместное отношение

$$\mathbf{Solution}(a,b,c_L,c_R,d,e,f,g,h) \Leftrightarrow$$

$$\Leftrightarrow \mathbf{SCod}(d,e,f,g,h) \,\&\, \exists s_L s_R t w \;\; [w > (1+a+h)^{d-1}(c_L+c_R) \,\&$$

$$\&\, \mathbf{Equal}(c_L,b,d^{e+1}+1,s_L,w,d^{e+1}+1) \,\&\, \mathbf{Equal}(c_R,b,d^{e+1}+1,s_R,w,d^{e+1}+1) \,\&$$

$$\&\, \mathbf{Equal}(h,g,d^e+1,t,w,d^e+1) \,\&$$

$$\&\, \mathbf{Elem}((1+aw+t)^{d-1}s_L,w,d^{e+1}+1) = \mathbf{Elem}((1+aw+t)^{d-1}s_R,w,d^{e+1}+1)]. \tag{8}$$

Как следует из (6),

$$\mathbf{ECode}(b,c_L,c_R,d,e,f) \Rightarrow$$

$$\Rightarrow [\exists gh[\mathbf{SCode}(d,e,f,g,h) \;\&\; \mathbf{Solution}(a,b,c_L,c_R,d,e,f,g,h)] \Leftrightarrow$$

$$\Leftrightarrow \exists x_1\ldots x_m D_{b,c_L,c_R,d,e,f}(a,x_1,\ldots,x_m) = 0]. \tag{9}$$

§ 4.5. Универсальные диофантовы уравнения

Отношение $\mathbf{Solution}(a,b,c_L,c_R,d,e,f,g,h)$, введённое в конце предыдущего параграфа, очевидно, является диофантовым, и мы можем построить диофантово уравнение

$$\mathbf{U}(a,b,c_L,c_R,d,e,f,g,h,y_9,\ldots,y_{\mathbf{m}})=0, \tag{1}$$

задающее это отношение. Нетрудно понять, что отнеся g и h к неизвестным, мы получим требуемое универсальное уравнение (2.9).

Используя технику § 4.1, мы можем теперь построить для каждого n универсальный полином $\mathbf{U}_n$ с одним параметром-кодом и $\mathbf{m}$ неизвестными. Полином $\mathbf{U}_1$ мы, согласно (1.4), определим равенством

$$\mathbf{U}_1(a,k,y_1,\ldots,y_{\mathbf{m}})=\mathbf{U}^2(a,y_1,\ldots,y_{\mathbf{m}})+(k-2^{2^6}\mathbf{Cantor}_6(y_1,\ldots,y_6))^2. \tag{2}$$

Соответственно если $\langle b,c_L,c_R,d,e,f\rangle$ — расширенный код некоторого уравнения

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

то в новой кодировке *кодом уравнения* (3) будет по определению число

$$2^{2^6}\mathbf{Cantor}_6(b,c_L,c_R,d,e,f). \tag{4}$$

При таком определении не каждое натуральное число оказывается кодом какого-либо уравнения. Этот «недостаток» легко можно устранить следующим образом. Ясно, что по каждому конкретному числу k можно узнать, представимо ли оно в виде (4), где $\langle b,c_L,c_R,d,e,f\rangle$ — расширенный код какого-либо уравнения. Если k *не* представимо в таком виде, то будем по определению считать число k *кодом уравнения*

$$\mathbf{U}_1(a,k,x_1,\ldots,x_{\mathbf{m}})=0 \tag{5}$$

с единственным параметром a и $\mathbf{m}$ неизвестными $x_1,\ldots,x_{\mathbf{m}}$. Очевидно, что, *каковы бы ни были значения a и k, уравнение* (5) *имеет решение тогда и только тогда, когда решение имеет уравнение с кодом k* независимо от того, является ли k кодом в первоначальном смысле (4) или кодом уравнения (5).

Для $n>1$ универсальный полином $\mathbf{U}_n$ определяется, согласно (1.6), следующим образом:

$$\mathbf{U}_n(a_1,\ldots,a_n,k,y_1,\ldots,y_{\mathbf{m}})=\mathbf{U}_1(2^n\mathbf{Cantor}_n(a_1,\ldots,a_n),k,y_1,\ldots,y_{\mathbf{m}}). \tag{6}$$

Наконец, определим универсальный полином $\mathbf{U}_0$ равенством

$$\mathbf{U}_0(k,y_1,\ldots,y_{\mathbf{m}})=\mathbf{U}_1(0,k,y_1,\ldots,y_{\mathbf{m}}), \tag{7}$$

считая любой код уравнения (3) также кодом уравнения без параметров

$$D(0,x_1,\ldots,x_m)=0. \tag{8}$$

§ 4.6. Диофантовы множества с недиофантовыми дополнениями

Универсальное диофантово уравнение позволяет нам легко построить пример диофантова множества с недиофантовым дополнением (другой пример будет указан в § 6.6). Существование таких множеств показывает, что мы не можем пополнить ни отрицанием $\neg$, ни квантором общности $\forall$ наш арсенал логических средств для построения диофантовых множеств (состоящий в данный момент из $\exists$, & и $\vee$), ибо дополнение диофантова множества, определяемого уравнением

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

задаётся формулами

$$\neg \exists x_1, \ldots, x_m [D(a, x_1, \ldots, x_m) = 0] \tag{2}$$

и

$$\forall x_1, \ldots, x_m [D(a, x_1, \ldots, x_m) \neq 0]. \tag{3}$$

Построение проводится по классической диагональной схеме. Рассмотрим универсальное диофантово уравнение

$$\mathbf{U}_1(p, q, y_1, \ldots, y_m) = 0 \tag{4}$$

и поставим на место обоих параметров параметр-элемент a:

$$\mathbf{U}_1(a, a, y_1, \ldots, y_m) = 0. \tag{5}$$

Получившееся уравнение определяет некоторое диофантово множество $\mathfrak{H}_1$ натуральных чисел. Проверим, что $\overline{\mathfrak{H}}_1$ — дополнение $\mathfrak{H}_1$ — диофантовым не является.

Допустим противное, тогда $\overline{\mathfrak{H}}$ имеет некоторый код k. Зададимся вопросом, разрешимо ли уравнение

$$\mathbf{U}_1(k, k, y_1, \ldots, y_m) = 0. \tag{6}$$

Если оно разрешимо, то по определению $\mathfrak{H}_1$ $k \in \mathfrak{H}_1$, а ввиду универсальности $\mathbf{U}_1$ $k \in \overline{\mathfrak{H}}_1$. Аналогично, если (6) не имеет решений, то по определению $\mathfrak{H}_1$ $k \notin \mathfrak{H}_1$, но ввиду универсальности $\mathbf{U}_1$ $k \notin \overline{\mathfrak{H}}_1$. Полученные противоречия показывают, что $\overline{\mathfrak{H}}_1$ не диофантово.

Множество $\mathfrak{H}_1$ является несколько искусственным примером. Более интересным является множество $\mathfrak{H}_0$, определяемое уравнением

$$\mathbf{U}_0(t, y_1, \ldots, y_m) = 0. \tag{7}$$

Как видно из определения, $\mathfrak{H}_0$ — множество кодов диофантовых уравнений (без параметров), имеющих решения. В этой терминологии 10-я проблема Гильберта — это вопрос о способе распознавания принадлежности данного числа a к множеству $\mathfrak{H}_0$.

Полином $\mathbf{U}_0$ был определён равенством (5.6), таким образом, решение уравнения (7) сводится к решению уравнения (4) при $p=0$, $q=t$. Для того чтобы доказать, что $\bar{\mathfrak{H}}_0$ — дополнение $\mathfrak{H}_0$ — не является диофантовым, мы установим обратную связь, а именно, покажем, что решение уравнения (4) при произвольных значениях параметров p и q сводится к решению уравнения (7) при подходящем значении t. Непосредственно в таком виде это утверждение очевидно, ибо при фиксированных значениях p и q можно взять в качестве t код уравнения (4), рассматриваемого как уравнение без параметров. Существенным для нас является то обстоятельство, что такой код может быть задан полиномом от p и q с целыми коэффициентами.

Итак, мы рассматриваем уравнение

$$W_{p,q}(y_1,\ldots,y_{\mathbf{m}})=0, \tag{8}$$

получившееся из (4) подстановкой конкретных значений p и q. Сначала мы построим расширенный код $\langle b,c_L,c_R,d,e,f\rangle$ этого уравнения. Понятно, что d и e, а следовательно, и f можно взять фиксированными, не зависящими от p и q. Разбиение (2.4) на полиномы с натуральными коэффициентами мы проведём не для случая $D=W_{p,q}$, а для случая $D=\mathbf{U}_1$, т. е. независимо от значений p и q. В результате коэффициенты $c_{L,i_0,\ldots,i_{\mathbf{m}}}$ и $c_{R,i_0,\ldots,i_{\mathbf{m}}}$ будут полиномами с натуральными коэффициентами от p и q. Соответственно мы можем найти полиномиальное выражение для b, удовлетворяющего (2.8), и для кодов полиномов c_L и c_R, определяемых (2.7). Наконец, код k уравнения (8) получается из расширенного кода $\langle b,c_L,c_R,d,e,f\rangle$ согласно (5.9) снова полиномиально. Таким образом, $k=K(p,q)$, где K — полином с целыми коэффициентами.

В итоге мы получаем следующую связь множеств $\mathfrak{H}_1$ и $\mathfrak{H}_0$:

$$a\in\mathfrak{H}_1 \iff K(a,a)\in\mathfrak{H}_0 \tag{9}$$

или, переходя к дополнениям,

$$a\in\bar{\mathfrak{H}}_1 \iff K(a,a)\in\bar{\mathfrak{H}}_0. \tag{10}$$

Если бы $\bar{\mathfrak{H}}_0$ было диофантовым, то, очевидно, диофантовым оказалось бы и $\bar{\mathfrak{H}}_1$. Поскольку это не так, мы получаем, что $\bar{\mathfrak{H}}_0$ не диофантово.

Упражнения

4.1. В § 4.1 уменьшение количества параметров-кодов достигается ценой увеличения количества неизвестных. Предложите способ преобразования универсального уравнения (1.1) в другое универсальное уравнение с w неизвестными и одним параметром-кодом.

4.2. В § 1.4 и упражнении 1.8 был специализирован вид параметрических диофантовых уравнений. Предложите специальные формы универсальных уравнений.

4.3. Установите диофантовость отношения **Format**.

4.4. Универсальные уравнения, построенные в этой главе, имеют довольно сложную структуру. Если же мы знаем, что существует какое-то универсальное уравнение

$$U(a, k, x_2, \ldots, x_m) = 0,$$

степень которого относительно всех переменных меньше d, то мы можем легко построить другое универсальное уравнение, имеющее весьма регулярную структуру. Например, универсальным будет уравнение

$$\sum_{i_0+\ldots+i_m<d} \left(c_{L,i_0,\ldots,i_m} - c_{R,i_0,\ldots,i_m}\right) a^{i_0} k^{i_1} x_2^{i_2} \ldots x_m^{i_m} = 0,$$

в котором a — параметр-элемент, $x_2, \ldots, x_m$ — неизвестные, а все остальные переменные — параметры-коды. Количество параметров-кодов можно уменьшить при сохранении регулярности структуры, если вместо канторовой нумерации использовать какой-либо другой полином, принимающий каждое свое значение не более одного раза, в частности, универсальным будет уравнение

$$\left[\sum_{i_0+\ldots+i_m<d} \left(c_{L,i_0,\ldots,i_m} - c_{R,i_0,\ldots,i_m}\right) a^{i_0} k^{i_1} x_2^{i_2} \ldots x_m^{i_m}\right]^2 +$$

$$+\left[b_L - \sum_{i_0+\ldots+i_m<d} c_{L,i_0,\ldots,i_m} c^{i_0 d^0 + \ldots + i_m d^m}\right]^2 +$$

$$+\left[b_R - \sum_{i_0+\ldots+i_m<d} c_{R,i_0,\ldots,i_m} c^{i_0 d^0 + \ldots + i_m d^m}\right]^2 +$$

$$+\left[c - 1 - \sum_{i_0+\ldots+i_m<d} \left(c_{L,i_0,\ldots,i_m} + c_{R,i_0,\ldots,i_m}\right)\right]^2 = 0,$$

в котором a — параметр-элемент, b_L, b_R, c и k — параметры-коды, а остальные переменные — неизвестные. Найдите какие-либо конкретные значения d и m, при которых эти уравнения будут универсальными.

Открытый вопрос

4.1. Существуют ли такие константы **d** и **m**, что для каждого n можно построить универсальное уравнение с n параметрами-элементами, одним параметром-кодом и **m** неизвестными, полная степень которого *относительно всех переменных* равна **d**?

Комментарии

Конструкция универсального диофантова уравнения, приведённая в этой главе, является чисто теоретико-числовой и могла бы, в принципе, быть найдена ещё в прошлом веке. Тем не менее это не произошло, и, по-видимому, не столько из-за технических трудностей, сколько из-за того, что специалисты по теории чисел и не подозревали о такой возможности. В этом отношении характерной представляется реакция на работу Девиса, Патнама и Робинсон [1961], из которой следовало существование универсального экспоненциально диофантова уравнения. Вот что писал референт этой работы Г. Крайзель [1962]:

«Эти результаты поверхностно связаны с десятой проблемой Гильберта об (обычных, т. е. не экспоненциально) диофантовых уравнениях. Доказательства результатов этих авторов, хотя и очень элегантные, не используют слишком трудных [recondite] фактов ни из теории чисел, ни из теории рекурсивно перечислимых множеств, так что скорее всего данный результат не имеет тесной связи с 10-й проблемой Гильберта. Также в целом неправдоподобно, чтобы все (обычные) диофантовы проблемы можно было единым методом свести к случаю фиксированного количества неизвестных и фиксированной степени».

В теории алгоритмов универсальные объекты — аналоги универсальных диофантовых уравнений — известны давно, это *креативные множестаа*, *универсальные машины Тьюринга*, *нормальная форма частично рекурсивных функций* и т. п. М. Девис [1953] высказал общую гипотезу (подробнее о ней см. комментарии к главе 5), из которой следовала переносимость на диофантовы уравнения основных идей теории алгоритмов и, в частности, существование универсального диофантова уравнения. Гипотеза Девиса была доказана в 1970 году (см. комментарии к главе 5), и первая конструкция универсального диофантова уравнения существенно использовала идеи и методы теории алгоритмов. В главе 6 будет приведена другая конструкция универсального диофантова уравнения, основанная как раз на таких идеях.

После установления самого факта существования универсальных диофантовых уравнений естественно возник вопрос о том, сколь малым может быть количество неизвестных в таком уравнении. В работе Матиясевича [1971в] была дана первоначальная грубая верхняя оценка в 200 неизвестных. В работе Матиясевича и Робинсон [1975] этот результат был улучшен до 13 неизвестных, причём это было достигнуто в результате привлечения новых теоретико-числовых идей вместо первоначальных теоретико-алгоритмических. Именно на этом пути и была найдена приведённая в этой главе чисто теоретико-числовая конструкция. Здесь она изложена без многочисленных технических деталей, позволяющих довести число неизвестных до 9, но затрудняющих восприятие основных идей. Эта оценка была объявлена в докладе Матиясевича [1977б] и изложена со всеми деталями в работе Джонса [1982б].

В этой же работе приведена следующая универсальная система диофантовых уравнений:

$$elg^2+\alpha=(b-xy)q^2,\quad q=b^{5^{60}},\quad \lambda+q^4=1+\lambda b^5,\quad \theta+2z=b^5,\quad l=u+1\theta,\quad e=y+m\theta,\quad n=q^{16},$$

$$r=[g+eq^3+lq^5+(2(e-z\lambda)(1+xb^5+g)^4+\lambda b^5+\lambda b^5q^4)q^4]\times[n^2-n]+$$

$$+[q^3-bl+l+\theta\lambda q^3+(b^5-2)q^5][n^2-1],$$

$$p=2ws^2r^2n^2,\quad p^2k^2-k^2=1=\tau^2,\quad 4(c-ksn^2)^2+\eta=k^2,\quad k=r+1+hp-h,\quad a=(wn^2+1)rsn^2,$$

$$c=2r+1+\varphi,\quad d=bw+ca-2c+4f\gamma-5\gamma,\quad d^2=(a^2-1)c^2+1,\quad f^2=(a^2-1)i^2c^4+1,$$

$$(d+of)^2=((a+f^2(d^2-a))^2-1)(2r+1+jc)^2+1.$$

Здесь x — параметр-элемент, u, y, z — параметры-коды, а остальные 28 переменных являются неизвестными, причём все параметры и неизвестные принимают только положительные целые значения. Отметим, что доказательство универсальности этой системы не является чисто теоретико-числовым, поскольку в нём (так же, как в упражнении 4.4) используется факт существования другого универсального уравнения.

Существование диофантова множества, дополнение которого не диофантово, было установлено в работе Девиса [1953]. Этот результат был получен там как прямое следствие существования алгоритмически неразрешимых проблем и возможности сформулировать их на полном арифметическом языке. Использование диагональной конструкции для этих целей восходит к доказательству Кантора несчётности множества вещественных чисел.

Что же касается конкретно множества $\mathfrak{D}_0$ — множества кодов диофантовых уравнений, имеющих решения, то вопрос о его диофантовости и недиофантовости его дополнения тесно связан с вопросом об алгоритмической неразрешимости 10-й проблемы Гильберта (подробнее об этом см. главу 5), и диофантовость $\mathfrak{D}_0$ и недиофантовость $\overline{\mathfrak{D}}_0$ была установлена одновременно с получением отрицательного решения 10-й проблемы Гильберта, т. е. с использованием логических средств. Изложенное в § 4.6 чисто теоретико-числовое доказательство является, по-видимому, первым.

Глава 5
АЛГОРИТМИЧЕСКАЯ НЕРАЗРЕШИМОСТЬ 10-Й ПРОБЛЕМЫ ГИЛЬБЕРТА

В этой главе будут описаны абстрактные вычислительные устройства — *машины Тьюринга*, и установлена их связь с диофантовыми уравнениями. Это и позволит дать отрицательное решение 10-й проблемы Гильберта.

§ 5.1. Машина Тьюринга

Теоретико-числовая техника, развитая в предыдущих главах, даёт нам возможность приступить к доказательству алгоритмической неразрешимости 10-й проблемы Гильберта. Предварительно мы должны уточнить, что понимать под гильбертовым *способом, при помощи которого возможно после конечного числа операций установить, разрешимо ли это уравнение в целых рациональных числах*. Такое уточнение можно сделать разными путями. Основная идея любого такого уточнения состоит в следующем. Мы можем считать, что имеем метод для решения какого-либо типа задач, если мы можем находить решение любой задачи этого типа без приложения творческих усилий, как говорят, чисто механически. Эту идею можно формализовать, сказав, что мы имеем метод, если мы можем построить машину, которая будет решать задачи данного типа без нашего участия, автоматически.

Машины Тьюринга — это абстрактные вычислительные устройства. Их можно описывать в чисто математических теоретико-множественных терминах, но мы будем следовать традиции, описывая машины Тьюринга, как если бы они были реальными устройствами.

Машина Тьюринга имеет память в виде *ленты*, разделённой на *клетки*. Лента имеет один конец, для определённости мы будем считать, что левый. Вправо лента является потенциально бесконечной. Потенциальная бесконечность ленты означает, в частности, что, в отличие от реальных машин, машина Тьюринга не может прервать свою работу с аварийной диагностикой «НЕ ХВАТАЕТ ПАМЯТИ». В то же время любое конкретное вычисление использует лишь конечный отрезок ленты.

Каждая клетка может быть либо пустой, либо содержать один *символ* из некоторого конечного множества символов $A=\{\alpha_1,\ldots,\alpha_w\}$, называемого *алфавитом*. Разные машины имеют, вообще говоря, разные алфавиты. Один символ играет выделенную роль — им всегда будет помечена самая левая клетка, и только она. В качестве такого маркера мы будем использовать символ "$\star$". Кроме того, нам удобно ввести ещё символ для обозначения пустой клетки, по традиции мы будем использовать для этой цели букву "Λ".

Символы на ленте читает и пишет *головка*, которая в каждый момент дискретного времени обозревает одну из клеток ленты. Головка может перемещаться вдоль ленты вправо и влево.

В каждый момент времени машина находится в одном из конечного числа *состояний*, которые по традиции мы будем обозначать посредством $q_1,\ldots,q_v$. Одно из состояний объявляется *начальным*, у нас это всегда будет q_1. Кроме того, одно или несколько состояний объявляются *заключительными*.

Очередное действие машины полностью определяется состоянием, в котором она находится, и символом, который видит головка. За один шаг машина может изменить символ в клетке, переместить головку на одну клетку влево или вправо и перейти в другое состояние. Действия машины задаются набором *инструкций* вида

$$q_i\alpha_j \Rightarrow \alpha_{A(i,j)}D(i,j)q_{Q(i,j)}, \tag{1}$$

где q_i — состояние, в котором находится машина, q_i не является заключительным;

α_j — символ, который видит головка, $\alpha_j\in A\cup\{\Lambda\}$, $\alpha_0=\Lambda$;

$\alpha_{A(i,j)}$ — символ, вписываемый в клетку, $\alpha_{A(i,j)}\in A$, возможно, что $\alpha_{A(i,j)}=\alpha_j$;

$D(i,j)$ — перемещение головки, для которого есть три возможности: L — сдвиг на одну клетку влево, R — вправо, S — без сдвига;

$q_{Q(i,j)}$ — новое состояние машины, возможно, что $q_{Q(i,j)}=q_i$.

В соответствии с нашим соглашением, если $\alpha_j=\star$, то $\alpha_{A(i,j)}=\star$, а $D(i,j)\neq L$; если же $\alpha_j\neq\star$, то $\alpha_{A(i,j)}\neq\star$. Для каждого незаключительного состояния и каждого символа из $A\cup\{\Lambda\}$ имеется ровно одна инструкция с соответствующей левой частью.

В исходный момент времени некоторый начальный отрезок ленты заполнен без пропусков какими-то символами из A, остальная часть потенциально бесконечной ленты пуста, головка помещена в одну из клеток, а машина находится в состоянии q_1. Далее работа машины проходит шаг за шагом в соответствии с инструкциями. Завершается работа машины после

выполнения инструкции, в которой $q_{Q(i,j)}$ — одно из заключительных состояний. Возможна и такая ситуация, что машина никогда не перейдёт в заключительное состояние и будет работать неограниченно долго.

Исходная информация определяется начальным содержимым ленты и положением головки на ней. Результат вычислений определяется заключительным содержимым ленты, положением головки на ней и состоянием, в котором произошла остановка. Интерпретация исходной информации и результата являются внешними событиями по отношению к машине Тьюринга. Например, мы можем записывать на ленте числа в двоичной системе счисления с помощью двух букв α и β, считая α нулем, а β — единицей, или наоборот; понятно, что при этом одна и та же машина будет вычислять, вообще говоря, разные функции.

§ 5.2. Композиция машин

Нам потребуется факт существования ряда машин Тьюринга с некоторыми специальными свойствами. Мы могли бы, в принципе, привести полную систему инструкций каждой такой машины, но это были бы довольно громоздкие и малообозримые построения. Вместо этого мы приведём инструкции лишь нескольких простейших машин и опишем два способа построения из них более сложных машин с требуемыми свойствами.

Все машины, которые мы будем строить, будут работать в одном и том же алфавите

$$\{\star, 0, 1, 2, 3, \lambda\}. \qquad (1)$$

Заключительными состояниями будут всегда состояния q_2 и q_3, причем остановку в состоянии q_2 мы будем интерпретировать как ответ «ДА», а в состоянии q_3 — как «НЕТ». Клетки, содержащие символ "λ", будут играть роль *дублёров* пустых клеток, а именно: справа от клетки с символом "λ" сможет находиться только либо клетка с символом "λ", либо пустая клетка; для любого состояния q_i у инструкций с левыми частями $q_i\lambda$ и $q_i\Lambda$ будут совпадать правые части.

Первый способ построения по двум машинам Тьюринга M_1 и M_2 новой машины M состоит в следующем:

во всех инструкциях машины M_1 заключительное состояние q_2 заменяется на q_{v+1}, где v — количество состояний машины M_1 (напомним, что заключительные состояния могут стоять только в правых частях инструкций);

во всех инструкциях машины M_2 каждое незаключительное состояние q_i заменяется на q_{v+i} (в частности, q_1 заменяется на q_{v+1});

модифицированные инструкции обеих машин объединяются и образуют систему инструкций новой машины M.

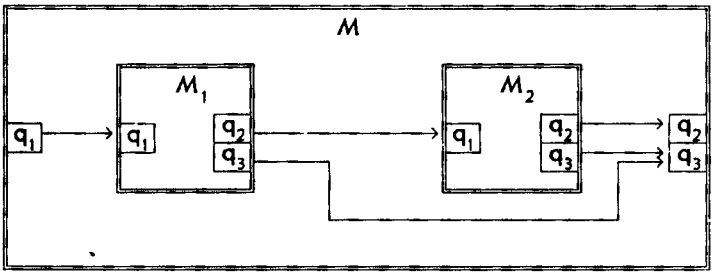

Рис. 1. Первый способ композиции

Действие машины M, построенной описанным выше способом, состоит, очевидно, в последовательном выполнении действий машин M_1 и M_2 при условии, что машина M_1 заканчивает работу в состоянии q_2. Для обозначения машины M мы будем использовать одну из трёх форм записи

$$M_1;M_2$$

$$M_1 \textbf{ and } M_2$$

или

$$\textbf{if } M_1 \textbf{ then } M_2$$

в соответствии с тем, которая из них в каждом конкретном случае естественнее для восприятия человеком.

Легко видеть, что описанная выше операция построения по двум машинам Тьюринга третьей является ассоциативной, и потому обозначение типа $M_1;M_2;M_3$ не является двусмысленным.

Второй способ построения по двум машинам Тьюринга M_1 и M_2 новой машины M состоит в следующем:

во всех инструкциях машины M_1 заключительное состояние q_2 заменяется на q_{v+1}, где v — количество состояний машины M_1, а заключительное состояние q_3 заменяется на q_2;

во всех инструкциях машины M_2 каждое незаключительное состояние q_i заменяется на q_{v+i}, а заключительное состояние q_2 заменяется на q_1;

модифицированные инструкции обеих машин объединяются и образуют систему инструкций новой машины M.

Построенную таким способом машину M мы будем обозначать посредством

$$\textbf{while } M_1 \textbf{ do } M_2 \textbf{ od}$$

Действие этой машины состоит в поочерёдном выполнении действий машин M_1 и M_2 до тех пор, пока одна из машин не перейдёт в состояние q_3.

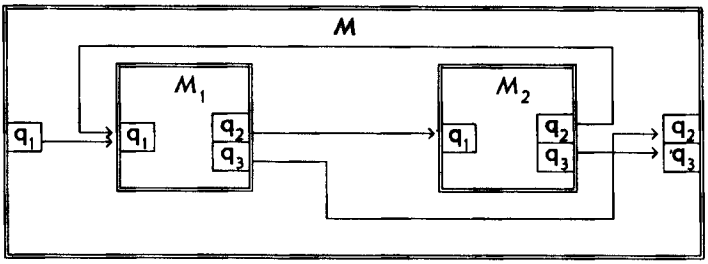

Рис. 2. Второй способ композиции

Введённые нами обозначения выглядят как некоторый примитивный язык программирования. Следует отметить, однако, что каждая «программа» является на самом деле обозначением конкретной машины Тьюринга.

§ 5.3. Базисные машины

В этом параграфе мы построим ряд конкретных машин Тьюринга и опишем их работу. Хотя машины Тьюринга могут обрабатывать словарную информацию, нас будет интересовать главным образом работа с натуральными числами. Для этого мы примем ряд соглашений по представлению чисел на ленте машины. А именно, мы будем использовать непозиционную единиричную систему счисления — *изображение числа* m будет занимать $m+1$ последовательную клетку. В самой левой из них будет записан символ "0", в остальных — символ "1". Естественно, что клетка, расположенная непосредственно справа от последней клетки, составляющей изображение числа, не может содержать символ "1".

Изображение кортежа

$$\langle a_1, \ldots, a_n \rangle \tag{1}$$

будет состоять из изображений чисел $a_1, \ldots, a_n$, стоящих вплотную друг к другу, начиная со второй клетки ленты (первая, как мы условились, всегда содержит маркер конца "$\star$"). Остальные клетки либо пусты, либо содержат в соответствии с нашим соглашением, принятым в § 5.2, символ "λ"; изображение, не содержащее клеток с этим символом, будем называть *каноническим*.

$\star$	0	1	1	0	1	0	0	1	1	1	λ	

Рис. 3. Изображение кортежа $\langle 2,1,0,3 \rangle$

Мы начнём с ряда простейших машин, которые будут заданы явно.

Машина LEFT с инструкциями

$$\begin{aligned} q_1\star &\Rightarrow \star S q_2 \\ q_1 0 &\Rightarrow 0 L q_2 \\ q_1 1 &\Rightarrow 1 L q_2 \\ q_1 2 &\Rightarrow 2 L q_2 \\ q_1 3 &\Rightarrow 3 L q_2 \\ q_1 \lambda &\Rightarrow \lambda L q_2 \\ q_1 \Lambda &\Rightarrow \lambda L q_2 \end{aligned} \tag{2}$$

сдвигает головку на одну клетку влево, если, конечно, головка не находилась на самой левой клетке, помеченной символом "$\star$".

Машина RIGHT с инструкциями

$$\begin{aligned} q_1\star &\Rightarrow \star R q_2 \\ q_1 0 &\Rightarrow 0 R q_2 \\ q_1 1 &\Rightarrow 1 R q_2 \\ q_1 2 &\Rightarrow 2 R q_2 \\ q_1 3 &\Rightarrow 3 R q_2 \\ q_1 \lambda &\Rightarrow \lambda S q_2 \\ q_1 \Lambda &\Rightarrow \lambda S q_2 \end{aligned} \tag{3}$$

сдвигает головку на одну клетку вправо, если только головка не стояла на пустой клетке или клетке, помеченной символом "λ".

Машина WRITE(0) с инструкциями

$$\begin{aligned} q_1\star &\Rightarrow \star S q_2 \\ q_1 0 &\Rightarrow 0 S q_2 \\ q_1 1 &\Rightarrow 0 S q_2 \\ q_1 2 &\Rightarrow 0 S q_2 \\ q_1 3 &\Rightarrow 0 S q_2 \\ q_1 \lambda &\Rightarrow 0 S q_2 \\ q_1 \Lambda &\Rightarrow 0 S q_2 \end{aligned} \tag{4}$$

вписывает в клетку, где находится головка, символ "0", если,

конечно, это не самая левая клетка с маркером "$\star$". Аналогичные действия производят машины WRITE(1), WRITE(2), WRITE(3), инструкции которых получаются из (4) заменой всюду в правых частях символа "0" на "1", "2" и "3" соответственно.

Машина READ(0) с инструкциями

$$\begin{aligned} q_1\star &\Rightarrow \star Sq_3 \\ q_10 &\Rightarrow 0Sq_2 \\ q_11 &\Rightarrow 1Sq_3 \\ q_12 &\Rightarrow 2Sq_3 \\ q_13 &\Rightarrow 3Sq_3 \\ q_1\lambda &\Rightarrow \lambda Sq_3 \\ q_1\Lambda &\Rightarrow \lambda Sq_3 \end{aligned} \tag{5}$$

распознаёт, записан ли в клетке, где находится головка, символ "0" или нет. В зависимости от этого она заканчивает работу в состоянии q_2 или q_3, что согласно нашей договоренности соответствует ответам «ДА» и «НЕТ». Аналогично машины READ(1), READ(2), READ(3) и READ($\star$) распознают наличие символов "1", "2", "3" и "$\star$" соответственно. В эту схему немного не укладываются действия машины READ(λ) с инструкциями

$$\begin{aligned} q_1\star &\Rightarrow \star Sq_3 \\ q_10 &\Rightarrow 0Sq_3 \\ q_11 &\Rightarrow 1Sq_3 \\ q_12 &\Rightarrow 2Sq_3 \\ q_13 &\Rightarrow 3Sq_3 \\ q_1\lambda &\Rightarrow \lambda Sq_2 \\ q_1\Lambda &\Rightarrow \lambda Sq_2 \end{aligned} \tag{6}$$

поскольку мы условились считать клетки с символом "λ" дублёрами пустых клеток.

Нам потребуются также две машины, которые существенных преобразований на ленте не производят. Машина STOP с инструкциями

$$\begin{aligned} q_1\star &\Rightarrow \star Sq_3 \\ q_10 &\Rightarrow 0Sq_3 \\ q_11 &\Rightarrow 1Sq_3 \\ q_12 &\Rightarrow 2Sq_3 \\ q_13 &\Rightarrow 3Sq_3 \\ q_1\lambda &\Rightarrow \lambda Sq_3 \\ q_1\Lambda &\Rightarrow \lambda Sq_3 \end{aligned} \tag{7}$$

не сдвигая головки, из состояния q_1 всегда переходит прямо в заключительное состояние q_3. Напротив, машина NEVERSTOP с инструкциями

$$\begin{aligned} q_1\star &\Rightarrow \star Sq_1 \\ q_1 0 &\Rightarrow 0Sq_1 \\ q_1 1 &\Rightarrow 1Sq_1 \\ q_1 2 &\Rightarrow 2Sq_1 \\ q_1 3 &\Rightarrow 3Sq_1 \\ q_1\lambda &\Rightarrow \lambda Sq_1 \\ q_1\Lambda &\Rightarrow \lambda Sq_1 \end{aligned} \tag{8}$$

никогда не меняет своего состояния и, таким образом, никогда не заканчивает работу.

Действие машины

READNOT(0) = **while** READ(0) **do** STOP **od**

прямо противоположно действию машины READ(0) — она распознаёт отсутствие символа "0" в клетке, где находится головка. Машины READNOT(2), READNOT(3), READNOT($\star$) и READNOT(λ) получаются заменой READ(0) на READ(2), READ(3), READ($\star$) и READ(λ) соответственно.

Машина

STAR = **while** READNOT($\star$) **do** LEFT **od**

устанавливает головку на левый конец ленты (помеченный символом "$\star$").

Машина

VACANT = STAR; **while** READNOT(λ) **do** RIGHT **od**

ставит головку на самую левую пустую клетку или её дублёра — клетку с символом "λ".

Машина

JUMP = **while** READNOT(0) **do** RIGHT **od**

передвигает головку вправо до ближайшей клетки с символом "0"; если все клетки с этим символом в исходный момент были левее головки, то машина не закончит работу никогда.

Определим серию машин FIND следующими рекуррентными соотношениями:

FIND(1) = STAR; JUMP

FIND(k+1) = FIND(k); RIGHT; JUMP

Машина FIND(k), очевидно, устанавливает головку на символ "0", соответствующий элементу a_k кортежа (1).

Машина

LAST = VACANT; **while** READNOT(0) **do** LEFT **od**

действует на кортеж (1) так же, как машина FIND(n), а именно, устанавливает головку на символ "0" в изображении последнего элемента a_n. Таким образом, одна машина LAST выполняет в подходящих ситуациях действия любой из бесконечной серии машин FIND.

Машина

NEW = VACANT; WRITE(0)

преобразует кортеж (1) в кортеж $\langle a_1, \ldots, a_n, 0\rangle$.

Машина

INC = VACANT; WRITE(1)

преобразует кортеж (1) в кортеж

$$\langle a_1, \ldots, a_{n-1}, a_n+1\rangle. \tag{9}$$

Машина

DEC = VACANT; LEFT; **if** READ(1) **then** WRITE(λ)

наоборот, преобразует кортеж (9) в кортеж (1); будучи же применена к кортежу, у которого последний элемент равен нулю, машина ничего на ленте не меняет, но останавливается в состоянии q_3, сигнализируя тем самым, что уменьшения последнего элемента не произошло.

Машина

```
DELETE = VACANT;
         while READNOT(0) do WRITE(λ); LEFT od;
         WRITE(λ)
```

усекает кортеж (1) до кортежа $\langle a_1, \ldots, a_{n-1}\rangle$.

Машина

MARK(2) = **while** RIGHT; READ(1) **do** WRITE(2) **od**

заменяет последовательность идущих подряд символов "1" на символы "2". Типичным является использование машины MARK(2) в паре с машиной FIND: машина FIND(k);MARK(2) выделяет в изображении кортежа (1) элемент a_k. Аналогично действует ма-

шина

MARK(3) = **while** RIGHT; READ(1) **do** WRITE(3) **od**.

Машина

THEREIS(2) = STAR;
while READNOT(2) **do**
if READNOT(λ) **then** RIGHT **od**

определяет, есть ли где-либо на ленте символ "2": она переходит в состояние q_2, если этот символ имеется, и в состояние q_3 в противном случае. Для работы машины THEREIS(2) существенно наше соглашение строить все машины так, чтобы правее клеток с символом "λ" не было клеток с другими символами.

Машина

THEREWAS(2) = **if** THEREIS(2) **then** WRITE(1)

не только определяет наличие символа "2", но, найдя клетку с символом "2", вписывает в неё вновь символ "1".

Машины THEREIS(3) и THEREWAS(3) определяются и действуют аналогично машинам THEREIS(2) и THEREWAS(2).

Машины THEREWAS(2) и THEREWAS(3) восстанавливают символ "1" только в одной клетке. В отличие от них машина

RESTORE = **while** THEREIS(2) **do** THEREWAS(2) **od**;
while THEREIS(3) **do** THEREWAS(3) **od**

восстанавливает все символы "1", ранее заменённые машинами MARK(2) или MARK(3) на "2" или "3".

Машина

APPEND(k) = FIND(k); MARK(2);
while THEREWAS(2) **do** INC **od**

преобразует кортеж (1) в $\langle a_1, \ldots, a_{n-1}, a_n+a_k\rangle$. Машина

COPY(k) = NEW; APPEND(k)

преобразует кортеж (1) в $\langle a_1, \ldots, a_n, a_k\rangle$. Наконец, машина

ADD(k, l) = COPY(k); APPEND(l)

преобразует кортеж (1) в $\langle a_1, \ldots, a_n, a_k+a_l\rangle$.

При $k \neq l$ машина

```
MULT(k, l) = NEW; FIND(k); MARK(3);
             while THEREWAS(3) do APPEND(l) od
```

преобразует кортеж (1) в $\langle a_1, \ldots, a_n, a_k a_l \rangle$. Для получения кортежа $\langle a_1, \ldots, a_n, a_k^2 \rangle$ следует применить машину

```
MULT(k, k) = NEW; FIND(k); APPEND(k);
             LAST; MARK(3); THEREWAS(3);
             while THEREWAS(3) do APPEND(k) od
```

При $k \neq l$ машина

```
NOTGREATER(k, l) = FIND(k); MARK(2); FIND(l); MARK(3);
                   while THEREIS(2) and THEREIS(3) do
                      THEREWAS(2); THEREWAS(3) od;
                   while THEREIS(2) do
                      RESTORE; STOP od;
                   RESTORE
```

сравнивает a_k и a_l по величине и останавливается в состоянии q_2 или q_3 в соответствии с тем, которое из неравенств $a_k \leq a_l$ или $a_k > a_l$ имеет место. Аналогично машины

```
EQUAL(k, l) = NOTGREATER(k, l) and NOTGREATER(l, k)
```

и

```
NOTEQUAL = while EQUAL(k, l) do STOP od
```

сравнивают a_k и a_l на точное совпадение.

Машина

```
NEXT = LAST; WRITE(1); RIGHT;
       while READ(λ) do WRITE(1); LAST; RIGHT od;
       WRITE(0)
```

преобразует кортеж (1) в кортеж $\langle a_1, \ldots, a_{n-2}, b, c \rangle$, где $\langle b, c \rangle$ — пара чисел, следующая за парой $\langle a_{n-1}, a_n \rangle$ в канторовом перечне пар (3.1.1). Наконец, машина

```
DECODE = LAST; MARK(2); NEW; NEW;
         while THEREWAS(2) do NEXT od
```

преобразует кортеж (1) в $\langle a_1, \ldots, a_n, b, c \rangle$, где $\langle b, c \rangle$ — пара чисел, канторов номер которой равен a_n.

§ 5.4. Распознавание диофантовых множеств машинами Тьюринга

В этом параграфе будет установлена первая связь диофантовых множеств с машинами Тьюринга. А именно, мы покажем, что *по произвольному параметрическому диофантову уравнению*

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

можно построить машину Тьюринга M, которая заканчивает работу над изображением кортежа

$$\langle a_1,\ldots,a_n\rangle \tag{2}$$

в том и только том случае, когда уравнение (1) *разрешимо относительно* $x_1,\ldots,x_{m+1}$.

Сначала мы построим вспомогательную машину M_1, которая по кортежу

$$\langle a_1,\ldots,a_n,y_0\rangle \tag{3}$$

проверяет, является ли y_0 канторовым номером кортежа $\langle x_1,\ldots,x_{m+1}\rangle$, дающего решение уравнения (1). Эта машина M_1 строится как линейная комбинация нескольких других машин. Первой идёт m-кратная итерация машины DECODE, которая преобразует кортеж (3) в кортеж

$$\langle a_1,\ldots,a_n,y_0,x_1,y_1,\ldots,x_m,y_m\rangle, \tag{4}$$

где $x_1,\ldots,x_m$, $y_1,\ldots,y_m$ — такие числа, что

$$y_{k-1}=\mathbf{Cantor}(x_k,y_k), \tag{5}$$

и потому

$$y_0=\mathbf{Cantor}_{m+1}(x_1,\ldots,x_m,y_m). \tag{6}$$

Уравнение (1) можно переписать в виде

$$C_L(a_1,\ldots,a_n,x_1,\ldots,x_m,y_m)=C_R(a_1,\ldots,a_n,x_1,\ldots,x_m,y_m), \tag{7}$$

где C_L и C_R — полиномы с натуральными коэффициентами. Процесс вычисления C_L и C_R можно представить в виде цепочки простейших операций

$$\begin{aligned} z_1 &= \alpha_1 \circ_1 \beta_1, \\ &\ldots\ldots\ldots\ldots \\ z_k &= \alpha_k \circ_k \beta_k, \end{aligned} \tag{8}$$

где α_j и β_j — одно из чисел 1, $a_1,\ldots,a_n$, $x_1,\ldots,x_m$, y_m, $z_1,\ldots,z_{i-1}$, $\circ_j$ — знак + или ×, и значения C_L и C_R встречаются среди $z_1,\ldots,z_k$. Понятно, что подходящая линейная комбиция машин типа NEW, INC, ADD и MULT преобразует кортеж (4) в кортеж

$$\langle a_1,\ldots,a_n,y_0,x_1,y_1,\ldots,x_m,y_m,1,z_1,\ldots,z_k\rangle. \tag{9}$$

Для завершения построения машины M осталось применить ещё машину NOTEQUAL с надлежащими индексами. В результате машина M_1 будет останавливаться в состоянии q_2, если в кортеже (2) y_0 не было канторовым кодом решения уравнения (1), и в состоянии q_3 в противном случае.

Очевидно, что $(2m+k+1)$-кратная итерация машины DELETE преобразует кортеж (9) в исходный кортеж (3); обозначим такую машину посредством M_2.

Машину M мы можем теперь определить так:

$$M = \text{NEW};\ \textbf{while}\ M_1\ \textbf{do}\ M_2;\ \text{INC}\ \textbf{od} \tag{10}$$

Она работает следующим образом. Сначала (машина NEW) преобразует кортеж (2) в кортеж

$$\langle a_1,\ldots,a_n,0\rangle. \tag{11}$$

Если машина M_1 установит, что 0 — это канторов номер решения уравнения (1), то работа машины M на этом закончится. В противном случае машины M_2 и INC построят кортеж

$$\langle a_1,\ldots,a_n,1\rangle, \tag{12}$$

и машина M_1 будет проверять кортеж с канторовым номером 1, и т. д. Если уравнение (1) имеет решение, то машина M в конце концов остановится, если же (1) решений не имеет, то M будет работать неограниченно долго.

§ 5.5. Диофантово моделирование машин Тьюринга

В предыдущем параграфе мы показали «полуразрешимость» диофантовых уравнений — если уравнение имеет решение, то этот факт можно установить чисто механически. Полуразрешимость — это интуитивно ясное свойство, и проведённое в предыдущем параграфе формальное доказательство добавляет нам немного знаний о диофантовых уравнениях. Скорее, наоборот, оно служит свидетельством того, что машины Тьюринга являются достаточно мощными вычислительными устройствами несмотря на примитивность их инструкций.

Главная же роль предыдущего параграфа состоит в том, что он мотивирует введение нового понятия. А именно, мы будем говорить, что множество $\mathfrak{M}$, состоящее из n-ок натуральных чисел, *полуразрешимо по Тьюрингу*, если существует машина Тьюринга M, которая, начав работу над каноническим изображением кортежа $\langle a_1,\ldots,a_n\rangle$ в состоянии q_1 и головкой, установленной на левом конце ленты, окончит работу в том и только том случае, когда $\langle a_1,\ldots,a_n\rangle\in\mathfrak{M}$.

В предыдущем параграфе было показано, что каждое диофантово множество является полуразрешимым по Тьюрингу. Цель настоящего параграфа — показать, что верно и обратное: *каждое полуразрешимое по Тьюрингу множество является диофантовым.*

Пусть дана машина Тьюринга M, полуразрешающая некоторое множество $\mathfrak{M}$, состоящее из n-ок натуральных чисел. Пусть

$$\{\alpha_1, \ldots, \alpha_w\} \tag{1}$$

— алфавит этой машины. На каждом шаге работы машины M заполнен только конечный отрезок ленты, скажем, длины l, и мы можем представить его кортежем

$$\langle s_1, s_2, \ldots, s_m, \ldots s_{l-1}, s_l \rangle \tag{2}$$

номеров символов, записанных в клетках (в частности, s_1 всегда будет равно номеру символа "$\star$" в (1)).

Текущее состояние q_i машины и положение головки можно представлять кортежем такой же длины

$$\langle 0, \ldots, 0, i, 0, \ldots, 0 \rangle, \tag{3}$$

все элементы которого, кроме одного, равны нулю; единственный ненулевой элемент, равный номеру состояния машины, указывает положение головки.

Тройку, состоящую из текущего содержимого ленты, состояния машины и положения головки, будем называть *конфигурацией*. Конфигурация, очевидно, однозначно определяется кортежами (2) и (3). Для представления кортежей (2) и (3) мы будем использовать позиционную систему кодирования с каким-либо фиксированным основанием β, которое не меньше 3, больше v — количества состояний машины M, и больше w — количества букв в её алфавите (1). *Кодом конфигурации* будем называть пару $\langle p, t \rangle$, где p и t — шифры по основанию β кортежей (3) и (2) соответственно. Как мы видим, код конфигурации не содержит информации о длине кортежей (2) и (3), но она и несущественна, поскольку в (3) всего один ненулевой элемент, а нулевые элементы кортежа (2) мы будем интерпретировать как пустые клетки. Таким образом, конфигурация однозначно определяется своим кодом, а использование вместо кодов кортежей (2) и (3) только их шифров соответствует потенциальной бесконечности ленты.

В этой терминологии наша первоочередная задача — это построить диофантово уравнение

$$D(p, t, x_1, \ldots, x_m) = 0 \tag{4}$$

такое, что *если $\langle p, t \rangle$ — код некоторой конфигурации, то уравнение* (4) *разрешимо относительно $x_1, \ldots, x_m$ тогда и только тогда, когда машина M, начав работу в этой конфигурации, ос-*

тановится через конечное число шагов. Вопрос о разрешимости или неразрешимости (4) в том случае, когда $\langle p,t\rangle$ не является кодом никакой конфигурации, нас интересовать не будет.

Естественно, что мы начнём с моделирования одного шага машины Тьюринга. Пусть из конфигурации с кодом $\langle p,t\rangle$ рассматриваемая машина M переходит непосредственно в конфигурацию с кодом $\langle \mathrm{NextP}(p,t), \mathrm{NextT}(p,t)\rangle$. Проверим, что NextP и NextT — диофантовы функции.

Это утверждение нуждается в следующем уточнении. Мы определили функции NextP и NextT пока только в случае, когда $\langle p,t\rangle$ — код конфигурации, причём конфигурации с незаключительным состоянием. Положим

$$\mathrm{NextP}(p,t)=0, \tag{5}$$

$$\mathrm{NextT}(p,t)=t, \tag{6}$$

если $\langle p,t\rangle$ — код конфигурации с заключительным состоянием. Утверждение о диофантовости NextP и NextT следует понимать как существование диофантовых функций, ведущих себя описанным выше образом на кодах конфигураций и произвольным образом, если значения аргументов отличны от кодов конфигураций.

Функции NextP и NextT, очевидно, должны зависеть от функций A, D и Q, задающих набор (1.1) инструкций машины M. В соответствии с (5)–(6) мы рассширим эти функции, считая, что если q_i — заключительное состояние, то $A(i,j)=j$, $D(i,j)=S$, $Q(i,j)=0$.

Диофантовость функции NextT почти очевидна, поскольку каждый элемент кортежа с шифром $\mathrm{NextT}(p,t)$ однозначно определяется элементами с теми же номерами кортежей с шифрами p и t. А именно, определим функцию A следующим образом:

$$\mathrm{A}(i,j)=\begin{cases} A(i,j), & \text{если } 0<i\le v,\ 0\le j\le w,\\ j & \text{в противном случае}\end{cases} \tag{7}$$

(напомним, что v и v — это количества состояний и символов машины M). Тогда NextT можно определить эквивалентностью

$$t'=\mathrm{NextT}(p,t) \Leftrightarrow \exists w[t'=\mathrm{A}[\beta](p,t,w)], \tag{8}$$

где $\mathrm{A}[\beta]$ — определённое в § 3.6 расширение функции A на кортежи.

Диофантовость функции NextP менее очевидна, поскольку k-й элемент кортежа с шифром $\mathrm{NextP}(p,t)$ однозначно определяется лишь элементами с номерами $k-1$, k и $k+1$ кортежей с шифрами p и t. Изложеная в § 3.6 техника позволяет расширять функции на кортежи лишь поэлементно, однако эта трудность легко преодолима. Положим

$$p^{\mathrm{R}}=p\beta, \qquad p^{\mathrm{L}}=p \ \mathbf{div}\ \beta, \tag{9}$$

$$t^{\mathrm{R}}=t\beta, \qquad t^{\mathrm{L}}=t \ \mathbf{div}\ \beta. \tag{10}$$

Очевидно, что если t — шифр кортежа (2), то t^R и t^L — шифры кортежей

$$\langle 0,\ s_1,\ldots,s_{m-1},\ldots,s_{l-1},s_l\rangle \tag{11}$$

и

$$\langle s_2,s_3,\ldots,s_{m+1},\ldots,s_l,0\rangle \tag{12}$$

(в кортежах (2), (11) и (12) выделены m-е элементы). Аналогично, если p — шифр кортежа (3), то p^R и p^L - шифры кортежей

$$\langle 0,\ldots,0,0,i,\ldots,0\rangle \tag{13}$$

и

$$\langle 0,\ldots,i,0,0,\ldots,0\rangle, \tag{14}$$

в которых ненулевой элемент сдвинут по сравнению с (3) на одну позицию вправо или влево.

Каждый элемент кортежа с шифром $\mathrm{NextP}(p,t)$ определяется элементами с тем же номером кортежей с шифрами p^L, p, p^R, t^L, t, t^R. Эта зависимость, очевидно, определяется функциями D и Q. Зададим её явно, введя функцию DQ следующим образом:

$$\mathrm{DQ}(i^L,i,i^R,j^L,j,j^R) = \begin{cases} Q(i^L,j^L), \text{ если } i^L>0,\ i=i^R=0 \text{ и } D(i^L,j^L)=\mathrm{L}, \\ Q(i,j), \text{ если } i^L=0,\ i>0,\ i^R=0 \text{ и } D(i,j)=\mathrm{S}, \\ Q(i^R,j^R), \text{ если } i^L=i=0,\ i^R>0 \text{ и } D(i^R,j^R)=\mathrm{R}, \\ 0 \quad \text{в противном случае} \end{cases} \tag{15}$$

(к «противным случаям» относятся и случаи, когда какое-то из чисел i^L, i, i^R больше v или какое-то из чисел j^L, j, j^R больше w, ибо тогда Q и D неопределены). Теперь мы можем указать диофантово представление для NextP:

$$p' = \mathrm{NextP}(p,t) \Leftrightarrow$$

$$\Leftrightarrow \exists w[p' = \mathrm{DQ}[b](pb,\ p,\ p\ \mathbf{div}\ b,\ tb,\ t,\ t\ \mathbf{div}\ b,\ w)]. \tag{16}$$

Функции NextP и NextT описывают один шаг работы рассматриваемой машины Тьюринга. Наша очередная цель — установить диофантовость трёхместных функций AfterP и AfterT, которые определяются как итерации функций NextP и NextT:

$$\begin{gathered} \mathrm{AfterP}(0,p,t)=p, \\ \mathrm{AfterT}(0,p,t)=t, \\ \mathrm{AfterP}(k+1,p,t)=\mathrm{NextP}(k,\mathrm{AfterP}(k,p,t),\mathrm{AfterT}(k,p,t)), \\ \mathrm{AfterT}(k+1,p,t)=\mathrm{NextT}(k,\mathrm{AfterP}(k,p,t),\mathrm{AfterT}(k,p,t)). \end{gathered} \tag{17}$$

Ясно, что если за k шагов машина M из конфигурации $\langle p,t\rangle$ перешла в конфигурацию $\langle p',t'\rangle$, то $p'=\mathrm{AfterP}(k,p,t)$, $t'=\mathrm{AfterT}(k,p,t)$.

Рассмотрим все промежуточные конфигурации

$$\langle p_0,t_0\rangle,\ldots,\langle p_k,t_k\rangle, \tag{18}$$

где

$$\langle p_0,t_0\rangle=\langle p,t\rangle, \tag{19}$$

$$\langle p_{i+1},t_{i+1}\rangle=\langle \mathrm{NextP}(p_i,t_i),\mathrm{NextT}(p_i,t_i)\rangle, \tag{20}$$

$$\langle p',t'\rangle=\langle p_k,t_k\rangle. \tag{21}$$

Пусть l столь велико, что

$$p<\beta^{l-k-2},\quad t<\beta^{l-k-2}. \tag{22}$$

Это означает, что в конфигурации $\langle p,t\rangle$ не более, чем $l-k-2$ первых клеток ленты заняты символами. За k шагов работы машина M сможет заполнить не более, чем k новых клеток, и потому при $i=0,\ldots,k$

$$p_i<\beta^{l-2},\quad t_i<\beta^{l-2}; \tag{23}$$

в частности,

$$p'<\beta^{l-2},\quad t'<\beta^{l-2}. \tag{24}$$

Построим две *суперконфигурации* $\langle p_L,t_L\rangle$ и $\langle p_R,t_R\rangle$ при помощи конкатенации конфигураций (18) (напомним, что диофантовость конкатенации кортежей с равными основаниями была установлена в § 3.3):

$$\langle p_L,\beta,kl\rangle=\langle p_0,\beta,l\rangle+\ldots+\langle p_{k-1},\beta,l\rangle, \tag{25}$$

$$\langle t_L,\beta,kl\rangle=\langle t_0,\beta,l\rangle+\ldots+\langle t_{k-1},\beta,l\rangle, \tag{26}$$

$$\langle p_R,\beta,kl\rangle=\langle p_1,\beta,l\rangle+\ldots+\langle p_k,\beta,l\rangle, \tag{27}$$

$$\langle t_R,\beta,kl\rangle=\langle t_1,\beta,l\rangle+\ldots+\langle t_k,\beta,l\rangle. \tag{28}$$

Суперконфигурации $\langle p_L,t_L\rangle$ и $\langle p_R,t_R\rangle$ конфигурациями не являются, поскольку кортежи с шифрами p_L и p_R содержат по k ненулевых элементов, а кортежи с шифрами t_L и t_R соответствуют лентам, на которых k клеток помечены символом "$\star$".

Суперконфигурации соответствуют *супермашине*, лента которой разделена символами "$\star$" на k участков, на каждом из которых работает своя головка в соответствии с инструкциями исходной машины M. Вместо k шагов работы машины M мы можем рассмотреть один шаг работы супермашины, при котором каждая головка независимо от других выполняет соответствующую инструкцию.

Таким образом, суперконфигурация $\langle p_R,t_R\rangle$ однозначно определяется суперконфигурацией $\langle p_L,t_L\rangle$; более того, введёные посредством (16) и (8) функции NextP и NextT без какой-либо

модификации описывают и работу супермашины:

$$p_R = \mathrm{NextP}(p_L, t_L), \quad t_R = \mathrm{NextT}(p_L, t_L). \tag{29}$$

Рассмотрим также суперконфигурацию $\langle p_M, t_M \rangle$, определяемую равенствами

$$\langle p_M, \beta, (k-1)l \rangle = \langle p_1, \beta, l \rangle + \ldots + \langle p_{k-1}, \beta, l \rangle, \tag{30}$$

$$\langle t_M, \beta, (k-1)l \rangle = \langle t_1, \beta, l \rangle + \ldots + \langle t_{k-1}, \beta, l \rangle. \tag{31}$$

Определения (25)–(26) можно переписать в новых обозначениях так:

$$\langle p_L, \beta, kl \rangle = \langle p, \beta, l \rangle + \langle p_M, \beta, (k-1)l \rangle, \tag{32}$$

$$\langle t_L, \beta, kl \rangle = \langle t, \beta, l \rangle + \langle t_M, \beta, (k-1)l \rangle, \tag{33}$$

$$\langle p_R, \beta, kl \rangle = \langle p_M, \beta, (k-1)l \rangle + \langle p', \beta, l \rangle, \tag{34}$$

$$\langle t_R, \beta, kl \rangle = \langle t_M, \beta, (k-1)l \rangle + \langle t', \beta, l \rangle. \tag{35}$$

Мы видели, что для любой конфигурации $\langle p, t \rangle$ и любого положительного k при любом l, удовлетворяющем (22), найдутся числа p_L, t_L, p_M, t_M, p_R, t_R, p', t', удовлетворяющие условиям (24), (27)–(29), (32)–(35). Покажем теперь, что выбор этих чисел однозначно определяется по k, l, p и t.

Действительно, согласно (32)–(33) первые l элементов кортежей с кодами $\langle p_L, b, kl \rangle$ и $\langle t_L, \beta, kl \rangle$ определены однозначно. Функции NextP и NextT были определены эквивалентностями (16) и (8) так, что первые m элементов кортежей с шифрами $\mathrm{NextP}(x, y)$ и $\mathrm{NextT}(x, y)$ однозначно определяются первыми $m+1$ элементами кортежей с шифрами x и y. Таким образом, согласно (29) первые $l-1$ элементы кортежей с кодами $\langle p_R, \beta, kl \rangle$ и $\langle t_R, \beta, kl \rangle$ определены однозначно. Далее, из (34)–(35) следует, что однозначно определены и первые $l-1$ элементы кортежей с кодами $\langle p_M, \beta, (k-1)l \rangle$ и $\langle t_M, \beta, (k-1)l \rangle$.

Возвращаясь к (32)–(33), мы видим, что однозначно определены первые $2l-1$ элемента кортежей с кодами $\langle p_L, \beta, kl \rangle$ и $\langle t_L, \beta, kl \rangle$, следовательно, по (29) первые $2l-2$ элемента кортежей с кодами $\langle p_R, \beta, kl \rangle$ и $\langle t_R, \beta, kl \rangle$ и по (34)–(35) первые $2l-2$ элемента кортежей с кодами $\langle p_M, \beta, (k-1)l \rangle$ и $\langle t_M, \beta, (k-1)l \rangle$.

Повторив это рассуждение достаточное число раз, мы получим, что однозначно определены все элементы кортежей с кодами $\langle p_L, \beta, kl \rangle$, $\langle t_L, \beta, kl \rangle$, $\langle p_M, \beta, (k-1)l \rangle$, $\langle t_M, \beta, (k-1)l \rangle$ и все, кроме, быть может, самых последних, элементы кортежей с кодами $\langle p_R, \beta, kl \rangle$, $\langle t_R, \beta, kl \rangle$, $\langle p', \beta, l \rangle$, $\langle t', \beta, l \rangle$. Но из неравенства (24) следует, что последние элементы кортежей с кодами $\langle p', \beta, l \rangle$ и $\langle t', \beta, l \rangle$ равны 0, и по (34)–(35) равны нулю и последние элементы кортежей с кодами $\langle p_R, \beta, kl \rangle$ и $\langle t_R, \beta, kl \rangle$.

Таким образом, мы установили, что *система диофантовых условий* (24), (27)-(29), (32)-(35) *для любой конфигурации* $\langle p,t\rangle$ *и любого положительного* k *при любом* l, *удовлетворяющем* (22), *имеет относительно* p_L, t_L, p_M, t_M, p_R, t_R, p', t' *ровно одно решение, и в этом единственном решении* $p' = \mathrm{AfterP}(k,p,t)$, $t' = \mathrm{AfterT}(k,p,t)$. Отсюда мы немедленно получаем диофантовость функций AfterP и AfterT.

Для построения диофантова уравнения (4) нам осталось сделать небольшой шаг. Пусть $\omega_1,\ldots,\omega_z$ — номера состояний машины M, объявленных заключительными. Тогда условие

$$\exists kr[\mathbf{Elem}(\mathrm{AfterT}(k,p,t),\beta,r)=\omega_1 \vee \ldots$$

$$\ldots \vee \mathbf{Elem}(\mathrm{AfterT}(k,p,t),\beta,r)=\omega_z] \qquad (36)$$

выполнено для конфигурации $\langle p,t\rangle$ в том и только том случае, когда, начав работу в этой конфигурации, машина остановится ровно через k шагов. Условие (36) является диофантовым и потому может быть преобразовано в требуемое уравнение (4).

Диофантово уравнение (4) — это ещё не совсем то, что нам требуется для установления диофантовости множества $\mathfrak{M}$, полуразрешаемого рассматриваемой машиной M, поскольку параметрами уравнения (4) являются p и t, образующие код конфигурации, а не $a_1,\ldots,a_n$, как требуется в диофантовом представлении множества. Тем не менее легко понять, что в начальной конфигурации

$$p=1 \qquad (37)$$

(машина находится в состоянии q_1, а головка расположена в крайней левой клетке) и

$$\langle t,\beta,a\rangle = \langle æ,\beta,1\rangle+\langle \mu,\beta,1\rangle+\langle \mathbf{Repeat}(\nu,\beta,a_1),\beta,a_1\rangle+\ldots$$

$$\ldots+\langle \mu,\beta,1\rangle+\langle \mathbf{Repeat}(\nu,\beta,a_n),\beta,a_n\rangle, \qquad (38)$$

где $a=a_1+\ldots+a_n+n+1$ — количество непустых клеток на ленте, $æ$, μ и ν — номера символов "$\star$", "0" и "1" в (1), т. е. $\alpha_{æ}=\star$, $\alpha_{\mu}=0$, $\alpha_{\nu}=1$. Объединяя (4), (37) и (38) и считая $a_1,\ldots,a_n$ параметрами, а все остальные переменные — неизвестными, мы получаем требуемое диофантово представление множества $\mathfrak{M}$.

§ 5.6. Неразрешимость 10-й проблемы Гильберта на машинах Тьюринга

В § 5.5 было введено понятие полуразрешимого по Тьюрингу множества, и в § 5.4–5.5 было установлено, что это понятие эквивалентно понятию диофантова множества. Мы сможем уточнить формулировку 10-й проблемы Гильберта, введя ещё од-

но понятие. А именно, будем говорить, что множество $\mathfrak{M}$, состоящее из n-ок натуральных чисел, *разрешимо по Тьюрингу*, если существует машина Тьюринга M, которая, начав в состоянии q_1 работу над каноническим изображением кортежа $\langle a_1,\ldots,a_n\rangle$ с головкой, установленной на левом конце ленты, закончит через некоторое время работу в заключительном состоянии q_2, если $\langle a_1,\ldots,a_n\rangle\in\mathfrak{M}$, и в заключительном состоянии q_3 в противном случае.

Естественно возникает вопрос о соотношении разрешимости и полуразрешимости по Тьюрингу. Нетрудно понять, что *если множество $\mathfrak{M}$ разрешимо, то оно и полуразрешимо по Тьюрингу*. Действительно, пусть M — машина Тьюринга, требуемая в определении разрешимости, тогда машина

while M **do** STOP **od**; NEVERSTOP (1)

полуразрешает множество $\mathfrak{M}$.

Нетрудно также увидеть, что *если $\mathfrak{M}$ разрешимо, то полуразрешимым является и дополнение $\mathfrak{M}$*. Для этого достаточно вместо машины (1) рассмотреть машину

while M **do** NEVESTOP **od** (2)

Гораздо менее очевидно, что справедливо и обратное: *если и множество $\mathfrak{M}$, и его дополнение полуразрешимы по Тьюрингу, то $\mathfrak{M}$ разрешимо по Тьюрингу*. Прямолинейный путь доказать это состоит в следующем. Пусть M_2 и M_3 — машины Тьюринга, полуразрешающие соответственно $\mathfrak{M}$ и его дополнение. Можно построить третью машину M, которая на одной ленте будет моделировать работу обеих машин M_2 и M_3, выполняя поочередно по одному шагу каждой машины (естественно, что моделировзние одного шага M_2 или M_3 требует выполнения многих шагов машины M). В конце концов одна из машин M_2 или M_3 остановится, и тогда M перейдет соответственно в заключительное состояние q_2 или q_3.

Технические детали одновременного моделирования работы двух машин достаточно сложны. Пользуясь установленной нами эквивалентностью полуразрешимости и диофантовости, мы можем дать более короткое доказательство. Вместо моделирования машин Тьюринга мы построим два диофантовых уравнения

$$D_2(a_1,\ldots,a_n,x_1,\ldots,x_m)=0 \tag{3}$$

и

$$D_3(a_1,\ldots,a_n,x_1,\ldots,x_m)=0, \tag{4}$$

задающих соответственно множество $\mathfrak{M}$ и его дополнение (не ограничивая общности, мы считаем, что оба уравнения имеют равное количество неизвестных). Эти два уравнения можно объеди-

нить в одно уравнение

$$((D_2(a_1,\ldots,a_n,x_1,\ldots,x_m))^2+(1-y_m)^2)\times$$
$$\times((D_3(a_1,\ldots,a_n,x_1,\ldots,x_m))^2+y_m)=0. \qquad (5)$$

Это уравнение, очевидно, имеет решение при любых значениях параметров, при этом $\langle a_1,\ldots,a_n\rangle\in\mathfrak{M}$ в том и только том случае, когда

$$y_m=1. \qquad (6)$$

Пусть M — это машина (5.10), построенная для случая, когда в качестве уравнения (5.1) было взято уравнение (5). В момент остановки машины на ленте будет записан кортеж (5.7). Машина, разрешающая $\mathfrak{M}$, получается как M;EQUAL(l,l+1), где l таково, что происходит проверка равенства (6).

Мы можем теперь уточнить формулировку 10-й проблемы Гильберта следующим образом: «*является ли множество кодов диофантовых уравнений* (без параметров), *имеющих решения, разрешимым по Тьюрингу*?» Это множество было рассмотрено в § 4.5. Там оно было обозначено посредством $\mathfrak{H}_0$, и мы установили, что его дополнение $\overline{\mathfrak{H}}_0$ диофантовым не является. Отсюда следует, что $\mathfrak{H}_0$ не является разрешимым по Тьюрингу. Иными словами, *нельзя построить машину Тьюринга, которая, начав работу над изображением числа k, останавливалась бы через конечное число шагов в состоянии q_2 или q_3 в соответствии с тем, разрешимо или неразрешимо диофантово уравнение с кодом k.*

Тот факт, что множество $\mathfrak{H}_0$ является диофантовым, а именно, задаётся уравнением (4.6.7), показывает, что машины Тьюринга не в состоянии распознавать не только наличие или отсутствие решений у *произвольных уравнений*, но даже наличие или отсутствие решений у уравнений *из одного конкретного семейства*.

§ 5.7. Тезис Чёрча

В предыдущих параграфах этой главы мы получили два, несомненно, замечательных результата, а именно, установили

совпадение диофантовости и полуразрешимости по Тьюрингу (1)

и

неразрешимость 10-й проблемы Гильберта на машинах Тьюринга. (2)

Однако эти технически достаточно сложные результаты порождают массу новых вопросов. Определение диофантова множества

является вполне естественным, в то время как определение множеств, полуразрешимых по Тьюрингу, «обременено» многочисленными техническими деталями, которые представляются произвольными. Например, можно было бы изображать числа на ленте не в единиричной системе счисления, а, скажем, в двоичной. Почему лента потенциально бесконечна только в одну сторону а не в обе? Вместо одной головки на ленте могли бы «трудиться» сразу несколько головок, имеющие каждая собственную систему инструкций и обменивающиеся друг с другом информацией о том, что они видят на ленте. Самих лент могло бы быть несколько, и вообще, память не обязана быть линейной — она могла бы быть, например, в виде плоскости, разделённой на клетки. Для каждой такой модификации машины Тьюринга можно вводить соответствующее понятие полуразрешимости и ставить вопрос о его связи с диофантовостью.

Использованное в § 5.6 уточнение формулировки 10-й проблемы Гильберта также не свободно от критики. Оно основано на весьма специальном способе кодирования диофантовых уравнений. Более естественным могла бы считаться прямая запись на ленте количества неизвестных, степени и коэффициентов уравнения в единиричной или какой-либо позиционной системе счисления. Д. Гильберт не накладывал никаких ограничений на предполагаемый метод решения 10-й проблемы, и если бы, скажем, при какой-либо модификации машины Тьюринга и подходящем способе записи полиномов удалось построить разрешающую машину, это следовало бы считать положительным решением 10-й проблемы Гильберта. В какой же степени установленную в § 5.6 неразрешимость по Тьюрингу можно считать отрицательным решением 10-й проблемы Гильберта?

Для каждого варианта машины Тьюринга (или какого-либо иного абстрактного вычислительного устройства) и для каждого способа представления исходных данных можно пытаться устанавливать результаты, аналогичные (1) и (2). Делать это можно разными путями — прямыми и косвенными. При прямом пути мы должны выбирать подходящие кодировки и устанавливать диофантовость возникающих при этом отношений и функций. При косвенном пути мы можем забыть на время про диофантовы уравнения и устанавливать, что класс полуразрешимых или разрешимых множеств не меняется при соответствующей модификации определений (см., например, упражнения 5.6, 5.7а). Такого рода исследования, устанавливающие связь между (полу)разрешимостью на различных абстрактных вычислительных устройствах, были проведены независимо от работ по 10-й проблеме и задолго до установления её неразрешимости в каком бы то ни было смысле. Эти исследования показали, что понятия полуразрешимого и разрешимого множества, которые у нас были введены на основе

машины Тьюринга, очень устойчивы к выбору вычислительного устройства и способа представления исходных данных. При любом «разумном» выборе получались те же самые классы множеств. Под «разумностью» выбора здесь имеется в виду, в частности, что элементарные шаги вычислений должны быть действительно элементарными, т. е. простыми, легко выполнимыми (нельзя, например, требовать за один шаг узнавать, есть ли решение у данного диофантова уравнения).

Задолго до появления математически строгих конкретных понятий абстрактных вычислительных устройств типа машины Тьюринга существовало интуитивное представление об алгоритмах как способах гарантированного механического решения определённых задач. Классический пример — алгоритм Евклида для нахождения наибольшего общего делителя двух положительных целых чисел. Каждый раз, когда предлагался алгоритм для решения задачи какого-либо конкретного типа, было ясно, что это действительно общий способ, хотя таких интуитивных представлений было еще недостаточно, чтобы доказывать невозможность какого-либо алгоритма.

Исходные данные для работы алгоритма (в интуитивном смысле) берутся из некоторого счётного множества объектов, и, по существу не ограничивая общности, мы будем рассматривать только случаи, когда исходными данными являются натуральные числа или кортежи натуральных чисел фиксированной длины (техника главы 4 показывает, как можно кодировать числами более сложные объекты).

Результатом выполнения алгоритма является построение некоторого объекта. Мы также могли бы ограничиться рассмотрением алгоритмов, выдающих в качестве ответа натуральные числа, но более близким по духу к тематике этой книги будет ограничиться алгоритмами, выдающими только два ответа «ДА» и «НЕТ». Соответственно наряду с интуитивным понятием алгоритма возникают интуитивные понятия разрешимого и полуразрешимого множества. Множество $\mathfrak{M}$ n-ок натуральных чисел разрешимо (в интуитивном смысле), если имеется алгоритм (также в интуитивном смысле), который заканчивает работу над каждой n-кой натуральных чисел и говорит «ДА» или «НЕТ» в соответствии с тем, принадлежит ли эта n-ка множеству или нет. Аналогично, для того чтобы $\mathfrak{M}$ было полуразрешимым множеством, необходимо наличие алгоритма, который говорит «ДА» для каждой n-ки из $\mathfrak{M}$, и говорит «НЕТ» или не заканчивает работу, если n-ка не принадлежит множеству. Всю теорию алгоритмов можно строить в терминах разрешимых и полуразрешимых множеств подобно тому, как можно изгнать понятие функции из математики и работать только с их графиками.

Между интуитивной разрешимостью и полуразрешимостью имеется та же связь, что и между разрешимостью и полуразрешимостью по Тьюрингу: множество разрешимо тогда и только тогда, когда оно само и его дополнение полуразрешимы.

Как же связана формальная (полу)разрешимость по Тьюрингу с (полу)разрешимостью в интуитивном смысле? Одна связь ясна: (полу)разрешимые по Тьюрингу множества признаются большинством математиков (полу)разрешимыми в интуитивном смысле. Обратное утверждение известно как

ТЕЗИС ЧЁРЧА. *Каждое (полу)разрешимое в интуитивном смысле множество n-ок натуральных чисел является (полу)разрешимым по Тьюрингу.*

Здесь мы встретились с таким редким в математике объектом, как *тезис*. Что же это такое? Это не теорема, ибо тезис Чёрча не имеет доказательства. Это не гипотеза, ибо он и не может быть доказан. Это даже не аксиома, которую мы вольны принимать или не принимать. Всё это так из-за того, что тезис Чёрча не является точным математическим утверждением, ибо он связывает строгое понятие (полу)разрешимости по Тьюрингу с нестрогим понятием (полу)разрешимости в интуитивном смысле.

Какие же имеются доводы в пользу тезиса Чёрча? Они бывают разнообразны по форме, но по существу все сводятся к одному: *до сих пор не найдено ни одного примера множества, которое было бы признано большей частью математиков (полу)разрешимым в интуитивном смысле, но для которого не удалось бы построить соответствующую машину Тьюринга.* Конечно, не следует воспринимать это утверждение так, как будто для каждого множества, признанного (полу)разрешимым, фактически строилась требуемая машина Тьюринга, — имеется большой арсенал средств для косвенного установления существования такой машины.

Зачем же нужен тезис Чёрча? С одной стороны, он может служить путеводной звездой — если мы интуитивно установили (полу)разрешимость, то наши шансы найти соответствующую машину Тьюринга очень велики (на самом деле, профессиональные математики обычно ограничиваются установлением интуитивной (полу)разрешимости и не снисходят до формальных доказательств).

С другой стороны, тезис Чёрча играет в математике роль, схожую с ролью закона сохранения энергии в физике, — до тех пор пока не обнаружено ни одно нарушение этого закона, не следует заниматься конструированием вечного двигателя. Аналогично, если установлена неразрешимость по Тьюрингу какого-либо множества, то не следует тратить время на поиски общего

метода, распознающего принадлежность к этому множеству. В частности, такой весьма специальный результат, как (2), даёт математикам, согласно тезису Чёрча, моральное право больше не заниматься бывшими до сих пор бесплодными поисками «способа», который предлагал найти Д. Гильберт в 10-й проблеме.

Вопрос о том, в какой мере (2) может считаться полным решением 10-й проблемы Гильберта, обсуждается с другой точки зрения в главе 7.

Упражнения

5.1. Постройте машину Тьюринга DOUBLE, которая преобразует кортеж (3.1) в кортеж $\langle a_1,\ldots,a_{n-1},2a_n\rangle$ при любом n.

5.2. Постройте машину Тьюринга ERASE, которая преобразует кортеж (3.1) в кортеж $\langle a_2,\ldots,a_n\rangle$.

5.3. Пусть *двоичное изображение числа* на ленте состоит из последовательности идущих подряд клеток с символами "0" и "1" (старшие разряды слева), за которыми следует клетка с символом ".", а *двоичное изображение кортежа* состоит из стоящих вплотную друг к другу двоичных изображений его элементов. Постройте машины Тьюринга BIN(n), которые переводят двоичное изображение n-членного кортежа в единиричное.

5.4. Используя двоичное представление кортежей из упражнения 5.3, можно естественным образом ввести понятие *двоично полуразрешимого по Тьюрингу множества*. Существование машин BIN показывает, что каждое диофантово множесто является двоично полуразрешимым по Тьюрингу. Покажите, что справедливо и обратное.

5.5. Будем говорить, что натуральнозначная функция F, определённая на n-ках натуральных чисел, *вычислима по Тьюрингу*, если существует машина Тьюринга M, которая, начав работу над каноническим изображением кортежа $\langle a_1,\ldots,a_n\rangle$, остановится в том и только том случае, когда значение $F(a_1,\ldots,a_n)$ определено, причём в момент остановки на ленте будет находиться изображение числа $F(a_1,\ldots,a_n)$ Покажите, что вычислимыми по Тьюрингу являются все диофантовы функции, и только они.

5.6. Покажите, что каждое множество, (полу)разрешимое машиной Тьюринга с лентой, бесконечной в обе стороны, (полу)разрешимо и некоторой машиной Тьюринга с лентой, имеющей один конец.

5.7. Помимо машины Тьюринга, было предложено (впоследствии) много других видов абстрактных вычислительных устройств. Некоторые из них можно использовать вместо машины Тьюринга для установления связи диофантовости с полуразрешимостью. Примером могут служить *регистровые машины*. Память такой машины состоит из конечного количества *регистров*, каждый из которых может содержать сколь угодно большое натуральное число. Действия машины определяются программой, которая состоит из конечного числа

инструкций, снабжённых метками. Инструкции могут быть четырёх типов:

I. Lj: Ri ← Ri+1;

II. Lj: Ri ← Ri−1;

III. Lj: **if** Ri = 0 **then goto** Lk;

IV. Lj: **stop**.

Инструкция типа I увеличивает содержимое одного из регистров на 1, инструкция типа II — уменьшает на 1. Инструкция типа III — это условный переход, прерывающий естественный порядок выполнения инструкций. Наконец, инструкция типа IV останавливает машину. Предполагается, что программы пишутся так, чтобы команды типа II выполнялись только в случае, когда соответствующий регистр не пуст. Понятие *множества, полуразрешимого на регистровой машине*, вводится естественным образом: элементы n-ки помещают в n входных регистров (остальные регистры содержат нули), машина начинает выполнять первую инструкцию, и если машина остановится, то исходная n-ка включается в множество.

а) Докажите, что понятия полуразрешимости по Тьюрингу и полуразрешимости на регистровой машине эквивалентны.

б) Дайте прямое доказательство эквивалентности диофантовости и полуразрешимости на регистровой машине путём её моделирования диофантовыми уравнениями.

5.8. Покажите, что любое диофантово множество представимо в виде

$$a \in \mathfrak{D} \iff \exists x_1 \ldots x_m \left[\sum_{k=1}^{l} \lambda(k) x_1^{P_{k1}(a)} \ldots x_m^{P_{km}(a)} = 0 \right],$$

где P_{kj} — полиномы с натуральными коэффициентами, $\lambda(k) = \pm 1$.

Комментарии

А. М. Тьюринг описал абстрактные вычислительные машины, ныне носящие его имя, в своей классической работе [1936]. Близкое понятие было введено также Э. Л. Постом [1936]. С того времени было предложено много модификаций машины Тьюринга–Поста. Использованный в § 5.1 вариант был выбран в этой книге как один из наиболее удобных для моделирования диофантовыми уравнениями.

Разными авторами были предложены другие подходы к уточнению общего понятия алгоритма (история становления теории алгоритмов изложена, в частности, в монографии Успенского и Семёнова [1987]). Все эти подходы приводят к эквивалентным понятиям разрешимого и полуразрешимого множества (для второго понятия более употребителен термин «перечислимое множество»). А. Чёрч [1936] был первым, кто осознал, что одно конкретное и, казалось бы, весьма специальное определение может адекватно отражать основополагающее понятие алгоритма. Тезис Чёрча имеет много эквивалентных переформулировок, определяемых выбором конкретного типа абстрактного

вычислительного устройства, и в том виде, как этот тезис сформулирован в § 5.7, его иногда называют *тезисом Тьюринга*. В работе Колмогорова и Успенского [1958] была предпринята попытка дать максимально общее определение абстрактного вычислительного устройства, удовлетворяющего требованию элементарности отдельных шагов, и установлена его эквивалентность более традиционным моделям вычислительных устройств, в частности, машине Тьюринга.

Первые работы, нацеленные на доказательство алгоритмической неразрешимости 10-й проблемы Гильберта, появились в начале 50-х годов (см. комментарии к главе 1). Уже тогда установление полуразрешимости (при любом стандартном определении этого понятия) диофантовых множеств не представляло труда. В это время М. Девис [1953] высказал смелую гипотезу о том, что справедливо и обратное – *каждое полуразрешимое множество диофантово*, и, таким образом, теоретико-числовое понятие диофантова множества совпадает с алгоритмическим понятием полуразрешимого множества.

М. Девис [1950, 1953] сделал первый шаг к доказательству своей гипотезы — показал, что каждое полуразрешимое множество $\mathfrak{M}$ натуральных чисел имеет представление типа

$$a \in \mathfrak{M} \iff \exists z \forall y_{\leq z} \exists x_1 \ldots x_m [D(a, x_1, \ldots, x_m, y, z) = 0]. \qquad (1)$$

Такое представление получило название *нормальной формы Девиса*.

Поскольку примеры полуразрешимых, но не разрешимых множеств были известны с 30-х годов, из гипотезы Девиса немедленно следовало отрицательное решение 10-й проблемы Гильберта. Доказательство этой гипотезы, однако, столкнулось с трудностями. В такой ситуации естественно было искать другие подходы, которые, не ведя к доказательству гипотезы Девиса, давали бы, тем не менее, отрицательное решение 10-й проблемы Гильберта.

Один из путей ослабления гипотезы Девиса состоит в следующем. В определении семейства уравнений в § 1.4 было сказано, что функция D в (1.4.1) является полиномом относительно *всех* переменных $a_1, \ldots, a_n$, $x_1, \ldots, x_m$. Вместо этого было бы достаточно потребовать полиномиальной зависимости только от $x_1, \ldots, x_m$. Зависимость от $a_1, \ldots, a_n$ могла бы быть любой, лишь бы при подстановке конкретных значений $a_1, \ldots, a_n$ получалось диофантово уравнение относительно $x_1, \ldots, x_m$. Ясно, что и при таком более слабом ограничении на D из положительного решения 10-й проблемы Гильберта следовала бы разрешимость множества с представлением (1.4.2).

В частности, можно было бы рассмотреть класс экспоненциально диофантовых уравнений, в которых неизвестные не могут входить в показатели степени. Подобный подход был предложен А. И. Мальцевым [1968], однако он, по не вполне понятной причине, разрешив параметрам входить в показатели степени, запретил параметрам входить полиномиально наравне с неизвестными. Таким образом, формально из гипотезы Девиса не следовал немедленно ответ на вопрос А. И. Мальцева, хотя такой ответ и может быть из неё легко получен (см. упражнение 5.8).

Другое ослабление гипотезы Девиса было предложено С. Ю. Масловым [1967].

Гипотеза Девиса была доказана в 1970 году, однако хронологический порядок получения доказательства был отличен от логического порядка, который использован в главах 1–5. Одним из важнейших шагов на этом пути было получение экспоненциально диофантова представления для произвольного полуразрешимого множества. Этот результат был первоначально получен М. Девисом и Х. Патнамом в условной форме. Результат был объявлен в сообщении Девиса и Патнама [1959а] и подробно изложен в их труднодоступном отчёте [1959б].

В своем доказательстве М. Девис и Х. Патнам исходили из недоказанной (и до сих пор — 1990г.) гипотезы о том, что существуют сколь угодно длинные арифметические прогрессии, состоящие только из простых чисел. Дж. Робинсон сумела избавиться от этого предположения. Результат был объявлен в кратком сообщении Дж. Робинсон [1960] и её докладе [1962], а затем опубликован в ставшей классической работе Девиса, Патнама и Робинсон [1961]. В этой работе экспоненциально диофантово представление было получено путём устранения ограниченного квантора общности из нормальной формы Девиса (1). Эта техника будет изложена в главе 6.

После получения экспоненциально диофантова представления любого полуразрешимого множества для доказательства гипотезы Девиса оставалось установить диофантовость возведения в степень. История этого этапа описана в комментариях к главе 2.

Установление диофантовости возведения в степень не только завершило доказательство гипотезы Девиса, но и открыло новые пути получения диофантовых представлений полуразрешимых множеств. В частности, представление Девиса (1) перестало быть неизбежным этапом в построении диофантовых представлений. Ранее его необходимость была обусловлена тем, что устранение ограниченного квантора перед диофантовым уравнением в (1) приводило к экспоненциально диофантову уравнению, и потому этот процесс нельзя было итерировать. Имея же возможность преобразовывать экспоненциально диофантовы уравнения в диофантовы, мы теперь можем исходить из арифметического представления полуразрешимого множества, содержащего любое количество ограниченных кванторов общности. Техника же получения арифметических представлений была заложена ещё К. Гёделем [1931].

С другой стороны, установление диофантовости возведения в степень дало возможность строить диофантовы представления, вообще обходясь без ограниченных кванторов общности, как это было сделано в главах 1–5. Впервые такой путь был реализован в работе Матиясевича [1976]. Исходное задание полуразрешимого множества было основано на машине Тьюринга, при этом основные трудности были связаны с необходимостью кодировать числами цепочки символов и последовательность их преобразований. В работах Джонса и Матиясевича [1984], Матиясевича [1984] изложена другая конструкция, где исходное задание полуразрешимого множества осуществляется с помощью *регистровых машин* (см. упражнение 5.7). Подобная модель абстрактных вычислительных устройств была предложена в работах Ламбека [1961], Мельзака [1961], Минского [1961, 1967], Шепердсона и Стёргиса [1963]. Регистровые машины удобны для построения диофантовых представлений тем, что

они, подобно машине Тьюринга, имеют весьма примитивные инструкции, но работают только с числами.

Описанный в § 5.5 метод диофантова моделирования машины Тьюринга отличается от использованного в работе Матиясевича [1976] и излагается здесь впервые.

В заключение приведём цитату из доклада Гильберта [1900], показывающую его отношение к «отрицательным» результатам:

«Вместе с тем бывает и так, что мы добиваемся ответа при недостаточных предпосылках, или идя в неправильном направлении, и вследствие этого не достигаем цели. Тогда возникает задача доказать неразрешимость данной проблемы при принятых предпосылках и выбранном направлении. Такие доказательства невозможности проводились ещё старыми математиками, например, когда они обнаруживали, что отношение гипотенузы равнобедренного прямоугольного треугольника к его катету есть иррациональное число. В новейшей математике доказательства невозможности решений определенных проблем играют выдающуюся роль; там мы констатируем, что такие старые и трудные проблемы, как доказательство аксиомы о параллельных, как квадратура круга или решение уравнения пятой степени в радикалах, получили всё же строгое, вполне удовлетворяющее нас решение, хотя и в другом направлении, чем то, которое сначала предполагалось.

Этот удивительный факт наряду с другими философскими основаниями создает у нас уверенность, которую разделяет, несомненно, каждый математик, но которую до сих пор никто не подтвердил доказательством, — уверенность в том, что каждая определенная математическая проблема непременно должна быть доступна строгому решению или в том смысле, что удаётся получить ответ на поставленный вопрос, или же в том смысле, что будет установлена невозможность её решения и вместе с тем доказана неизбежность неудачи всех попыток её решить».

Глава 6
ОГРАНИЧЕННЫЕ КВАНТОРЫ ОБЩНОСТИ

В § 6.1–6.3 будут приведены три разных способа преобразования формул с ограниченными кванторами общности в эквивалентные формулы, содержащие только кванторы существования. В § 6.4–6.6 на различных задачах будет продемонстрировано, каким мощным средством построения диофантовых представлений является эта техника.

§ 6.1. Первая конструкция: машины Тьюринга

Мы хотим показать, что *если* $\mathcal{R}(a_1,\ldots,a_n)$ — *диофантово отношение, то диофантовым является и отношение, задаваемое формулой*

$$\forall y_{<a_n}\mathcal{R}(a_1,\ldots,a_{n-1},y). \tag{1}$$

Приведём сначала эвристические соображения в пользу этого факта, основанные на тезисе Чёрча. Для этого мы должны в предположении полуразрешимости отношения $\mathcal{R}$ предложить алгоритм (в интуитивном смысле) для установления истинности (1) при подходящих значениях $a_1,\ldots,a_n$. Формула (1) по определению истинна при $a_n=0$; при $a_n>0$ она эквивалентна утверждению о том, что истинно каждое из следующих утверждений:

$$\begin{gathered}\mathcal{R}(a_1,\ldots,a_{n-1},0),\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ \mathcal{R}(a_1,\ldots,a_{n-1},a_n-1).\end{gathered} \tag{2}$$

По предположению о полуразрешимости $\mathcal{R}$ мы можем установить истинность любого из этих утверждений за конечное число шагов, и, проделав это для каждого из утверждений (2), мы установим истинность (1).

Это рассуждение ещё не является формальным доказательством; кроме того, оно не даёт явного способа для преобразования (1) в эквивалентное диофантово уравнение, когда $\mathcal{R}$ задано диофантовым уравнением. Чтобы получить формальное доказательство, мы должны описать конструкцию соответствующей машины Тьюринга, что и будет сейчас сделано.

Итак, пусть $\mathcal{R}$ — отношение, задаваемое диофантовым уравнением

$$D(a_1, \ldots, a_n, x_1, \ldots, x_{m+1}) = 0. \tag{3}$$

Возьмём это уравнение в качестве уравнения (5.4.1) и построим по нему описанным в § 5.4 способом машину M, полуразрешающую $\mathcal{R}$.

В момент остановки машины M на ленте записан кортеж (5.4.9). Определим машину M' следующим образом:

$$M' = M; M_2; \mathrm{DELETE} \tag{4}$$

где M_2 — машина из определения (5.4.10) машины M. Машина M' также полуразрешает $\mathcal{R}$, но в момент её остановки на ленте вновь записан исходный кортеж $\langle a_1, \ldots, a_n \rangle$.

Машина M'', полуразрешающая (1), легко теперь строится:

$$M'' = \textbf{while } \mathrm{DEC} \textbf{ do } M' \textbf{ od} \tag{5}$$

Эта машина, очевидно, работает следующим образом. Если $a_n = 0$, то машина DEC остановится в состоянии q_3, что приведёт к остановке машины M'' в состоянии q_2. Если же a_n было больше 0, то машина M' начнёт проверять выполнение условия $\mathcal{R}(a_1, \ldots, a_{n-1}, a_n - 1)$. Если проверка закончится успешно, то машина DEC проверит равенство $a_n - 1 = 0$ и в случае его невыполнения машина M' начнёт проверять условие $\mathcal{R}(a_1, \ldots, a_{n-1}, a_n - 2)$ и т. д. Если все условия (2) выполнены, то машина M'' в конце концов остановится в состоянии q_2.

Для получения диофантова уравнения

$$E(a_1, \ldots, a_n, x_1, \ldots, x_w) = 0, \tag{6}$$

эквивалентного формуле (1), осталось указанным в § 5.5 способом смоделировать работу машины M''.

Описанный выше переход от уравнения (3) к уравнению (6) является вполне конструктивным, но довольно окольным. В последующих параграфах будут описаны более прямые, теоретико-числовые методы осуществления такого перехода.

§ 6.2. Вторая конструкция: гёделево кодирование

Для упрощения обозначений мы проведём доказательство для случая, когда $n = 2$ в (1.1) и, соответственно, в (1.3). Доказательство в общем случае проводится совершенно аналогично; другой способ обобщения на случай произвольного n состоит в использовании канторовой нумерации (ср. с § 4.4).

Итак, наша задача — установить диофантовость множества пар, задаваемого формулой

$$\forall y_{<b} \exists x_1 \ldots x_m [D(a, y, x_1, \ldots, x_m) = 0], \tag{1}$$

где D, как обычно, — произвольный полином с целыми коэффициентами. Для этого мы должны построить новый полином E такой, что формула (1) эквивалентна формуле

$$\exists z_0 \ldots z_k [E(a, b, z_0, \ldots, z_k) = 0]. \tag{2}$$

Истинность (2) при каких-то значениях a и b влечёт истинность (1), т. е. существование b кортежей

$$\begin{array}{c} \langle x_{1,0}, \ldots, x_{m,0} \rangle, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \langle x_{1,b-1}, \ldots, x_{m,b-1} \rangle \end{array} \tag{3}$$

таких, что для любого y от 0 до b-1

$$D(a, y, x_{1,y}, \ldots, x_{m,y}) = 0. \tag{4}$$

Естественно ожидать, что информация о числах (3) должна содержаться в каком-то виде в числах $z_0, \ldots, z_k$, существование которых утверждается в (2).

Вместо (3) — *переменного количества кортежей фиксированной длины* — мы рассмотрим *фиксированное количество кортежей переменной длины*

$$\begin{array}{c} \langle x_{1,0}, \ldots, x_{1,b-1} \rangle, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \langle x_{m,0}, \ldots, x_{m,b-1} \rangle. \end{array} \tag{5}$$

Для работы с (5) мы будем использовать кодировку, близкую к рассматривавшейся в § 3.2 гёделевой кодировке. А именно, будут выбраны попарно взаимно простые числа $q_0, \ldots, q_{b-1}$ такие, что при $i = 1, \ldots, m$, $y = 0, \ldots, b$-1

$$x_{i,y} = \mathbf{rem}(z_i, q_y). \tag{6}$$

Число z_0 будет удовлетворять при $y = 0, \ldots, b$-1 условию

$$y = \mathbf{rem}(z_0, q_y). \tag{7}$$

Достоинство кодировки, основаной на китайской теореме об остатках, состоит в том, что она позволяет вычислять значение полинома прямо по кодам без предварительного нахождения кодируемых элементов. А именно,

$$D(a, y, x_{1,y}, \ldots, x_{m,y}) \equiv D(a, z_0, z_1, \ldots, z_m) (\mathbf{mod}\ q_y), \tag{8}$$

и, следовательно, если q_y столь велико, что выполнено не только (6), но и

$$|D(a, y, x_{1,y}, \ldots, x_{m,y})| < q_y, \tag{9}$$

то выполнение равенства (4) для какого-то y эквивалентно справедливости сравнения

$$D(a, z_0, z_1, \ldots, z_m) \equiv 0 (\mathbf{mod}\ q_y). \tag{10}$$

В (10) от y зависит только выбор модуля, и потому выполнение равенства (4) для всех значений y от 0 до b-1 эквивалентно справедливости сравнения

$$D(a, z_0, z_1, \ldots, z_m) \equiv 0 (\mathbf{mod}\ q_0 \cdots q_{b-1}). \tag{11}$$

То, что мы проделали до сих пор, ещё не избавило нас от ограниченного квантора общности — например, в (11) он приобрёл форму многоточия в правой части. Здесь устранение квантора общности произойдёт благодаря тому, что, пользуясь нашей свободой в выборе $q_0, \ldots, q_{b-1}$, мы выберем эти числа так, что произведение $q_0 \cdots q_{b-1}$ окажется диофантовой функцией от b. А именно, в отличие от выбора Гёделя (3.2.7) мы положим при $y = 0, \ldots, b-1$

$$q_y = \frac{q+1}{y+1} - 1, \tag{12}$$

где q велико, а $q+1$ кратно $b!^2$. В этом случае

$$q_0 \cdots q_{b-1} = \prod_{y=0}^{b-1} \frac{q-y}{y+1} = \binom{q}{b}, \tag{13}$$

а диофантовость биномиальных коэффициентов была установлена в § 3.4. В результате (10) можно переписать в виде диофантова условия

$$D(a, z_0, z_1, \ldots, z_m) \equiv 0 (\mathbf{mod}\ \binom{q}{b}). \tag{14}$$

Мы ещё не полностью избавились от квантора общности, поскольку должны обеспечить выполнение при $y = 0, \ldots, b-1$ условий (7) и (9), где $x_{i,y}$ определены в (6). Первое не вызывает трудностей благодаря удачному выбору q_y — легко проверить, что можно положить

$$z_0 = q. \tag{15}$$

Строго говоря, мы не добьёмся выполнения именно (9). Вместо этого мы будем иметь аналоги (9) и (10) — неравенство

$$|D(a, y, x_{1,y}, \ldots, x_{m,y})| < p_y \tag{16}$$

и сравнение

$$D(a, y, x_{1,y}, \ldots, x_{m,y}) \equiv 0 (\mathbf{mod}\ p_y), \tag{17}$$

где

$$p_y | q_y, \tag{18}$$

$$x_{i,y} = \mathbf{rem}(z_i, p_y). \tag{19}$$

Очевидно, что этого достаточно для выполнения (4).

Чтобы получить (16), мы введём вспомогательную переменную w и потребуем, чтобы для $i=1,\dots,m$, $y=0,\dots,b-1$

$$x_{i,y}<w. \tag{20}$$

При фиксированных значениях a и b такую границу w, очевидно, можно найти. Далее, очевидно, что

$$|D(a,y,x_{1,y},\dots,x_{m,y})|\le B(a,b,w), \tag{21}$$

где $B(a,b,w)$ — полином, получающийся из полинома $D(a,y,x_1,\dots,x_m)$ изменением знака у всех отрицательных коэффициентов и последующей подстановкой b вместо y и w вместо $x_1,\dots,x_m$. Для получения (16) мы будем добиваться, чтобы

$$p_y>B(a,b,w), \tag{22}$$

и было выполнено (20) при $x_{i,y}$, определяемых согласно (19).

Из (6) и (20) следует, что

$$q_y \,\Big|\, \prod_{k=0}^{w-1}(z_i-k). \tag{23}$$

Мы выберем q так, что

$$b!(b+w+B(a,b,w))!\,|\,q+1, \tag{24}$$

тогда q_y будет взаимно просто с $w!$, и из (23) будет следовать, что

$$q_y \,\Big|\, \binom{z_i}{w}. \tag{25}$$

Наконец, в силу (13) система из bm условий (25) сворачивается в m диофантовых условий

$$\begin{gathered}\binom{q}{b}\,\Big|\,\binom{z_1}{w},\\ \dots\dots\dots\dots\\ \binom{q}{b}\,\Big|\,\binom{z_m}{w}.\end{gathered} \tag{26}$$

В итоге мы получили систему из $m+3$ диофантовых условий (14), (15), (24) и (26), которая разрешима относительно q, w, $z_0,\dots,z_m$ при условии, что выполнено (1). Проверим теперь что справедливо и обратное — из разрешимости системы (14), (15), (24), (26) следует справедливость (1).

Пусть y — произвольное число, такое, что $y<b$. Определим число q_y согласно (12). Из (26) следует (25) и тем более (23). К сожалению, из (23) не следует (20), если $x_{i,y}$

определено равенством (6), так как q_y, вообще говоря, число составное. Именно поэтому мы рассмотрим вместо q_y какой-либо его простой делитель p_y, естественно, удовлетворяющий (18). Из (23) следует, что

$$p_y \mid \prod_{x=0}^{w-1}(z_i-x). \tag{27}$$

Отсюда ввиду простоты p_y следует существование чисел $x_{1,y},\ldots,x_{m,y}$, удовлетворяющих (20) и таких, что

$$p_y \mid z_i-x_{i,y}. \tag{28}$$

Из (15), (12) и (17) получаем, что

$$p_y \mid z_0-y, \tag{29}$$

отсюда и из (14) получаем справедливость (10), а следовательно, и (17). Нетрудно видеть, что благодаря (24) все простые делители q_y больше $B(a,b,w)$, так что выполнено (22), а следовательно, и (16). Как уже указывалось, из (16)–(17) следует (4) и ввиду произвольности y мы получаем и справедливость (1).

Для получения искомого диофантова уравнения (2) остаётся устранить из (14), (15), (24) и (26) биномиальные коэффициенты и факториалы (средства для этого описаны в § 3.4) и объединить получающиеся при этом диофантовы уравнения в одно.

§ 6.3. Третья конструкция: суммирование

Мы снова решаем ту же задачу, что и в § 6.1–6.2, — устанавливаем диофантовость множества пар, задаваемого формулой

$$\forall y_{<b}\exists x_1\ldots x_m[D(a,y,x_1,\ldots,x_m)=0], \tag{1}$$

где D — полином с целыми коэффициентами. В § 6.2 мы использовали для этого разновидность гёделева кодирования, и по значениям неизвестных, удовлетворяющим (1.2), для каждого значения y легко находились соответствующие значения $x_1,\ldots,x_m$. В конструкции, которая будет изложена ниже, такого явного соответствия значений переменных нет.

Мы начнём с того, что воспользуемся техникой, аналогичной применённой в § 1.4, и изолируем переменную, стоящую в (1) под квантором общности, а именно, преобразуем (1) в эквивалентную формулу вида

$$\forall y_{<b}\exists x_0\ldots x_m[D_1(a,x_0,\ldots,x_m)=y], \tag{2}$$

где

$$D_1(a,x_0,\ldots,x_m)=(x_0+1)(1-D^2(a,x_0,\ldots,x_m))-1. \tag{3}$$

Далее, так же, как в § 6.2, мы введём явную границу и на значения $x_0,\dots,x_m$, а именно, перепишем (2) в виде эквивалентной формулы

$$\exists w \forall y_{<b} \exists x_{0_{<w+1}} \dots x_{m_{<w+1}} [D_1(a, x_0, \dots, x_m) = y]. \tag{4}$$

(по причине, которая станет ясной позднее, нам будет важно, чтобы граница была положительной).

Так же, как в § 6.2, нам потребуется полином $B(a,w)$ с натуральными коэффициентами такой, что при

$$x_i \le w, \quad i = 0,\dots,m \tag{5}$$

справедливо неравенство

$$|D_1(a, x_0, \dots, x_m)| < B(a,w). \tag{6}$$

В дальнейшем нам потребуются двухсторонние оценки некоторых величин, причём верхние и нижние оценки будут близки друг другу. Каждая такая пара оценок будет содержать одинаковый главный член A и небольшие добавочные члены B^- и B^+, точный вид которых для нас будет несущественным. Для упрощения записи и выделения главного члена вместо неравенств

$$A - B^- \le X \le A + B^+ \tag{7}$$

мы будем писать символическое равенство

$$X = A + \theta(B), \tag{8}$$

где $\theta(B)$ будет обозначать некоторую величину, лежащую в интервале $[-B, B]$. Подобно символу $O(T)$, $\theta(B)$ в разных формулах может иметь разное значение.

В § 6.2 для объединения переменного количества уравнений в одно условие мы переходили от равенства нулю к сравнению по большому модулю. Здесь мы сделаем менее очевидное преобразование. Существенную роль при этом будет играть функция **unit**(t) — *количество единиц в двоичной записи числа* t, обладающая, очевидно, следующим свойством:

$$2^q > s \Rightarrow \mathbf{unit}(r) + \mathbf{unit}(s) = \mathbf{unit}(2^q r + s). \tag{9}$$

Пусть натуральные числа p и q и целые числа α и β удовлетворяют неравенствам

$$p > 2q, \quad 2^q > |\alpha|, \quad 2^q > |\beta|. \tag{10}$$

Нетрудно проверить, что

$$\mathbf{unit}(2^p - 1 + \alpha - \beta) = \begin{cases} p + \theta(q), & \text{если } \alpha \le \beta, \\ \theta(q) & \text{в противном случае.} \end{cases} \tag{11}$$

Меняя α и β местами и применяя (9), получаем, что

$$\mathbf{unit}(2^{p+1}(2^p-1+\alpha-\beta)+2^p-1-\alpha+\beta) = \\ = \begin{cases} 2p, \text{ если } \alpha=\beta, \\ p+\theta(2q) \text{ в противном случае.} \end{cases} \tag{12}$$

Мы используем этот критерий равенства, положив

$$\alpha = D_1(a, x_0, \ldots, x_m), \tag{13}$$

$$\beta = y, \tag{14}$$

$$q = B(a, w)+b+1, \tag{15}$$

$$p = (b+1)(4(w+1)^{m+1}+2)q. \tag{16}$$

Введём следующие обозначения для получающихся при этом выражений:

$$E(x_0, \ldots, x_m, w) = (2^{p+1}-1)D_1(a, x_0, \ldots, x_m)+2^{2p+1}-2^p-1, \tag{17}$$

$$F(w) = 2^{p+1}-1 \tag{18}$$

(E и F зависят также и от a и b, но для упрощения обозначений зависимость от этих параметров не будет указываться явно). В этих обозначениях

$$\mathbf{unit}(E(x_0, \ldots, x_m, w)-F(w)y) = \\ = \begin{cases} 2p, \text{ если } D_1(a, x_0, \ldots, x_m) = y, \\ p+\theta(2q) \text{ в противном случае.} \end{cases} \tag{19}$$

Таким образом, мы сумели построить натуральное число, а именно,

$$E(x_0, \ldots, x_m, w)-F(w)y, \tag{20}$$

которое имеет много или мало единиц в двоичной записи в соответствии с тем, образуют ли $x_0, \ldots, x_m$ и y решение уравнения

$$D_1(a, x_0, \ldots, x_m) = y. \tag{21}$$

При этом

$$0 \le E(x_0, \ldots, x_m, w)-F(w)y < 2^{2p+2}, \tag{22}$$

и мы можем, согласно (6), объединить все $(w+1)^{m+1}$ чисел (16), соответствующих разным значениям $x_0, \ldots, x_m$, удовлетворяющим (5), в одно число

$$G(w, y) = K(w)-L(w)y, \tag{23}$$

где

$$K(w) = \sum_{x_0=0}^{w} \dots \sum_{x_m=0}^{w} 2^{(2p+2)(x_m(w+1)^m+\dots+x_0)} E(x_0,\dots,x_m,w), \tag{24}$$

$$L(w) = \sum_{x_0=0}^{w} \dots \sum_{x_m=0}^{w} 2^{(2p+2)(x_m(w+1)^m+\dots+x_0)} F(w). \tag{25}$$

Согласно (19)

$$\mathbf{unit}(G(w,y)) = ((w+1)^{m+1}+s)p+\theta(2(w+1)^{m+1}q), \tag{26}$$

где s — количество наборов $x_0,\dots,x_m$, удовлетворяющих (5) и (21). Таким образом, для разрешимости уравнения (21) в неизвестных $x_0,\dots,x_m$, удовлетворяющих неравенствам (5), *необходимо*, чтобы

$$\mathbf{unit}(G(w,y)) \geq (w+1)^{m+1}p+p-2(w+1)^{m+1}q, \tag{27}$$

и *достаточно*, чтобы

$$\mathbf{unit}(G(w,y)) > (w+1)^{m+1}p+2(w+1)^{m+1}q. \tag{28}$$

Благодаря (16) неравенство (27) сильнее, чем (28), и любое промежуточное по силе неравенство будет необходимым и достаточным. По причине, которая станет яснее позже, мы выберем в качестве необходимого и достаточного условия неравенство

$$\mathbf{unit}(G(w,y)) \geq I(w)-J(w)y, \tag{29}$$

где

$$I(w) = (w+1)^{m+1}p+p-2(w+1)^{m+1}q, \tag{30}$$

$$J(w) = (4(w+1)^{m+1}+2)q. \tag{31}$$

Далее мы снова используем теорему Куммера (см. Приложение 3), которая даёт следующее выражение для $\mathbf{unit}(t)$:

$$\mathbf{unit}(t) = \mathbf{deg}_2\binom{2t}{t}, \tag{32}$$

где $\mathbf{deg}_2(r)$ — показатель, с которым число 2 входит в разложение r на простые множители.

Равенство (32) позволяет нам устранить функцию **unit** из (29), переписав это условие в виде

$$2^{J(w)} \mid C(w,y), \tag{33}$$

где

$$C(w,y) = 2^{J(w)y}\binom{2G(w,y)}{G(w,y)}. \tag{34}$$

Левая часть в (33) не зависит от y, и мы можем просуммиро-

вать правые части по y:

$$2^{l(w)} \mid S(w), \tag{35}$$

где

$$S(w) = \sum_{y=0}^{b-1} C(w,y). \tag{36}$$

Очевидно, что из справедливости (33) для $y = 0,\ldots,b-1$ следует справедливость (35). Менее очевидно, что *из одной делимости* (35) *суммы нескольких чисел следует делимость* (33) *каждого слагаемого*. Проверим, что тем не менее это именно так.

Предположим противное, т. е. что (35) справедливо, но для некоторого y, такого, что $y < b$, (33) не выполнено; пусть y_0 — наименьшее значение, при котором это происходит. Иными словами, уравнение (21) при $y < y_0$ имеет решение, удовлетворяющее (5), а при $y = y_0$ — не имеет.

Согласно (34), (32), (28), (16), (30) и (31)

$$\begin{aligned}\mathbf{deg}_2(C(w,y_0)) &= J(w)y_0+\mathbf{unit}(G(w,y_0)) \le \\ &\le J(w)y_0+(w+1)^{m+1}p+2(w+1)^{m+1}q < l(w).\end{aligned} \tag{37}$$

Согласно (34), (32), (27), (30) и (37) при $y < y_0$

$$\mathbf{deg}_2(C(w,y)) = J(w)y+\mathbf{unit}(G(w,y)) \ge l(w) > \mathbf{deg}_2(C(w,y_0)). \tag{38}$$

Согласно (34), (32), (26), (30), (31) и (37) при $y > y_0$

$$\begin{aligned}\mathbf{deg}_2(C(w,y)) &= J(w)y+\mathbf{unit}(G(w,y)) \ge \\ &\ge J(w)(y_0+1)+(w+1)^{m+1}p-2(w+1)^{m+1}q > \mathbf{deg}_2(C(w,y_0)).\end{aligned} \tag{39}$$

Таким образом, при $y \ne y_0$

$$\mathbf{deg}_2(C(w,y)) > \mathbf{deg}_2(C(w,y_0)), \tag{40}$$

и потому

$$\mathbf{deg}_2(S(w)) = \mathbf{deg}_2(C(w,y_0)) < l(w), \tag{41}$$

что даёт искомое противоречие с (35).

В итоге мы получили, что формула (35) эквивалентна формуле

$$\forall y_{<b} \exists x_{0_{<w+1}} \ldots x_{m_{<w+1}} [D_1(a,x_0,\ldots,x_m) = y], \tag{42}$$

и, следовательно, формулы (4), (2) и (1) эквивалентны формуле

$$\exists w[2^{l(w)} \mid S(w)]. \tag{43}$$

Таким образом, мы избавились от ограниченного квантора общности, но платой за это является появление в (24), (25) и (36) суммирования с переменным верхним пределом. К счастью, все эти суммы легко вычисляются, и S оказывается диофантовой функцией.

Кратная сумма в (25) равна, очевидно, произведению

$$\left(\sum_{x_0=0}^{w} 2^{(2p+2)x_0}\right)\times \cdots \times\left(\sum_{x_0=0}^{w} 2^{(2p+2)(w+1)^m x_m}\right)F(w), \tag{44}$$

в котором первые $m+1$ сомножителей — геометрические прогрессии, знаменатели которых отличны от 1 (именно ради этого в (4) была взята положительная граница). Таким образом,

$$L(w)=\frac{2^{(2p+2)(w+1)}-1}{2^{2p+2}-1}\times \cdots \times\frac{2^{(2p+2)(w+1)^{m+1}}-1}{2^{(2p+2)(w+1)^m}-1}F(w)=$$

$$=\frac{L_1(w)-L_2(w)}{L_3(w)-L_4(w)}, \tag{45}$$

где $L_1(w)$, $L_2(w)$, $L_3(w)$ и $L_4(w)$ — выражения, построенные из конкретных натуральных чисел и переменных a, b и w с помощью сложения, умножения и возведения в степень, причём всегда $L_3(w)>L_4(w)$.

Согласно (17)

$$E(x_0,\ldots,x_m,w) = \sum_{i_0,\ldots,i_m} \lambda_{i_0,\ldots,i_m} x_0^{i_0}\ldots x_m^{i_m}, \tag{46}$$

где целочисленные коэффициенты $\lambda_{i_0,\ldots,i_m}$ зависят от a, b и w. Подставляя это выражение для E в (24) и меняя порядок суммирования, получаем, что

$$K(w)=$$

$$=\sum_{i_0,\ldots,i_m} \lambda_{i_0,\ldots,i_m}\sum_{x_0=0}^{w}\cdots\sum_{x_m=0}^{w} 2^{(2p+2)(x_m(w+1)^m+\ldots+x_0)} x_0^{i_0}\ldots x_m^{i_m}. \tag{47}$$

Внутренняя $(m+1)$-кратная сумма в (47) равна, очевидно, произведению однократных сумм вида

$$\sum_{x=0}^{w} 2^{(2p+2)x(w+1)^k} x^{i_k}. \tag{48}$$

В Приложении 4 описаны формулы для суммирования таких обоб-

щённых геометрических прогрессий. В итоге для $K(w)$ получается представление

$$K(w)=\frac{K_1(w)-K_2(w)}{K_3(w)-K_4(w)}, \tag{49}$$

где аналогично (45) $K_1(w)$, $K_2(w)$, $K_3(w)$ и $K_4(w)$ — выражения, построенные из конкретных натуральных чисел и переменных a, b и w с помощью сложения, умножения и возведения в степень, причём всегда $K_3(w)>K_4(w)$.

Обратимся теперь к сумме (36). Входящие в неё величины $C(w,y)$ определены в (34) через биномиальные коэффициенты. Диофантовость последних была установлена в § 3.4 путём построения позиционного кода кортежа (3.4.1). Сейчас мы построим шифр некоторого кортежа по достаточно большому основанию u, один из элементов которого равен $S(w)$.

Имеем:

$$(u+1)^{2G(w,y)} = \sum_{i=0}^{2G(w,y)} \binom{2G(w,y)}{i} u^i. \tag{50}$$

Интересующий нас коэффициент

$$\binom{2G(w,y)}{G(w,y)} \tag{51}$$

стоит в (50) при $u^{G(w,y)}=u^{K(w)-L(w)y}$.

Умножим (50) на $2^{J(w)y}u^{L(w)y}$ и просуммируем по y:

$$\sum_{y=0}^{b-1} 2^{J(w)y}u^{L(w)y}(u+1)^{2K(w)-2L(w)y} =$$

$$= \sum_{y=0}^{b-1} \sum_{i=0}^{2G(w,y)} 2^{J(w)y}\binom{2G(w,y)}{i} u^{i+L(w)y}. \tag{52}$$

Полагая здесь $u=1$, получаем, что

$$\sum_{y=0}^{b-1} \sum_{i=0}^{2G(w,y)} 2^{J(w)y}\binom{2G(w,y)}{i} =$$

$$=\sum_{y=0}^{b-1} 2^{2K(w)+(J(w)-2L(W))y} \le 2^{2K(w)+J(w)b}(b+1). \tag{53}$$

Таким образом, если

$$u>2^{2K(w)+J(w)b}(b+1), \tag{54}$$

то число (52) является шифром по основанию u некоторого кортежа, $(K(w)+1)$-й элемент которого равен $S(w)$. Но слева в (52) стоит сумма арифметической прогрессии, и мы получаем, что

$$S(w) = \mathbf{Elem}((u+1)^{2K(w)}(((2^{J(w)}u^{L(w)}(u+1)^{2K(w)})^b-1)\mathbf{div}$$
$$(2^{J(w)}u^{L(w)}(u+1)^{2K(w)}-1)), u, K(w)+1) \qquad (55)$$

при условии, что выполнено (54).

Равенства (44), (46), (52), (30) и (31) показывают, что I, J, K, L и S — диофантовы функции (трёх аргументов a, b и w) и, следовательно, (43) можно рассматривать как обобщённое диофантово представление множества, задаваемого формулой (1).

§ 6.4. Связи между 8-й и 10-й проблемами Гильберта

Техника, развитая в предыдущих параграфах этой главы, позволяет нам пополнить ограниченным квантором общности наш арсенал логических средств, допустимых при построении диофантовых представлений. Легко понять, что в качестве границы можно брать не только переменные, но и значение любой диофантовой функции. Формула может содержать несколько ограниченных кванторов общности, преобразование такой формулы следует начинать с устранения самого внутреннего квантора общности.

Квантор общности, даже ограниченный, является мощным средством установления диофантовости различных множеств. Например, очевидно, что множество простых чисел задаётся формулой

$$a > 1 \,\&\, \forall x_{<a} \forall y_{<a} [a \neq (x+2)(y+2)], \qquad (1)$$

которая может быть теперь преобразована в диофантово представление этого множества:

$$\mathbf{Prime}(a) \Leftrightarrow \exists x_1 \ldots x_m [\mathbf{P}(a, x_1, \ldots, x_m) = 0]. \qquad (2)$$

В § 2.5 мы видели, что среди индивидуальных подпроблем 10-й проблемы Гильберта мы можем указать такую, которая эквивалентна «Великой теореме Ферма». Хотя такой возможности не было до 1970 года, этот факт всё же не слишком удивителен, поскольку в «Великой теореме Ферма» речь идёт также с диофантовых уравнениях. В этом параграфе мы увидим, что ещё две знаменитые проблемы, казалось бы далекие от диофантовых уравнений, могут быть переформулированы как утверждения о неразрешимости конкретных диофантовых уравнений.

Мы начнём с *гипотезы Гольдбаха*, включённой Д. Гильбертом в 8-ю проблему. Эта гипотеза, всё ещё (1990г.) не доказанная и не опровергнутая, состоит в том, что *каждое чётное число, большее, чем 2, представимо как сумма двух простых чисел*. Имея в своём распоряжении полином **P** из (2), мы можем переформулировать гипотезу Гольдбаха как утверждение о том, что диофантово уравнение

$$(2a+4-p_1-p_2)^2+\mathbf{P}^2(p_1,x_1,\ldots,x_m)+\mathbf{P}^2(p_2,y_1,\ldots,y_m)=0 \qquad (3)$$

разрешимо относительно p_1, p_2, $x_1,\ldots,x_m$, $y_1,\ldots,y_m$ при всех значениях параметра a. Эта переформулировка ещё не делает гипотезу Гольдбаха индивидуальной подпроблемой 10-й проблемы Гильберта, ибо Д. Гильберт предлагал найти способ для распознавания разрешимости отдельнных уравнений, а не параметрических семейств.

Чтобы свести гипотезу Гольдбаха к одному уравнению, заметим, что утверждение о том, что число $2a+4$ *не* представимо в виде суммы двух простых чисел, легко записывается с помощью ограниченного квантора общности:

$$\forall z_{<a+1}\exists xy[z+2=(x+2)(y+2)\ \vee\ (2a+2-z)=(x+2)(y+2)]. \qquad (4)$$

Мы можем преобразовать эту формулу в диофантово уравнение

$$\mathbf{G}(a,x_1,\ldots,x_m)=0, \qquad (5)$$

разрешимое относительно $x_1,\ldots,x_m$ для тех и только тех значений параметра a, которые удовлетворяют условию (4), т. е. опровергают гипотезу Гольдбаха. Заменяя теперь параметр a на неизвестную, мы получаем, что *гипотеза Гольдбаха эквивалентна утверждению о том, что уравнение*

$$\mathbf{G}(x_0,\ldots,x_m)=0 \qquad (6)$$

не имеет решений.

В 8-ю проблему Гильберта включена и другая знаменитая гипотеза, также связанная с простыми числами и также до сих пор (1990г.) не доказанная и не опровергнутая — *гипотеза Римана*. Эта гипотеза касается комплексных нулей *дзета-функции Римана*, которая может быть определена при $\mathbf{Re}(\alpha)>1$ равенством

$$\zeta(\alpha)=\sum_{n=1}^{\infty}\frac{1}{n^{\alpha}}. \qquad (7)$$

Увидеть, что дзета-функция Римана имеет связь с простыми числами, можно из найденного Л. Эйлером тождества

$$\sum_{n=1}^{\infty}\frac{1}{n^{\alpha}}=\prod_{p}\left(1-\frac{1}{p^{\alpha}}\right)^{-1}. \qquad (8)$$

где произведение в правой части берётся по всем простым числам. Выражение под знаком произведения в (8) можно переписать в виде

$$\left(1-\frac{1}{p^{\alpha}}\right)^{-1}=1+\frac{1}{p^{\alpha}}+\frac{1}{p^{2\alpha}}+\ldots, \tag{9}$$

и тогда станет видно, что тождество (8) — это аналитическая запись основной теоремы арифметики.

Ряд и произведение в (8) сходятся только при $\mathbf{Re}(\alpha)>1$ и определяют в этой полуплоскости аналитическую функцию, которая стандартными методами математического анализа может быть продолжена на всю комплексную плоскость, кроме точки $\alpha=1$, где дзета-функция имеет простой полюс. Известно, что

$$0=\zeta(-2)=\zeta(-4)=\zeta(-6)=\ldots, \tag{10}$$

и числа −2, −4, −6,... называют *тривиальными нулями* дзета-функции. Гипотеза Римана утверждает, что все остальные, *нетривиальные* комплексные нули лежат на прямой $\mathbf{Re}(\alpha)=0,5$.

Гипотеза Римана играет важную роль в исследовании распределения простых чисел в натуральном ряду. Пусть $\pi(n)$, как принято, обозначает количество простых чисел, не превосходящих n. Согласно *закону распределения простых чисел*

$$\pi(n) = \frac{n}{\ln(n)}(1+o(1)). \tag{11}$$

Элементарная функция $n/\ln(n)$ является на самом деле не очень хорошим приближением к $\pi(n)$; гораздо более хорошим приближением является неэлементарная функция

$$\mathbf{Li}(n) = \int_0^n \frac{d\alpha}{\ln(\alpha)}. \tag{12}$$

Гипотеза Римана может быть переформулирована как утверждение о том, что

$$\pi(n) = \mathbf{Li}(n)+O(\mathbf{sqrt}(n)\ln(n)). \tag{13}$$

Технически удобнее работать не с функцией π, а с родственной ей *функцией Чебышева* ψ, которую можно определить равенством

$$\psi(n) = \ln(\mathbf{LCM}(1,2,\ldots,n)). \tag{14}$$

Если функция π прыгает на 1 на каждом простом числе p, то функция ψ прыгает на $\ln(p)$ на само́м p и на всех его степенях. В терминах функции ψ закон распределения простых чисел (11) записывается в виде

$$\psi(n) = n+o(n), \tag{15}$$

причём главный член n здесь является хорошим приближением, а

гипотеза Римана эквивалентна утверждению о том, что

$$\psi(n) = n+O(\mathbf{sqrt}(n)\mathbf{ln}^2(n)). \tag{16}$$

Чтобы иметь возможность сформулировать гипотезу Римана как утверждение о неразрешимости конкретного уравнения, нам надо знать значение константы, подразумеваемой в символе O; известно, что из гипотезы Римана следует, что

$$|\psi(n)-n| < \mathbf{sqrt}(n)\mathbf{ln}^2(n) \tag{17}$$

при

$$n \geq 600. \tag{18}$$

Диофантовость функции **LCM**, входящей в (14), была установлена в § 1.6, но там эта функция рассматривалась как функция двух аргументов. Ограниченный квантор общности позволяет легко преодолеть трудность, обусловленную переменным количеством аргументов у **LCM** в (14). А именно, число m является общим кратным чисел $1,\ldots,n$ тогда и только тогда, когда

$$\forall y_{<n}[(y+1)|m], \tag{19}$$

и наименьшим общим кратным, если, кроме того,

$$m>0 \ \& \ \forall y_{<m}\exists x[x<n \,\&\, (x+1)\nmid m]. \tag{20}$$

Мы не можем ставить вопрос о диофантовости функции **ln**, также входящей в (14), поскольку её значения, вообще говоря, целочисленными не являются. Можно было бы установить диофантовость функции $[\mathbf{ln}(n)]$, где $[\alpha]$ обозначает целую часть числа α, но это потребовало бы использования такого нетривиального факта, как иррациональность основания натуральных логарифмов (это число мы будем обозначать буквой **e**, чтобы не нарушать соглашения об обозначении курсивными латинскими буквами только натуральных чисел).

Вместо функции **ln** мы введём отношение

$$\mathbf{explog}(a,b) \Leftrightarrow \exists x\left[x>b+1 \,\&\, \left(1+\frac{1}{x}\right)^{xb} \leq a+1 < 4\left(1+\frac{1}{x}\right)^{xb}\right] \tag{21}$$

и установим, что, во-первых, для всех a и b

$$\mathbf{explog}(a,b) \Rightarrow |b-\mathbf{ln}(a+1)| < 2, \tag{22}$$

и, во-вторых,

$$\forall a\exists b[\mathbf{explog}(a,b)]. \tag{23}$$

Действительно, как известно из анализа,

$$\mathbf{e} = \lim_{x\to\infty}\left(1+\frac{1}{x}\right)^x = \lim_{x\to\infty}\left(1+\frac{1}{x}\right)^{x+1}, \tag{24}$$

причём при $x>0$

$$\left(1+\frac{1}{x}\right)^x < \mathbf{e} < \left(1+\frac{1}{x}\right)^{x+1}. \tag{25}$$

Возводя в степень b, получаем, что

$$\left(1+\frac{1}{x}\right)^{xb} \le \mathbf{e}^b \le \left(1+\frac{1}{x}\right)^{(x+1)b} \tag{26}$$

и, следовательно,

$$\frac{\mathbf{e}^b}{\mathbf{e}} \le \frac{\left(1+\frac{1}{x}\right)^{(x+1)b}}{\left(1+\frac{1}{x}\right)^{x}} < \left(1+\frac{1}{x}\right)^{xb} \le a+1 < 4\left(1+\frac{1}{x}\right)^{xb} \le 4\mathbf{e}^b, \tag{27}$$

откуда следует справедливость неравенства в (22).

С другой стороны, при любом a можно найти такое b, что

$$b \le \mathbf{ln}(a+1) < b+\mathbf{ln}(3). \tag{28}$$

Выбирая затем x очень большим, мы можем согласно (24) сделать обе величины

$$\left(1+\frac{1}{x}\right)^{x}, \quad \left(1+\frac{1}{x}\right)^{x+1} \tag{29}$$

сколь угодно близкими к $\mathbf{e}$ и обеспечить тем самым выполнение всех неравенств в (21).

Покажем, что *отрицание гипотезы Римана эквивалентно существованию чисел k, l, m и n, удовлетворяющих условиям* (18)–(20) *и*

$$\mathbf{explog}(m-1, l), \tag{30}$$

$$\mathbf{explog}(n-1, k), \tag{31}$$

$$(l-n)^2 > 4n^2k^4. \tag{32}$$

Предположим сначала, что такие числа k, l, m и n нашлись. Тогда согласно (19) и (20)

$$m = \mathbf{e}^{\psi(n)}, \tag{33}$$

и согласно (22) из (31) следует, что

$$|l-\psi(n)| < 2. \tag{34}$$

Аналогично из (32) следует, что

$$|k-\mathbf{ln}(n)| < 2. \tag{35}$$

Отсюда получаем, что

$$|\psi(n)-n| \ge |l-n|-|l-\psi(n)| > 2\mathbf{sqrt}(n)k^2-2 > \mathbf{sqrt}(n)\mathbf{ln}^2(n), \tag{36}$$

что даёт искомое противоречие с (17).

Предположим теперь, что гипотеза Римана не верна. Тогда согласно (16) найдётся n, удовлетворяющее (18) и такое, что

$$|\psi(n)-n| > 10\mathbf{sqrt}(n)\mathbf{ln}^2(n). \tag{37}$$

Выберем m согласно (33), тогда условия (19) и (20) будут выполнены. Далее, найдём согласно (23) числа k и l, удовлетворяющие (30) и (31). Согласно (22) будут выполнены неравенства (34) и (35). Из них получаем, что

$$|l-n| \geq |\psi(n)-n|-|l-\psi(n)| > 10\mathbf{sqrt}(n)\ln^2(n)-2 >$$
$$> 2\mathbf{sqrt}(n)(\ln(n)+2)^2 > 2\mathbf{sqrt}(n)k^2, \qquad (38)$$

т. е. неравенство (32) также выполнено.

Пользуясь тем, что все условия (18)–(20), (30)–(32) диофантовы, мы можем построить диофантово уравнение, неразрешимость которого эквивалентна гипотезе Римана.

Не следует полагать, что все проблемы можно свести к диофантовым уравнениям. Мы можем устранять только ограниченные кванторы, что не даёт непосредственной возможности, например, переформулировать в виде утверждения о разрешимости или неразрешимости конкретного диофантова уравнения гипотезу о бесконечности пар простых чисел-близнецов, также включённую Д. Гильбертом в 8-ю проблему.

§ 6.5. Ещё одно универсальное уравнение

В этом параграфе мы увидим, как с помощью устранения ограниченного квантора общности можно легко построить ещё одно универсальное диофантово уравнение.

Кодировка диофантовых уравнений будет отлична от той, что использовалась в главе 4. Кодировке уравнений, естественно, предшествует нумерация полиномов. Не ограничивая общности, мы будем нумеровать только полиномы с переменными $x_1, x_2, \ldots$ Определим *универсальную последовательность полиномов* следующим образом:

$$\begin{aligned} \mathbf{P}_{4k} &= k, \\ \mathbf{P}_{4k+1} &= \mathbf{P}_i+\mathbf{P}_j, \\ \mathbf{P}_{4k+2} &= \mathbf{P}_i\mathbf{P}_j, \\ \mathbf{P}_{4k+3} &= x_{k+1}, \end{aligned} \qquad (1)$$

где i, j и k связаны соотношением

$$k = \mathbf{Cantor}(i, j) \qquad (2)$$

(это определение корректно, поскольку отображение **Cantor**, введённое в § 3.1, осуществляет взаимно однозначное соответствие между множеством всех натуральных чисел и множеством всех пар натуральных чисел).

Последовательность

$$\mathbf{P}_0, \mathbf{P}_1, \ldots, \tag{3}$$

очевидно, является универсальной в следующем смысле: *каждый полином с натуральными коэффициентами от переменных* $x_1, x_2, \ldots$ *встречается в* (3).

Кортеж натуральных чисел

$$\langle p_0, p_1, \ldots, p_{r-1} \rangle \tag{4}$$

будем называть *реализацией* последовательности (3), если при некотором выборе значений $x_1, x_2, \ldots$

$$p_k = \mathbf{P}_k(x_1, x_2, \ldots) \tag{5}$$

для $k = 0, 1, \ldots, r-1$.

У нас имеются два способа кодировать кортежи произвольной длины — гёделево кодирование, введённое в § 3.2, и позиционное кодирование, введённое в § 3.3. Мы с равным успехом могли бы использовать здесь любое из этих кодирований. Поскольку диофантовость функции **GElem**, определённой в (3.2.15), установить гораздо проще, чем диофантовость функции **Elem**, определённой в (3.3.8), естественнее использовать гёделево кодирование.

Отношение $\mathbf{Real}(p, q, r)$ — *кортеж* $\langle p, q, r \rangle$ *является кодом некоторой реализации* — легко записывается с помощью ограниченного квантора общности:

$$\begin{aligned}
&\mathbf{Real}(p, q, r) \Leftrightarrow \\
&\Leftrightarrow \forall l_{<r} \exists ijk[k = \mathbf{Cantor}(i, j) \ \& \ [[l = 4k \ \& \ \mathbf{GElem}(p, q, l+1) = k] \vee \\
&\vee [l = 4k+1 \ \& \ \mathbf{GElem}(p, q, l+1) = \mathbf{GElem}(p, q, i+1) + \mathbf{GElem}(p, q, j+1)] \vee \\
&\vee [l = 4k+2 \ \& \ \mathbf{GElem}(p, q, l+1) = \mathbf{GElem}(p, q, i+1)\mathbf{GElem}(p, q, j+1)]]].
\end{aligned} \tag{6}$$

Номером уравнения

$$\mathbf{P}_i(a_1, \ldots, a_n, x_{n+1}, \ldots) = \mathbf{P}_j(a_1, \ldots, a_n, x_{n+1}, \ldots) \tag{7}$$

будет число $\mathbf{Cantor}(i, j)$. Очевидно, что уравнение с номером k имеет решение тогда и только тогда, когда параметры $a_1, \ldots, a_n$ удовлетворяют условию

$$\begin{aligned}
&\exists ijpqr[k = \mathbf{Cantor}(i, j) \ \& \ r > i \ \& \ r > j \ \& \\
&\quad \& \ \mathbf{Real}(p, q, r) \ \& \ \mathbf{GElem}(p, q, i+1) = \mathbf{GElem}(p, q, j+1) \ \& \\
&\quad \& \ \mathbf{GElem}(p, q, 5) = a_1 \ \& \ \ldots \ \& \ \mathbf{GElem}(p, q, 4n+1) = a_n].
\end{aligned} \tag{8}$$

Это условие, очевидно, диофантово, и потому может быть преобразовано в искомое универсальное уравнение.

§ 6.6. Ещё одно диофантово множество с недиофантовым дополнением

В § 10.1 нам потребуется факт существования диофантова множества натуральных чисел $\mathfrak{S}$ с недиофантовым дополнением $\overline{\mathfrak{S}}$, которое обладает ещё одним специальным свойством. А именно, недиофантовость $\overline{\mathfrak{S}}$ означает, что для любого диофантова множества $\mathfrak{D}$ справедливо по крайней мере одно из следующих утверждений:

$$\textit{существует } a \textit{ такое, что } a \in \mathfrak{D}, \textit{ но } a \notin \overline{\mathfrak{S}}, \tag{1}$$

$$\textit{существует } a \textit{ такое, что } a \notin \mathfrak{D}, \textit{ но } a \in \overline{\mathfrak{S}}. \tag{2}$$

Множество $\overline{\mathfrak{S}}$, очевидно, должно быть бесконечным, поэтому утверждение (2) будет выполнено для любого конечного $\mathfrak{D}$. Оказывается, что $\mathfrak{S}$ можно определить так, что для любого бесконечного $\mathfrak{D}$ будет выполнено (1). Иными словами, $\mathfrak{S}$ будет содержать по представителю из каждого бесконечного диофантова множества. Диофантово множество $\mathfrak{S}$ такое, что для любого бесконечного диофантова множества $\mathfrak{D}$ выполнено (1), а для любого конечного $\mathfrak{D}$ выполнено (2), называют *простым*.

Для построения простого множества $\mathfrak{S}$ мы возьмём какое-либо универсальное диофантово уравнение

$$U(a, k, x_1, \ldots, x_m) = 0 \tag{3}$$

(у нас теперь есть две техники построения таких уравнений, изложенные в предыдущем параграфе и § 4.5). Определим множество $\mathfrak{S}$ формулой

$$\begin{aligned}&\exists k[\exists x_1 \ldots x_m[2k < a \,\&\, U(a, k, x_1, \ldots, x_m) = 0] \,\&\\ &\&\, \forall y_{<\mathbf{Cantor}_{m+1}(a, x_1, \ldots, x_m)} \exists z_0 \ldots z_m[y = \mathbf{Cantor}_{m+1}(z_0, \ldots, z_m) \,\&\\ &\&\, [2k \geq z_0 \vee U(z_0, k, z_1, \ldots, z_m) \neq 0]]].\end{aligned} \tag{4}$$

Проверим выполнение условий (1) и (2). Пусть $\mathfrak{D}$ — бесконечное диофантово множество, тогда найдётся такое число k, что это множество задаётся уравнением

$$U(a, k, x_1, \ldots, x_m) = 0. \tag{5}$$

Ввиду бесконечности $\mathfrak{D}$ найдутся числа a, $x_1, \ldots, x_m$, удовлетворяющие (5) и дополнительному неравенству

$$2k < a. \tag{6}$$

Из всех таких $(m+1)$-членных кортежей выберем один с наименьшим канторовым номером. Нетрудно видеть, что первый элемент этого кортежа годится на роль a в (1).

Пусть теперь $\mathfrak{D}$ — конечное множество, имеющее l элементов $d_1,\ldots,d_l$. Предположим, что (2) не выполнено, т. е. любое a, отличное от $d_1,\ldots,d_l$, принадлежит $\mathfrak{S}$. Для каждого a из $\mathfrak{S}$ будем обозначать посредством k_a то число, существование которого утверждается в (4). В частности, среди чисел $0,1,\ldots,2l$ имеется $l+1$ чисел $a_0,\ldots,a_l$, входящих в $\mathfrak{S}$, и должны существовать $l+1$ соответствующих чисел $k_{a_0},\ldots,k_{a_l}$. Нетрудно увидеть, что эти числа должны быть попарно различными и удовлетворять неравенствам

$$k_{a_i} < a_i/2 < l, \tag{7}$$

что невозможно. Полученное противоречие доказывает (2).

Упражнения

6.1. Покажите, что ограниченный квантор общности можно устранять, выбирая модули согласно (3.2.7) вместо (2.12).

6.2. Покажите, что имеет место следующая *мультипликативная форма принципа Дирихле*: если $q|s_1\ldots s_n$, то найдутся такие числа r и k, что $r|q$, $1\le k\le n$, $r|s_k$ и $r^n\ge q$.

6.3. Обобщите предыдущее упражнение следующим образом: если $t\ne 0$ и

$$q|ts_{1,1}\ldots s_{1,n_1},\ \ldots\ldots,\ q|ts_{m,1}\ldots s_{m,n_m},$$

то найдутся числа r и $k_1,\ldots,k_m$ такие, что

$$r|q,\ 1\le k_i\le n_i,\ r|s_{i,k_i}\ \text{и}\ tr^{n_1\ldots n_m}\ge q.$$

6.4. Покажите с помощью предыдущего упражнения, что условие (2.24) можно заменить на достаточно сильное неравенство вида $q>\ldots$, устраняя тем самым необходимость установления диофантовости факториала.

6.5. Помимо (2.13) и произведения из упражнения 3.3, есть и другие случаи, когда удаётся дать прямое доказательство диофантовости произведения с переменным верхним пределом. Проверьте, что

$$\alpha_b(2n)=(\alpha_b(n+1)-\alpha_b(n-1))\alpha_b(n)$$

и соответственно

$$\prod_{k=1}^{m}(\alpha_b(2^k+1)-\alpha_b(2^k-1))=\alpha_b(2^{m+1}),$$

и используйте затем последнее тождество вместо (2.13) для устранения ограниченного квантора общности.

6.6. Покажите, что знаменитая проблема четырёх красок также может быть переформулирована как утверждение о неразрешимости конкретного диофантова уравнения.

6.7. Установите недиофантовость множества номеров диофантовых уравнений без параметров, не имеющих решений.

6.8. Свойство $\mathcal{R}(a_1,\ldots,a_n)$ называется *полиномиальным*, если оно имеет диофантово представление без неизвестных, т. е.

$$\mathcal{R}(a_1,\ldots,a_n) \iff R(a_1,\ldots,a_n)=0,$$

где R — полином с целыми коэффициентами. Покажите, что если $\mathcal{R}$ — полиномиальное отношение, то полиномиальным является и отношение, задаваемое формулой (6.1.1).

Комментарии

Как было сказано в комментариях к главе 5, устранение ограниченного квантора общности было одним из основных шагов в решении 10-й проблемы Гильберта. Впервые соответствующая техника была предложена в работе Девиса, Патнама и Робинсон [1961]. В § 6.2 мы следовали этой работе с небольшими упрощениями. Более существенные модификации предлагались в работах Матиясевича [1972а, 1973] (см. упражнение 6.4) и работе Хиросе и Ииды [1973] (см. упражнение 6.5).

Устранение ограниченного квантора общности методом, изложенным в § 6.1, стало возможным после нахождения прямого способа моделирования машины Тьюринга диофантовыми уравнениями в работе Матиясевича [1976].

Третья конструкция, приведенная в § 6.3, излагается здесь впервые. Она является развитием техники, первоначально предложенной в работе Матиясевича [1979] для уменьшения количества неизвестных в экспоненциально диофантовых уравнениях (см. § 8.2). Новым шагом по сравнению с этой работой является сворачивание системы делимостей (3.33) в одну делимость (3.35).

Возможность переформулировать многие проблемы на арифметическом языке была продемонстрирована ещё К. Гёделем [1931], и с появлением возможности устранять ограниченный квантор общности перевод таких проблем на язык диофантовых уравнений стал тривиальным. Исключение, пожалуй, составляет гипотеза Римана, имеющая дело с континуумом комплексных чисел. А. М. Тьюринг [1939] показал, что эта гипотеза эквивалентна некоторому утверждению вида

$$\forall y \exists x \mathcal{T}(x,y), \tag{1}$$

где $\mathcal{T}$ — разрешимое отношение между натуральными x и y. Этого, однако, недостаточно для сведения отрицания гипотезы Римана к неразрешимости конкретного диофантова уравнения, ибо кванторы в (1) не ограничены. Из работы Крайзеля [1958], содержащей весьма общие результаты по арифметизации утверждений, связанных с аналитическими функциями, следует, в частности, усиление результата Тьюринга — гипотеза Римана может быть сформулирована в виде

$$\forall y \mathcal{K}(y), \tag{2}$$

где $\mathcal{K}$ — разрешимое свойство. Отрицание $\mathcal{K}$ полуразрешимо и потому диофантово:

$$\neg \mathcal{K}(y) \iff \exists x_1 \ldots x_m [\mathbf{K}(y,x_1,\ldots,x_m)=0]; \tag{3}$$

следовательно, гипотеза Римана эквивалентна неразрешимости уравнения

$$K(x_0,\ldots,x_m)=0. \tag{4}$$

Конструкция Г. Крайзеля является весьма общей и потому приводит к чрезвычайно громоздкому уравнению. Более прямой путь, основанный на связи гипотезы Римана с распределением простых чисел, был описан в обзоре Девиса, Матиясевича и Робинсон [1976]. Изложенный в § 6.4 вариант включает дальнейшее упрощение, которое предложили автору А. Шинцель и М. Ютила. Это упрощение связано с переходом от использования интеграла

$$\psi_1(n) = \int_1^n \psi(\alpha)d\alpha \tag{5}$$

к использованию подинтегральной функции ψ. Использование функции ψ_1 в обзоре Девиса, Матиясевича и Робинсон [1975] было связано с необходимостью иметь конкретное значение константы в символе O. Сейчас благодаря работе Шёнфилда [1976] мы имеем такую константу в (6.4.21) и для функции ψ.

Поскольку в главе 5 мы установили неразрешимость 10-й проблемы Гильберта, сведение различных проблем к диофантовым уравнениям оставляет мало надежды на то, что эти проблемы будут решены путём анализа соответствующих уравнений. Более плодотворным может оказаться обратный взгляд на такие сведения — решение, например, проблемы четырёх красок может быть изложено как очень нетривиальный метод установления неразрешимомсти соответствующего диофантова уравнения (см. упражнение 6.6).

Использованная в § 6.5 нумерация полиномов, основанная на их построении из простейших полиномов с помощью сложения и умножения, была приведена в работе Дж. Робинсон [1969б], а в её работе [1971] применена для построения универсального уравнения.

Понятие простого множества было введено Э. Л. Постом; он же [1944] построил пример простого множества (естественно, что вместо диофантовости Э. Л. Пост говорил о полуразрешимости).

Глава 7
МАССОВЫЕ ПРОБЛЕМЫ ТЕОРИИ ЧИСЕЛ

Благодаря чрезвычайной простоте полиномов с целыми коэффициентами как математических объектов, 10-я проблема Гильберта оказалась весьма удобным средством для установления алгоритмической неразрешимости других массовых проблем. В этой главе мы рассмотрим некоторые такие проблемы, относящиеся к теории чисел.

§ 7.1. Количество решений у диофантовых уравнений

С каждым диофантовым уравнением

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

связана величина **Card**(D) — количество решений этого уравнения. Значения **Card** принадлежат множеству $\mathfrak{N}=\{0,1,\ldots,\infty\}$. Для каждого множества $\mathfrak{A}$ такого, что $\mathfrak{A}\subseteq\mathfrak{N}$, можно рассмотреть множество $\mathbf{Card}^{-1}(\mathfrak{A})$ — полный прообраз $\mathfrak{A}$. Допуская некоторую вольность языка, мы будем рассматривать $\mathbf{Card}^{-1}(\mathfrak{A})$ и как множество уравнений, и как множество натуральных чисел — кодов этих уравнений.

Множество

$$\mathbf{Card}^{-1}(\{1,2,\ldots,\infty\}) \tag{2}$$

уже рассматривалось нами в § 4.6 — это множество диофантовых уравнений, имеющих решения, и 10-я проблема Гильберта — это в точности вопрос о способе распознавания элементов множества (2) среди всех уравнений. В главе 5 было установлено, что множество (2) неразрешимо (в интуитивном смысле). Точная формулировка этого утверждения состоит в том, что множество (2), рассматриваемое как множество кодов, неразрешимо по Тьюрингу. Согласно § 5.6 это эквивалентно утверждению о том, что либо само множество (2), либо его дополнение не диофантово, и действительно, в § 4.6 была установлена диофантовость множества (2) и недиофантовость его дополнения, т. е. множества $\mathbf{Card}^{-1}(\{0\})$.

В этом параграфе мы обобщим этот результат, показав, что *если* $\mathbf{Card}^{-1}(\mathfrak{A})$ *диофантово, то либо* $\mathfrak{A}$ *пусто, либо* $\infty\in\mathfrak{A}$. В частности, полуразрешимыми не являются ни множество $\mathbf{Card}^{-1}(\{1\})$ — множество уравнений, имеющих ровно одно решение, ни множество $\mathbf{Card}^{-1}(\{0,1,\ldots\})$ — множество уравнений, имеющих конечное число решений.

Поскольку

$$\overline{\mathbf{Card}^{-1}(\mathfrak{A})}=\mathbf{Card}^{-1}(\overline{\mathfrak{A}}), \tag{3}$$

где черта сверху обозначает дополнение, то, *кроме двух крайних случаев* $\mathfrak{A}=\varnothing$ *и* $\mathfrak{A}=\mathfrak{N}$, *множество* $\mathbf{Card}^{-1}(\mathfrak{A})$ *неразрешимо*, ибо либо оно, либо его дополнение не содержит ∞ и, следовательно, не полуразрешимо. Это утверждение можно перефразировать так: если на какой-то вопрос о количестве решений у диофантова уравнения может быть дан, в зависимости от уравнения, как утвердительный, так и отрицательный ответ, то этот ответ для произвольного уравнения не может быть получен алгоритмически.

Мы ограничимся полуформальным доказательством, использующим тезис Чёрча, т. е. будем говорить о полуразрешимоси в интуитивном смысле. Доказательство проведём методом от противного, т. е. предположим, что для некоторого непустого $\mathfrak{A}$, не содержащего ∞, множество $\mathbf{Card}^{-1}(\mathfrak{A})$ полуразрешимо. Покажем, что в этом случае полуразрешимым было бы и множество $\mathbf{Card}^{-1}(\{0\})$.

Пусть имеется произвольное уравнение (1). Выберем и зафиксируем какой-то элемент a множества $\mathfrak{A}$ и рассмотрим уравнение

$$((x_1+x_2+1-a)^2+x_3^2+\ldots+x_{m+1}^2)D(x_1,\ldots,x_m)=0. \tag{4}$$

Легко видеть, что если уравнение (1) решений не имеет, то уравнение (4) имеет ровно a решений

$$\begin{aligned}
&x_1=0,\ x_2=a-1,\ x_3=\ldots=x_{m+1}=0;\\
&x_1=1,\ x_2=a-2,\ x_3=\ldots=x_{m+1}=0;\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&x_1=a-1,\ x_2=0,\ x_3=\ldots=x_{m+1}=0.
\end{aligned} \tag{5}$$

С другой стороны, если уравнение (1) имеет хотя бы одно решение, то уравнение (4) имеет бесконечно много решений ввиду произвола в выборе x_{m+1}. Таким образом, уравнение (1) принадлежит $\mathbf{Card}^{-1}(\{0\})$ тогда и только тогда, когда уравнение (4) принадлежит $\mathbf{Card}^{-1}(\mathfrak{A})$. Следовательно, гипотетический метод для полуразрешения $\mathbf{Card}^{-1}(\mathfrak{A})$ позволял бы полуразрешать и $\mathbf{Card}^{-1}(\{0\})$, что, как отмечено выше, невозможно и тем самым даёт искомое противоречие.

§ 7.2. Неэффективизируемые оценки в теории экспоненциально диофантовых уравнений

В главе 2 была установлена диофантовость возведения в степень, что дало нам метод преобразования экспоненциально диофантовых уравнений в эквивалентные по разрешимости диофантовы. Казалось бы, что все результаты об экспоненциально диофантовых уравнениях должны переноситься на диофантовы. Это, однако, не совсем так. В этом параграфе будет изложен один результат об экспоненциально диофантовых уравнениях, который в настоящее время не удаётся усилить до аналогичного результата о диофантовых уравнениях.

В теории чисел имеется много теорем о том, что диофантовы уравнения того или иного специального вида имеют конечное число решений. Классическим примером может служить теорема Туэ [1909] о том, что уравнение

$$F(x,y)=a, \tag{1}$$

где F — неприводимая бинарная форма не менее чем третьей степени, имеет при каждом значении параметра a конечное число решений. Таким образом, для каждого значения a имеется число b такое, что любое решение уравнения (1) удовлетворяет неравенствам $x<b$, $y<b$. Однако доказательство Туэ проводилось методом от противного, и никакого значения b извлечь из этого доказательства не удаётся. В такой ситуации говорят, что мы имеем *неэффективную* оценку величины решений.

После того как для некоторого класса уравнений получена неэффективная оценка величины решений, естественно возникает задача эффективизации, т. е. нахождения эффективно вычислимой функции от значений параметров уравнения, ограничивающей сверху максимально возможное значение неизвестных. Установление эффективной оценки даёт возможность находить, по крайней мере в принципе, и все решения уравнения (или устанавливать их отсутствие) путём полного перебора всех сочетаний значений неизвестных, не превосходящих этой оценки. В случае теоремы Туэ такая эффективизация была достигнута А. Бейкером [1968] только более полувека спустя, и это потребовало привлечения радикально новых идей. Для многих других классов диофантовых уравнений в настоящее время имеются только неэффективные оценки.

Цель настоящего параграфа — показать, что на пути эффективизации могут лежать принципиальные алгоритмические препятствия. В настоящее время это удаётся сделать только для оценок решений экспоненциально диофантовых уравнений. А именно, мы покажем, что *можно построить экспоненциально дио-*

фантово уравнение

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

которое при любом значении параметра a имеет не более одного решения, но это единственное решение не может быть оценено сверху никакой функцией, эффективно вычислимой при любом значении параметра a.

Для того чтобы придать этому результату строгую формулировку, мы должны были бы дать формальное определение эффективно вычислимой функции. Это можно было бы сделать на основе понятия машины Тьюринга (см. упражнение 5.5), но мы ограничимся здесь ссылкой на тезис Чёрча, воспользовавшись указанной выше связью между наличием эффективной оценки решений и возможностью установить существование или отсутствие решений. А именно, нетрудно понять, что в качестве экспоненциально диофантова уравнения (2) можно взять любое уравнение, определяющее неразрешимое множество и имеющее при каждом значении параметра a не более одного решения.

Это приводит к следующему понятию: говорят, что множество $\mathfrak{M}$ n-ок натуральных чисел имеет *однократное* представление

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \iff \exists x_1 \ldots x_m [E(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0], \tag{3}$$

если входящее сюда уравнение имеет для каждого набора значений параметров не более одного решения. В зависимости от вида уравнения говорят об однократном диофантовом или экспоненциально диофантовом представлении. Аналогично можно говорить об однократности или неоднократности представления свойства, отношения или функции.

Основной результат настоящего параграфа состоит в том, что *любое диофантово множество имеет однократное экспоненциально диофантово представление.* Усилить этот результат до однократного диофантова представления в настоящее время не удаётся из-за того, что техника главы 2 даёт бесконечнократное диофантово представление возведения в степень.

Итак, пусть имеется некоторое диофантово множество $\mathfrak{M}$. Ниже будут описаны три способа для нахождения его однократного экспоненциально диофантова представления.

Первый способ использует технику главы 5. По диофантову представлению множества $\mathfrak{M}$ мы можем, следуя § 5.4, найти машину Тьюринга M, полуразрешающую $\mathfrak{M}$, а затем, используя технику § 5.5, построить по этой машине экспоненциально диофантово представление $\mathfrak{M}$. Машина M в поисках решения диофантова уравнения, определяющего $\mathfrak{M}$, перебирает потенциальные решения в порядке их канторовых номеров и останавливается, как только найдёт решение с наименьшим номером. Образно выражаясь, машина «не видит» другие возможные решения исходного диофан-

това́ уравнения с бо́льшими номерами. Слегка модифицировав технику § 5.5, мы получим экспоненциально диофантово уравнение, единственное решение которого соответствует наименьшему решению исходного диофантова уравнения.

Модификацию техники моделирования машины Тьюринга с помощью экспоненциально диофантовых уравнений мы должны начать с главы 1.

Если (1.4.3) и (1.4.4) — однократные представления двух множеств, то (1.4.6) — однократное представление их пересечения, так что мы можем свободно использовать конъюнкцию при построении обобщённых однократных представлений. С другой стороны, (1.4.5), очевидно, может не быть однократным представлением объединения, и, следовательно, мы должны избегать использования дизъюнкции, если хотим получить однократное представление.

Представления (1.5.1), (1.6.1) и (1.6.2), очевидно, являются однократными, так что отношения $\neq$, $\leq$ и $<$ остаются в нашем арсенале. Представление (1.6.3) не является однократным, ибо так введённое отношение делимости истинно при $a=b=0$, причём в этом случае x можно выбирать произвольно. По этой причине мы либо должны следить за тем, чтобы хотя бы один аргумент у отношения $|$ всегда был гарантированно отличен от нуля, либо заменить (1.6.3) на обобщённое однократное представление

$$a|b \Leftrightarrow \exists x[ax=b \,\&\, x\leq b]. \tag{4}$$

В любом случае мы можем рассматривать (1.6.4) как обобщённое однократное представление функции **rem**. В свою очередь, это обеспечивает однократность представлений (1.6.7)–(1.6.9), так что мы можем свободно пользоваться отношением $\upharpoonright$, функцией **div** и сравнениями.

Главу 2 нам пересматривать не надо, поскольку нас интересуют экспоненциально диофантовы представления.

В главе 3 нам достаточно рассмотреть только то, что связано с позиционным кодированием.

Формула (3.3.7), очевидно, является однократным экспоненциально диофантовым представлением отношения **Code**. Нетрудно также убедиться в однократности представления (3.3.8) функции **Elem**.

Эквивалентность (3.3.9) не является представлением девятиместного отношения **Concat**, поскольку в левой части совпадают второй, пятый и восьмой аргументы. Представление же (3.5.15) этого отношения однократным явно не является. Нам, однако, и не требуется однократное представление для **Concat** как девятиместного отношения, ибо в § 5.5 мы работаем с кодами с фиксированным основанием и нам достаточно опера-

ции +, определённой на таких кодах; формула (3.3.9) оправдывает использование этой операции при построении однократных экспоненциально диофантовых представлений.

Формулы (3.4.2) и (3.4.6), очевидно, являются однократными представлениями биномиальных коэффициентов и факториала. Нетрудно было бы модифицировать представление (1.6.10) для наибольшего общего делителя так, чтобы оно стало однократным, делая тем самым однократным и представление (3.4.7) для простых чисел. Мы, однако, выберем несколько более простой путь. Диофантовость простых чисел нам требовалась для того, чтобы, используя теорему Куммера, получить диофантовы представления (3.5.6) для **PNotGreater** и (3.5.8) для **PSmall**, а затем (3.5.12) для **Eq**, (3.5.4) для **Equal**, (3.5.13) для **NotGreater** и (3.5.14) для **Small**. В главе 5 мы работаем с фиксированным основанием, от которого требуется только, чтобы оно было больше количества состояний машины Тьюринга и количества символов на ленте, и теперь мы дополнительно потребуем, чтобы это основание было простым числом. Соответственно нам достаточно указать однократное экспоненциально диофантово представление

$$\mathbf{PNotGreater}_p(a_1,a_2) \Leftrightarrow p \nmid \binom{a_2}{a_1} \tag{5}$$

для двухместного отношения $\mathbf{PNotGreater}_p$, получающегося из трёхместного отношения **PNotGreater** фиксированием третьего аргумента равным простому числу p. Аналогом (3.5.8) становится однократное представление

$$\mathbf{PSmall}_p(a,c,e) \Leftrightarrow \quad e<p \ \& \ \mathbf{PNotGreater}_p(a,e(p^c-1)/(p-1),c). \tag{6}$$

Этого достаточно для получения следующего однократного аналога представления (3.6.8):

$$\mathbf{Ort}_p(q_1,q_2,r) \Leftrightarrow$$
$$\Leftrightarrow \mathbf{PSmall}_p(q_1,r,1) \ \& \ \mathbf{PSmall}_p(q_2,r,1) \ \& \ \mathbf{Small}_p(q_1+q_2,r,1). \tag{7}$$

Как было отмечено в § 3.6, условия (3.6.5)–(3.6.7) однозначно определяют числа $h_0,\ldots,h_{b-1}$, так что получающееся в результате экспоненциально диофантово представление функции $F[b]$ при простом b будет однократным.

В представлении (5.5.8) функции NextT в качестве значения z можно брать любое число, не меньшее длины кортежей с шифрами p и t. Для получения однократного представления можно, например, положить $z=p+t$:

$$t' = \mathrm{NextT} \Leftrightarrow t' = \mathrm{A}[b](p,t,p+t). \tag{8}$$

То же самое можно сделать для преобразования представления (5.5.16) функции NextP в однократное.

Как проверено в § 5.5, при фиксированных значениях k, l, p и t числа p_L, t_L, p_M, t_M, p_R, t_R, p', t' определяются однозначно. Число l определяется по k, p и t неоднозначно — в качестве значения l можно брать любое число, удовлетворяющее неравенствам (5.5.22). Для получения однократности мы можем заменить (5.5.22), скажем, на равенство

$$l = k+p+t+3. \tag{9}$$

Число k однозначно определяется по p и t количеством шагов машины Тьюринга до остановки. Число r, удовлетворяющее (5.5.36), также определяется однозначно — положением головки в момент остановки. Тем не менее мы не можем использовать условие (5.5.36) в таком виде, ибо оно содержит дизъюнкцию. Нетрудно, однако, проверить, что машина (5.4.10) может остановиться только в состоянии q_2, и потому роль (5.5.36) может играть условие

$$\exists kr[\mathbf{Elem}(\mathrm{AfterT}(k,p,t),b,r)=2]. \tag{10}$$

Наконец, условия (5.5.37) и (5.5.38) однозначно определяют начальную конфигурацию $\langle p,t\rangle$ по значению параметров $a_1,\ldots,a_n$.

Второй способ построения однократных представлений состоит в модификации техники § 6.2. Не ограничивая общности, мы можем считать, что $\mathfrak{M}$ одномерно и имеет диофантово представление

$$a\in\mathfrak{M} \iff \exists x_2\ldots x_m[M(a,x_2,\ldots,x_m)=0]. \tag{11}$$

Используя ограниченный квантор общности, мы легко можем записать условие *числа $a_2,\ldots,a_m$ образуют решение диофантова уравнения $M(a,x_2,\ldots,x_m)=0$ с наименьшим канторовым номером*, а именно

$$\begin{aligned} M(a,a_2,\ldots,a_m)=0 \,\&\, \exists b[b=\mathbf{Cantor}_{m-1}(a_2,\ldots,a_m)\,\& \\ \&\, \forall y_{<b}\exists x_1,\ldots,x_m[y=\mathbf{Cantor}_{m-1}(x_2,\ldots,x_m)\,\& \\ \&\, M^2(a,x_2,\ldots,x_m)=x_1+1]]. \end{aligned} \tag{12}$$

Для получения однократного экспоненциально диофантова представления множества $\mathfrak{M}$ остаётся модифицировать технику § 6.2 так, чтобы все неизвестные, возникающие при устранении ограниченного квантора общности из (12), однозначно определялись по a и b.

На выбор значения неизвестной w налагалось лишь одно ограничение — выполнение неравенств (6.2.20). Легко убедиться, что функции **Cantor** и $\mathbf{Cantor}_{m-1}$ не убывают ни по одному из своих аргументов, и потому для $x_2,\ldots,x_m$ из (12) справедливо неравенство

$$x_i\le y<b. \tag{13}$$

Это позволяет получить оценку и величины x_1:

$$x_1 < C^2(a,b), \tag{14}$$

где $C(a,b)$ — полином, который получается из $D(a,x_2,\ldots,x_m)$ изменением знака у всех отрицательных коэффициентов и последующей подстановкой переменной b вместо $x_2,\ldots,x_n$. Таким образом, устраняя ограниченный квантор общности из (12), мы можем наложить на w дополнительное требование

$$w = b + C^2(a,b), \tag{15}$$

однозначно определяющее w по a и b.

На выбор значения неизвестной q налагалось также только одно ограничение — делимость (6.2.24). Заменив в этом условии знак делимости на знак равенства, мы обеспечим однозначный выбор q и, согласно (6.2.15), также и однозначный выбор z_0.

На выбор значений $z_1,\ldots,z_m$ накладывалось одно ограничение — при $0 \le y < b$ числа $x_{1,y},\ldots,x_{m,y}$, определяемые (6.2.6), должны давать решение исходного уравнения (6.2.4). Поэтому по китайской теореме об остатках (см. Приложение 2) на $z_1,\ldots,z_m$ можно наложить дополнительное ограничение

$$z_i < \binom{q}{b}, \tag{16}$$

поскольку, согласно (6.2.13), правая часть в (16) есть произведение $q_0 \ldots q_{w-1}$. Проверим, что это условие делает выбор $z_1,\ldots,z_m$ однозначным.

Пусть p — простое число и

$$p^k \mid \binom{q}{b}. \tag{17}$$

Поскольку все сомножители в левой части (6.2.13) попарно взаимно просты, найдётся ровно одно значение y, такое, что $0 \le y < b$ и $p \mid q_y$, и потому

$$p^k \mid q_y. \tag{18}$$

Условие (18) является аналогом условия (6.2.18). Аналогом делимости (6.2.27) будет

$$p^k \mid \prod_{x=0}^{w-1} (z_i - x). \tag{19}$$

Общий делитель любых двух разных сомножителей в произведении в (19) не больше абсолютной величины их разности и, следовательно, меньше w; с другой стороны, благодаря (6.2.24), $p > w$. Таким образом в произведении в (19) только один сомножитель может делиться на p, и потому он должен делиться и на p^k.

Определим числа $x_{1,y},\ldots,x_{m,y}$ условием

$$p^k \mid z_i - x_{i,y} \tag{20}$$

и неравенствами (6.2.20). Это условие является аналогом условия (6.2.28); очевидно, что имеет место и следующий аналог (6.2.29):

$$p^k \mid z_0 - y. \tag{21}$$

Так же, как в § 6.2, отсюда можно получить, что $x_{1,y},\ldots,x_{m,y}$ образуют решение исходного уравнения (6.2.4), т. е. в нашем случае

$$y = \mathbf{Cantor}_{m-1}(x_{2,y},\ldots,x_{m,y}), \tag{22}$$

$$M^2(a, x_{2,y},\ldots,x_{m,y}) = x_{1,y} + 1. \tag{23}$$

Мы видим, что значения $x_{1,y},\ldots,x_{m,y}$ однозначно определяются по y, а следовательно, и по p; иными словами, в любом решении остаток $\mathbf{rem}(z_i, p^k)$ имеет одно и то же значение. Поскольку на p и k было наложено только условие (17), то однозначно определён и остаток

$$\mathbf{rem}\left(z_i, \binom{q}{b}\right), \tag{24}$$

который, согласно (16), равен z_i.

Таким образом, значения всех неизвестных q, w, $z_1,\ldots,z_m$ однозначно определяются значениями параметров a и b. Однократность биномиальных коэффициентов и факториала была уже проверена. Нам остаётся в преобразованной формуле (12) объявить $a_2,\ldots,a_m$ неизвестными, что мы можем сделать, ибо их значения и тем самым и значение b, очевидно, однозначно определяются по a.

Третий способ построения однократных представлений состоит в модификации техники § 6.3. Преобразуем диофантово представление (11) в представление

$$\forall y_{<1} \exists x_1 \ldots x_m [D(a, y, x_1, \ldots, x_m) = 0], \tag{25}$$

где

$$D(a, y, x_1, \ldots, x_m) = M^2(a, x_2, \ldots, x_m) + (x_1 - 1)^2. \tag{26}$$

Роль второго слагаемого в (26) прояснится позднее; квантор общности по y, конечно, является фиктивным — y может равняться только нулю. Квантор общности добавлен только для того, чтобы мы могли воспользоваться обозначениями, введёнными в § 6.3, — представление (25) является формальным аналогом представления (6.3.2) с $b = 1$.

В § 6.3 показано, что формула (6.3.42) эквивалентна формуле (6.3.35), соответственно в нашем случае формула

$$\exists x_{1_{<w+1}} \ldots \exists x_{m_{<w+1}} [D(a,0,x_1,\ldots,x_m)=0] \tag{27}$$

эквивалентна формуле

$$2^{l(w)} | S(w), \tag{28}$$

где $l(w)$ и $S(w)$ определяются формулами (6.3.3), (6.3.15), (6.3.16), (6.3.17), (6.3.23), (6.3.24), (6.3.30), (6.3.34) и (6.3.36) при $b=1$, $y=0$.

Благодаря слагаемому $(x_1-1)^2$ в (26), утверждения (27) и (28) ложны при $w=0$. Таким образом, если уравнение в (11) имеет решение, то существует число u такое, что при $w \le u$ формулы (27) и (28) ложны, а при $w > u$ — истинны. Такое число u, очевидно, единственно, а формула (11) эквивалентна формуле

$$\exists u [2^{l(u)} \nmid S(u) \,\&\, 2^{l(u+1)} | S(u+1)]. \tag{29}$$

В § 6.3 было проверено, что l и S — диофантовы функции. Более того, $l(w)$ имеет явное выражение, определяемое (6.3.30), (6.3.15) и (6.3.16), так что экспоненциально диофантово представление для l вообще не имеет неизвестных и потому однократно. Далее, согласно (6.3.36), (6.3.34) и (6.3.23)

$$S(w) = C(w) = \binom{2K(w)}{K(w)}. \tag{30}$$

Однократность отношений делимости и неделимости и биномиальных коэффициентов была проверена выше, а $K(w)$ имеет явное выражение (6.3.49). Таким образом, (29) можно рассматривать как обобщённое однократное экспоненциально диофантово представление множества $\mathfrak{M}$.

§ 7.3. Аналог 10-й проблемы Гильберта для гауссовых чисел

В этом параграфе мы будем рассматривать решения уравнений в кольце $\mathbb{G}$ *гауссовых чисел*, т. е. чисел вида $p+q\mathbf{i}$, где p и q — целые числа, а $\mathbf{i}$ — мнимая единица. По этой причине в этом параграфе не будет действовать принятое в § 1.3 соглашение о том, что строчные курсивные латинские буквы обозначают натуральные числа. Под $\mathbf{sqrt}(z)$ мы будем понимать значение квадратного корня с неотрицательной вещественной частью.

Итак, пусть имеется уравнение

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

где D — полином с гауссовыми коэффициентами, и мы интересуемся разрешимостью этого уравнения в гауссовых $x_1,\ldots,x_m$.

Ясно, что уравнение (1) имеет решение тогда и только тогда, когда уравнение

$$D(p_1+q_1\mathbf{i},\ldots,p_m+q_m\mathbf{i})=0 \tag{2}$$

имеет решение в вещественных целых $p_1,\ldots,p_m$, $q_1,\ldots,q_m$. Уравнение (2), вообще говоря, имеет гауссовы коэффициенты, но мы можем легко разделить вещественную и мнимую часть, а именно, пусть

$$D(p_1+q_1\mathbf{i},\ldots,p_m+q_m\mathbf{i})=$$
$$=D_{\mathrm{R}}(p_1,\ldots,p_m,q_1,\ldots,q_m)+D_{\mathrm{I}}(p_1,\ldots,p_m,q_1,\ldots,q_m)\mathbf{i}, \tag{3}$$

где D_{R} и D_{I} — полиномы с вещественными целыми коэффициентами. В итоге мы сводим вопрос о разрешимости (1) в гауссовых числах к вопросу о разрешимости в вещественных целых числах уравнения

$$D_{\mathrm{R}}^2(p_1,\ldots,p_m,q_1,\ldots,q_m)+D_{\mathrm{I}}^2(p_1,\ldots,p_m,q_1,\ldots,q_m)=0, \tag{4}$$

все коэффициенты которого — вещественные целые числа.

Таким образом, положительное решение 10-й проблемы Гильберта давало бы нам способ распознавать и разрешимость диофантовых уравнений в гауссовых числах. Цель настоящего параграфа — показать, что из отрицательного решения 10-й проблемы Гильберта следует *отрицательное решение её аналога для гауссовых чисел.*

Для этого мы установим *диофантовость множества натуральных чисел в кольце гауссовых чисел.* Это понятие диофантовости нуждается в некотором уточнении. Мы сделаем это в общей постановке.

Пусть R — произвольное кольцо, являющееся расширением кольца целых чисел $\mathbb{Z}$, C — подкольцо R, A и X — подмножества R,

$$D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0, \tag{5}$$

— полиномиальное уравнение, коэффициенты которого принадлежат C, а переменные разбиты на параметры $a_1,\ldots,a_n$ и неизвестные $x_1,\ldots,x_m$. Такое уравнение определяет некоторое множество n-ок, а именно, множество

$$\{\langle a_1,\ldots,a_n\rangle \mid a_1,\ldots,a_n\in A\ \&\ \exists x_1\ldots x_m[x_1,\ldots,x_m\in X\ \&$$
$$\&\ D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0]\}. \tag{6}$$

Такие множества мы будем называть (A,C,X)-*диофантовыми.* В этих обозначениях диофантовость, которую мы изучали в предыдущих главах, — это $(\mathbb{N},\mathbb{Z},\mathbb{N})$-диофантовость, совпадающая, как следует из § 1.3, с $(\mathbb{N},\mathbb{Z},\mathbb{Z})$-диофантовостью, где $\mathbb{N}$ — множество натуральных чисел.

Ниже мы установим $(\mathbb{G},\mathbb{Z},\mathbb{G})$-*диофантовость множества* $\mathbb{Z}$, т. е. найдём диофантово уравнение

$$Z(a,u_1,\ldots,u_l)=0, \tag{7}$$

разрешимое в гауссовых $u_1,\ldots,u_l$, если a — вещественное целое число, и неразрешимое при других гауссовых значениях a. Подобно переходу от (1.3.2) к (1.3.3), это позволит сводить вопрос о разрешимости произвольного диофантова уравнения

$$D(y_1,\ldots,y_m)=0 \tag{8}$$

в вещественных целых $y_1,\ldots,y_m$ к разрешимости системы

$$\begin{gathered} D(y_1,\ldots,y_m)=0, \\ Z(y_1,u_{1,1},\ldots,u_{1,l})=0, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ Z(y_m,u_{m,1},\ldots,u_{m,l})=0 \end{gathered} \tag{9}$$

в гауссовых $y_1,\ldots,y_m$, $u_{1,1},\ldots,u_{m,l}$. Мы, однако, не можем повторить переход от (1.1.1) к (1.1.2) для свёртывания системы (9) в одно уравнение и должны пользоваться более глубоким алгебраическим фактом, а именно, иррациональностью **sqrt(2)**, чтобы преобразовывать систему из двух уравнений

$$\begin{gathered} D_1(x_1,\ldots,x_k)=0, \\ D_2(x_1,\ldots,x_k)=0 \end{gathered} \tag{10}$$

в гауссовых $x_1,\ldots,x_k$ в одно эквивалентное уравнение

$$D_1^2(x_1,\ldots,x_k)+2D_2^2(x_1,\ldots,x_k)=0. \tag{11}$$

Применяя эту процедуру систематически, мы сможем преобразовать систему (9) в искомое уравнение, разрешимость которого в гауссовых числах эквивалентна разрешимости исходного уравнения (8) в вещественных целых числах.

Наше доказательство $(\mathbb{G},\mathbb{Z},\mathbb{G})$-диофантовости $\mathbb{Z}$ будет снова использовать последовательности $\alpha_b(n)$, введённые в (2.1.4). Теперь нам будет достаточно рассмотреть только одну последовательность при $b=4$, поэтому нижний индекс мы будем опускать. Соответственно характеристическое уравнение (2.1.12) принимает вид

$$x^2-4xy+y^2=1. \tag{12}$$

Согласно (2.1.11) это уравнение имеет в натуральных числах решения вида

$$x=\alpha(n+1),\quad y=\alpha(n) \tag{13}$$

и

$$x=\alpha(n),\quad y=\alpha(n+1) \tag{14}$$

при $n=0,1,\ldots$ В гауссовых числах, очевидно, появляются ещё решения вида

$$x=-\alpha(n+1),\quad y=-\alpha(n) \tag{15}$$

и

$$x=-\alpha(n),\quad y=-\alpha(n+1) \tag{16}$$

при $n=0,1,\ldots$ Мы можем объединить (13) с (16) и (14) с (15), определив при $n=-1,-2,\ldots$

$$\alpha(n)=-\alpha(-n). \tag{17}$$

При таком доопределении рекуррентное соотношение

$$\alpha(n+1)=4\alpha(n)-\alpha(n-1) \tag{18}$$

справедливо для всех вещественных целых n и, соответственно, для всех n справедливо и равенство (2.1.9):

$$\mathrm{A}(n)=\begin{pmatrix}\alpha(n+1) & -\alpha(n)\\ \alpha(n) & -\alpha(n-1)\end{pmatrix}=\Xi^n. \tag{19}$$

Покажем, что *все решения уравнения* (12) *в гауссовых* x *и* y *исчерпываются сериями* (13) *и* (14) *при произвольных вещественных целых значениях* n. Пусть x и y удовлетворяют (12). Рассмотрим матрицу

$$\mathrm{B}=\begin{pmatrix}4x-y & -x\\ x & -y\end{pmatrix} \tag{20}$$

и покажем, что для некоторого вещественного целого m либо

$$\mathrm{B}=\mathrm{A}(m), \tag{21}$$

либо

$$\mathrm{B}=-\mathrm{A}(m). \tag{22}$$

В первом случае x и y удовлетворяют (13) с $n=m$, во втором случае они удовлетворяют (14) с $n=-m$.

Как же по x и y найти соответствующее m? Матрица Ξ имеет собственный вектор

$$\begin{pmatrix}1\\ 2-\mathbf{sqrt}(3)\end{pmatrix}, \tag{23}$$

соответствующий собственному числу

$$\lambda=2+\mathbf{sqrt}(3). \tag{24}$$

Вектор (23) является собственным вектором и матрицы B, соответствующее собственное число равно

$$\mu=\lambda x-y. \tag{25}$$

Определим значение m неравенствами

$$1\le|\mu|\lambda^{-m}<\lambda \tag{26}$$

и рассмотрим матрицу

$$\mathrm{B}\mathrm{A}(-m)=\mathrm{B}\Xi^{-m}=\begin{pmatrix}4u-v & -u\\ u & -v\end{pmatrix}, \tag{27}$$

где

$$\begin{aligned} u&=-\alpha(m-1)x+\alpha(m)y,\\ v&=-\alpha(m)x+\alpha(m+1)y. \end{aligned} \tag{28}$$

Мы имеем:

$$u^2-4uv+v^2=\mathbf{det}(\mathrm{B}\Xi^{-m})=1. \tag{29}$$

Если $u=0$, то $v=1$ или $v=-1$ и, соответственно, выполнено (22) или (21), так что нам остаётся проверить, что других значений у u и v быть не может.

Пусть $u\neq 0$, тогда согласно (29)

$$v=(2+\nu)u \tag{30}$$

или

$$v=(2-\nu)u, \tag{31}$$

где

$$\nu=\mathbf{sqrt}(3+u^{-2}). \tag{32}$$

Легко видеть, что имеет место неравенство

$$\mathbf{Re}(\nu)\geq\mathbf{sqrt}(2), \tag{33}$$

а при большом $|u|$ ν близко к $\mathbf{sqrt}(3)$:

$$|\nu-\mathbf{sqrt}(3)|=|\mathbf{sqrt}(3+u^{-2})-\mathbf{sqrt}(3)|=\frac{1}{|u|^2|\nu+\mathbf{sqrt}(3)|}<\frac{1}{2|u|^2}. \tag{34}$$

Вектор (23), очевидно, является собственным для матрицы (27) и соответствует собственному числу

$$\lambda u-v=\mu\lambda^{-m}, \tag{35}$$

так что согласно (26)

$$1\leq|\lambda u-v|<\lambda. \tag{36}$$

Из (30) и (34) следует, что

$$|\lambda u-v|=|\mathbf{sqrt}(3)-\nu||u|<\frac{1}{2|u|}, \tag{37}$$

что противоречит левому неравенству в (36). Таким образом, из двух возможных равенств, (30) и (31), справедливо может быть только последнее.

Из (31) и (33) следует, что

$$|\lambda u-v|=|\mathbf{sqrt}(3)+\nu||u|>|\mathbf{sqrt}(3)+\mathbf{sqrt}(2)||u|, \tag{38}$$

что вместе с правым неравенством в (36) дает оценку $|u|^2<2$, так что u может иметь только значения ±1 и $\pm i$. В первом слу-

чае $\nu=2$, $v=0$ и не выполнено правое неравенство в (36). Во втором случае $\nu=\mathbf{sqrt}(2)$, и $v=\pm(2-\mathbf{sqrt}(2))\mathbf{i}$ не является гауссовым числом. Таким образом, и равенство (31) не может быть выполнено, а полученное противоречие доказывает, что $u=0$.

Итак, мы установили, что все решения уравнения (12) в гауссовых x и y на самом деле вещественны, и мы знаем, что это уравнение имеет сколь угодно большие решения вида (13). Как же из них можно получить все вещественные целые числа?

Понятно, что арифметические операции, в частности деление, не выводят за множество вещественных чисел, поэтому в любом решении системы

$$x^2-4xy+y^2=1, \tag{39}$$

$$u^2-4uv+v^2=1, \tag{40}$$

$$v=qy, \tag{41}$$

$$y\neq 0 \tag{42}$$

в гауссовых q, u, v, x, y все эти числа являются вещественными.

Определим трёхместное отношение **grem** эквивалентностью

$$\mathbf{grem}(a,b,c) \Leftrightarrow \exists z[a=b+cz \;\&\; |a|<|c|]. \tag{43}$$

(Это отношение, в отличие от (1.6.4), не определяет функцию, поскольку выбор a, вообще говоря, не однозначен.) Проверим, что из $\mathbf{grem}(a,b,c)$ и вещественности b и c следует вещественность a. Пусть в (43) $z=g+h\mathbf{i}$, где g и h вещественны. Тогда

$$c^2>|a|^2=|b+cz|^2=|b+c(g+h\mathbf{i})|^2=(b+cg)^2+c^2h^2, \tag{44}$$

откуда $h=0$, и, следовательно, z и a вещественны.

Таким образом, в любом решении системы, состоящей из условий (39)–(41) и

$$p=q+zy, \tag{45}$$

$$|p|<|y|, \tag{46}$$

все неизвестные вещественны.

Ниже мы проверим, что система (39)–(41), (45)–(46) имеет решение с любым нечётным вещественным числом в качестве значения p. Получение всего множества $\mathbb{Z}$ далее не представляет труда, но условие (46) нас устроить не может, ибо очевидный путь установления его $(\mathbb{G},\mathbb{Z},\mathbb{G})$-диофантовости лежит через установление $(\mathbb{G},\mathbb{Z},\mathbb{G})$-диофантовости $\mathbb{N}$ или хотя бы $\mathbb{Z}$. Поэтому мы заменим условие (46) на два условия

$$x=4(3p^2+1)w, \tag{47}$$

$$x\neq 0. \tag{48}$$

Из (47)–(48) следует, что

$$|x|=4|3p^2+1||w|>6p, \tag{49}$$

$$|x|=4|3p^2+1||w|\geq 4, \tag{50}$$

а отсюда и из (39) — что

$$|y| = |2 \pm \mathbf{sqrt}(3+x^{-2})|\,|x| \geq (2-\mathbf{sqrt}(3\tfrac{1}{16}))|x| = \tfrac{1}{4}|x| > |p|. \tag{51}$$

Мы избавились от отношения $<$ в (46) ценой появления отношения $\neq$ в (48). Последнее условие мы заменим на

$$rx+(8s+3)t = 1 \tag{52}$$

— это уравнение не имеет решения в гауссовых r, s и t при $x=0$.

Итак, мы построили систему из диофантовых уравнений (39)–(41), (45), (47) и (52) и установили, что в любом её гауссовом решении p обязательно вещественно. Проверим теперь, что для каждого нечётного вещественного значения p эта система имеет решение относительно q, r, s, t, u, v, x, y, z. Не ограничивая общности, мы будем считать, что $p>0$ (в противном случае достаточно найти решение для противоположного по знаку значения p и изменить в нём знаки у q, v, x, y и z).

Рассмотрим последовательность

$$\alpha(0), \alpha(1), \ldots, \alpha(n), \ldots \tag{53}$$

Благодаря рекуррентному соотношению эта последовательность **modulo** $4(3p^2+1)$ является чисто периодической. Поскольку $\alpha(0)=0$, то отсюда следует, что в (53) бесконечно много членов, кратных $4(3p^2+1)$. Как легко увидеть из рекуррентного соотношения (или из (2.2.7)),

$$\alpha(n) \equiv n (\mathbf{mod}\ 2). \tag{54}$$

Таким образом, найдётся нечётное значение n такое, что $n>3$ и

$$\alpha(n+1) \equiv 0 (\mathbf{mod}\ 4(3p^2+1)). \tag{55}$$

Положим

$$x = \alpha(n-1), \quad y = \alpha(n), \tag{56}$$

тогда равенство (39) будет выполнено, и можно найти w, удовлетворяющее (47). Выберем s так, чтобы x и $8s+3$ были взаимно просты, тогда мы сможем найти r и t, удовлетворяющие (52).

Положим

$$u = \alpha(pn+1), \quad v = \alpha(pn), \tag{57}$$

тогда равенство (40) будет выполнено. Согласно (2.3.9)

$$v \equiv px^{pn-1}y (\mathbf{mod}\ y^2), \tag{58}$$

так что мы можем найти значение q, удовлетворяющее (41), причём это значение будет удовлетворять сравнению

$$q \equiv px^{pn-1} (\mathbf{mod}\ y). \tag{59}$$

Согласно (39)

$$x^2 \equiv 1 (\mathbf{mod}\ y), \tag{60}$$

так что из (59) и (60) и нечётности pn следует, что

$$q \equiv p (\mathbf{mod}\ y), \tag{61}$$

и мы можем найти z, удовлетворяющее (45).

Для получения $(\mathbb{G}, \mathbb{Z}, \mathbb{G})$-диофантова представления множества $\mathbb{Z}$ остаётся объединить согласно (11) вместе уравнения (39)–(41), (45), (47), (52) и уравнение

$$2a+1 = q, \tag{62}$$

объявить a параметром, а остальные переменные — неизвестными.

§ 7.4. Однородные уравнения и рациональные решения

На протяжении большей части этой книги мы рассматриваем решения диофантовых уравнений только в натуральных числах. Д. Гильберт в 10-й проблеме спрашивал про решения в целых числах. Сам же Диофант интересовался решениями в рациональных числах. Если у нас есть диофантово уравнение

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

с рациональными неизвестными $x_1, \ldots, x_m$, то мы можем вместо него рассмотреть уравнение с целыми неизвестными

$$H(r_1, \ldots, r_m, q) = 0, \tag{2}$$

где

$$H(r_1, \ldots, r_m, q) = q^k D\left(\frac{r_1}{q}, \ldots, \frac{r_m}{q}\right), \tag{3}$$

а k — степень полинома D. Полином H является однородным степени k, и потому уравнение (2) заведомо имеет *тривиальное решение* $r_1 = \ldots = r_m = q = 0$. По этой причине, когда говорят о разрешимости или неразрешимости однородного диофантова уравнения, то имеют в виду наличие или отсутствие у него нетривиального решения.

Основная цель настоящего параграфа — установить эквивалентность двух массовых проблем: *проблемы распознавания наличия рациональных решений у произвольных диофантовых уравнений* и *проблемы распознавания наличия нетривиальных решений в целых числах у однородных диофантовых уравнений*.

Мы начнём со сведéния второй из этих проблем к первой. Пусть

$$F(r_1, \ldots, r_m) = 0 \tag{4}$$

— произвольное однородное диофантово уравнение. Если оно имеет нетривиальное решение с $r_i \neq 0$, то уравнение

$$F(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_m) = 0 \tag{5}$$

имеет рациональное решение

$$x_j = \frac{r_j}{r_i}. \tag{6}$$

Наоборот, каждое решение уравнения (5) в рациональных $x_1, \ldots, x_{i-1}, \quad x_{i+1}, \ldots, x_m$ порождает целочисленное решение уравнения (4), в котором

$$r_i = d, \; r_j = dx_j, \quad j = 1, \ldots, i-1, i+1, \ldots, m, \tag{7}$$

где d — общий знаменатель $x_1, \ldots, x_{i-1}, \quad x_{i+1}, \ldots, x_m$. Таким образом, для того чтобы узнать, есть ли нетривиальное решение у (4), достаточно узнать, есть ли рациональное решение хотя бы у одного из m уравнений

$$\begin{gathered} F(1, x_2, \ldots x_{m-1}, x_m) = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ F(x_1, x_2, \ldots, x_{m-1}, 1) = 0. \end{gathered} \tag{8}$$

(Обратите внимание, что здесь мы получили сведéние несколько иного характера, чем все сведéния, которые мы получали ранее. А именно, до сих пор при сведéнии одной массовой проблемы P_1 к другой массовой проблеме P_2 мы находили по каждой индивидуальной подпроблеме проблемы P_1 эквивалентную ей индивидуальную подпроблему проблемы P_2. Мы могли бы поступить так же и здесь, перемножив левые части (8) и сведя вопрос о разрешимости (4) к разрешимости одного уравнения в рациональных числах. Это, однако, не требуется — понятно, что если бы имелся алгоритм для распознавания наличия рациональных решений то, применив его m раз к уравнениям из (8), мы узнали бы, имеет ли нетривиальное решение уравнение (4). В теории алгоритмов изучаются и ещё более общие виды сведéний, при которых, например, количество индивидуальных подпроблем проблемы P_2, ответы на которые надо установить при нахождении ответа на одну индивидуальную подпроблему проблемы P_1, не ограничено.)

Второе сведéние менее очевидно. Если уравнение (1) имеет решение в рациональных $x_1, \ldots, x_m$, то уравнение (2) имеет нетривиальное решение, но обратное, вообще говоря, не верно, ибо и в нетривиальном решении уравнения (2) значение q может оказаться равным 0. Мы должны добавить к (2) условие

$$r_1^2 + \ldots + r_m^2 \neq 0 \Rightarrow q \neq 0, \tag{9}$$

но должны суметь это сделать в виде однородного уравнения.

Здесь на помощь снова приходит уравнение (3.12). Как мы знаем из § 2.1, это уравнение имеет решения со сколь угодно большим x. В то же время уравнение

$$x^2 - 4xy + y^2 = 0 \tag{10}$$

имеет только тривиальное решение, ибо

$$x^2-4xy+y^2=(x-(2+\mathrm{sqrt}(3))y)(x-(2-\mathrm{sqrt}(3))y). \tag{11}$$

Отсюда получаем, что уравнение

$$x^2-4xy+y^2=q^4 \tag{12}$$

имеет решение с любым ненулевым q и сколь угодно большим x, но если $q=0$, то $x=0$. Это позволяет переписать условие (9) в виде неравенства

$$x\geq r_1^2+\ldots+r_m^2. \tag{13}$$

Для достижения однородности остаётся воспользоваться теоремой о четырёх квадратах (см. Приложение 1). А именно, мы можем ввести новые неизвестные и дать следующие явные выражения для x и y:

$$x=r_1^2+\ldots+r_m^2+s_1^2+s_2^2+s_3^2+s_4^2, \tag{14}$$

$$y=t_1^2+t_2^2+t_3^2+t_4^2. \tag{15}$$

Подстановка этих выражений в (12) даёт искомое однородное диофантово уравнение

$$(r_1^2+\ldots+r_m^2+s_1^2+s_2^2+s_3^2+s_4^2)^2-$$

$$-4(r_1^2+\ldots+r_m^2+s_1^2+s_2^2+s_3^2+s_4^2)(t_1^2+t_2^2+t_3^2+t_4^2)+(t_1^2+t_2^2+t_3^2+t_4^2)^2=q^4. \tag{16}$$

разрешимое относительно s_1, s_2, s_3, s_4, t_1, t_2, t_3, t_4 при любых q, $r_1,\ldots,r_m$, причём в любом нетривиальном решении (16) $q\neq 0$.

Нам остаётся объединить два уравнения (2) и (16). Мы не можем непосредственно воспользоваться техникой § 1.2, ибо если однородные уравнения (1.2.1) имеют разные степени, то уравнение (1.2.2) не однородно. Это препятствие легко преодолимо — система из двух однородных диофантовых уравнений

$$\begin{aligned} D_1(x_1,\ldots,x_m)&=0,\\ D_2(x_1,\ldots,x_m)&=0 \end{aligned} \tag{17}$$

степеней соответственно k_1 и k_2 эквивалентна одному однородному уравнению

$$D_1^{2k_2}(x_1,\ldots,x_m)+D_2^{2k_1}(x_1,\ldots,x_m)=0 \tag{18}$$

степени $2k_1k_2$.

Таким образом, положительное решение ограничения 10-й проблемы Гильберта на случай однородных уравнений давало бы и способ для распознавания наличия рациональных решений у произвольных диофантовых уравнений.

Упражнения

7.1. Аналогично **Card**, можно рассмотреть **ECard** — количество решений у экспоненциально диофантова уравнения. Покажите, что множество $\mathbf{ECard}^{-1}(\mathfrak{A})$ полуразрешимо в том и только том случае, когда либо $\mathfrak{A}$ пусто, либо $\mathfrak{A}=\{\mathfrak{n}\mid \mathfrak{n}\geq m,\ \mathfrak{n}\in\mathfrak{N}\}$, где m — конечный элемент множества $\mathfrak{N}$ (точная постановка задачи требует рассмотрения $\mathbf{ECard}^{-1}(\mathfrak{A})$ как множества натуральных чисел, для чего надо предварительно ввести понятие кода экспоненциального диофантова уравнения).

7.2. Пусть $F(\mathfrak{n})=c_0+c_1\binom{\mathfrak{n}}{1}+\ldots+c_m\binom{\mathfrak{n}}{m}$. Будем рассматривать F как отображение множества $\mathfrak{N}$ в него же, полагая, что $\binom{\infty}{k}=\infty$. Покажите, что по произвольному (экспоненциально) диофантову уравнению $D_1=0$ можно построить другое (экспоненциально) диофантово уравнение $D_2=0$, такое, что $\mathbf{Card}(D_2)=F(\mathbf{Card}(D_1))$ ($\mathbf{ECard}(D_2)=F(\mathbf{ECard}(D_1))$ соответственно).

7.3. Покажите, что при $b>1$ каждое диофантово множество имеет однократное унарное экспоненциально диофантово представление с основанием b.

7.4. Покажите, что объединение двух непересекающихся множеств, имеющих однократные диофантовы представления, также имеет однократное диофантово представление.

7.5. Покажите, что каждое диофантово множество $\mathfrak{D}$ имеет однократное «почти диофантово» представление вида

$$a\in\mathfrak{D} \iff \exists x_1\ldots x_m y\left[D(a,x_1,\ldots,x_m)=y+4^y\right].$$

7.6. Пусть A — кольцо целых алгебраических чисел из квадратичного поля $\mathbb{Q}(\mathbf{sqrt}(Z))$, где целое число Z отлично от полного квадрата. Установите $(A,\mathbb{Z},A)$-диофантовость множества $\mathbb{N}$.

7.7. Описанный в § 1.2 способ понижения степени уравнения приводит, вообще говоря, к неоднородным уравнениям. Покажите, что любое однородное параметрическое диофантово уравнение может быть преобразовано в эквивалентное однородное уравнение степени 4.

Открытые вопросы

7.1. Верно ли, что если $\mathfrak{A}$ — непустое множество, для которого множество $\mathbf{Card}^{-1}(\mathfrak{A})$ полуразрешимо, то $\mathfrak{A}=\{\mathfrak{n}\mid \mathfrak{n}\geq m,\ \mathfrak{n}\in\mathfrak{N}\}$ для некоторого конечного m?

7.2. Можно ли по произвольному экспоненциально диофантову уравнению $E=0$ эффективно найти диофантово уравнение $D=0$ такое, что $\mathbf{ECard}(E)=\mathbf{Card}(D)$?

7.3. Верно ли, что объединение любых двух множеств, имеющих однократные диофантовы представления, также имеет однократное диофантово представление?

Нерешённые проблемы

7.1. Имеет ли каждое диофантово множество однократное диофантово представление?

7.2. Пусть $\mathbb{O}$ — кольцо целых алгебраических чисел из какого-либо расширения конечной степени поля рациональных чисел $\mathbb{Q}$. Верно ли, что множество $\mathbb{Z}$ является $(\mathbb{O},\mathbb{O},\mathbb{O})$-диофантовым?

Комментарии

В докладе Д. Гильберта [1900] 10-й проблеме уделено места меньше, чем какой-либо другой. Как пишет К. Рид [1970], из-за ограниченного времени Д. Гильберт во время выступления вообще не сказал ни слова про 10-ю проблему (как и про некоторые другие), а просто включил её в печатный текст доклада. В результате мы не имеем ни развернутого обоснования важности этой проблемы, ни объяснения, почему она, в отличие от многих других из того же перечня, сформулирована столь конкретно.

Возможное объяснение этого таково. Судя по духу доклада, Д. Гильберт ожидал положительного решения 10-й проблемы. Как мы видели, в этом случае мы имели бы не только способ распознавать наличие решений в целых числах у отдельных уравнений, но и способы узнавать разрешимость в натуральных, рациональных и гауссовых числах отдельных диофантовых уравнений и систем таких уравнений. Таким образом, Д. Гильберт мог предполагать, что, ограничиваясь целочисленными решениями, он ставит наиболее трудную проблему, решение которой автоматически даст решения других аналогичных проблем.

Как мы теперь знаем, 10-я проблема в том конкретном виде, как она была сформулирована Гильбертом, оказалась неразрешимой, а это не влечёт в качестве прямого следствия неразрешимость всех других родственных проблем. В связи с этим 10-ю проблему Гильберта можно трактовать в более широком смысле, включая в неё все те проблемы, положительное решение которых немедленно следовало бы из положительного решения 10-й проблемы в её узкой трактовке.

К таким проблемам в первую очередь относятся аналоги 10-й проблемы, касающиеся разрешимости в других кольцах алгебраических чисел. Устанавливая в § 7.3 алгоритмическую неразрешимость в случае кольца гауссовых чисел, мы следовали работе Денефа [1975]. На самом деле там получен более общий результат, касающийся произвольных квадратичных расширений (см. упражнение 7.6). Этот результат был обобщён дальше в совместной работе Денефа и Липшица [1978] (см. упражнение 7.7), в этой же работе была сформулирована нерешённая проблема 7.2. Дальнейшие продвижения в исследовании этой проблемы были получены в работах Денефа [1980], Фейдаса [1988], Шапиро и Шляпентох [1989] и Шляпентох [1989].

В качестве контрастного результата упомянем работу Румли [1986], в которой указан метод для распознавания разрешимости диофантовых уравнений в *произвольных* целых алгебраических числах. Этот результат, однако, выходит за рамки 10-й проблемы даже при расширенном её толковании, ибо не видно прямого пути для преобразования диофантова уравнения, неизвестные которого могут быть целыми алгебраическими числами из рас-

ширения *любой* степени, в диофантово уравнение с рациональными целыми неизвестными.

Очень важным для приложений является вопрос о разрешимости диофантовых уравнений в рациональных числах. Достижений в этой области мало, трудности объясняются, по-видимому, тем, что в этом случае мы лишены такого важного инструмента, как аппарат делимостей и сравнений. Сведение диофантовых уравнений с рациональными неизвестными к однородным уравнениям, скорее всего, было известно давно, но, похоже, не публиковалось. В § 7.4 мы следовали доказательству, предложенному Р. М. Робинсоном (см. работу Сморинского [1987]).

В работах Липшица [1977, 1978а, 1978б] исследовалась алгоритмическая разрешимость систем диофантовых условий специального вида с коэффициентами и неизвестными из некоторых колец целых алгебраических чисел. В работах Девиса и Патнама [1963], Денефа [1978а, 1978б], Фейдаса [1987а, 1987б] и Шляпентох [1990] изучались алгоритмические вопросы, связанные с решением диофантовых уравнений в нечисловых кольцах.

Существование однократных экспоненциально диофантовых представлений было установлено в работе Матиясевича [1974] способом, аналогичным второму способу из § 7.2. Первый способ имеет своим прототипом работу Матиясевича [1976], а третий — работу Матиясевича [1979].

Неразрешимость множества $\mathbf{Card}^{-1}(\{1\})$ (как следствие неразрешимости 10-й проблемы Гильберта) была получена в диссертации Адлера [1969в]. Неразрешимость $\mathbf{Card}^{-1}(\mathfrak{A})$ в общем случае была установлена в работе Девиса [1972]. Его доказательство было упрощено в работе Сморинского [1977] (см. также обзор Девиса [1977]). Там же была получена более детальная характеризация аналогичных множеств экспоненциально диофантовых уравнений благодаря тому, что в экспоненциальном случае существуют однократные представления (см. упражнение 7.1). В этой же работе были поставлены открытые вопросы 7.1 и 7.2 и ряд других.

Глава 8

ДИОФАНТОВА СЛОЖНОСТЬ

В этой главе мы рассмотрим вопросы, связанные с количественным усилением некоторых из полученных ранее результатов.

§ 8.1. Основные понятия

До сих пор почти все полученные нами результаты носили качественный характер — устанавливалась диофантовость тех или иных свойств и отношений и алгоритмическая неразрешимость тех или иных массовых проблем, связанных с диофантовыми множествами. Между тем большинству из этих результатов можно придать количественное усиление.

Рассмотрим основное понятие настоящей книги — понятие диофантова множества. Напомним, что множество $\mathfrak{D}$ n-ок натуральных чисел называется диофантовым, если

$$\langle a_1,\ldots,a_n\rangle\in\mathfrak{D} \Leftrightarrow \exists x_1\ldots x_m[D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0], \qquad (1)$$

где D — полином с целыми коэффициентами. Для каждого диофантова множества $\mathfrak{D}$ можно поставить следующие два вопроса:

какова минимально возможная степень полинома D относительно неизвестных в диофантовом представлении (1) *множества* $\mathfrak{D}$?

каково минимально возможное значение m — количества неизвестных в представлении (1)?

Первую характеристику будем называть *порядком* множества $\mathfrak{D}$ и обозначать посредством $\mathbf{ord}(\mathfrak{D})$, вторую будем называть *рангом* $\mathfrak{D}$ и обозначать посредством $\mathbf{rank}(\mathfrak{D})$.

Понятно, что минимальная степень и минимальное количество неизвестных могут достигаться, вообще говоря, при разных полиномах D, и поэтому можно спрашивать об *относительном порядке* $\mathbf{ordrank}(\mathfrak{D},m)$ — наименьшей степени полинома D в представлении (1) с m неизвестными, а также *относительном ранге* $\mathbf{rankord}(\mathfrak{D},d)$ — наименьшем количестве неизвестных в диофантовом представлении (1), в котором степень полинома D равна d; при $m<\mathbf{rank}(\mathfrak{D})$ полагаем $\mathbf{ordrank}(\mathfrak{D},m)=\infty$; аналогично, $\mathbf{rankord}(\mathfrak{D},d)=\infty$ при $d<\mathbf{ord}(\mathfrak{D})$.

Диофантовы множества распадаются на классы с равными значениями **ord**($\mathfrak{D}$) или **rank**($\mathfrak{D}$). A priori можно было ожидать, что все эти классы будут не пусты, но универсальное диофантово уравнение показывает, что это не так; *существуют такие константы* **d** *и* **m**, *что любое диофантово множество имеет представление* (1), *в котором одновременно степень уравнения относительно неизвестных не более* **d**, *а количество неизвестных не более* **m**. В качестве **d** и **m**, очевидно, можно взять степень и число неизвестных в каком-либо универсальном уравнении (такие уравнения были построены в § 4.5 и § 6.5). Иными словами, для любого диофантова множества $\mathfrak{D}$

$$\mathbf{ordrank}(\mathfrak{D},\mathbf{m})\le\mathbf{d}, \tag{2}$$

$$\mathbf{rankord}(\mathfrak{D},\mathbf{d})\le\mathbf{m}. \tag{3}$$

Таким образом, традиционное деление диофантовых уравнений на «уравнения первой степени», «уравнения второй степени», . . . , «уравнения степени d», . . . и на «уравнения с одной неизвестной», «уравнения с двумя неизвестными», . . . , «уравнения с m неизвестными», . . . осмыслено только при малых значениях d и m.

Пару чисел $\langle\mathbf{d},\mathbf{m}\rangle$, удовлетворяющих для любого диофантова множества $\mathfrak{D}$ неравенству (2) (или, что эквивалентно, неравенству (3)), будем называть *универсальной границей сложности* диофантовых множеств. Числа **d** и **m**, удовлетворяющие для любого диофантова множества $\mathfrak{D}$ неравенствам

$$\mathbf{ord}(\mathfrak{D})\le\mathbf{d} \tag{4}$$

и

$$\mathbf{rank}(\mathfrak{D})\le\mathbf{m}, \tag{5}$$

будем называть соответственно *универсальной границей порядка* и *универсальной границей ранга* диофантовых множеств.

Ещё в § 1.5 был приведён первый количественный результат — показано, что число 4 является универсальной границей порядка. Аналогичного простого способа для уменьшения количества неизвестных пока не найдено. Универсальную границу ранга можно найти, оценив количество неизвестных в универсальном уравнении, построенном в § 4.5 или в § 6.5. При этом получится величина порядка нескольких сотен, поскольку мы не заботились об «экономном» использовании неизвестных.

В качестве ещё одной, но менее традиционной характеристики полинома и, соответственно, диофантова множества можно рассмотреть **oper**($\mathfrak{D}$) — наименьшее количество арифметических операций, необходимое для вычисления значений полинома D в диофантовом представлении (1) множества $\mathfrak{D}$. Понятно, что не может быть универсальной оценки количества операций, пригодной для множеств любой размерности, но универсальное уравне-

ние опять-таки показывает существование для каждого n *универсальной границы количества операций* $\mathbf{p}_n$.

Для примера возьмём в качестве $\mathfrak{D}$ множество всех чисел, имеющих не менее $10^{10}\mathbf{p}_1$ простых делителей. Оказывается, что для проверки этого свойства у любого элемента множества $\mathfrak{D}$ достаточно выполнить всего $\mathbf{p}_1$ операций!

Имея ещё одну сложностную характеристику, можно рассматривать *относительные порядки* **ordoper**, **ordrankoper**, *относительные ранги* **rankoper, rankordoper**, *относительные количества операций* **operord, operrank, operordrank**.

С каждым конкретным диофантовым представлением (1) можно связать ещё одну сложностную характеристику, отражающую скорость роста значений неизвестных в «наименьшем» решении уравнения при данных значениях параметров. Под «наименьшим» решением можно понимать решение, для которого минимальное значение имеет $\mathbf{max}(x_1,\ldots,x_m)$, $x_1+\ldots+x_m$, $\mathbf{Cantor}_m(x_1,\ldots,x_m)$ или какая-либо другая подобная функция $F(x_1,\ldots,x_m)$, для которой количество решений неравенства $F(x_1,\ldots,x_m)<b$ конечно для любого b. Будем называть функцию $T(a_1,\ldots,a_n)$ *тестирующей* для представления (1), если справедливо не только оно, но и

$$\langle a_1,\ldots,a_n\rangle\in\mathfrak{D} \Leftrightarrow \exists x_1\ldots x_m[D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0\ \&$$
$$\&\ F(x_1,\ldots,x_m)\le T(a_1,\ldots,a_n)]. \qquad (6)$$

Это название отражает тот факт, что для проверки принадлежности кортежа $\langle a_1,\ldots,a_n\rangle$ множеству $\mathfrak{D}$ достаточно «испытать» конечное множество кортежей $\langle x_1,\ldots,x_m\rangle$, удовлетворяющих неравенству $F(x_1,\ldots,x_m)\le T(a_1,\ldots,a_n)$.

Подчеркнём, что, в отличие от порядка и ранга, понятие тестирующей функции введено не по отношению к диофантову множеству, а по отношению к его конкретному представлению. Очевидным препятствием к переносу этого понятия на множества является отсутствие линейного порядка на множестве тестирующих функций. Мы могли бы ввести частичный порядок $\le\le$, считая, что $T_1\le\le T_2$, если для всех достаточно больших $a_1,\ldots,a_n$ $T_1(a_1,\ldots,a_n)\le T_2(a_1,\ldots,a_n)$, и назвать, скажем, минимальной тестирующей функцией для данного диофантова множества $\mathfrak{D}$ минимальную по отношению $\le\le$ тестирующую функцию для какого-либо его представления. Этот план не проходит по отнюдь не очевидной причине: *существуют диофантовы множества, не имеющие минимальной тестирующей функции* (см. упражнение 8.11, где сформулировано ещё более сильное утверждение).

До сих пор мы рассматривали оригинальное определение диофантова множества через представление вида (1). В действительности, как мы видели в главах 1–3 и 6, существуют более широкие классы формул, задающих диофантовы множества.

Для каждого такого класса формул можно вводить свои сложностные характеристики. Рассмотрим в качестве примера экспоненциально диофантовы представления.

Экспоненциально диофантово представление

$$\langle a_1,\ldots,a_n\rangle\in\mathfrak{D} \Leftrightarrow$$
$$\Leftrightarrow \exists x_1\ldots x_m[E_1(a_1,\ldots,a_n,x_1,\ldots,x_m)=E_2(a_1,\ldots,a_n,x_1,\ldots,x_m)] \qquad (7)$$

порождает понятие *экспоненциального ранга* **erank**($\mathfrak{D}$). Поскольку каждое диофантово представление с точностью до переноса отрицательных членов в другую сторону от знака равенства является экспоненциально диофантовым, **erank**($\mathfrak{D}$)$\leq$**rank**($\mathfrak{D}$). В § 8.2 будет получена *универсальная граница экспоненциального ранга* **erank**($\mathfrak{D}$)≤ 3.

Некоторым аналогом степени уравнения в (1) может служить *уровень итерированности уравнения* в (7), определяемый следующим образом:

константы имеют нулевой уровень итерированности;

переменные имеют первый уровень итерированности;

уровень итерированности E_1+E_2, E_1E_2 и $E_1=E_2$ равен максимальному из уровней итерированности E_1 и E_2;

уровень итерированности $E_1^{E_2}$ равен $\max(i_1,1)+i_2$, где i_1 и i_2 — уровни итерированности E_1 и E_2.

Можно было бы определить **iter**($\mathfrak{D}$) — *уровень итерированности множества* $\mathfrak{D}$ как наименьший уровень итерированности уравнения в экспоненциально диофантовом представлени множества $\mathfrak{D}$, но, очевидно, что **iter**($\varnothing$)=**iter**($\mathbb{N}$)=0, а для любого другого диофантова множества $\mathfrak{D}$ **iter**($\mathfrak{D}$)=1. Интерес представляют только *относительный уровень итерированности* **itererank** и *относительный экспоненциальный ранг* **erankiter**.

§ 8.2. Оценка количества неизвестных в экспоненциально диофантовых представлениях

В этом параграфе мы установим, что *любое диофантово множество имеет экспоненциально диофантово представление, содержащее всего три неизвестные.*

Благодаря тому, что **Cantor**$_n$ является не просто диофантовой функцией, а полиномом с рациональными коэффициентами, нам опять достаточно провести доказательство в одномерном случае.

Пусть $\mathfrak{M}$ — произвольное диофантово множество натуральных чисел. Так же, как в изложенном в § 7.2 третьем способе построения однократных представлений, мы будем использовать модифицированную технику § 6.3. Для этого на

диофантова представления (7.2.11) множества $\mathfrak{M}$. Как показано в § 7.2,

$$a \in \mathfrak{M} \Leftrightarrow \exists w[2^{l(w)} \mid S(w)], \tag{1}$$

где $l(w)$ и $S(w)$ определены формулами (6.3.3), (6.3.15), (6.3.16), (6.3.17), (6.3.23), (6.3.24), (6.3.30), (6.3.34) и (6.3.36) при $b=1$, $y=0$. В § 6.3 мы условились не указывать явно, что $l(w)$ и $S(w)$ зависят также от a; для дальнейшего упрощения записи мы будем опускать теперь и указание на зависимость от w. Представление (1) множества $\mathfrak{M}$ содержит всего одну неизвестную, однако это представление не является экспоненциально диофантовым, ибо содержит отношение делимости $\mid$ и биномиальный коэффициент (7.2.30). Устранение отношения делимости согласно (1.6.3) требует введения дополнительной неизвестной, а устранение биномиального коэффициента согласно (3.4.2) и (3.3.8) — ещё трёх неизвестных. Таким образом, если мы хотим получить представление, содержащее лишь три неизвестные, то должны действовать более экономным способом.

Согласно (7.2.30)

$$S = \binom{2K}{K}. \tag{2}$$

Очевидно, что

$$(u+1)^{2K} = pu^K + q, \tag{3}$$

где

$$p = \sum_{i=K}^{2K} \binom{2K}{i} u^{i-K}, \tag{4}$$

$$q = \sum_{i=0}^{K-1} \binom{2K}{i} u^i. \tag{5}$$

Если u достаточно велико, например,

$$2^{2K} < u, \tag{6}$$

то

$$q < u^K, \tag{7}$$

ибо

$$u^K > 2^{2K} u^{K-1} = \sum_{i=0}^{2K} \binom{2K}{i} u^{K-1}. \tag{8}$$

Легко видеть, что значения p и q однозначно определяются условиями (3) и (7).

Очевидно, что

$$p \equiv \binom{2K}{K} (\mathbf{mod}\ u), \tag{9}$$

так что если

$$2^l \mid u, \tag{10}$$

то делимость в (1) эквивалентна

$$2^l | p. \tag{11}$$

Таким образом, у нас нет необходимости иметь в явном виде неизвестную, значение которой было бы равно биномиальному коэффициенту, и мы получаем следующее представление для множества $\mathfrak{M}$:

$$a \in \mathfrak{M} \Leftrightarrow$$
$$\Leftrightarrow \exists pquw[(u+1)^{2K} = pu^K + q \;\&\; 2^{2K} < u \;\&\; q < u^K \;\&\; 2^l | u \;\&\; 2^l | p]. \tag{12}$$

Вводя ещё одну неизвестную, мы можем заменить условие (11) на равенство

$$p = 2^l r. \tag{13}$$

Вместо (6) мы возьмём более сильное неравенство

$$2^{2K+l+2} < u, \tag{14}$$

из которого аналогично (8) получается более сильное, чем (7), неравенство

$$2^{l+2} q < u^K. \tag{15}$$

Согласно (15), (3) и (14)

$$2^{l+2} q < u^K \le \frac{(u+1)^{2K}}{u^K} - 1 \le p \le \frac{(u+1)^{2K}}{u^K} < 2u^K, \tag{16}$$

и согласно (13)

$$q < r, \tag{17}$$

$$r < u^K. \tag{18}$$

Таким образом, если выполнено неравенство (14), то из (4), (5) и (13) следует (17), а из (17) следует (7). В результате мы получаем новое представление для $\mathfrak{M}$:

$$a \in \mathfrak{M} \Leftrightarrow$$
$$\Leftrightarrow \exists pqruw[(u+1)^{2K} = pu^K + q \;\&\; 2^{2K+l+2} < u \;\&\; 2^l | u \;\&\; p = 2^l r \;\&\; q < r]. \tag{19}$$

Мы можем теперь легко получить представление с тремя неизвестными, заменив неравенство (17) на равенство

$$r = q + s + 1, \tag{20}$$

используя равенства (13) и (20) для устранения p и r и равенство

$$u = 2^{2K+l+2} \tag{21}$$

для устранения u. Получающееся при этом представление

$$a \in \mathfrak{M} \Leftrightarrow \exists rsw[(2^{2K+l+2}+1)^{2K} = 2^l(q+s+1)2^{(2K+l+2)K} + q] \tag{22}$$

ещё не является искомым экспоненциально диофантовым пред-

ставлением, ибо согласно (6.3.49)

$$K = \frac{K_1-K_2}{K_3-K_4}, \tag{23}$$

а экспоненциально диофантово уравнение, как было определено в § 2.5, не может содержать вычитаний и делений.

Чтобы устранить деления, вместо (21) мы определим u равенством

$$u=(K_3-K_4)T, \tag{24}$$

где

$$T=K_1+J+2. \tag{25}$$

При этом вместо уравнения из (22) получится уравнение

$$\left(2^{(K_3-K_4)T}+1\right)^{\frac{2K_1-2K_2}{K_3-K_4}} = 2^J(q+s+1)2^{(K_1-K_2)T}+q. \tag{26}$$

Возведя обе части этого равенства в степень K_3-K_4, мы получим уравнение

$$\left(2^{(K_3-K_4)T}+1\right)^{2K_1-2K_2} = \left(2^J(q+s+1)2^{(K_1-K_2)T}+q\right)^{K_3-K_4}. \tag{27}$$

Для устранения вычитаний сначала умножим обе части на

$$\left(2^{(K_3-K_4)T}+1\right)^{2K_2}\left(2^J(q+s+1)2^{(K_1-K_2)T}+q\right)^{K_4}, \tag{28}$$

получая уравнение

$$\left(2^{(K_3-K_4)T}+1\right)^{2K_1}\left(2^J(q+s+1)2^{(K_1-K_2)T}+q\right)^{K_4} =$$

$$= \left(2^{(K_3-K_4)T}+1\right)^{2K_2}\left(2^J(q+s+1)2^{(K_1-K_2)T}+q\right)^{K_3}. \tag{29}$$

Наконец, умножим обе части ещё на

$$2^{(2(K_1+K_2)K_4+K_2K_3)T} \tag{30}$$

и получим окончательное экспоненциально диофантово уравнение

$$2^{K_2K_3T}\left(2^{K_3T}+2^{K_4T}\right)^{2K_1}\left(2^J(q+s+1)2^{K_1T}+q2^{K_2T}\right)^{K_4} =$$

$$= 2^{2K_1K_2T}\left(2^{K_3T}+2^{K_4T}\right)^{2K_2}\left(2^J(q+s+1)2^{K_1T}+q2^{K_2T}\right)^{K_3}. \tag{31}$$

Это уравнение разрешимо относительно q, s и w для тех и только тех значений параметра a, которые принадлежат множеству $\mathfrak{M}$.

Упражнения

8.1. Покажите, что пятиместное отношение $(a+1)|(b-c)\&d>e$ имеет диофантово представление с одной неизвестной.

8.2. Пусть $S_1,\ldots,S_k$ — полиномы с целыми коэффициентами. Покажите, что отношение

$$\exists x_1\ldots x_k[\mathop{\&}_{i=1}^{k} S_i(a_1,\ldots,a_n)=x_i^2]$$

имеет диофантово представление, содержащее всего одну неизвестную.

8.3. Проверьте, что если p — простое число, $l=\mathbf{deg}_p(q)\equiv 1(\mathbf{mod}\ 2)$, $k>0$, то из одной делимости

$$p^{2kl}|a^2q+b^2$$

следуют две делимости

$$p|a,\ p^{kl}|b.$$

Обобщите это свойство так, чтобы из одной делимости следовало m делимостей.

8.4. Воспользуйтесь предыдущим упражнением, чтобы заменить m делимостей (6.2.26) на одну.

8.5. Покажите, что любое диофантово множество представимо в нормальной форме Девиса

$$a\in\mathfrak{D} \iff \exists w\forall z_{\le w}\exists yx[D(a,w,x,y,z)=0]$$

с всего лишь двумя переменными под вторым квантором существования.

8.6. Покажите, что любое диофантово множество имеет представление вида

$$a\in\mathfrak{D} \iff \exists xy\forall z_{\le B(a,x,y)}[D(a,x,y,z)>0],$$

где B и D — полиномы с целыми коэффициентами.

8.7. Покажите, что любое диофантово множество имеет представление вида

$$a\in\mathfrak{D} \iff \exists x\forall y_{\le B(a,x)}\forall z_{\le C(a,x,y)}[D(a,x,y,z)>0],$$

где B, C и D — полиномы с целыми коэффициентами.

8.8. Покажите, что каждое диофантово множество имеет обобщённые диофантовы представления вида

$$a\in\mathfrak{D} \iff \exists x\mathop{\&}_{i=1}^{k}\exists yz[D_i(a,x,y,z)>0]$$

и

$$a\in\mathfrak{D} \iff \exists xy\mathop{\&}_{i=1}^{k}\exists z[D_i(a,x,y,z)>0]$$

8.9. Согласно упражнению 4.2 существует такое число m, что любое диофантово множество представимо как множество *натуральных* значений некоторого полинома с *целыми* коэффициентами с m переменными. Покажите, что для каждого m существует множество, представимое как множество *всех* значений полинома *с натуральными коэффициентами*, но в любом таком представлении количество переменных не меньше m.

8.10. Усильте результат § 8.2, показав, что каждое диофантово множество имеет однократное унарное экспоненциально диофантово представление с тремя неизвестными.

8.11. Покажите, что для любой диофантовой функции $T(a,b)$, определённой при всех значениях a и b, можно найти одномерное диофантово множество $\mathfrak{D}$, у которого дополнение также диофантово, причём для любого диофантова представления

$$D(a,x_1,\ldots,x_m)=0 \qquad (\star)$$

(дополнения) множества $\mathfrak{D}$ не могут не существовать другое диофантово представление

$$E(a,y_1,\ldots,y_n)=0 \qquad (\star\star)$$

(дополнения) множества $\mathfrak{D}$ и число a_0 такие, что для любых a, $x_1,\ldots,x_m$, удовлетворяющих $(\star)$ и неравенству $a>a_0$, существуют числа $y_1,\ldots,y_n$, удовлетворяющие $(\star\star)$ и неравенству

$$T(a,y_1+\ldots+y_n)<x_1+\ldots+x_m.$$

Нерешённая проблема

8.1. Пусть **D** обозначает класс всех отношений $\mathcal{R}$, имеющих представления вида

$$\mathcal{R}(a_1,\ldots,a_n) \iff$$
$$\iff \exists x_1\ldots x_m\left[D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0 \,\&\, x_1+\ldots+x_m\le 2^{|a_1+\ldots+a_n|^k}\right],$$

где D — полином с целыми коэффициентами, а $|a|$ обозначает длину двоичной записи числа a. Верно ли, что **D** = **NP**, где **NP** — класс отношений, распознаваемых на недетерминированной машине Тьюринга за полиномиальное число шагов?

(Строгое определение класса **NP** см., например, в монографии Гэри и Джонса [1979]. Обратите внимание, что в определении класса **D** *не* предполагается, что

$$\mathcal{R}(a_1,\ldots,a_n) \iff \exists x_1\ldots x_m[D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0.])$$

Комментарии

С самого начала исследований, нацеленных на отрицательное решение 10-й проблемы Гильберта, стали вызывать интерес и количественные вопросы, связанные с диофантовыми и близкими к ним представлениями. Так,

вскоре после установления М. Девисом нормальной формы (см. комментарии к главе 5) Р. М. Робинсон [1956] показал, что в ней всегда можно брать $m=4$. Позднее [1972] он улучшил этот результат до $m=3$, а в работе Матиясевича [1972б] было показано, что можно брать $m=2$ (см. упражнение 8.5). Другие арифметические представления с малым числом кванторов (существования и общности) предложены в работах Матиясевича и Робинсон [1974], Джонса [1981] и Джонса, Левица и Уилки [1986].

После того как была установлена диофантовость полуразрешимых множеств, начались исследования по оценкам диофантова ранга конкретных множеств и нахождению возможно меньшей универсальной границы ранга. Последнее, естественно, связано с построением универсальных диофантовых уравнений, и, как сказано в комментариях к главе 4, лучшая в настоящее время (1990г.) универсальная граница ранга — 9 неизвестных — была получена Ю. В. Матиясевичем. Детальное доказательство приведено в работе Джонса [1982б]. В этой же работе указаны следующие универсальные границы сложности диофантовых множеств:

$$\langle 4, 58\rangle,\ \langle 8, 38\rangle,\ \langle 12, 32\rangle,\ \langle 16, 29\rangle,\ \langle 20, 28\rangle,\ \langle 24, 26\rangle,\ \langle 28, 25\rangle,$$
$$\langle 36, 24\rangle,\ \langle 96, 21\rangle,\ \langle 2668, 19\rangle,\ \langle 2\times 10^5, 14\rangle,\ \langle 6{,}6\times 10^{43}, 13\rangle,$$
$$\langle 1{,}3\times 10^{44}, 12\rangle,\ \langle 4{,}6\times 10^{44}, 11\rangle,\ \langle 8{,}6\times 10^{44}, 10\rangle,\ \langle 1{,}6\times 10^{45}, 9\rangle.$$

Здесь же получена универсальная граница $p_1=100$ для количества операций.

Из оценок ранга конкретных множеств наибольший интерес привлекало, что вполне естественно, множество всех простых чисел. В течение долгого времени благодаря специфике этого множества удавалось получать для него оценку ранга лучшую, чем известная на соответствующий момент универсальная граница ранга. В настоящее время (1990г.) наименьшее количество неизвестных в диофантовом представлении множества простых чисел совпадает с известной ныне универсальной границей ранга, хотя, конечно, конструкция полинома и доказательство для этого множества проще, чем в общем случае (см. комментарии к главе 3).

Некоторое представление о приёмах сокращения количества неизвестных дают упражнения 8.1–8.8.

Приведённая в § 8.2 универсальная граница экспоненциального ранга была получена в работе Матиясевича [1979]. Более того, там было установлено существование однократных экспоненциально диофантовых представлений с 3 неизвестными. Этот результат был усилен в работе Джонса и Матиясевича [1982б] до унарных однократных представлений (см. упражнение 8.10).

Немного общих результатов известно про диофантовы множества с малым (экспоненциальным) рангом. Очевидна разрешимость множеств, диофантов ранг которых равен 1. В работе Левица [1985] установлена разрешимость множеств, унарный (с основанием 2) экспоненциальный ранг которых равен 1. В работе Р. М. Робинсона [1951] описана структура множеств, задаваемых арифметическими формулами с одним квантором (общности или существования). Эти результаты были далее развиты в работе Тунга [1988].

Как сказано в комментариях к главе 1, универсальная граница $d=4$ порядка диофантовых множеств была получена задолго до развёртывания систе-

матических исследований класса диофантовых множеств и она не может быть улучшена более, чем на 1. Вопрос о том, является ли $d = 3$ универсальной границей порядка, сформулирован как нерешённая проблема 1.1.

Нерешённая проблема 8.1 была поставлена в докладе Адлемана и Мандерса [1976] (см. также работу Мандерса и Адлемана [1978]). Они ввели понятие *недетерминированной диофантовой машины*. Каждая такая машина задаётся некоторым параметрическим диофантовым уравнением

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

и работает следующим образом: получив входные данные — значения параметров $a_1, \ldots, a_n$, машина «угадывает» значения $x_1, \ldots, x_m$ (в этом и состоит недетерминированность) и выдаёт ответ «ДА» или «НЕТ» в соответствии с тем, выполнено ли равенство (1). С помощью техники главы 5 можно легко показать, что недетерминированные диофантовы машины имеют ту же вычислительную силу, что и *недетерминированные машины Тьюринга*, т. е. машины, которые могут иметь несколько инструкций с одинаковыми левыми частями и каждый раз «угадывают», какую именно инструкцию использовать. В проблеме 8.1 ставится вопрос о сравнении недетерминированных машин Тьюринга и диофантовых машин по «быстродействию». В случае положительного решения проблемы 8.1 мы имели бы новую теоретико-числовую характеризацию класса **NP**, который вызывает сейчас большой интерес у исследователей. В докладе Адлемана и Мандерса [1976] (см. также работу Мандерса и Адлемана [1978]) сообщается о частичном продвижении в этом направлении. В работах Кента и Ходжсона [1982], Юкны [1982а, 1982б] и Ходжсона и Кента [1983] класс **NP** характеризуется через арифметические представления с ограниченными кванторами общности.

В работе Виноградова и Косовского [1975] показано, что, ограничивая величину неизвестных в диофантовых представлениях, можно получить известную иерархию Гжегорчика.

Глава 9
МАССОВЫЕ ПРОБЛЕМЫ МАТЕМАТИЧЕСКОГО АНАЛИЗА

В этой главе будут рассмотрены массовые проблемы, связанные с континуумом вещественных чисел $\mathbb{R}$. Строчные курсивные латинские буквы попрежнему будут обозначать натуральные числа; для обозначения вещественных чисел будут использоваться строчные греческие буквы.

§ 9.1. Диофантово вещественные числа

Массовые проблемы не типичны для традиционного курса математического анализа. Это объясняется, по-видимому, тем, что основополагающим объектом изучения там является континуум вещественных чисел $\mathbb{R}$. Вещественное же число, при любом традиционном определении, требует для своего задания, вообще говоря, бесконечного объёма информации, в то время как каждая индивидуальная подпроблема из составляющих какую-либо массовую проблему должна, как говорилось в § 1.1, специфицироваться конечным объёмом информации. Конечность исходной информации обусловлена тем, что мы хотим получить ответ за конечное число элементарных шагов. Например, бессодержательно ставить задачу следующим образом: в исходный момент вся бесконечная лента машины Тьюринга заполнена десятичной записью некоторого вещественного числа; машина должна за конечное число шагов узнать, является ли это число рациональным.

Таким образом, если мы хотим, чтобы индивидуальные подпроблемы специфицировались вещественными параметрами, мы должны использовать какой-то способ задания вещественных чисел посредством конечной информации. Один такой способ был предложен А. М. Тьюрингом и связан, естественно, с машиной Тьюринга. А именно, вещественное число μ может задаваться машиной Тьюринга, которая работает неограниченно долго, выписывая все больше и больше цифр числа μ. Сама машина Тьюринга при этом задаётся, как обычно, конечным набором инструкций. Таким образом, можно ставить вопрос о распознавании *по набору инструкций* машины, задаёт ли она рациональное вещественное число или нет.

Оставаясь в языке диофантовых уравнений, мы можем определить *диофантово вещественное число* как диофантово уравне-

ние

$$D(a,b,c,d,x_1,\ldots,x_m)=0 \tag{1}$$

с четырьмя параметрами, обладающее следующими двумя свойствами:

для любого натурального числа d существуют натуральные числа a_d, b_d, c_d, такие что уравнение

$$D(a_d,b_d,c_d,d,x_1,\ldots,x_m)=0 \tag{2}$$

разрешимо относительно $x_1,\ldots,x_m$;

если

$$D(a',b',c',d',x'_1,\ldots,x'_m)=0 \tag{3}$$

и

$$D(a'',b'',c'',d'',x''_1,\ldots,x''_m)=0, \tag{4}$$

то

$$\frac{a'-b'}{c'+1}-\frac{a''-b''}{c''+1}\le\frac{1}{d'+1}+\frac{1}{d''+1}. \tag{5}$$

Полагая последовательно $d=0,1,\ldots$, мы можем найти натуральные числа a_0, b_0, c_0, a_1, b_1, $c_1,\ldots$, для которых разрешимо уравнение (2), и рассмотреть последовательность рациональных чисел

$$\frac{a_0-b_0}{c_0+1},\ \frac{a_1-b_1}{c_1+1},\ \ldots. \tag{6}$$

Согласно (5) эта последовательность сходится в себе и тем самым сходится к некоторому вещественному числу α. Опять-таки благодаря (5), это число не зависит от конкретного выбора a_d, b_d и c_d, и потому можно говорить, что α — вещественное число, определяемое уравнением (1).

Нетрудно установить, что все вещественные алгебраические числа определяются диофантово вещественными числами (см. упражнение 9.1). Используя технику главы 3 для работы с кортежами произвольной длины и технику главы 6 для устранения ограниченных кванторов, можно построить диофантово вещественные числа, определяющие классические константы математического анализа, — число π, основание натуральных логарифмов и т. п. (см. упражнения 9.2–9.4).

На множестве диофантово вещественных чисел нетрудно ввести арифметические операции. Например, суммой диофантово

вещественных чисел

$$D_1(a,b,c,d,x_1,\ldots,x_m)=0 \tag{7}$$

и

$$D_2(a,b,c,d,x_1,\ldots,x_m)=0 \tag{8}$$

является, как легко проверить, диофантово вещественное число

$$D_1^2(p_1,q_1,r_1,2d+1,x_1,\ldots,x_m)+D_2^2(p_2,q_2,r_2,2d+1,y_1,\ldots,y_m)+$$
$$+((r_2+1)p_1+(r_1+1)p_2-a)^2+((r_2+1)q_1+(r_1+1)q_2-b)^2+$$
$$+((r_1+1)(r_2+1)-c)^2=0 \tag{9}$$

(мы рассматриваем (9) как уравнение с параметрами a, b, c и неизвестными p_1, p_2, q_1, q_2, r_1, r_2, $x_1,\ldots,x_m$, $y_1,\ldots,y_m$). Зафиксировав какой-либо универсальный полином, мы можем перенумеровать все диофантово вещественные числа. Можно проверить, что при этом арифметическим операциям на множестве диофантово вещественных чисел соответствуют диофантовы функции на множестве номеров диофантово вещественных чисел, например, диофантовой является функция, которая по кодам уравнений (7) и (8) даёт код уравнения (9). В этом направлении можно пойти дальше и установить диофантовость функций, соответствующих квадратному корню, логарифму, синусу и другим элементарным функциям.

Итак, теперь у нас есть возможность ставить массовые проблемы, содержащие вещественные числа в спецификации индивидуальных подпроблем. Оказывается, что алгоритмически неразрешимыми являются уже простейшие проблемы.

Так, неразрешимо свойство *быть диофантово вещественным числом*, ибо уравнение

$$(a+b)D(x_1,\ldots,x_m)=0 \tag{10}$$

является диофантово вещественным числом в том и только том случае, когда уравнение

$$D(x_1,\ldots,x_m)=0 \tag{11}$$

не имеет решений. Эту трудность мы обойдём, позволив алгоритмам, разрешающим массовые проблемы, связанные с вещественными числами, давать произвольный ответ или не давать ответа вообще в случае, когда поступившие на вход числа не являются кодами диофантово вещественных чисел.

Даже при такой свободе поведения на «неправильных» исходных данных оказывается неразрешимой проблема равенства диофантово вещественного числа нулю. Действительно, пусть

дано некоторое диофантово уравнение (11). Формула

$$a=1\ \&\ b=0\ \&$$
$$\&\ \forall y_{<c}\exists x_1\ldots x_m[y=\mathbf{Cantor}_m(x_1,\ldots,x_m)\ \&\ D(x_1,\ldots,x_m)\neq 0]\ \&$$
$$\&\ [c=d\ \vee\ \exists x_1,\ldots,x_m[c=\mathbf{Cantor}_m(x_1,\ldots,x_m)\ \&\ D(x_1,\ldots,x_m)=0]] \qquad (12)$$

может быть преобразована в эквивалентное диофантово уравнение, которое, как нетрудно проверить, всегда будет диофантово вещественным числом, причём это число будет равно 0 в том и только том случае, когда уравнение (11) не имеет решений.

Таким образом, мы видим, что хотя некоторые вещественные числа можно задавать конечным объёмом информации — диофантово вещественными числами, вещественное число остаётся сложным объектом с алгоритмической точки зрения. Многие массовые проблемы математического анализа оказываются неразрешимыми именно из-за алгоритмической сложности вещественных чисел, специфицирующих индивидуальные проблемы. Существуют, однако, и алгоритмически неразрешимые проблемы, касающиеся свойств вещественных чисел, но не требующие задания вещественных чисел для спецификации индивидуальных проблем. Именно такие проблемы и будут рассмотрены в последующих параграфах.

§ 9.2. Уравнения, неравенства и тождества с вещественными переменными

Естественно начать с аналога 10-й проблемы Гильберта для вещественных неизвестных, т. е. с рассмотрения уравнений вида

$$D(x_1,\ldots,x_m)=0, \qquad (1)$$

где D — полином с целыми коэффициентами, а $x_1,\ldots,x_m$ — вещественные неизвестные. В отличие от случая диофантовых уравнений, существует способ узнать, есть ли у (1) вещественные решения или нет. Для $m=1$ такой способ дает известный *метод Штурма*; далеко идущее обобщение этого метода, найденное А. Тарским, позволяет работать с любым количеством неизвестных.

Таким образом, если мы хотим устанавливать алгоритмическую неразрешимость уравнений в вещественных числах, то должны разрешить использовать при построении уравнений наряду со сложением, вычитанием и умножением и какие-то другие функции. Простейший способ получить неразрешимость — это добавить функцию **sin**. *Пусть $\mathcal{F}_0$ обозначает класс функций от многих вещественных переменных, которые можно построить при помощи суперпозиции из константы* 1, *операций сложения, вычитания, умножения и функции* **sin**. *Не существует способа распо-*

знавать по произвольной функции Φ из $\mathcal{F}_0$, разрешимо ли в вещественных неизвестных уравнение

$$\Phi(x_1,\ldots,x_k)=0. \tag{2}$$

Для доказательства этого факта возьмём произвольное диофантово уравнение

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

и преобразуем его в следующее уравнение типа (2):

$$D^2(x_1^2,\ldots,x_m^2)+\sin^2(3+\psi^2)+(7\psi^2+\omega^2-1)^2+$$
$$+\sin^2((3+\psi^2)x_1^2)+\ldots+\sin^2((3+\psi^2)x_m^2)=0. \tag{4}$$

Очевидно, что любое решение уравнения (3) в натуральных $x_1,\ldots,x_m$ порождает решение уравнения (4) в вещественных ω, ψ, $x_1,\ldots,x_m$ — достаточно положить

$$\psi=\mathbf{sqrt}(\pi-3),\ \omega=\mathbf{sqrt}(22-7\pi),\ x_i=\mathbf{sqrt}(x_i). \tag{5}$$

С другой стороны, в любом решении (4) в вещественных ω, ψ, $x_1,\ldots,x_m$ всегда $3+\psi^2=\pi$, и потому $x_1^2,\ldots,x_m^2$ — натуральные числа, образующие решение (3). Таким образом, алгоритмическая неразрешимость 10-й проблемы Гильберта влечёт алгоритмическую неразрешимость уравнений вида (2) в вещественных числах.

Для того, чтобы получить алгоритмическую неразрешимость диофантовых уравнений, мы должны были рассматривать уравнения с достаточно большим количеством неизвестных. Переход от (3) к (4) увеличивает количество неизвестных ещё на 2. Тем не менее мы сможем усилить предыдущий результат, заменив $\mathcal{F}_0$ на его собственное подмножество $\mathcal{F}_1$, состоящее из функций одной переменной.

Для этой цели нам полезно было бы иметь вещественный аналог функции $\mathbf{Cantor}_k$, введённой в § 3.1, точнее, вещественные аналоги обратных функций $\mathbf{Elem}_{k,1},\ldots,\mathbf{Elem}_{k,k}$. Действительно, допустим, что мы нашли функции $E_1,\ldots,E_k$ из $\mathcal{F}_1$ такие, что для любых вещественных $x_1,\ldots,x_k$ существует вещественное η такое, что

$$E_1(\eta)=x_1,\ \ldots,\ E_k(\eta)=x_k. \tag{6}$$

В таком случае вопрос о разрешимости уравнения (2) свёлся бы к вопросу о разрешимости уравнения

$$\Phi(E_1(\eta),\ldots,E_k(\eta))=0 \tag{7}$$

с одной неизвестной η.

К сожалению, таких функций $E_1,\ldots,E_k$ в классе $\mathcal{F}_1$ нет. Тем не менее с помощью функций из $\mathcal{F}_1$ мы можем отобразить $\mathbb{R}$ на всюду плотное подмножество $\mathbb{R}^k$, и этого окажется достаточно для наших целей.

Рассмотрим функции

$$\mathbf{E}(\eta) = \eta\sin(\eta), \tag{8}$$

$$\mathbf{H}(\eta) = \eta\sin(\eta^3) \tag{9}$$

и проверим, что *для любых вещественных* χ, ψ *и положительного* ε *найдется такое* η, *что*

$$|\mathbf{E}(\eta)-\chi| < \varepsilon, \tag{10}$$

$$\mathbf{H}(\eta) = \psi. \tag{11}$$

Будем искать такое η в интервале

$$[2k\pi-\pi/2,\ 2k\pi+\pi/2], \tag{12}$$

где k — большое число. Когда η пробегает весь интервал (12), $\sin(\eta)$ меняется от -1 до 1, а $\mathbf{E}(\eta)$ меняется от $-2k\pi+\pi/2$ до $2k\pi+\pi/2$. Следовательно, если

$$k > |\chi|+1, \tag{13}$$

то в интервале (12) найдётся такое η_0, что

$$\mathbf{E}(\eta_0) = \chi. \tag{14}$$

Найдём положительное δ такое, что для любого η из интервала

$$[\eta_0-\delta,\ \eta_0+\delta] \tag{15}$$

справедливо требуемое неравенство (10). Очевидно, что

$$|\mathbf{E}(\eta)-\chi| = |\mathbf{E}(\eta)-\mathbf{E}(\eta_0)| = \mathbf{E}'(\bar{\eta})\delta = (\sin(\bar{\eta})+\bar{\eta}\cos(\bar{\eta}))\delta, \tag{16}$$

где $\bar{\eta}$ также лежит в интервале (15), и потому

$$|\mathbf{E}(\eta)-\chi| \le (1+\eta_0+\delta)\delta. \tag{17}$$

Не ограничивая общности, будем считать, что $\varepsilon < 1$, и положим

$$\delta = \frac{\varepsilon}{2k\pi+3}. \tag{18}$$

Когда η пробегает интервал (15), η^3 пробегает интервал

$$[(\eta_0-\delta)^3,\ (\eta_0+\delta)^3], \tag{19}$$

ширина которого легко оценивается снизу:

$$(\eta_0+\delta)^3-(\eta_0-\delta)^3 = 6\eta_0^2\delta+2\delta^3 > \frac{6(2k\pi-\pi/2)^2}{2k\pi+3}. \tag{20}$$

При достаточно большом k ширина интервала (19) больше 2π, и потому, когда η пробегает интервал (15), $\sin(\eta^3)$ меняется от -1 до 1, а диапазон изменения $\mathbf{H}(\eta)$ не у́же чем $[-\eta_0+\delta, \eta_0-\delta]$. Таким образом, при достаточно большом k в интервале (15) найдётся η, удовлетворяющее (11) и, по выбору этого интервала, (10).

Теперь мы можем ввести функции, являющиеся, в каком-то смысле, аналогами функций $\mathbf{Elem}_{k,n}$:

$$\mathbf{E}_k(\eta)=\mathbf{E}(\underbrace{\mathbf{H}(\ldots\mathbf{H}}_{(k-1)\text{ раз}}(\eta)\ \ldots)). \tag{21}$$

Индукцией по k легко можно показать, что *для любых вещественных* $x_1,\ldots,x_k$ *и положительного* ε *найдётся такое* η, *что*

$$|\mathbf{E}_i(\eta)-x_i|<\varepsilon,\quad i=1,\ldots,k. \tag{22}$$

Мы не можем непосредственно использовать функции $\mathbf{E}_1,\ldots,\mathbf{E}_k$ в роли функций $E_1,\ldots,E_k$ для перехода от произвольного уравнения (2) к (7) и должны будем воспользоваться специфическими свойствами уравнения (3). Прежде всего, мы заменим его на неравенство

$$M^2(x_1^2,\ldots,x_m^2)[D^2(x_1^2,\ldots,x_m^2)+\sin^2(3+\psi^2)+(7\psi^2+\omega^2-1)^2+$$

$$+\sin^2((3+\psi^2)x_1^2)+\ldots+\sin^2((3+\psi^2)x_m^2)]<1, \tag{23}$$

где M — некоторый никогда не обращающийся в ноль полином, выбор которого будет описан ниже. Очевидно, что числа $x_1,\ldots,x_m$, ψ и ω, определёные посредством (5), где $x_1,\ldots,x_m$ — решение уравнения (3), удовлетворяют неравенству (23). Наша задача — выбрать полином M так, чтобы для любого решения неравенства (23) числа

$$x_i=\lceil x_i^2\rfloor \tag{24}$$

давали решение уравнения (3) ($\lceil\alpha\rfloor$ обозначает целое число, ближайшее к α).

Пусть неравенство (23) выполнено. Для краткости положим $\mu=M(x_1,\ldots,x_m)$, $\varphi=3+\psi^2$. Полином M будет выбран так, что

$$\mu>6. \tag{25}$$

Из (23) и (25) следует, что

$$7\psi^2+\omega^2-1<1/6 \tag{26}$$

и, следовательно, φ лежит в интервале

$$[3,\ 3\tfrac{1}{6}]. \tag{27}$$

Далее из (23) получаем, что

$$\mu^{-1}>|\sin(\varphi)|=|\sin(\varphi)-\sin(\pi)|=|\cos(\bar\varphi)(\varphi-\pi)|, \tag{28}$$

где $\bar\varphi$ также принадлежит (27), и потому $|\cos(\bar\varphi)|>0{,}5$, а следовательно,

$$|\varphi-\pi|<2/\mu. \tag{29}$$

Аналогично из (23) получаем, что

$$|\sin(\varphi x_i^2)|<1/6, \tag{30}$$

и потому φx_i^2 лежит в некотором интервале вида

$$[\pi(k_i-1/6),\ \pi(k_i+\tfrac{\pi}{6})]; \tag{31}$$

более того,

$$|\varphi x_i^2-\pi k_i| < \frac{2}{\mu}\ . \tag{32}$$

Из (29) и (32) получаем, что

$$|x_i^2-k_i| = \left|\frac{\pi-\varphi}{\pi}x_i^2 - \frac{\varphi x_i^2-\pi k_i}{\pi}\right| < \frac{x_i^2+1}{\mu}. \tag{33}$$

Таким образом, $k_i = x_i$, и мы можем теперь оценить левую часть :

$$|D(x_1,\dots,x_m)| \le |D(x_1^2,\dots,x_m^2)| + |D(x_1,\dots,x_m)-D(x_1^2,\dots,x_m^2)| \le$$

$$\le \frac{1}{\mu} + \sum_{i=1}^{m}\left|\frac{\partial D}{\partial x_i}\right| |x_i^2-x_i| \le \frac{1}{\mu}\left(1+\sum_{i=1}^{m}\left|\frac{\partial D}{\partial x_i}\right|(x_i^2+1)\right). \tag{34}$$

Поскольку D — полином, то полиномами являются и все его частные производные, и мы можем выбрать полином M столь большим, что будет выполнено (25), а из (34) будет следовать, что

$$|D(x_1,\dots,x_m)| < 1, \tag{35}$$

и потому справедливо равенство (3).

Заменим теперь в (23) x_i на $\mathbf{E}_i(\eta)$, φ на $\mathbf{E}_{m+1}(\eta)$ и ω на $\mathbf{E}_{m+2}(\eta)$. Мы получим неравенство вида

$$\Psi(\eta) < 1, \tag{36}$$

где $\Psi \in \mathcal{F}_1$, причём, как нетрудно понять, это неравенство выполняется для какого-либо η в том и только том случае, когда неравенство (23) выполняется для каких-то $x_1,\dots,x_m$, φ и ω, т. е. в том и только том случае, когда имеет решение уравнение (3). Таким образом, мы установили, что *не существует способа распознавать по произвольной функции* Φ *из* $\mathcal{F}_1$ *выполнимость неравенства*

$$\Phi(\eta) < 0 \tag{37}$$

при каком-то η.

Для получения уравнения (а не неравенства) заметим, что если (3) имеет решение, то $\Psi(\eta)$ может быть сделано сколь угодно близким к 0 за счёт выбора такого η, при котором $\mathbf{E}_1^2(\eta),\dots,\mathbf{E}_m^2(\eta)$, $\mathbf{E}_{m+1}^2(\eta)$ и $\mathbf{E}_{m+2}^2(\eta)$ достаточно близки соответственно к $x_1,\dots,x_m$, $\pi-3$ и $22-7\pi$. С другой стороны,

$\Phi_1(\eta)$ всегда может быть сделано сколь угодно большим, например, за счёт выбора такого η, при котором $\mathbf{E}_{m+2}(\eta)$ велико. Таким образом, уравнение (3) имеет решение тогда и только тогда, когда имеет решение уравнение

$$2\Phi(\eta)=1. \tag{38}$$

Это доказывает, что *не существует способа распознавать по произвольной функции* Φ *из* $\mathcal{F}_1$ *разрешимость уравнения*

$$\Phi(\eta)=0. \tag{39}$$

Расширим класс рассматриваемых функций. *Пусть* $\mathcal{F}_2$ *обозначает класс одноместных функций, которые можно построить при помощи суперпозиции из константы* 1, *операций сложения, вычитания, умножения и функций* **sin** *и* **abs** (абсолютной величины). *Не существует способа распознавать по произвольной функции* Φ *из* $\mathcal{F}_2$, *является ли равенство*

$$\Phi(\eta)=0 \tag{40}$$

тождеством. Чтобы убедиться в этом, достаточно заметить, что равенство

$$1-\Phi(\eta)+|1-\Phi(\eta)|=0 \tag{41}$$

выполнено для всех η тогда и только тогда, когда для всех η неравенство (36) *не* выполнено.

§ 9.3. Системы обыкновенных дифференциальных уравнений

Как было сказано в предыдущем параграфе, если рассмотреть дословный аналог 10-й проблемы Гильберта для случая вещественных неизвестных, т. е. вопрос о наличии вещественных решений полиномиальных уравнений с целыми коэффициентами, то алгоритмическая неразрешимость не возникает. Для достижения алгоритмической неразрешимости в предыдущем параграфе класс рассматриваемых уравнений был расширен за счёт разрешения использовать при построении уравнений функцию **sin** в явном виде. В этом параграфе мы будем рассматривать только полиномиальные уравнения, но зато это будут обыкновенные дифференциальные уравнения, точнее, системы таких уравнений. Таким образом, неизвестными у нас будут не вещественные числа, а вещественные дифференцируемые функции независимой переменной τ, пробегающей, для определенности, интервал $[0,1]$.

Для моделирования вещественных неизвестных мы будем использовать постоянные функции, т. е. функции, удовлетворяющие дифференциальному уравнению

$$X'(\tau)=0. \tag{1}$$

Как нетрудно проверить, в любом решении системы

$$\Pi'(\tau)=0, \quad \Xi''(\tau)+\Pi^2(\tau)\Xi(\tau)=0 \tag{2}$$

с граничными условиями

$$0\le\Pi(0)\le 4, \quad \Xi(0)=0, \quad \Xi(1)=0, \quad \Xi'(0)=1 \tag{3}$$

$\Pi(\tau)$ будет тождественно равно π, а $\Xi(\tau)=\sin(\pi\tau)/\pi$. Соответственно в любом решении системы

$$X'(\tau)=0, \quad \Phi''(\tau)+\Pi^2(\tau)X^2(\tau)\Phi(\tau)=0 \tag{4}$$

с граничными условиями

$$0\le X(0), \quad \Phi(0)=\Phi(1)=0, \quad \Phi'(0)=1 \tag{5}$$

$X(\tau)$ будет тождественно равно некоторому натуральному числу x, а $\Phi(\tau)=\sin(\pi x\tau)/\pi x$.

Таким образом, диофантово уравнение

$$D(x_1,\dots,x_m)=0 \tag{6}$$

имеет решение в натуральных $x_1,\dots,x_m$ тогда и только тогда, когда система дифференциальных уравнений

$$\begin{gathered}
\Pi'(\tau)=0,\\
\Xi''(\tau)+\Pi^2(\tau)\Xi(\tau)=0,\\
X_1'(\tau)=0,\\
\Phi_1''(\tau)+\Pi^2(\tau)X^2(\tau)\Phi_1(\tau)=0,\\
\dots\dots\dots\dots\dots\dots\dots\dots\\
X_m'(\tau)=0,\\
\Phi_m''(\tau)+\Pi^2(\tau)X^2(\tau)\Phi_m(\tau)=0,\\
D(X_1(\tau),\dots,X_m(\tau))=0
\end{gathered} \tag{7}$$

имеет на $[0,1]$ решение, удовлетворяющее краевым условиям

$$\begin{gathered}
0\le\Pi(0)\le 4,\\
\Xi(0)=\Xi(1)=0, \quad \Xi'(0)=1,\\
\Phi_1(0)=\Phi_1(1)=0, \quad \Phi_1'(0)=1,\\
\dots\dots\dots\dots\dots\dots\dots\dots\\
\Phi_m(0)=\Phi_m(1)=0, \quad \Phi_m'(0)=1,\\
X_1(0)\ge 0,\dots,X_m(0)\ge 0.
\end{gathered} \tag{8}$$

Вводя новые неизвестные функции, мы легко можем заменить все эти краевые условия на дополнительные уравнения. А именно, условие типа

$$\Phi(0)\ge 0 \tag{9}$$

может быть заменено на

$$\Phi(\tau)=Z^2(\tau), \tag{10}$$

поскольку условия типа (9) накладывались только на функции, удовлетворяющие уравнению $\Phi'(\tau)=0$; условие типа

$$\Phi(\alpha)=\beta, \tag{11}$$

где α и β — константы, может быть заменено на уравнение

$$\Phi(\alpha)-\beta=(\tau-\alpha)Z(\tau). \tag{12}$$

Уравнения, содержащие Φ'', можно стандартным способом заменить на систему из двух уравнений первого порядка относительно Φ' и дополнительной функции Z. Таким образом, вопрос о существовании натуральных решений у диофантова уравнения может быть сведён к вопросу о существовании решения некоторой системы полиномиальных дифференциальных уравнений первого порядка, следовательно, *не существует способа распознавать по произвольной системе дифференциальных уравнений вида*

$$\begin{gathered} P_1(\tau,X_1(\tau),\ldots,X_k(\tau),X_1'(\tau))=0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ P_k(\tau,X_1(\tau),\ldots,X_k(\tau),X_k'(\tau))=0, \end{gathered} \tag{13}$$

где $P_1,\ldots,P_k$ — полиномы с целыми коэффициентами, имеет ли эта система решение на интервале $[0,1]$.

Нетрудно проследить, что если система (13) была построена описанным выше способом по диофантову уравнению (6), имеющему решение, то она имеет решение, в котором не все функции $X_1,\ldots,X_k$ тождественно равны нулю. Следовательно, система

$$\begin{gathered} Q_1(\tau,X_1(\tau),\ldots,X_k(\tau),X_1'(\tau))=0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ Q_k(\tau,X_1(\tau),\ldots,X_k(\tau),X_k'(\tau))=0, \end{gathered} \tag{14}$$

где

$$Q_j(\tau,x_1,\ldots,x_k,\eta)=(x_1^2+\ldots+x_k^2)P_j(\tau,x_1,\ldots,x_k,\eta), \tag{15}$$

имеет единственное решение $X_1(\tau)=\ldots=X_k(\tau)=0$ тогда и только тогда, когда исходное диофантово уравнение (6) решений не имеет. Таким образом, *не существует способа распознавать по произвольной системе дифференциальных уравнений вида* (13), *имеет ли она ровно одно решение на* $[0,1]$.

§ 9.4. Интегрируемость

В этом параграфе мы установим алгоритмическую неразрешимость двух массовых проблем, одна из которых связана с определёнными интегралами, другая — с неопределёнными.

В § 9.2 был указан способ построения по произвольному диофантову уравнению (2.3) функции Φ из класса $\mathcal{F}_1$ такой, что:

1) если уравнение (2.3) имеет решение, то для некоторого η_0

$$\Phi(\eta_0)=0,5; \tag{1}$$

2) если уравнение (2.3) не имеет решений, то для всех η

$$\Phi(\eta)\geq 1. \tag{2}$$

Рассмотрим интеграл

$$\int_{-\infty}^{+\infty}\frac{d\eta}{(\eta^2+1)(2\Phi(\eta)-1)^2}. \tag{3}$$

Из указанных выше свойств функции Φ следует, что этот интеграл сходится в том и только том случае, когда уравнение (2.3) решений не имеет. Подинтегральная функция в (3) не принадлежит классу $\mathcal{F}_1$, так что нам придётся расширить этот класс. *Пусть $\mathcal{F}_3$ обозначает класс функций одной вещественной переменной, которые можно построить при помощи суперпозиции из константы* 1, *операций сложения, вычитания, умножения, деления и функции* sin. *Не существует способа распознать по произвольной функции Φ из $\mathcal{F}_3$, сходится ли интеграл*

$$\int_{-\infty}^{+\infty}\Phi(\eta)d\eta. \tag{4}$$

Проблема нахождения неопределённого интеграла, которую мы сейчас рассмотрим, будет связана не с одним, а с двумя классами $\mathcal{F}_4$ и $\mathcal{F}_5$ функций одного аргумента. *Пусть Φ — функция из $\mathcal{F}_4$; существует ли в классе $\mathcal{F}_5$ функция I такая, что для всех η $\Phi(\eta)=I'(\eta)$?* Для того чтобы ответ не был всегда утвердительным, мы должны иметь в $\mathcal{F}_4$ по крайней мере одну функцию, не имеющую первообразной из $\mathcal{F}_5$. Для доказательства нам потребуется более сильное свойство классов $\mathcal{F}_4$ и $\mathcal{F}_5$, а именно, мы будем предполагать, что *в $\mathcal{F}_4$ есть всюду определённая функция H, такая, что ни для какого непустого интервала $[a,b]$ в классе $\mathcal{F}_5$ нет функции I такой, что $H(\eta)=I'(\eta)$ для η из $[a,b]$*. Примером такой функции может служить функция e^{x^2}, первообразная которой ни на каком интервале не представима в виде суперпозиции элементарных функций.

Мы будем также предполагать, что *класс $\mathcal{F}_4$ содержит класс $\mathcal{F}_2$ и замкнут относительно умножения*. В частности, класс $\mathcal{F}_4$ должен содержать функцию

$$M(\eta)=\begin{cases}2, & \text{если } \eta\leq 0,75,\\ 8-8\eta, & \text{если } 0,75\leq\eta\leq 1,\\ 0, & \text{если } 1\leq\eta,\end{cases} \tag{5}$$

ибо

$$M(\eta)=1+|4\eta-4|-|4\eta-3|. \tag{6}$$

Рассмотрим функцию

$$T(\eta) = M(\Phi(\eta))H(\eta). \tag{7}$$

Если уравнение (2.3) не имеет решений, то согласно (2) и (5) $T(\eta)=0$ для любого η, и потому T имеет в качестве первообразной любую константу. Если же уравнение (2.3) имеет решение, то согласно (1) и (5) в некоторой окрестности η_0 $T(\eta)=2H(\eta)$ и, следовательно, T не имеет первообразной. Таким образом, *при сделанных выше предположениях о классах $\mathcal{F}_4$ и $\mathcal{F}_5$ не существует способа по произвольной функции из $\mathcal{F}_4$ распознать, имеет ли она первообразную из класса $\mathcal{F}_5$.*

Упражнения

9.1. Покажите, что диофантово вещественными являются все вещественные алгебраические числа.

9.2. Покажите, что если A, B, C и E — диофантовы функции, определённые на всех натуральных числах, причём для всех n

$$|S(E(n))| < n^{-1},$$

где

$$S(m) = \sum_{k=m}^{\infty} \frac{A(k)-B(k)}{C(k)+1},$$

то $S(0)$ является диофантово вещественным числом.

9.3. Покажите, что числа e и π являются диофантово вещественными.

9.4. Перенесите результаты § 9.3 на случай одного уравнения в частных производных.

Комментарии

Первоначально А. М. Тьюринг [1936] определил вычислимое вещественное число как число, позиционную запись которого выписывает на своей ленте некоторая машина Тьюринга. Это понятие оказалось не вполне удачным — по двум машинам, задающим два вычислимых вещественных числа, нельзя было построить машину, вычисляющую сумму. Вскоре А. М. Тьюринг [1937] устранил этот недостаток, перейдя к системе с дробным основанием и отказавшись от однозначного соответствия между вещественными числами и их позиционными представлениями. Введённое в § 9.1 понятие диофантово вещественного числа эквивалентно модифицированному таким образом понятию вычислимого числа.

Математику, получившему традиционное образование, счётное множество диофантово вещественных чисел представляется слишком бедным. Тем не менее таких чисел вполне достаточно для построения содержательной теории (см., например, монографию Мартин-Лёфа [1975]).

Содержание § 9.2–9.4 основано на работах Ричардсона [1968], Адлера [1969а], Кавинеса [1970] и Ванга [1974]. Первые три работы были написаны до того, как была установлена алгоритмическая неразрешимость 10-й проблемы Гильберта. По этой причине в первых двух работах в качестве исходного был взят более слабый результат об алгоритмической неразрешимости экспоненциально диофантовых уравнений, и соответственно возведение в степень использовалось при построении функций. В третьей работе результаты были получены в условной форме — в предположении неразрешимости 10-й проблемы Гильберта.

Алгоритмическая неразрешимость ряда других массовых проблем математического анализа была установлена на основе алгоритмической неразрешимости (экспонеицциально) диофантовых уравнений в работах Денефа и Липшица [1984, 1989], Зингера [1978], Папаса [1985], Пензина [1978], Скарпеллини [1963].

Алгоритмическая неразрешимость многих массовых проблем, связанных с вещественными числами, накладывает принципиальные ограничения на возможности систем аналитических вычислений, ставших в последнее время рабочим инструментом математиков. Эти трудности обсуждаются в работах Бартона и Фича [1972а, 1972б], Макгетрика [1977], Мозеса [1971] и Фича [1973].

Глава 10

ДРУГИЕ ПРИЛОЖЕНИЯ ДИОФАНТОВЫХ ПРЕДСТАВЛЕНИЙ

Тематически разнородные результаты, включённые в эту главу, объединяет только то, что их нетрудно доказать, используя диофантовость полуразрешимых множеств.

§ 10.1. Диофантовы игры

Пусть имеется некоторое диофантово уравнение

$$D(a_1,\ldots,a_m,b_1,\ldots,b_m)=0, \tag{1}$$

в котором переменные разбиты на две группы; не ограничивая общности, мы считаем, что количество переменных в обеих группах одинаково, хотя фактически полином D может и не зависеть от каких-то переменных. Каждое такое уравнение задаёт *диофантову игру* двух лиц A и B со следующими правилами:

на первом ходу A *выбирает значение* a_1;

на втором ходу B *выбирает значение* b_1;

.....

.....

на $(2m-1)$*-м ходу* A *выбирает значение* a_m;

на $2m$*-м ходу* B *выбирает значение* b_m;

если выбранные значения $a_1,\ldots,a_m$, $b_1,\ldots,b_m$ *удовлетворяют* (1), *то победителем объявляется игрок* B, *в противном случае — игрок* A.

Каждая диофантова игра является конечной антагонистической детерминированной игрой с полной информацией, и потому один из игроков имеет *выигрышную стратегию*, т. е. при «правильной» игре победа ему «обеспечена» независимо от ходов противника. Легко понять, что B имеет выигрышную стратегию в том и только том случае, когда справедливо утверждение

$$\forall a_1\exists b_1\forall a_2\exists b_2\ldots\forall a_m\exists b_m[D(a_1,\ldots,a_m,b_1,\ldots,b_m)=0]. \tag{2}$$

Например, для игры, задаваемой уравнением

$$(b_1+a_2)^2+1=(b_2+2)(b_3+2), \tag{3}$$

игрок A имеет выигрышную стратегию в том и только том слу-

чае, когда существует бесконечно много простых чисел вида k^2+1. Хотя эта проблема давно привлекала специалистов по теории чисел, мы до сих пор (1990г.) не знаем, кто же из игроков, A или B, имеет выигрышную стратегию в игре, задаваемой таким простым уравнением, как (3).

Легко понять, что проблема определения по произвольному уравнению (1) игрока с выигрышной стратегией алгоритмически неразрешима, даже если мы ограничимся вырожденными играми, в которых полином D не зависит от $a_1,\ldots,a_m$. В этой связи представляют интерес сложностные вопросы, например, при сколь малом m нельзя алгоритмически определить игрока с выигрышной стратегией.

Алгоритмические трудности могут возникать и в тех играх, для которых известно, у какого игрока есть выигрышная стратегия. Рассмотрим сначала случай, когда выигрышную стратегию имеет игрок A. Для того чтобы фактически выиграть, A должен сначала «правильно» выбрать a_1, затем, зная b_1, «правильно» выбрать a_2 и т.д. Выберем в качестве D полином, задающий какое-либо диофантово множество $\mathfrak{D}$ натуральных чисел с недиофантовым дополнением:

$$a_1\in\mathfrak{D}\Leftrightarrow\exists x_1\ldots x_m[D(a_1,\ldots,a_m,x_1,\ldots,x_m)=0] \tag{4}$$

(зависимость D от $a_2,\ldots,a_m$ фиктивна; примеры таких множеств были построены в § 4.6 и § 6.6). Ясно, что множество $\mathfrak{A}_1$, состоящее из всех «правильных» выборов a_1, — это дополнение $\mathfrak{D}$, которое в нашем случае не диофантово или, что то же самое, не полуразрешимо. Таким образом, игрок A не имеет возможности алгоритмически проверять по произвольному a_1, годится ли это число для первого хода.

Это не очень интересный факт, поскольку игроку A на самом деле не требуется распознавать принадлежность произвольного a_1 к $\mathfrak{A}_1$. Ему достаточно один раз каким-то способом найти один элемент $\mathfrak{A}_1$, который он сможет затем использовать во всех играх на первом ходе.

Рассмотрим теперь более интересную ситуацию, когда выигрышная стратегия имеется у игрока B. Чтобы фактически выигрывать у A, игрок B должен уметь по произвольному a_1 находить «правильный» второй ход b_1. Обозначим посредством $\mathfrak{L}_1$ множество всех таких пар $\langle a_1,b_1\rangle$, где b_1 — «правильный» ответ игрока B на ход a_1 игрока A. Игроку B также не требуется распознавать принадлежность произвольной пары $\langle a_1,b_1\rangle$ к $\mathfrak{L}_1$, а достаточно уметь распознавать пары из произвольного подмножества $\mathfrak{L}_1^\star$ множества $\mathfrak{L}_1$ такого, которое для каждого a_1 содержит хотя бы одну пару вида $\langle a_1,b_1\rangle$; в такой ситуации будем говорить, что $\mathfrak{L}_1^\star$ *трассирует* $\mathfrak{L}_1$. Имея в своем распоряжении разрешимое множество $\mathfrak{L}_1^\star$, трассирующее $\mathfrak{L}_1$, игрок B мог бы

находить «правильный» ответ на первый ход a_1, перебирая пары $\langle a_1,0\rangle$, $\langle a_1,1\rangle,\ldots$ и проверяя поочередно каждую на принадлежность к $\mathfrak{L}_1^*$ до тех пор, пока не нашлась бы пара $\langle a_1,b_1\rangle$ из $\mathfrak{L}_1^*$, дающая «правильный» ход b_1.

Более того, достаточно, чтобы $\mathfrak{L}_1^*$ было хотя бы полуразрешимым, а не разрешимым. Действительно, пусть

$$B_1(a_1,b_1,x_2,\ldots,x_n)=0 \tag{5}$$

— диофантово уравнение, определяющее такое полуразрешимое $\mathfrak{L}_1^*$. Игрок B может начать перебирать числа $0,1,\ldots$, рассматривая каждое число как канторов номер некоторой n-ки $\langle b_1,x_2,\ldots,x_n\rangle$ и проверяя для каждой такой n-ки равенство (5). Первый элемент n-ки, удовлетворяющей (5), очевидно, годится в качестве правильного второго хода.

Покажем, что *существует диофантова игра с выигрышной стратегией у* B, *для которой никакое множество* $\mathfrak{L}_1^*$, *трассирующее множество «правильных» ответов* $\mathfrak{L}_1$, *не является полуразрешимым*. Исходным пунктом для нас будет диофантово представление

$$a\in\mathfrak{S}\Longleftrightarrow\exists x_2\ldots x_m[P(a,x_2,\ldots,x_m)=0] \tag{6}$$

простого множества $\mathfrak{S}$, построенного в § 6.6. Рассмотрим диофантову игру, задаваемую уравнением

$$P^2(a_1+b_1,a_2,\ldots,a_m)-b_m-1=0. \tag{7}$$

Нетрудно видеть, что b_1 будет «правильным» ответом на данное a_1 в том и только том случае, когда $a_1+b_1\notin\mathfrak{S}$, ибо в этом и только этом случае игрок B сможет согласно (6) выбрать b_m, удовлетворяющее (7), независимо от того, какие значения $a_2,\ldots,a_m$ будут выбраны игроком A. Поскольку $\overline{\mathfrak{S}}$ бесконечно, такое b_1 всегда найдётся, так что у игрока B действительно есть выигрышная стратегия.

Предположим теперь, что для игры (7) имеется диофантово трассирующее множество $\mathfrak{L}_1^*$. Рассмотрим диофантово множество $\mathfrak{D}$, определяемое равенством

$$a\in\mathfrak{D}\iff\exists a_1b_1[a=a_1+b_1\ \&\ \langle a_1,b_1\rangle\in\mathfrak{L}_1^*]. \tag{8}$$

Поскольку любая пара $\langle a_1,b_1\rangle$ из $\mathfrak{L}_1^*$ даёт «правильный» ответ, $\mathfrak{D}$ является подмножеством $\overline{\mathfrak{S}}$. С другой стороны, $\mathfrak{D}$ бесконечно, ибо для каждого a_1 найдётся подходящее значение b_1, а бесконечность $\mathfrak{D}$ противоречит простоте множества $\mathfrak{S}$.

Полученное противоречие показывает, что никакое трассирующее множество не может быть диофантовым, т. е. полуразрешимым и тем более разрешимым. С другой стороны, если бы игрок B мог по произвольному a_1 эффективно находить некоторое «правильное» $b_1=B_1(a_1)$, то трассирующее множество, состоящее

из всех пар вида $\langle a_1, B_1(a_1)\rangle$, было бы разрешимо (в интуитивном смысле) и потому диофантово. Таким образом, согласно тезису Чёрча, мы получаем, что *хотя для любого первого хода игрока* A *у игрока* B *не может не быть второго хода, ведущего к победе, игрок* B *не может эффективно находить такой ход.*

§ 10.2. Обобщённые кони на многомерной шахматной доске

Поля обычной шахматной доски можно занумеровать парами $\langle q, r\rangle$, где

$$0 \le q,\ 0 \le r, \tag{1}$$

$$q \le 7,\ r \le 7, \tag{2}$$

а правила перемещения коня могут быть изложены так: с поля $\langle q, r\rangle$ конь может пойти на одно из восьми полей

$$\langle q \pm 2,\ r \pm 1\rangle,\ \langle q \pm 1,\ r \pm 2\rangle \tag{3}$$

при условии, что координаты нового поля удовлетворяют неравенствам, аналогичным (1)–(2).

В этом параграфе мы рассмотрим обобщённые шахматы. Доска будет n-мерной, её поля будут нумероваться произвольными n-ками натуральных чисел $\langle r_1, \ldots, r_n\rangle$. Таким образом, у нас будет аналог ограничения (1), но не будет аналога ограничения (2), что естественно, поскольку для конечной доски разумные массовые проблемы оказываются разрешимыми. По этой бесконечной доске будут ходить (обобщённые) кони. Правила передвижения коня $\mathfrak{K}$ задается конечным множеством

$$\langle \delta_{1,1}, \ldots, \delta_{1,n}\rangle, \ldots, \langle \delta_{k,1}, \ldots, \delta_{k,n}\rangle \tag{4}$$

n-ок целых чисел. С поля $\langle r_1, \ldots, r_n\rangle$ конь $\mathfrak{K}$ может пойти на поле $\langle r_1 + \delta_{l,1}, \ldots, r_n + \delta_{l,n}\rangle$, разумеется, при условии, что все элементы этой n-ки неотрицательны.

Правила (4) определяют на множестве полей рефлексивное и транзитивное *отношение достижимости* одного поля из другого. Для обобщённого коня, в отличие от классического (3), это отношение может быть не симметричным, так что в этом отношении обобщённые кони ближе к пешкам.

Посредством $\mathfrak{K}(r_1, \ldots, r_n)$ мы будем обозначать *множество достижимости* — множество всех полей, на которых может побывать конь $\mathfrak{K}$, выйдя с поля $\langle r_1, \ldots, r_n\rangle$. Легко видеть, что отношение достижимости обладает следующим *свойством аддитивности*:

если

$$\langle r', \ldots, r'_n\rangle \in \mathfrak{K}(r_1, \ldots, r_n), \tag{5}$$

то

$$\langle r'_1 + t_1, \ldots, r'_n + t_n\rangle \in \mathfrak{K}(r_1 + t_1, \ldots, r_n + t_n). \tag{6}$$

На множество $\mathfrak{K}(r_1,\ldots,r_n)$ можно смотреть как на меру «шахматной силы» коня $\mathfrak{K}$, стоящего на поле $\langle r_1,\ldots,r_n\rangle$. В связи с этим можно сформулировать различные массовые проблемы, касающиеся сравнения «шахматной силы» коней. Мы рассмотрим две следующие проблемы.

Сравнение на включение: *по двум коням $\mathfrak{K}'$ и $\mathfrak{K}''$ и полю $\langle r_1,\ldots,r_n\rangle$ узнать, верно ли, что конь $\mathfrak{K}'$ «не слабее» коня $\mathfrak{K}''$, т. е. что*

$$\mathfrak{K}'(r_1,\ldots,r_n)\geq\mathfrak{K}''(r_1,\ldots,r_n). \tag{7}$$

Сравнение на равенство: *по двум коням $\mathfrak{K}'''$ и $\mathfrak{K}''''$ и полю $\langle p_1,\ldots,p_n\rangle$ узнать, верно ли, что «шахматная сила» обоих коней одинакова, т. е. что*

$$\mathfrak{K}'''(p_1,\ldots,p_n)=\mathfrak{K}''''(p_1,\ldots,p_n). \tag{8}$$

Понятно, что вторая проблема сводится к первой — для проверки (8) достаточно узнать, верно ли (7) при $\mathfrak{K}'=\mathfrak{K}'''$ и $\mathfrak{K}''=\mathfrak{K}''''$ и верно ли (7) при $\mathfrak{K}'=\mathfrak{K}''''$ и $\mathfrak{K}''=\mathfrak{K}'''$. Таким образом, было бы достаточно установить неразрешимость проблемы сравнения на равенство, однако по техническим причинам мы сначала докажем неразрешимость проблемы сравнения на включение.

(Как уже отмечалось, для алгоритмической неразрешимости существенно, что у нас нет аналога ограничению (2), т. е. что кони ходят по бесконечной доске. Менее очевидно, что для неразрешимости существенно и то, что у нас есть аналог ограничения (1), т. е. что доска по каждой размерности в одном из направлений ограничена. Действительно, на доске $\mathbb{Z}^n$ все ходы коней коммутативны, поэтому вопрос о достижимости поля $\langle r''_1,\ldots,r''_n\rangle$ из поля $\langle r'_1,\ldots,r'_n\rangle$ сводится к вопросу о разрешимости в целых числах системы линейных диофантовых уравнений

$$\begin{gathered}\delta_{1,1}x_1+\ldots+\delta_{k,1}x_k=r''_1-r'_1\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ \delta_{1,n}x_1+\ldots+\delta_{k,n}x_k=r''_n-r'_n\ ,\end{gathered} \tag{9}$$

а множество $\mathfrak{K}(r_1,\ldots,r_n)$ имеет вполне регулярную структуру.)

Для доказательства неразрешимости сравнения «шахматной силы» нам будет достаточно рассматривать только коней, задаваемых такими правилами (4), в которых $\delta_{l,m}$ может иметь лишь одно из трёх значений −1, 0, 1. По этой причине мы можем использовать и другую форму записи правил, а именно, правило, соответствующее n-ке $\langle\delta_1,\ldots,\delta_n\rangle$, мы будем записывать также в виде

$$\mathrm{R}_{i_1}\ldots\mathrm{R}_{i_a}\Rightarrow\mathrm{R}_{j_1}\ldots\mathrm{R}_{j_b}, \tag{10}$$

если $\delta_{i_1}=\ldots=\delta_{i_a}=-1$, $\delta_{j_1}=\ldots=\delta_{j_b}=1$ и других чисел, отличных от ± 1, среди $\delta_1,\ldots,\delta_n$ нет.

Понятно, что в (10) всю информацию несут только индексы, а буква R смысловой нагрузки не имеет. В дальнейшем вместо буквы R мы будем использовать в записи правил и другие буквы, но это будет делаться исключительно для облегчения восприятия правил человеком, так что, например, правило

$$T_{i_1}\ldots T_{i_a} \Rightarrow S_{j_1}\ldots S_{j_b} \tag{11}$$

эквивалентно правилу (10).

С помощью движения коня по доске мы будем моделировать работу некоторой (недетерминированной) *шахматной машины*. Подобно машине Тьюринга, шахматная машина может находиться в одном из конечного числа *состояний* $Q_{i_1},\ldots,Q_{i_l}$ (нумерация состояний не обязательно последовательная). В отличие от машины Тьюринга, память шахматной машины состоит из конечного числа *регистров* $R_{j_1},\ldots,R_{j_k}$ (нумерация регистров также не обязательно последовательная; номера регистров должны отличаться от номеров состояний). Каждый из регистров может содержать произвольное натуральное число. *Инструкции* шахматной машины имеют вид

$$Q_{i_0}R_{i_1}\ldots R_{i_k} \Rightarrow Q_{j_0}R_{j_1}\ldots R_{j_l}, \tag{12}$$

причём среди индексов $i_0,\ldots,i_k$, $j_0,\ldots,j_l$ нет двух одинаковых. Инструкция (12) может выполняться, если машина находится в состоянии Q_{i_0}, а все регистры $R_{i_1},\ldots,R_{i_k}$ не пусты. Выполнение этой инструкции состоит в том, что содержимое каждого из регистров $R_{i_1},\ldots,R_{i_k}$ уменьшается на 1, а содержимое каждого из регистров $R_{j_1},\ldots,R_{j_l}$ увеличивается на 1, после чего машина переходит в состояние Q_{j_0}. Существенное отличие шахматной машины от машины Тьюринга состоит в недетерминированности первой из них, а именно, не предполагается, что в каждый момент выполнимой будет оказываться только одна инструкция.

Содержимое регистров будет моделироваться координатами полей, а нахождение в состоянии Q_i будет моделироваться тем, что i-я координата будет равна 1, а остальные координаты, соответствующие состояниям, равны нулю. Работе машины соответствует движение по доске коня, правила перемещения которого, благодаря принятым соглашениям, совпадают с инструкциями машины. Пользуясь этой связью, мы будем свободно чередовать обе терминологии — терминологию перемещений коня и терминологию шахматной машины.

Наша ближайшая цель состоит в том, чтобы показать, что шахматная машина может вычислять значения некоторых полиномов. Прежде всего, мы должны уточнить, что будет пониматься под вычислением на таком недетерминированном устройстве, как шахматная машина. Пусть $F(x_1,\ldots,x_m)$ — натуральнозначная функция натуральных аргументов, $\mathfrak{K}$ — шахматная машина, у которой выделены *начальное состояние* Q_b, *заключительное состояние* Q_e, *входные регистры* $I_{i_1},\ldots,I_{i_m}$ и *выходной регистр* O_k. Для вычисления $F(x_1,\ldots,x_m)$ конь помещается на поле

$$\langle r_1,\ldots,r_n\rangle, \tag{13}$$

где $r_b=1$, $r_{i_l}=x_l$, а все остальные координаты равны 0. Мы будем говорить, что данная шахматная машина вычисляет функцию F, если выполнены следующие три условия:

если с поля (13) *достижимо некоторое поле* $\langle r'_1,\ldots,r'_n\rangle$, *то* $r'_k\le F(x_1,\ldots,x_n)$;

для любого y, *такого, что* $y\le F(x_1,\ldots,x_n)$, *с поля* (13) *достижимо некоторое поле* $\langle r'_1,\ldots,r'_n\rangle$, *у которого* $r'_k=y$, $r'_e=1$;

состояние Q_e *не встречается в левых частях инструкций.*

Нетрудно понять, что из-за свойства аддитивности шахматная машина может вычислять только функции, монотонно неубывающие по каждому аргументу.

Следующая машина с начальным состоянием Q_1, входными регистрами I_4, I_5, выходным регистром O_6 и заключительным состоянием Q_3 вычисляет сумму:

$$\begin{aligned} Q_1I_4 &\Rightarrow Q_2O_6\\ Q_1I_5 &\Rightarrow Q_2O_6\\ Q_1 &\Rightarrow Q_3\\ Q_2 &\Rightarrow Q_1. \end{aligned} \tag{14}$$

Шахматная машина, вычисляющая произведение, чуть сложнее:

$$\begin{aligned} Q_1I_6 &\Rightarrow Q_2\\ Q_2I_7 &\Rightarrow Q_3R_8O_9\\ Q_3 &\Rightarrow Q_2\\ Q_3 &\Rightarrow Q_4\\ Q_4R_8 &\Rightarrow Q_1I_7\\ Q_1 &\Rightarrow Q_4\\ Q_1 &\Rightarrow Q_5. \end{aligned} \tag{15}$$

Начальным состоянием является Q_1, входными регистрами I_6 и I_7, выходным — O_9, заключительное состояние — Q_5. Пусть x и

y — начальное содержимое входных регистров I_6 и I_7. u и v — такие числа, что $u \le x$ и $v \le y$. Предположим, что машина прошла следующую цепочку состояний:

$$Q_1((Q_2Q_3)^y(Q_4Q_1)^y)^u(Q_2Q_3)^v(Q_4Q_1)^vQ_5. \tag{16}$$

В этом случае в регистре O_9 окажется число $uy+v$. Таким образом, к моменту перехода машины в состояние Q_5 в регистре O_9 может оказаться любое число, не превосходящее xy. С другой стороны, содержимое регистра O_9 увеличивается на 1 только при переходе из состояния Q_2 в Q_3, но для любой цепочки состояний

$$(Q_2Q_3)^v \tag{17}$$

справедливо неравенство $v \le y$, ибо в любой момент времени регистры I_7 и I_8 содержат вместе ровно y. Любой другой путь из состояния Q_3 в состояние Q_2 содержит переход из Q_1 в Q_2 и тем самым уменьшает I_6 на 1. Таким образом, цепочек вида (17) может быть не более чем x, и, значит, содержимое регистра O_9 никогда не превысит xy.

Если мы имеем две шахматные машины $\mathfrak{K}_1$ и $\mathfrak{K}_2$, вычисляющие некоторые функции $F_1(x_1,\ldots,x_{m_1})$ и $F_2(y_1,\ldots,y_{m_2})$, то мы можем построить машину $\mathfrak{K}$, вычисляющую функцию

$$F(z_1,\ldots,z_{m_1+m_2}) = F_1(z_1,\ldots,z_{m_1}) + F_2(z_{m_1+1},\ldots,z_{m_1+m_2}). \tag{18}$$

Для этого сначала перенумеруем состояния, регистры и машины $\mathfrak{K}_1$ и $\mathfrak{K}_2$ так, чтобы:

номер заключительного состояния машины $\mathfrak{K}'_1$ (получающейся в результате перенумерации) совпал с номером начального состояния машины $\mathfrak{K}'_2$, а все другие номера состояний и регистров машин $\mathfrak{K}'_1$ и $\mathfrak{K}'_2$ были различны;

заключительным состоянием машины $\mathfrak{K}'_2$ стало состояние Q_1;

выходным регистром машины $\mathfrak{K}'_1$ стал регистр O_4, а машины $\mathfrak{K}'_2$ — регистр O_5;

номера всех остальных состояний и регистров, кроме явно указанных выше, были больше 6.

Инструкции машины $\mathfrak{K}$ теперь могут быть получены объединением инструкций машины§ $\mathfrak{K}'_1$, $\mathfrak{K}'_2$ и инструкций (14). Начальное состояние машины $\mathfrak{K}$ совпадает с начальным состоянием машины $\mathfrak{K}'_1$, входные регистры — с входными регистрами машин $\mathfrak{K}'_1$ и $\mathfrak{K}'_2$, выходным регистром является O_6, а заключительным состоянием — Q_3.

Аналогично, используя вместо машины для сложения (14) машину для умножения (15), мы можем вычислить $F_1(z_1,\ldots,z_{m_1}) \times F_2(z_{m_1+1},\ldots,z_{m_1+m_2})$. Таким образом, мы можем вычислять любой полином, в записи которого каждая неизвест-

ная встречается не более одного раза, а все ненулевые коэффициенты равны 1.

Пусть

$$D(x_1,\ldots,x_m)=0 \tag{19}$$

— произвольное диофантово уравнение. Наша очередная задача — построить шахматные машины $\mathfrak{K}_1'$ и $\mathfrak{K}_2''$ и начальное положение коней такие, что включение (7) имеет место в том и только том случае, когда уравнение (19) не имеет решений.

Пусть A и B — полиномы с натуральными коэффициентами такие, что

$$D^2(x_1,\ldots,x_m)=A(x_1,\ldots,x_m)-B(x_1,\ldots,x_m). \tag{20}$$

Таким образом, при всех значениях $x_1,\ldots,x_m$

$$A(x_1,\ldots,x_m)\geq B(x_1,\ldots,x_m), \tag{21}$$

а если уравнение (19) решений не имеет, то

$$A(x_1,\ldots,x_m)\geq B(x_1,\ldots,x_m)+1. \tag{22}$$

Пусть, далее, $A'(y_1,\ldots,y_{mw})$ и $B'(z_1,\ldots,z_{mw})$ — полиномы с коэффициентами 0 и 1 такие, что

$$A(x\ ,\ldots,x\ )=A'(\underbrace{x_1,\ldots,x_1}_{w\ \text{раз}},\ \ldots\ ,\ \underbrace{x_m,\ldots,x_m}_{w\ \text{раз}}), \tag{23}$$

$$B(x_1,\ldots,x_m)+1=B'(\underbrace{x_1,\ldots,x_1}_{w\ \text{раз}},\ \ldots\ ,\ \underbrace{x_m,\ldots,x_m}_{w\ \text{раз}}). \tag{24}$$

Пусть, наконец, $\mathfrak{K}_A$ и $\mathfrak{K}_B$ — шахматные машины, вычисляющие A' и B' соответственно. Не ограничивая общности, мы будем считать, что выходным регистром машины $\mathfrak{K}_B$ является B_{m+1}, а номера остальных регистров и состояний не меньше $m+9$.

Добавим к инструкциям машины $\mathfrak{K}_B$ инструкции вида

$$\begin{aligned}
Q_{m+2} &= Q_{m+3}R_{i_{1,1}}\ldots R_{i_{1,w}}X_1\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
Q_{m+2} &= Q_{m+3}R_{i_{m,1}}\ldots R_{i_{1,w}}X_1\\
Q_{m+3} &= Q_{m+2}\\
Q_{m+3} &= Q_bT,
\end{aligned} \tag{25}$$

где $R_{i_{1,1}},\ldots,R_{i_{m,w}}$, T — входные регистры машины $\mathfrak{K}_B$, а Q_b — её начальное состояние. Обозначим получившуюся машину посредством $\mathfrak{K}_B''$. Начальным состоянием машины $\mathfrak{K}_B''$ будет Q_{m+2}, заключительным — заключительное состояние машины $\mathfrak{K}_B$. Мы не будем смотреть на машину $\mathfrak{K}_B''$ как на машину, вычисляющую какую-либо функцию, поэтому никакие регистры не выделяются в качестве входных и выходных.

Будучи запущена в состоянии Q_{m+2} при пустых регистрах, машина $\mathfrak{K}''_B$ сначала порождает некоторые числа $x_1,\ldots,x_m$ в регистрах $X_1,\ldots,X_m$ и входных регистрах машины $\mathfrak{K}_B$, а затем вычисляет в регистре B_{m+1} значение полинома $B(x_1,\ldots,x_m)+1$, т. е. в этом регистре может оказаться любое число от 0 до этого значения включительно.

Аналогично мы можем построить машину $\mathfrak{K}'_A$, которая будет вычислять в регистре A_{m+1} значение $A(x_1,\ldots,x_m)$. Если уравнение (19) имеет решение, то у машины $\mathfrak{K}''_B$ в регистре B_{m+1} может оказаться значение, на 1 большее максимального значения в регистре A_{m+1} машины $\mathfrak{K}'_A$ (при одинаковых значениях в регистрах $X_1,\ldots,X_m$, дающих решение уравнения (19)). Если же уравнение (19) решений не имеет, то справедливо неравенство (20) и любое значение, которое окажется в B_{m+1} у машины $\mathfrak{K}''_B$, может оказаться и в A_{m+1} у машины $\mathfrak{K}'_A$. Этого ещё не достаточно, чтобы устанавливать выполнение или невыполнение (7), ибо там сравнение идёт по содержимому всех регистров.

Чтобы устранить это препятствие, мы модифицируем машины $\mathfrak{K}'_A$ и $\mathfrak{K}''_B$. При этом, не ограничивая общности, мы будем считать, что одинаковые номера у этих машин имеют только начальные состояния Q_b, регистры $X_1,\ldots,X_m$, где порождаются значения неизвестных $x_1,\ldots,x_m$, и регистры A_{m+1} и B_{m+1}, где вычисляются значения полиномов A и B. Пусть Q_t — состояние, не используемое ни в $\mathfrak{K}''_A$, ни в $\mathfrak{K}''_B$, причём $t > m+8$, а Q_s — заключительное состояние машины $\mathfrak{K}''_A$. Добавим к инструкциям машины $\mathfrak{K}''_A$ следующие группы инструкций:

инструкции вида

$$Q_sR_i \Rightarrow Q_t \tag{26}$$

для каждого регистра R_i машины $\mathfrak{K}''_A$, отличного от $X_1,\ldots,X_{m+1}$;

инструкции вида

$$Q_s \Rightarrow Q_tR_j \tag{27}$$

для каждого регистра R_j машины $\mathfrak{K}''_B$, отличного от $X_1,\ldots,X_{m+1}$;

инструкции вида

$$Q_s \Rightarrow Q_k \tag{28}$$

для каждого состояния Q_k машины $\mathfrak{K}''_B$;

инструкцию

$$Q_t \Rightarrow Q_s. \tag{29}$$

Получающуюся при этом машину обозначим посредством $\mathfrak{K}'$.

Машине $\mathfrak{K}''_B$ мы не будем добавлять новые инструкции, но добавим (по существу, фиктивно) новые регистры с номерами, равными номерам состояний и регистров машины $\mathfrak{K}''_A$. Получающуюся при этом машину обозначим посредством $\mathfrak{K}''$.

Начальным полем будет

$$\langle r_1,\ldots,r_n\rangle, \tag{30}$$

где $r_{m+2}=1$, а все остальные элементы n-ки (30) равны 0. Сравним множества достижимости машин $\mathfrak{K}'(r_1,\ldots,r_n)$ и $\mathfrak{K}''(r_1,\ldots,r_n)$. Выше уже отмечалось, что если уравнение (19) имеет решения, то машина $\mathfrak{K}''_B$, а следовательно, и машина $\mathfrak{K}''$ может поместить в R_{m+1} значение, недоступное машине $\mathfrak{K}'_A$, а следовательно, и машине $\mathfrak{K}'$, при одинаковых значениях регистров $X_1,\ldots,X_m$. Таким образом, если уравнение (19) имеет решение, то включение (7) не имеет места.

Пусть теперь уравнение (19) решений не имеет, а конь $\mathfrak{K}''$, отправившись с поля (30), дошёл до некоторого поля

$$\langle r'_1,\ldots,r'_n\rangle. \tag{31}$$

Проверим, что конь $\mathfrak{K}'$, отправившись с того же поля, также может дойти до поля (31).

Прежде всего, с помощью инструкций типа (25) надо породить в регистрах $X_1,\ldots,X_m$ значения $r'_1,\ldots,r'_m$. Далее, мы знаем, что

$$r'_{m+1}\le B(r_1,\ldots,r_m)+1, \tag{32}$$

а потому согласно (22)

$$r'_{m+1}\le A(r_1,\ldots,r_m). \tag{33}$$

Следовательно, при помощи инструкций машины $\mathfrak{K}'_A$ мы можем занести в R_{m+1} число r'_{m+1}. Далее, при помощи инструкций вида (26) и (29) мы можем обнулить все регистры машины $\mathfrak{K}'_A$, кроме $X_1,\ldots,X_m$, R_{m+1}, а затем при помощи инструкций вида (27) и (29) занести в регистры машины $\mathfrak{K}'_B$ соответствующие координаты поля (31) и, наконец, по инструкциям (28) и (29) перейти в состояние, в котором машина $\mathfrak{K}''$ достигла поля (31).

Таким образом, включение (7) имеет место тогда и только тогда, когда уравнение (19) не имеет решений, т. е. 10-я проблема Гильберта сводится к вопросу о сравнении «шахматной силы» на включение, и потому эта массовая проблема также неразрешима.

Обратимся теперь к сравнению на равенство. Очевидно, что

$$\mathfrak{K}'(r_1,\ldots,r_n)\supseteq\mathfrak{K}''(r_1,\ldots,r_n) \Leftrightarrow$$
$$\Leftrightarrow \mathfrak{K}'(r_1,\ldots,r_n)=\mathfrak{K}'(r_1,\ldots,r_n)\cup\mathfrak{K}''(r_1,\ldots,r_n). \tag{34}$$

Таким образом, нам было бы достаточно суметь определить коня $\mathfrak{K}'''$ так, чтобы

$$\mathfrak{K}'''(r_1,\ldots,r_n)=\mathfrak{K}'(r_1,\ldots,r_n)\cup\mathfrak{K}''(r_1,\ldots,r_n). \tag{35}$$

В действительности конь $\mathfrak{K}'''$, которого мы определим ниже, будет обладать не в точности свойством (35), но близким к нему.

Чтобы объединить множества достижимости мы, грубо говоря, объединим правила обоих коней. Если сделать это непосредственно, то получится слишком мощная фигура, поскольку такой конь сможет произвольно чередовать ходы по правилам одного и другого коня. Для исключения возможности такого смешения будет использован следующий механизм.

По нашему соглашению машины $\mathfrak{K}'$ и $\mathfrak{K}''$ не имеют регистров и состояний с номерами от $m+4$ до $m+8$, так что во время движения коней $\mathfrak{K}'$ и $\mathfrak{K}''$ с поля (30) соответствующие координаты оставались нулевыми. Заменим каждое правило (10) коня $\mathfrak{K}'$ на два правила

$$T_{m+4}R_{i_1}\ldots R_{i_a} \Rightarrow T_{m+5}R_{j_1}\ldots R_{j_b} \tag{36}$$

и

$$T_{m+5}R_{i_1}\ldots R_{i_a} \Rightarrow T_{m+4}R_{j_1}\ldots R_{j_b}. \tag{37}$$

Аналогично, если (10) — правило коня $\mathfrak{K}''$, то заменим его на правила

$$T_{m+6}R_{i_1}\ldots R_{i_a} \Rightarrow T_{m+7}R_{j_1}\ldots R_{j_b} \tag{38}$$

и

$$T_{m+7}R_{i_1}\ldots R_{i_a} \Rightarrow T_{m+6}R_{j_1}\ldots R_{j_b}. \tag{39}$$

Объединим все правила вида (36)–(39) и добавим ещё четыре правила

$$Q_{m+8} \Rightarrow T_{m+4}Q_{m+2}, \tag{40}$$

$$Q_{m+8} \Rightarrow T_{m+5}Q_{m+2}, \tag{41}$$

$$Q_{m+8} \Rightarrow T_{m+6}Q_{m+2}, \tag{42}$$

$$Q_{m+8} \Rightarrow T_{m+7}Q_{m+2}. \tag{43}$$

Обозначим полученного коня через $\mathfrak{K}_{AB}$ и рассмотрим его движение с поля

$$\langle p_1,\ldots,p_n\rangle, \tag{44}$$

где $p_{m+8}=1$, а все остальные координаты равны 0. Своим первым ходом конь $\mathfrak{K}_{AB}$ делает выбор, движение какого коня он будет имитировать дальше. А именно, если первым ходом будет ход по правилу (40) или (41), то в дальнейшем регистры T_{m+6} и T_{m+7} всегда будут пусты, а из двух регистров T_{m+4} и T_{m+5} один всегда будет пуст, а другой содержать 1, так что дальнейшие ходы коня $\mathfrak{K}_{AB}$ будут осуществляться по правилам (36)–(37). Наоборот, если первым ходом был ход по правилу (42) или (43), то все последующие ходы будут по правилам (38)–(39).

Наконец, мы можем определить коней $\mathfrak{K}'''$ и $\mathfrak{K}''''$, чью «шахматную силу» мы будем сравнивать на точное совпадение.

Конь $\mathfrak{K}''''$ может делать все ходы, разрешённые коню $\mathfrak{K}_{AB}$, и ещё два хода по правилам

$$\begin{aligned} T_{m+4} &\Rightarrow \quad , \\ T_{m+5} &\Rightarrow \quad , \end{aligned} \tag{45}$$

т. е. уменьшать содержимое регистров T_{m+4} и T_{m+5}, не увеличивая при этом содержимого каких-либо других регистров. Конь $\mathfrak{K}'''$ может делать все ходы, разрешённые коню $\mathfrak{K}''''$, и ещё два хода по правилам

$$\begin{aligned} T_{m+6} &\Rightarrow \quad , \\ T_{m+7} &\Rightarrow \quad . \end{aligned} \tag{46}$$

Сравним множества полей, достижимых конями $\mathfrak{K}'''$ и $\mathfrak{K}''''$ с поля (44). Очевидно, что конь $\mathfrak{K}'''$ может достичь любое поле, которое может достичь конь $\mathfrak{K}''''$. Допустим теперь, что есть поле

$$\langle p'_1, \ldots, p'_n \rangle, \tag{47}$$

которое конь $\mathfrak{K}'''$ может достичь, а конь $\mathfrak{K}''''$ — нет. Нетрудно понять, что это возможно лишь в том случае, когда первым применялось одно из правил (42)–(43), а последним — одно из правил (46), недоступных коню $\mathfrak{K}''''$. Это означает, что остальными ходами конь $\mathfrak{K}'''$ имитировал движение коня $\mathfrak{K}''$, и этот конь может достичь поле (47) с поля (39). Поскольку конь $\mathfrak{K}''''$ не может достичь поля (47), его не может достичь и конь $\mathfrak{K}'$ с поля (30). Таким образом, включение (7) имеет место тогда и только тогда, когда имеет место равенство (8), следовательно, и проблема сравнения на равенство также алгоритмически неразрешима.

Упражнения

10.1. Проведённое в § 10.1 построение диофантовой игры с невычислимой выигрышной стратегией было основано на примере простого множества, построенного в § 6.5. Этот пример в свою очередь использовал универсальное диофантово уравнение (такие уравнения были построены в главе 4 и § 6.4) и устранимость ограниченного квантора общности (различная техника для этого была описана в § 6.1–6.3). Получающаяся в итоге диофантова игра (1.7) задается чрезвычайно громоздким полиномом. Эту конструкцию можно несколько упростить, обойдясь без явного построения диофантова представления простого множества (но используя сам факт его существования). Рассмотрим следующую игру, основанную на универсальном уравнении

$$U_1(a, k, x_1, \ldots, x_m) = 0,$$

но не задаваемую этим уравнением в смысле (1.1):

на первом ходу A *выбирает число* k;

на втором ходу B *выбирает число* b;

на третьем ходу A *выбирает число* a;

A *объявляется победителем в том и только том случае, когда уравнение*

$$\mathbf{U}_1(a, k, x_1, \ldots, x_m) = 0$$

решений не имеет, а уравнение

$$\mathbf{U}_1(b, k, y_1, \ldots, y_m) = 0$$

имеет решение.

а) Приведите эту игру к каноническому виду (1.1).

б) Покажите, что выигрышную стратегию имеет игрок B.

в) Покажите, что B не может эффективно реализовать свою выигрышную стратегию.

10.2. Рассмотрим класс программ без циклов и условных переходов, состоящих из операторов вида $x \leftarrow 1$, $x \leftarrow x+y$, $x \leftarrow (x \operatorname{div} y)$. Покажите алгоритмическую неразрешимость проблемы распознавания по таким программам, вычисляют ли они функцию, тождественно равную 1.

Комментарии

Диофантовы игры были введены в работе Джонса [1974]. При этом он использовал идеи работы Рабина [1957], где аналогичные игры рассматривались с общеалгоритмических позиций. После того как была установлена диофантовость полуразрешимых множеств, перенос этих идей на диофантовы уравнения не представлял труда. Основное достижение в работе Джонса [1982a] состояло не в чистых теоремах существования, как в § 10.1, а в возможности явно выписать полиномы, определяющие диофантовы игры, для которых неразрешима та или иная массовая проблема. Так, в качестве примера диофантовой игры, в которой второй игрок имеет выигрышную, но не эффективно вычислимую стратегию, в этой работе приводено уравнение

$$\begin{aligned}
&\{\{a_1+a_5+1-b_4\}^2\{[(a_6+a_7)^2+3a_7+a_6-2b_4]^2+[[(b_9-a_7)^2+(b_{10}-a_9)^2]\times\\
&\times[(b_9-a_6)^2+(b_{10}-a_8)^2((b_4-a_1)^2+(b_{10}-a_9-b_1)^2)]\times\\
&\times[(b_9-3b_4)^2+(b_{10}-a_8-a_9)^2]\times[(b_9-3b_4-1)^2+(b_{10}-a_8a_9)^2]-a_{12}-1]^2+\\
&+[[b_{10}+a_{12}+a_{12}b_9a_4-a_3]^2+[b_{10}+a_{13}-b_9a_4]^2]\}-b_{13}-1\}\times\\
&\times\{a_1+b_5+1-a_5\}\{[(b_5-b_6)^2+3b_6+b_5-2a_5]^2+[[(a_{10}-b_6)^2+(a_{11}-b_8)^2]\times\\
&\times[(a_{10}-b_5)^2+(a_{11}-b_7)^2((a_5-a_1)^2+(a_{11}-b_8-a_2)^2)]\times\\
&\times[(a_{10}-3a_5)^2+(a_{11}-b_7-b_8)^2][(a_{10}-3a_5-1)^2+(a_{11}-b_7b_8)^2]-b_{11}-1]^2+\\
&+[[a_{11}+b_{11}+b_{11}a_{10}b_3-b_2]^2+[a_{11}+b_{12}-a_{10}b_3]^2]\}=0.
\end{aligned}$$

Доказательство основано на идее, несколько более сложной, чем использованная в § 10.1.

В § 10.2 для придания наглядности была использована шахматная терминология. Проблемы, рассмотренные в этом параграфе, известны в литературе и под другими названиями. В первую очередь здесь следует назвать *системы векторного сложения*, которые адекватны обобщённым коням. Благодаря тому, что во всех правилах (10.2.4) рассмотренных нами коней $|\delta_{i,j}| \leq 1$, их передвижение по доске легко имитируется *сетями Петри* с соответствующим перенесением результатов. Системы векторного сложения и сети Петри были предложены как аппарат для исследования, в частности, параллельных вычислений.

Алгоритмическую неразрешимость проблемы сравнения на включение установил М. Рабин в 1966 г. (см. работу Хека [1976]). Поскольку в то время неразрешимость 10-й проблемы Гильберта ещё не была доказана, М. Рабин использовал более слабый результат — алгоритмическую неразрешимость экспоненциально диофантовых уравнений (историю получения этого результата см. в комментариях к главе 5) и был вынужден устанавливать вычислимость на шахматной машине не только сложения и умножения, но и возведения в степень. В 1972 г. М. Рабин представил упрощённое доказательство, основанное уже на неразрешимости 10-й проблемы Гильберта (см. работу Хека [1976]).

М. Рабин не опубликовал и это доказательство. В § 10.2 мы следовали работе Хека [1976], в которой был получен и более сильный результат — неразрешимость проблемы сравнения на равенство.

10-я проблема Гильберта была использована для установления неразрешимости многих других массовых проблем. Все приложения обозреть в этой книге невозможно, в частности, потому, что многие из них технически сложны или требуют специальных знаний в соответствующей области. Мы ограничимся здесь указанием литературных источников.

Для исследования массовых проблем алгебры 10-я проблема Гильберта использовалась в работах Айвазяна [1983, 1988], Аника [1985], Бокутя [1972], Важенина [1987, 1988, 1989], Валиева [1975], Губер-Дайсон [1974], Дурнева [1974], Клеймана [1979], Линдона и Шуппа [1977], Миллера [1973], Мясникова и Ремесленникова [1986], Розенблата [1985], Сапира [1989], Сапира и Харлампович [1989], Ремесленникова [1979], Репина [1983], Романькова [1977, 1979] и Харлампович [1989а, 1989б].

Совпадение полуразрешимости и диофантовости находит приложения в теории моделей и теории доказательств — см. работы Адлера [1969б], Бакстера [1978], Баура [1974], Гайфмана [1972], Гайфмана и Димитракопулоса [1982], Германо [1976], Гольдфарба [1981], Гуаспари [1979], Дайсон, Джонса и Шепердсона [1982], Девиса [1989], Джозеф и Янга [1981], Зикмана [1989], Зингера [1978], Кая [1987, 1990], Кая, Париса и Димитрокопулоса [1988], Карстенса [1977], Косовского [1967], Липшица [1979], Макалуна [1978], Макинтайра и Симмонса [1973], Маневица [1976а, 1976б], Минца [1975], Париса и Димитрокопулоса [1982], А. Робинсона [1973], Дж. Робинсон [1973], Уилки [1975], Уилмерса [1985], Фридрихсдорфа [1976], Хетчера

и Ходжсона [1981], Хиршфельда [1975], Хиршфельда и Уилера [1975], Чейтина [1974, 1987].

Неразрешимость 10-й проблемы Гильберта оказалась полезной при исследовании ряда вопросов теоретического программирования — см. работы Бека [1975], Гурари [1985], Гурари и Ибарры [1982], Данько [1980], Ибарры и Лейнингера [1980, 1982, 1983], Касами и Токуры [1971], Стетмана [1981], Туракайнена [1978, 1981], Хавела, Пнуели и Стави [1983], Хека [1976].

Неразрешимость 10-й проблемы Гильберта влечёт невозможность алгоритмов для некоторых задач математического программирования — см. работы Дурнева и Кораблёвой [1988], Ерослова [1973], Манаса [1971], Тарасова и Хачияна [1980].

В заключение укажем работу Гудстейна [1975], которая по своему характеру отличается от большинства других работ, использующих неразрешимость 10-й проблемы Гильберта. В этой работе получено *неалгоритмическое* следствие двух *алгоритмических* результатов — неразрешимости диофантовых уравнений и установленной в работе Гудстейна и Ли [1966] алгоритмической разрешимости уравнений специального вида.

ПРИЛОЖЕНИЯ

1. Теорема о четырёх квадратах

ТЕОРЕМА (Лагранж [1772]). *Диофантово уравнение*

$$x_1^2+x_2^2+x_3^2+x_4^2=a \tag{1}$$

имеет решение в целых x_1, x_2, x_3, x_4 *при любом неотрицательном целом* a.

Из тождества Эйлера

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)=$$
$$=(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2+$$
$$+(x_1y_3-x_3y_1+x_2y_4-x_4y_2)^2+(x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2 \tag{2}$$

следует, что теорему достаточно доказать для случая, когда a — нечётное простое число.

Будем считать значение a фиксированным и рассмотрим уравнение

$$x_1^2+x_2^2+x_3^2+x_4^2=ab \tag{3}$$

с параметром b и четырьмя неизвестными x_1, x_2, x_3, x_4. Покажем, во-первых, что существует число b_0 такое, что

$$0<b_0<a \tag{4}$$

и уравнение (3) имеет решение при $b=b_0$, и, во-вторых, если для некоторого b' такого, что

$$1<b'<a, \tag{5}$$

уравнение (3) имеет решение при $b=b'$, то существует число b'' такое, что

$$0<b''<b' \tag{6}$$

и уравнение (3) имеет решение при $b=b''$. Ясно, что этого достаточно для доказательства теоремы.

Легко проверить, что все $(a+1)/2$ чисел

$$0^2,\ 1^2,\ldots,\ ((a-1)/2)^2 \tag{7}$$

попарно несравнимы друг с другом **modulo** a. Аналогично попарно несравнимы $(a+1)/2$ чисел

$$-1-0^2,\ -1-1^2,\ldots,\ -1-((a-1)/2)^2. \tag{8}$$

Списки (7) и (8) вместе содержат $a+1$ число, следовательно, в этих списках есть два числа, которые сравнимы по **modulo** a, т. е. существуют числа x_1, x_2 и b_0 такие, что

$$0\le x_1\le((a-1)/2),\quad 0\le x_2\le((a-1)/2) \tag{9}$$

и

$$x_1^2+x_2^2+1=ab_0. \tag{10}$$

Левое неравенство в (4) очевидно, а правое легко получается из (9).

Пусть теперь

$$x_1^2+x_2^2+x_3^2+x_4^2=ab', \tag{11}$$

где b' удовлетворяет (5). Пусть, далее, y_1, y_2, y_3, y_4 — такие целые числа, что

$$y_i \equiv x_i (\mathbf{mod}\ b'), \tag{12}$$

$$-b'/2<y_i \le b'/2. \tag{13}$$

Согласно (11) и (12)

$$y_1^2+y_2^2+y_3^2+y_4^2=b'b'' \tag{14}$$

для некоторого b''. Из (13) следует, что $b'' \le b'$. Равенство здесь возможно, лишь если $y_1=y_2=y_3=y_4=b'/2$, а в таком случае $|x_1|=|x_2|=|x_3|=|x_4|=b'/2$ и $b'=a$, что противоречит (5). Таким образом, правое равенство в (6) выполнено. Если же $b''=0$, то $y_1=y_2=y_3=y_4=0$ и $b' \mid a$, что противоречит (5) и простоте a. Следовательно, левое неравенство в (6) также выполнено.

Перемножая (11) и (14) и пользуясь тождеством Эйлера, мы получаем, что ab'^2b'' представимо в виде суммы четырёх квадратов из правой части (2). Из (12) и (11) следует, что каждый из них, делится на b'^2, и, сокращая, мы получаем искомое решение уравнения (3), в котором $b=b''$.

2. Китайская теорема об остатках

ТЕОРЕМА. *Пусть $q_1,\dots,q_n$ — попарно взаимно простые числа, а $a_1,\dots,a_n$ — произвольные числа такие, что*

$$0 \le a_i < q_i, \quad i=1,\dots,n. \tag{1}$$

Тогда существует ровно одно число a такое, что

$$a_i=\mathbf{rem}(a,q_i), \quad i=1,\dots,n \tag{2}$$

и

$$0 \le a < q_1 \dots q_n. \tag{3}$$

Для доказательства рассмотрим $q_1 \dots q_n$ n-ок

$$\begin{gathered} \langle \mathbf{rem}(0,q_1),\dots,\mathbf{rem}(0,q_n)\rangle, \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ \langle \mathbf{rem}(q_1\dots q_n-1,q_1),\dots,\mathbf{rem}(q_1\dots q_n-1,q_n)\rangle. \end{gathered} \tag{4}$$

Они все различны, ибо если

$$\mathbf{rem}(a',q_i)=\mathbf{rem}(a'',q_i), \tag{5}$$

то

$$q_i \mid a'-a'', \tag{6}$$

и ввиду взаимной простоты $q_1,\ldots,q_n$

$$q_1\cdots q_n \mid a'-a'', \tag{7}$$

что возможно, лишь если $a'=a''$.

Количество n-ок $\langle a_1,\ldots,a_n\rangle$, удовлетворяющих (1), очевидно, равно $q_1\cdots q_n$, и каждая n-ка $\langle a_1,\ldots,a_n\rangle$ из $q_1\cdots q_n$ n-ок (4) удовлетворяет (1). Отсюда получаем, что каждая n-ка, удовлетворяющая (1), встречается в (4) ровно один раз.

3. Теорема Куммера

ТЕОРЕМА (Куммер [1852]). *Если p — простое число, то степень, в которой оно входит в разложение на простые множители биномиального коэффициента $\binom{m+n}{m}$, равна количеству переносов из разряда в разряд при сложении чисел m и n в позиционной системе счисления с основанием p.*

Для доказательства заметим, что из равенства

$$\binom{m+n}{m} = \frac{(m+n)!}{m!\,n!} \tag{1}$$

следует, что

$$\mathbf{deg}_p\left(\binom{m+n}{m}\right) = \mathbf{deg}_p((m+n)!)-\mathbf{deg}_p(m!)-\mathbf{deg}_p(n!), \tag{2}$$

где $\mathbf{deg}_p(k)$ — степень, в которой p входит в разложение k. Нетрудно понять, что

$$\mathbf{deg}_p(k!)= k \;\mathbf{div}\; p + k \;\mathbf{div}\; p^2 + \ldots, \tag{3}$$

поскольку среди чисел $1,\ldots,k$ ровно $k \;\mathbf{div}\; p$ чисел делятся на p, ровно $k \;\mathbf{div}\; p^2$ чисел делятся на p^2 и т. д. Таким образом,

$$\mathbf{deg}_p\left(\binom{m+n}{m}\right)= \sum_{k\geq 1} ((m+n) \;\mathbf{div}\; p^k - m \;\mathbf{div}\; p^k - n \;\mathbf{div}\; p^k). \tag{4}$$

Осталось заметить, что в этой сумме каждое слагаемое равно 1 или 0 в соответствии с тем, происходит ли перенос из $(k-1)$-го в k-й разряд или нет.

4. Суммирование обобщённой геометрической прогрессии

Пусть

$$G_n(q,w) = \sum_{i=0}^{w} q^i i^n \tag{1}$$

— сумма обобщённой геометрической прогрессии. Как известно, в случае обычной геометрической прогрессии, т. е. при $n=0$,

$$G_n(q,w) = \frac{q^{w+1}-1}{q-1} \tag{2}$$

для $q\neq 1$. Покажем по индукции, что для любого n имеются полиномы P_n с це-

лыми коэффициентами такие, что

$$G_n(q,w) = \frac{P_n(q,q^w w)}{(q-1)^{n+1}}. \tag{3}$$

Подставляя $w+1$ вместо w в (1) и дифференцируя по q, получаем, что

$$\frac{\partial}{\partial q}G_n(q,w+1) = \sum_{i=0}^{w+1} q^{i-1} i^{n+1} = \sum_{i=0}^{w} q^i (i+1)^{n+1} =$$

$$= \sum_{i=0}^{w} \sum_{j=0}^{n+1} \binom{n+1}{j} q^i i^j = \sum_{j=0}^{n+1} \binom{n+1}{j} G_j(q,w). \tag{4}$$

Полиномы P_n можно теперь найти на основе рекуррентного соотношения

$$G_{n+1}(q,w) = \frac{\partial}{\partial q}G_n(q,w+1) - \sum_{j=0}^{n} \binom{n+1}{j} G_j(q,w). \tag{5}$$

УКАЗАНИЯ К УПРАЖНЕНИЯМ

1.1. Очевидно, что уравнение (1.3.2) разрешимо в натуральных числах тогда и только тогда, когда уравнение $D(x_1-1,\dots,x_m-1)=0$ разрешимо в положительных целых числах. Аналогично, уравнение (1.3.2) разрешимо в положительных целых числах тогда и только тогда, когда уравнение $D(x_1+1,\dots,x_m+1)=0$ разрешимо в натуральных числах.

1.2. Известно, что любое натуральное число вида $4x+1$ представимо в виде суммы квадратов трех целых чисел. Ясно, что два из них чётны, а одно нечётно, и, следовательно, x имеет представление $x=y_1^2+y_2^2+y_3^2+y_3$, которое позволяет ограничиться трёхкратным увеличением количества неизвестных. Известно также, что любое натуральное число представимо в виде суммы $y_1(y_1-1)/2+y_2(y_2-1)/2+y_3(y_3-1)/2$ трёх *треугольных чисел*. Это даёт другой путь к лишь трёхкратному увеличению количества неизвестных.

Так называемое *уравнение Пелля* $y^2-dz^2=1$ разрешимо относительно y и z при любом значении d, не являющимся полным квадратом. Это позволяет заменить последние m уравнений системы (1.3.3) на $y_i^2-(4x_i-1)z_i^2=1$, что также даёт трёхкратное увеличение количества неизвестных. Используя упражнение 8.2, можно устранить $y_1,\dots,y_m$ ценой введения всего одной неизвестной, что приведёт к уравнению с $2m+1$ неизвестной.

Мощная техника главы 4 позволяет установить существование такой константы **m**, что любое уравнение может быть преобразовано в эквивалентное уравнение с **m** целочисленными неизвестными (см. также § 8.1).

1.3. Вместо (1.3.6) можно взять уравнение

$$\prod D(\pm x_1,\dots,\pm x_m) = 0,$$

где произведение берётся по всем 2^m вариантам выбора знаков "+" или "−".

1.4. Вместо уравнения (4.8) можно взять уравнение

$$(\chi_{0,1}^2+\chi_{0,2}^2+\chi_{0,3}^2+\chi_{0,4}^2+1)\times$$

$$\times(1-D^2(\chi_{0,1}^2+\chi_{0,2}^2+\chi_{0,3}^2+\chi_{0,4}^2,\dots,\chi_{m,1}^2+\chi_{m,2}^2+\chi_{m,3}^2+\chi_{m,4}^2))-1=a.$$

1.5. Пусть полином $P(x_1,\dots,x_m)$ принимает только простые значения. Положим $p=|P(1,\dots,1)|$ и рассмотрим полином $Q(y_1,\dots,y_m)=$ $=P(py_1+1,\dots,py_m+1)$. Очевидно, что $Q(y_1,\dots,y_m)\equiv P(1,\dots,1)\equiv 0 \pmod p$ и, следовательно, $Q(y_1,\dots,y_m)=\pm p$. Таким образом, Q, а значит, и P — тождественные полиномы.

1.6. Вместо уравнения (1.4.8) в случае натуральнозначных неизвестных можно взять уравнение

$$x_0(1-x_0D^2(x_0-1,x_1,\dots,x_m))-1-(x_0+1)x_{m+1}(1+x_0D^2(x_0-1,x_1,\dots,x_m))=a.$$

1.7. Множество, задаваемое уравнением (1.4.7), есть в точности множество всех целочисленных значений дроби

$$\frac{x_0+D^2(x_0,\ldots,x_m)}{1+(x_0+1)D^2(x_0,\ldots,x_m)}.$$

1.8. а) В качестве A можно взять любой полином с неотрицательными коэффициентами, принимающий каждое своё значение ровно один раз (примеры таких полиномов см. в § 3.1 и упражнении 3.1). Аналогом уравнения (1.4.8) будет уравнение

$$(A(y_1,\ldots,y_n)+1)(1-D^2(y_1,\ldots,y_n,x_1,\ldots,x_m))-1=A(a_1,\ldots,a_n),$$

где $D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0$ — уравнение, задающее множество $\mathfrak{M}$.

б) В качестве такой системы можно взять

$$(y_1+1)(1-D^2(y_1,\ldots,y_n,x_1,\ldots,x_m))-1=a_1,$$

$$y_2=a_2,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$y_m=a_m.$$

1.9. Можно положить

$$E(b_1,\ldots,b_n,x_0,\ldots,x_m)=(x_0+1)(1-D^2(x_0,b_1,\ldots,b_n,x_1,\ldots,x_m))-1,$$

где D — полином из представления (1.5.5).

1.10. Вот соответствующие представления:

а) $(x+2)(y+2)=a$;

б) $x(2y+3)=a$;

в) $x^2<a<(x+1)^2$.

1.11. Впервые это было установлено Дж. Робинсон [1952]. Другое представление легко может быть получено на основе техники главы 2.

1.12. Необходимым и достаточным условием для того, чтобы p/q и r/s были последовательными подходящими дробями является выполнение равенства $|ps-qr|=1$ и одного из двух двусторонних неравенств $p/q\leq X\leq r/s$ или $r/s\leq X\leq p/q$. Число X может быть задано рациональными числами a/b и c/d и полиномом $A(x)$ с целыми коэффициентами такими, что X — единственный корень уравнения $A(\eta)=0$ на интервале $[a/b,c/d]$, причём $A(a/b)<0$, $A(c/d)>0$. В этом случае $x/y<X \iff x/y<a/b\vee[x/y<c/d\&A(x/y)<0]$.

1.13. Понятие тригонометрического диофантова уравнения было введено в работе Конвея и Джонса [1976] в формально более широкой постановке, чем в упражнении 1.11, и там же получена сводимость к 10-й проблеме Гильберта.

1.14. См., например, работу Амика [1964].

1.15. Этот результат, принадлежащий А. Тарскому, был опубликован Дж. Робинсон [1952]. Доказательство было основано на найденном А. Тарским обобщении теоремы Штурма о количестве вещественных корней по-

линома в данном интервале. Другое доказательство легко может быть получено на основе развитой в главе 6 техники устранения ограниченного квантора общности и несложных оценок величины корня через коэффициенты.

2.1. Это было сделано Дж. Робинсон [1952].

2.2. Это также было сделано Дж. Робинсон [1952]. Если четвёрка $\langle a_1, b_1, a_2, b_2\rangle$ принадлежит множеству из упражнения 2.1, $b_2=b_1+1$ и b_1 достаточно велико, то $n = ((a_2-a_1)b_1)\ \mathbf{div}\ a_1$.

2.3. Это было сделано в работе Матиясевича [1968в] с помощью разложения в цепную дробь квадратичных иррациональностей вида

$$\mathbf{sqrt}(((2b+1)^m+b+1)^2-2b-1).$$

2.4. Значения x и z связаны соотношением $z=x-ay/2$.

2.5. Эти последовательности были использованы, в частности, в работе Матиясевича [1972а]. Для них характеристическим уравнением, аналогичным (2.1.12), является

$$x^2-bxy-y^2=\pm 1.$$

2.6. Можно, например, воспользоваться сравнением (2.1.5) — при достаточно большом d

$$\alpha_b(n)=\mathbf{rem}(\alpha_{b+d}(n),\ d).$$

2.7. Доказательство легко проводится индукцией по n. При достаточно большом x

$$b^c=\mathbf{rem}((x-b)\alpha_x(c)-\alpha_x(c+1),\ bx-b^2-1).$$

Идея этого диофантова представления восходит к работе Дж. Робинсон [1952], где указано аналогичное сравнение для решений уравнения Пелля из упражнения 1.2.

2.8. Это было сделано в работе Дж. Робинсон [1952].

2.9. Если мы знаем наименьшую высоту башни экспонент, то, как показано в работе Дж. Робинсон [1952], мы можем дать обобщённое диофантово представление для некоторого отношения экспоненциального роста, после чего остаётся воспользоваться упражнением 2.8.

2.9. В работе Девиса [1968] это сделано в более сильном предположении о единственности решения $u=r=1$, $v=s=0$. Ослабление этого предположения до ограниченного количества решений трудностей не вызывает.

3.1. Этот полином был предложен в качестве нумерующего в работе Косовского [1971].

3.2. В работе Больман и Лаплазы [1978] говорится, что это было установлено в (труднодоступном) отчёте Лью и Розенберга [1975].

3.3. Первоначально диофантовость этой функции была установлена в работе Девиса, Патнама и Робинсон [1961] с помощью равенства

$$\prod_{k\le c}(a+bk)=\binom{a/b+c}{c+1}b^{c+1}(c+1)!.$$

Другое доказательство, не требующее установления диофантовости биномиальных коэффициентов с рациональными аргументами, было предложено в работе Дж. Робинсон [1971]. Оно основано на сравнении

$$\prod_{k\le c}(a+bk)\equiv\binom{x+c}{c+1}b^{c+1}(c+1)!(\mathbf{mod}\ m),$$

справедливом, если $a\equiv bx(\mathbf{mod}\ m)$.

3.4. См. работу Джонса и Матиясевича [1982б]. При достаточно большом x целая часть числа $x^n/\mathbf{sqrt}(1-4/x)$ является шифром по основанию x кортежа, первый элемент которого равен $\binom{2n}{n}$.

3.5. Если $2<m$, $q_m<m^m$, $m^{2m}<t$, то неравенство

$$\left|t^m e^{1/t}-\frac{p_m}{q_m}\right|<\frac{1}{t}$$

эквивалентно равенству

$$\frac{p_m}{q_m}=\sum_{k=0}^{m}\frac{t^{m-k}}{k!}.$$

Выражение $e^{1/t}$ можно заменить на $\left(1+\frac{1}{yt}\right)^y$ при достаточно большом y, и остаётся заметить, что

$$m!=\left(\frac{p_m}{q_m}-t\times\frac{p_{m-1}}{q_{m-1}}\right)^{-1}.$$

3.6. Используйте тождество

$$\sum_{k=0}^{\infty}\frac{B_k}{k!}\tau^k=\frac{\tau}{e^{\tau}-1}$$

аналогичное тождеству из упражнения 3.5.

3.7. Воспользуйтесь тем, что по теореме Штаудта-Клаузена

$$B_{2m}=Z-\sum\frac{1}{p},$$

где Z — целое число, а суммирование идёт по всем простым p таким, что $p-1\mid 2m$.

3.8. $\neg\mathbf{Code}(a,b,c)\iff b<2\vee a\ge b^c$;

$$\neg\mathbf{Equal}(a_1,b_1,c_1,a_2,b_2,c_2)\iff$$
$$\iff\neg\mathbf{Code}(a_1,b_1,c_1)\vee\neg\mathbf{Code}(a_2,b_2,c_2)\vee c_1\ne c_2\vee$$
$$\vee\exists k[\mathbf{Elem}(a_1,b_1,k)\ne\mathbf{Elem}(a_2,b_2,k)];$$

$$\neg\mathbf{NotGreater}(a_1,b_1,a_2,b_2)\iff\exists k[\mathbf{Elem}(a_1,b_1,k)>\mathbf{Elem}(a_2,b_2,k)];$$

$$\neg\mathbf{Small}(a,b,c,e)\iff\neg\mathbf{Code}(a,b,c)\vee\exists k[\mathbf{Elem}(a,b,k)>e].$$

3.9. $a=\mathbf{Mult}(p,q,r,u,v,w)\iff$

$$\iff\exists xy[a=xy\&\mathbf{Equal}(p,q,r,u,(qv)^w,r)\&\mathbf{Equal}(u,v,w,y,qv,w)];$$

$$\mathbf{Add}(p,q,r,u,v,w)=$$
$$=\mathbf{Mult}(p,q,r,\mathbf{Repeat}(1,v,w),v,w)+\mathbf{Mult}(\mathbf{Repeat}(1,q,r),q,r,u,v,w).$$

3.10. $s=\mathbf{Sum}(a,b,c) \iff \exists x[\mathbf{Equal}(a,b,c,z,bc+2,c)\&s=\mathbf{rem}(x,bc+1)]$.

3.11. $l=\mathbf{Less}(a_1,a_2,b) \iff \exists wx_1x_2y[\mathbf{Small}(l,b,w,1)\&$
$\&\mathbf{Equal}(a_1,b,w,x_1,2b,w)\&\mathbf{Equal}(a_2,b,w,x_2,2b,w)\&\mathbf{Equal}(l,b,w,y,2b,w)\&$
$\&\mathbf{NotGreater}(x_1+y,2b,x_2,2b)\&\mathbf{NotGreater}(x_2,2b,x_1+by,2b)]$.

3.12. Не ограничивая общности будем считать, что $a\geq 2$. Пусть $b=a+1$, $c=a-1$, $y=\mathbf{Repeat}(1,b,c)$, а z — шифр по основанию b кортежа $\langle 2,3,\ldots,a\rangle$ длины c. (Этот шифр явно вычисляется по a, b и c — см. Приложение 4). Кортеж с шифром $x=\mathbf{Mult}(z,b,c,z,b,c)$ содержит все составные числа, не превосходящие a. Число q, также не превосходящее a, будет простым тогда и только тогда, когда

$$\mathbf{NotEqual}(x,\mathbf{Repeat}(q,b^2,c^2),c^2)=w,$$

где

$$\mathbf{NotEqual}(a_1,a_2,d)=\mathbf{Less}(a_1,a_2,d)+\mathbf{Less}(a_2,a_1,d),\qquad w=\mathbf{Repeat}(1,b^2,c^2).$$

Положим $u=\mathbf{NotEqual}(\mathbf{Mult}(y,b,c,x,b^2,c^2),\mathbf{Mult}(z,b,c,w,b^2,c))$. В кортеже с кодом $\langle u,b^{3c^2},c\rangle$ ровно $\pi(a)$ элементов равны w, так что

$$\pi(a)=c-\mathbf{Sum}(\mathbf{NotEqual}(u,\mathbf{Repeat}(w,b^{3c^2},c),b^{3c^2}),b^{3c^2},c).$$

3.13. Число p является n-ым простым числом, если и только если $\pi(p-1)=n-1$, $\pi(p)=n$. Остаётся воспользоваться упражнениями 3.7 и 1.9.

3.14. Можно воспользоваться тем, что двоичная запись числа получается из его 2^d-ичной записи путём замены каждой цифры на её двоичную запись (дополненную, при необходимости, нулями). Это позволяет с помощью теоремы Куммера дать диофантово представление четырёхместного отношения $\mathbf{Small}(a,2^d,c,2^l)$.

3.15. Это было сделано в работе Матиясевича [1971б]. Шифр d кортежа $\langle\delta(0),\ldots,\delta(n)\rangle$ удовлетворяет сравнению

$$(b_0w^k+\ldots+b_{k-1}w)d\equiv a_0+\ldots+a_{k-1}w^{k-1}+d(\mathbf{mod}\ \ w^{n+1})$$

и неравенству $d<w^{n+1}$ при достаточно большом основании w и определяется этими условиями.

3.16. $m=\mathbf{Min}(a_1,a_2,b) \iff \mathbf{NotGreater}(m,b,a_1,b)\&\mathbf{NotGreater}(m,b,a_2,b)\&$
$\&\mathbf{Less}(\mathbf{Less}(m,a_1,b),\mathbf{Less}(m,a_2,b))=\mathbf{Less}(m,a_2,b)\&$
$\&\mathbf{Less}(\mathbf{Less}(m,a_2,b),\mathbf{Less}(m,a_1,b))=\mathbf{Less}(m,a_1,b)$.

3.17. Существование и единственность представления были установлены в работе Нильсена [1924]. Конкатенации соответствует перемножение соответствующих матриц.

4.1. Рассмотрим уравнение

$$U^2(a_1,\ldots,a_{n-1},x_0,\ldots,x_l,y_1,\ldots,y_w)+(a_n-2^{2^l}\mathbf{Cantor}_{l+1}(x_0,\ldots,x_l))^2=0.$$

Пусть $k_1^D,\ldots,k_l^D$ — такие числа, что это уравнение разрешимо относительно $x_0,\ldots,x_l$, $y_1,\ldots,y_w$ одновременно с уравнением (4.1.3), тогда уравнение

$$U(a_1,\ldots,a_{n-1},\ 2^{2^l}\mathbf{Cantor}(a_n,k),\ k_1^D,\ldots,k_l^D,\ y_1,\ldots,y_w)=0$$

также будет универсальным.

4.2. В работе Матиясевича [1972б] построены универсальные уравнения следующих видов:

$$V(a_1,\ldots,a_n,x_1,\ldots,x_m)=k;$$
$$V(k,x_1,\ldots,x_m)=W(a_1,\ldots,a_n);$$
$$V(x_1,\ldots,x_m)=W(a_1,\ldots,a_n,k).$$

4.3. $\mathbf{Format}(d,e,f) \iff d>1\&\mathbf{Equal}(f+2,\ 2,\ d^e+1,\ f+2^{d^{e+1}},\ 2^d,\ d^e+1).$

4.4. Идея универсального уравнения с «прозрачной» структурой была предложена в работе Косовского [1971]. Конкретные значения d и m были определены, в частности, в работе Джонса [1982б] — см. комментарии к главе 8.

```
5.1. DOUBLE = LAST; MARK(3);
               while THEREWAS(3) do INC od

5.2. ERASE = STAR; RIGHT; WRITE(2); MARK(2);
             while THEREIS(2) do
               while READ(2) do RIGHT od;
               while READ(0) do LEFT; WRITE(0); RIGHT; WRITE(2) od;
               while READ(1) do LEFT; WRITE(1); RIGHT; WRITE(2) od;
               while READ(λ) do
                 while LEFT; READ(2) do WRITE(λ) od od od
5.3. BIN(1) = NEW;
              while READNOT(.) do STAR; RIGHT;
                 while READ(2) do RIGHT od;
                 while READ(0) do WRITE(2); DOUBLE od;
                 while READ(1) do WRITE(2); DOUBLE; INC od od;
              WRITE(2); ERASE

     BIN(n + 1) = BIN(1); BIN(n)
```

5.4. Это можно сделать двумя путями. Первый из них состоит в построении машины Тьюринга, которая преобразует единиричное представление кортежа в двоичное. Второй способ состоит в модификации условия (5.5.38), которое надо заменить на

$$\langle t,b,a\rangle=\langle æ,b,1\rangle+\langle d_1,b,c_1\rangle+\langle Q,b,1\rangle+\ldots+\langle d_n,b,c_n\rangle+\langle Q,b,1\rangle,$$

где Q — номер символа ",", а числа $d_1,\ldots,d_n$, $c_1,\ldots,c_n$ удовлетворяют условиям $\mathbf{Equal}(a_1,2,c_1,d_1,b,c_1),\ldots,\mathbf{Equal}(a_n,2,c_n,d_n,b,c_n)$.

5.5. Чтобы установить диофантовость функции, вычислимой по Тьюрингу, достаточно извлечь её значение из кортежа с шифром $\mathrm{AfterT}(k,p,t)$.

где k, p и t определены условиями (5.5.36)–(5.5.38), что легко сделать по аналогии с (5.5.38).

Пусть теперь

$$D_F(a_0,a_1,\ldots,a_n,x_1,\ldots,x_m)=0$$

— диофантово представление некоторой функции F. Возьмём в качестве уравнения (5.4.1) уравнение

$$D_F(x_{m+1},a_1,\ldots,a_n,x_1,\ldots,x_m)=0$$

и построим по нему машину M, описанную в § 5.4. В момент остановки машины M на ленте записан кортеж (5.4.9), в котором $y_m=F(a_1,\ldots,a_n)$. Остаётся применить $2m+n+2$ раза машину ERASE и $k+1$ раз машину DELETE.

5.6. Пусть M — машина Тьюринга, имеющая ленту, бесконечную в обе стороны, на которой она пишет слова из алфавита $\{\alpha_1,\ldots,\alpha_w\}$. Работу этой машины можно смоделировать некоторой машиной M', лента которой имеет конец. Машина M' работает в алфавите

$$\{\star,\alpha_1,\ldots,\alpha_w,\beta_1,\ldots,\beta_w,\gamma_{11},\ldots,\gamma_{ww}\}.$$

Лента машины M' имитирует ленту машины M, сложенную пополам. Чтобы «распрямить» ленту машины M', надо снять с неё две копии: в одной копии β_j заменяется на пустые клетки, γ_{ij} — на α_j, в другой копии α_i заменяется на пустые клетки, β_i и γ_{ij} — на α_i. Клетки с маркером конца "$\star$" отрезаются, и две полубесконечные ленты склеиваются в одну ленту машины M.

Количество состояний удваивается: для каждого состояния q_i машины M имеются два состояния q_i^L и q_i^R машины M', соответствующие нахождению головки машины M на левой или правой половине ленты. Инструкции машины M' естественным образом получаются из инструкций машины M. А именно, каждой инструкции $q_i\alpha_j \Rightarrow \alpha_k D q_l$ машины M соответствуют инструкции $q_i^R\alpha_j \Rightarrow \alpha_k D q_l^R$, $q_i^R\gamma_{mj} \Rightarrow \gamma_{mk} D q_l^R$, $q_i^L\beta_j \Rightarrow \beta_k \bar{D} q_l^L$, $q_i^L\gamma_{jm} \Rightarrow \gamma_{km} \bar{D} q_l^L$ машины M', где $\bar{D}$ — направление, противоположное D, т. е. $\bar{L}=R$, $\bar{R}=L$, $\bar{S}=S$. Аналогично, каждой инструкции $q_i\Lambda \Rightarrow \alpha_k D q_l$ соответствуют инструкции $q_i^R\beta_m \Rightarrow \gamma_{mk} D q_l^R$, $q_i^L\alpha_m \Rightarrow \gamma_{km} \bar{D} q_l^L$, $q_i^R\Lambda \Rightarrow \alpha_k \bar{D} q_l^R$, $q_i^L\Lambda \Rightarrow \beta_k \bar{D} q_l^L$. Кроме того, имеются инструкции $q_i^R\star \Rightarrow \star R q_i^L$, $q_i^L\star \Rightarrow \star R q_i^R$.

5.7. а) Эквивалентность регистровых машин машинам Тьюринга была установлена в тех работах, где вводилось это понятие (см. комментарии к главе 5).

б) Диофантово моделирование регистровых машин см. в работах Джонса и Матиясевича [1984], Матиясевича [1984].

5.8. Это было показано в работах Чудновского [1971, 1984]. Пусть

$$b\in\{2^a \mid a\in\mathfrak{D}\} \iff \exists x_1\ldots x_m[D(b,x_1,\ldots,x_m)],$$

тогда требуемое представление множества $\mathfrak{D}$ лишь формой записи отличается от

$$D^2(x_0^a,x_1,\ldots,x_m)+(x_0-2)^2=0.$$

6.1. Именно такой была оригинальная конструкция из работы Девиса, Патнама и Робинсон [1961]. См. упражнение 3.3 для аналога (2.13).

6.2. Такая форма принципа Дирихле была использована в работе Матиясевича [1972].

6.3. Это легко получается путем m-кратного применения мультипликативного принципа Дирихле из упражнения 6.2 (см., например, работы Матиясевича [1972, 1973]).

6.4. См. работы Матиясевича [1972, 1973].

6.5. Эта идея была предложена в работе Хиросе и Иды [1973].

6.6. См. работу Девиса, Матиясевича и Робинсон [1975].

6.7. Доказательство могло бы быть аналогичным доказательству недиофантовости множества $\mathfrak{H}_0$ в § 4.6, если бы мы смогли установить диофантовость функции, которая по p и q выдаёт номер уравнения (4.6.8), получающегося из уравнения (4.6.4) подстановкой конкретных значений параметров. Проще, однако, вместо уравнения (4.6.8) рассмотреть уравнение с $\mathbf{m}+2$ неизвестными

$$\mathbf{U}_1^2(x_{\mathbf{m}+1}, x_{\mathbf{m}+2}, x_1, \ldots, x_{\mathbf{m}})+(x_{\mathbf{m}+1}-p)^2+(x_{\mathbf{m}+2}-q)^2=0.$$

Пусть i и j — такие числа, что

$$\mathbf{U}_1(x_{\mathbf{m}+1}, x_{\mathbf{m}+2}, x_1, \ldots, x_{\mathbf{m}})=\mathbf{P}_i(x_1, \ldots, x_{\mathbf{m}+2})-\mathbf{P}_j(x_1, \ldots, x_{\mathbf{m}+2}),$$

тогда предыдущее уравнение можно переписать в виде уравнения

$$\mathbf{P}_i^2(x_1, \ldots, x_{\mathbf{m}+2})+\mathbf{P}_j^2(x_1, \ldots, x_{\mathbf{m}+2})+x_{\mathbf{m}+1}^2+x_{\mathbf{m}+2}^2+p^2+q^2=$$
$$=2(\mathbf{P}_i(x_1, \ldots, x_{\mathbf{m}+2})\mathbf{P}_j(x_1, \ldots, x_{\mathbf{m}+2})+px_{\mathbf{m}+1}+qx_{\mathbf{m}+2}),$$

номер которого, как нетрудно понять, является значением некоторого полинома $L(i, j, p, q)$ с рациональными коэффициентами.

6.8. Это было доказано Р. М. Робинсоном [1956], доказательство можно также найти в монографии Девиса [1974].

7.1. Это доказано в работе Сморинского [1977] с использованием однократных экспоненциальных диофантовых представлений.

7.2. См. работу Сморинского [1977].

7.3. $d^c=\mathbf{rem}(b^{c(c+1)(d+1)}, b^{(c+1)(d+1)}-d)$.

7.4. Вместо (1.4.5) можно взять уравнение

$$(D_1^2(a_1, \ldots, a_n, x_1, \ldots, x_{m_1})+y_1^2+\ldots+y_{m_2}^2)\times(D_2^2(a_1, \ldots, a_n, y_1, \ldots, y_{m_2})+x_1^2+\ldots+x_{m_1}^2)=0.$$

7.5. Это доказано в работе Матиясевича [1973].

7.6. Первоначально это было установлено в работе Денефа [1975]. Более сильные результаты были затем получены в работах Денефа и Липшица [1978] и Денефа [1980].

7.7. Это было показано в работе Адлера [1971]. В работе Сморинского [1977] приведена более простая конструкция, использующая технику, изложенную в § 7.4.

8.1. Это отношение задаётся формулой

$$\exists x[(b^2+c^2+1)(d-e)=\left(\frac{b-c}{a+1}\right)^2+x+1].$$

8.2. В работе Матиясевича и Робинсон [1975] показано, что таким представлением является

$$\exists x[\prod(x\pm\mathbf{sqrt}(S_1(a_1,\ldots,a_n))\pm\mathbf{sqrt}(S_2(a_1,\ldots,a_n))W\pm\ldots\pm\mathbf{sqrt}(S_k(a_1,\ldots,a_n))W^{k-1})=0].$$

Здесь W — сокращение для суммы $1+S_1^2(a_1,\ldots,a_n)+\ldots+S_k^2(a_1,\ldots,a_n)$, а произведение берётся по всем 2^k способом выбора знаков $\pm$, так что после элементарных алгебраических преобразований все квадратные корни исчезают.

8.3. По условию

$$\mathbf{deg}_p(a^2q)=2\mathbf{deg}_p(a)+\mathbf{deg}_p(q)\equiv 1\not\equiv 0\equiv\mathbf{deg}_p(b^2)(\mathbf{mod}\ 2),$$

поэтому $2kl\le\mathbf{deg}_p(a^2q+b^2)=\mathbf{min}(\mathbf{deg}_p(a^2q),\mathbf{deg}_p(b^2))$. По индукции легко получить, что из делимости

$$q^{2^{m-1}}\mid a_1^2q+(a_2^2q+(\ldots(a_{m-1}^2q+a_m^2)^2\ldots)^2)^2$$

следуют делимости $p\mid a_1,\ldots,p\mid a_m$.

8.4. Не ограничивая общности, мы можем считать, что $B(a,b,w)\ge 4$, а следовательно, $q_y\equiv -1(\mathbf{mod}\ 4)$, и потому среди простых делителей q_y вида $4n-1$ найдётся такой, который входит в нечётной степени.

8.5. Первоначально это было доказаио в работе Матиясевича [1972], другое доказательство см. в работе Джонса [1981].

8.6. См. работу Матиясевича и Робинсон [1974].

8.7. См. работу Джонса [1981].

8.8. См: работу Матиясевича [1972].

8.9. Таким свойством обладает, в частности, множество всех значений полинома $x_1^k+2x_2^k+\ldots+2^{m-1}x_m^k$, когда k велико по сравнению с m. Этот пример, предложенный Р. М. Робинсоном, приведён в работе Матиясевича и Робинсон [1975].

8.10. Это было сделано в работе Джонса и Матиясевича [1982] с использованием вместо универсального представления (3.4.2) произвольного биномиального коэффициента специального представления центрального биномиального коэффициента из упражнения 3.4.

8.11. Этот результат был получен в работе Девиса [1973б] как прямое следствие известной теоремы Блюма [1967] об ускорении.

9.1. Пусть χ — единственный корень алгебраического уравнения $A(\chi)=0$ на интервале $[\alpha,\beta]$ с рациональными концами, причём $A(\alpha)<0$, $A(\beta)>0$. Требуемым диофантово вещественным числом будет

$$\alpha<\frac{a-b}{c+1}<\frac{a-b+1}{c+1}<\beta\ \&\ c>d\ \&\ A\left(\frac{a-b}{c+1}\right)<0\ \&\ A\left(\frac{a-b+1}{c+1}\right)>0.$$

9.2. Ясно, что достаточно установить диофантовость функций D, E и F таких, что

$$\frac{D(n)-E(n)}{F(n)+1} = \sum_{k=0}^{n} \frac{A(k)-B(k)}{C(k)+1} .$$

Для этого можно рассмотреть кортежи $\langle D(0),\ldots,D(n)\rangle$, $\langle E(0),\ldots,E(n)\rangle$, $\langle F(0),\ldots,F(n)\rangle$. Элементы этих кортежей связаны очевидными соотношениями, которые легко могут быть записаны с помощью ограниченного квантора общности.

9.3. $\mathbf{e} = \frac{1}{0!}+\frac{1}{1!}+\ldots$, $\frac{\pi}{4} = 1-\frac{1}{3}+\frac{1}{5}-\ldots$ Остаётся применить упражнение 9.2.

9.4. Вместо системы функций $X_1(\tau),\ldots,X_k(\tau)$ можно взять одиу функцию $X(\sigma_1,\ldots,\sigma_k,\tau)$, удовлетворяющую уравнениям

$$\frac{\partial^2 X}{\partial\sigma_i\partial\sigma_j}=0,$$

и подставить в (9.3.13) и (9.3.14) $\partial X/\partial\sigma_i$ вместо X_i. Эта идея была предложена в работе Адлера [1969].

10.1. а) Поскольку в разрешимости первого уравнения заинтересован игрок B, заменим неизвестные $x_1,\ldots,x_m$ на $b_2,\ldots,b_{m+1}$. Аналогично, в разрешимости второго уравнения заинтересован игрок A, поэтому заменим $y_1,\ldots,y_m$ на $a_3,\ldots,a_{m+2}$. Выбирая значения последней переменной b_{m+2}, игрок B будет иметь возможность продемонстрировать, что $a_3,\ldots,a_{m+2}$ не являются решением. Окончательно получаем диофантову игру, задаваемую уравнением

$$U_1(a_2,a_1,b_2,\ldots,b_{m+1})\times[U_1^2(b_1,a_1,a_3,\ldots,a_{m+2})-b_{m+2}-1]=0.$$

б) Допустим, что игрок B однажды проиграл; в дальнейшем он всегда будет выигрывать, выбирая вторым ходом то число, которое игрок A выбрал третьим ходом, приведшим его к победе.

в) См. работу Джонса [1982a].

10.2. Это установлено в работе Ибарры и Лейнингера [1983], где показано, что такие программы могут вычислять значения полиномов с натуральными коэффициентами и сравнивать числа.

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 négative du 10e problème de Hilbert // Lect. Notes Math.- V. 244.- P. 11-28.

Айвазян С. В.

[1983] О некоторых бесконечных цепях многообразий групп // Докл. АН АрмССР.- Т. 26, № 5.- С. 198-200.

[1988] Об одной проблеме А. И. Мальцева // Сиб. мат. ж.- Т. 29, № 6.- С. 3-11.

Амик (Amic Y.)

[1964] Interpolation p-adique // Bull. Soc. math. France.- V. 92, N 2.- P. 118-180.

Аник (Anick D. J.)

[1985] Diophantine equations, Hilbert series, and undecidable spaces // Ann. Math.- V. 122, N 1.- P. 87-112.

Бакстер (Baxter L.D.)

[1978] The undecidability of the third order dyadic unification problem // Inf. and Contr.- V. 38, N 2.- P. 170-178.

Бартон и Фич (Barton D., Fitch J. P.)

[1972a] Application of algebraic manipulation programs in physics // Rept. Progress Phys.- V. 35, N 3.- P. 235-314.

[19726] A review of algebraic manipulative programs and their application // Comput. J.- V. 15, N 4.- P. 362-381.

Баур (Baur W.)

[1974] Über rekursive Strukturen // Invent. math.- Bd 23, N 2.- S. 89-95.

Бейкер (Baker A.)

[1968] Contributions to the theory of diophantine equations I. On the representation of integers by binary forms // Philos. Trans. Roy. Soc. London (A).- V. 263, N 1139.- P. 173-191.

Бек (Beck H.)

[1975] Zur Entscheibarkeit der funktionalen Äquivalenz // Lect. Notes Computer Sci.- V. 33.- P. 127-133.

Белл и Маховер (Bell J. L., Machover M.)

[1977] A course in mathematical logic.- Amsterdam; New York; Oxford: North Holland.

Блюм (Blum M.)

[1967] A machine independent theory of the complexity of recurcive functions // J. Assoc. Comput. Mach.- V.14, N 2.- P. 322-336.- Русский перевод в сб. Проблемы матем. логики. М.: Мир, 1970.- С. 401-422.

Бокуть Л. А.

[1972] Неразрешимость проблемы равенства и подалгебры конечно-определенных алгебр Ли // Изв. АН СССР. Сер. мат.- Т. 35, № 6.- С. 1179-1225.

Больман и Лаплаза (Bollman D., Laplaza M.)

[1978] Some decision problems for polynomial mappings // Theor. Comput. Sci.- V. 6, N 3.- P. 317-325.

Бриттон (Britton J.L.)

[1979] Integer solution of systems of quadratic equations // Math. Proc. Cambridge Phil. Soc.- V. 86, part 3.- P. 385-389.

Вада (Wada H.)

[1975] Полиномиальное представление простых чисел (японск.) // Сугаку.- Т. 27, №2.- С. 160-161.

Важенин Ю. М.

[1987] Алгоритмические проблемы и иерархии языков первого порядка // Алгебра и логика.- Т. 26, № 4.- С. 419-434.

[1988] Критические теории // Сиб. мат. ж.- Т.29, № 1.- С. 23-31.

[1989] Критические теории некоторых классов неассоциативных колец // Алгебра и логика.- Т. 28, № 4.-С. 393-401.

Валиев М. К.

[1975] On polinomial reducibility of word problem under embedding of recursively presented groups in finitely presented groups // Lect. Notes Computer Sci.- V. 32.- P. 432-438.

Ванг П. (Wang P.)

[1974] The undecidability of the existence of zeros of real elementary functions // J. Assoc. Comput. Mach.- V. 21, N 4.- P. 586-589.

Виноградов А. К. и Косовский Н. К.

[1975] Иерархия диофантовых представлений примитивно рекурсивных предикатов // Вычисл. техн. и вопр. кибериет.- № 12.- Л.: ЛГУ.- С. 99-107.

Вольстенхольм (Wolstenholme J.)

[1862] On certain properties of prime numbers // Quart. J. Math.- V. 5.- P. 35-39.

Гайфман (Gaifman H.)

[1975] A note on models and submodels of arithmetic // Lect. Notes Math.- V. 255.- P. 128-144.

Гайфман и Димитракопулос (Gaifman H., Dimitracopoulos C.)

[1982] Fragments of Peano's arithmetic and the MRDP theorem // Enseign. math.- V 30.- P. 187-206.

Гёдель (Gödel K.)

[1931] Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme. I // Monatsh. Math. und Phys.- Bd 38, H. 1.- S. 173-198.

Германо (Germano G.)

[1976] An arithmetical reconstruction of the liar's antinomy using addition and multiplication // Notre Dame J. Formal Logic.- V. 17, N 3.- P. 457-461.

Гермес (Hermes H.)

[1972] Die Unlösbarkeit des zehnten Hilbertschen Problem // Enseign. math. (2).- Bd 18, N 1.- P. 47-56.

[1978] Die Unlösbarkeit des zehnten Hilbertschen Problems // Math. und Naturwiss. Unterr.- Bd 31, N 5.- S. 260-263.

Гильберт (Hilbert D.)

[1900] Mathematische Probleme. Vortrag, gehalten auf dem internationalen Mathematiker Kongress zu Paris 1900 // Nachr. K. Ges. Wiss., Göttingen, Math.-Phis. Kl.- S. 253-297.- Русский перевод в сб.: Проблемы Гильберта.- М.: Наука, 1969.- С. 11-64.

Гольдфарб (Goldfarb W.D.)

[1981] The undecidability of the second-order unification problem // Theor. Comput. Sci.- V. 13, N 2.- P. 225-230.

Гуаспари (Guaspari D.)

[1979] Partially conservative extensions of arithmetic // Trans. Amer. Math. Soc.- V. 254.- P. 47-68.

Губер-Дайсон (Huber-Dyson V.)

[1984] HNN-constructing finite groups // Lect. Notes Math. // V. 1098.- P. 58-62.

Гудстейн (Goodstein R.L.)

[1975] Hilbert's tenth problem and the independence of recursive difference // J. London Math. Soc. (2).- V. 10, N 2.- P. 175-176.

Гудстейн и Ли (Goodstein R. L., Lee R. D.)

[1966] A decidable class of equations in recursive arithmetic // Z. math. Log. und Grundl. Math.- Bd 12.- S. 235-239.

Гурари (Gurari E. M.)

[1985] Decidable problems for powerful programs // J. Assoc. Comput. Mach.- V. 32, N 2.- P. 466-483.

Гурари и Ибарра (Gurari E. M., Ibarra O. H.)

[1982] Two-way counter machines and diophantine equations // J. Assoc. Comput. Math.- V. 29, N 3.- P. 863-873.

Гэри и Джонсон (Garey M. R., Johnson D. S.)

[1979] Computers and Intractability. A Guide to the Theory of NP-Completeness.- San Francisco: W.H.Freeman.- Русский перевод: Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи.- М.: Мир, 1982.

Дайсон, Джонс и Шепердсон
(Dyson V. H., Jones J. P., Shepherdson J. C.)

[1982] Some diophantine forms of Gödel's theorem // Arch. math. Logik Grundlagenforsch.- Bd 22, N 1-2.- S. 51-60.

Данько (Dańko W.)

[1980] A criterion of undecidability of algorithmic theories // London Math. Soc. Lect. Note Ser.- V. 88.- P. 205-218.

Девис (Davis M.)

[1950] Arithmetical problems and recursively enumerable predicates (abstract) // J. Symbolic Logic.- V. 15, N 1.- P. 77-78.

[1953] Arithmetical problems and recursively enumerable predicates // J. Symbol. Log.- V. 18, N 1, P. 33-41. Русский перевод: Математика, 1964, Т. 8, № 5.- С. 15-22.

[1962] Applications of recursive function theory to number theory // Proc. Symp. Pure Math.- V. 5.- P. 135-138.

[1963] Extentions and corollaries of recent work on Hilbert's tenth problem // Illinois J. Math.- V. 7, N 2.- P. 246-250.

[1966] Diophantine equation and recursively enumerable sets // Automata Theory.- New York: Academic Press.- P. 146-152.

[1968] One equation to rule them all // Trans. New York Acad. Sci, Ser. II.- V. 30, N 6.- P. 766-773.

[1971] An explicit diophantine definition of the exponential function // Commun. Pure Appl. Math.- V. 24, N 2.- P. 137-145.

[1972] On the number of solutions of Diophantine equations // Proc. Amer. Math. Soc.- V. 35, N 2.- P. 552-554.

[1973a] Hilbert's tenth problem is unsolvable // Amer. Math. Monthly.- V. 80, N 3.- P. 233-269.

[1973б] Speed-up theorems and Diophantine equations // Courant Comput. Sci. Symp. 7: Comput. Complex. N.Y., P. 87-95.

[1974] Computability and unsolvability.- New York; Toronto; London: McGrow Hill.

[1977] Unsolvable problems // Studies in Logic and the Found. of Math.- V. 90.- Русский перевод: Девис М. Неразрешимые проблемы // Справочная книга по математической логике. Часть III. Теория рекурсий.- М.: Наука.- С. 51-76.

[1989] Teaching the incompleteness theorem // Logic Colloquium '88. Proc. Colloq. Assoc. Symb. Logic (Padoba, 1988).- Amsterdam: North-Holland.- P. 385-392.

Девис, Матиясевич Ю. В. и Робинсон
(Davis M., Robinson J.)

[1976] Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution // Proc. Symp. Pure Math.- V. 28.- P. 323-378.

Девис и Патнам (Davis M., Putnam H.)

[1958] Reductions of Hilbert's tenth problem // J. Symbolic Logic.- V. 23, N 2.- P. 183-187.

[1959a] On Hilbert's tenth problem // Notices Amer. Math. Soc.- V. 6, N 5(40).- P. 544

[1959б] On Hilbert's tenth problem // U.S. Air Force O.S.R. Report AFOSR TR 59-124, Part III.

[1963] Diophantine sets over polynomial rings // Illinois J. Math.- V. 7, N 2.- P. 251-256.- Русский перевод: Математика, 1964, Т. 8, № 5.- С. 85-90.

Девис, Патнам и Робинсон (Davis M., Putnam H., Robinson J.)

[1961] The decision problem for exponential diophantine equations // Ann. Math.- V. 74, N 3.- P. 425-436.

Денеф (Denef J.)

[1975] Hilbert's tenth problem for quadratic rings // Proc. Amer. Math. Soc.- V. 48, N 1.- P. 214-220.

[1978a] Diophantine sets over $\mathbb{Z}[T]$ // Proc. Amer. Math. Soc.- V. 69, N 1.- P. 148-150.

[1978б] The diophantine problem for polynomial rings and fields of rational functions // Trans. Amer. Math. Soc.- V. 242.- P. 391-399.

[1980] Diophantine sets over algebraic integer rings. II. // Trans. Amer. Math. Soc.- V. 257, N 1.- P. 227-236.

Денеф и Липшиц (Denef J., Lipshitz L.)

[1978] Diophantine sets over some rings of algebraic integers // J. London Math. Soc.(2).- V. 18, N 3.- P. 385-391.

[1984] Power series solutions of algebraic differantial equations // Math. Ann.- V. 267, N 2.- P. 213-238.

[1989] Decision problems for differential equations // J. Symbolic Logic.- V. 54, N 3.- P. 941-950.

Джозеф и Янг (Joseph D., Young P.)

[1981] A survey of some recent results on computational compexity in weak theories of arithmetic // Lect. Notes Comput. Sci.- V. 118.- P. 46-60.

Джонс (Jones J. P.)

[1974] Recursive undecidability - an exposition // Amer. Math. Mon.- V. 81, N 7.- P. 724-738.

[1978] Three universal representations of recursively enumerable sets // J. Symbolic Logic.- V. 43, N 2.- P. 335-351.

[1979] Diophantine representation of Mersenne and Fermat primes // Acta arithm.- V. 35, N 3.- P. 107-119.

[1980] Undecidable diophantine equations // Bull. Amer. Math. Soc.- V. 3, N 2.- P. 859-862.

[1981] Classification of quantifier prefixes over diophantine equations // Z. math. Logik Grundl. Math.- Bd 27, N 5.- S. 403-410.

[1982a] Some undecidable determined games // Int. J. Game Theory.- V. 11, N 2.- P. 63-70.

[1982б] Universal diophantine equation // J. Symbolic Logic.- V. 47, N 3.- P. 549-571.

Джонс, Левиц и Уилки (Jones J. P., Levitz H., Wilkie A. J.)

[1986] Classification of quantifier prefixes over exponential diophantine equations // Z. math. Logik Grundl. Math.- Bd 32, N 5.- S. 399-406.

Джонс и Матиясевич Ю. В. (Jones J. P.)

[1982a] Exponential Diophantine representation of recursively enumerable sets // Studies in Logic and The Foundations of Math.- V. 107.- P. 159-177.

[1982б] A new representation for the symmetric binomial coefficient and its applications // Ann. Sc. math. Québec.- V. 6, N 1.- P. 81-97.

[1984] Register machine proof of the theorem on exponential diophantine representation of enumerable sets // J. Symbol. Log.- V. 49, N 3.- P. 818-829.

Джонс, Сато, Вада и Вьенс (Jones J.P., Sato D., Wada H., Wiens D.)

[1976] Diophantine representation of the set of prime numbers // Amer. Math. Mon.- V. 83, N 6.- P. 449-464.

Диофант (Διοφαντος)

[1974] Арифметика и книга о многоугольных числах.- М.: Наука.

Дурнев В. Г.

[1974] Об уравнениях на свободных полугруппах и группах // Мат. заметки.- Т. 16, № 5.- С. 717-724.

Дурнев В. Г. и Кораблёва Н. Б.

[1988] Об одной алгоритмически неразрешимой задаче для систем линейных диофантовых уравнений // Вопросы теории групп и гомологич. алгебры.- Ярославль: ЯГУ.- С. 93-96.

Ерослов (Jeroslow R.G.)

[1973] There cannot be any algorithm for integer programming with quadratic constraits // Oper. Res.- V. 21, N 1.- P. 221-224.

Захаров Д. А.

[1970] Рекурсивные функции.- Новосибирск.

[1986] Диофантовость рекурсивно перечислимых множеств и предикатов // В книге Мальцева [1986].- С. 355-364.

Зигель (Siegel K. L.)

[1972] Zur Theorie der quadratischen Formen // Nachr. Akad. Wiss. Göttingen. II. Math.-Phys. Kl.- N 3.- S. 21-46.

Зикман и Сабо (Siekmann J., Szabo P.)

[1989] The undecidability of the D_A-unification problem // J. Symbolic Logic.- V. 54, N 2.- P. 402-414.

Зингер (Singer M. F.)

[1978] The model theory of ordered differential fields // J. Symbolic Logic.- V. 43, N 1, P. 82-91.

Ибарра и Лейнингер (Ibarra O. H., Leininger B. S.)

[1980] The complexity of the equivalence problem for straight-line programs // Twelfth Annual ACM Symposium on Theory of Computing.- Los Angeles.- P. 273-280.

[1982] Straight-line programs with one input variable // SIAM J. Comput.- V. 11, N 1.- P. 1-14.

[1983] On the simplification and equivalence problems for straight-line programs // J. Assoc. Comput. Mach.- V. 30, N 3.- P. 641-656.

Кавинес (Caviness B.F.)

[1970] On canonical form and simplification // J. Assoc. Comput. Mach.- V. 17, N 2.- P. 385-396.

Кай (Kaye R.)

[1987] Parameter free induction in arithmetic.// Seminarber. Humbold-Univ. Berlin, Sect. Math.- S. 70-81.

[1990] Diophantine induction // Ann. Pure Appl. Logic.- V. 46.- P. 1-40.

Кай, Парис и Димитракопулос (Kaye R., Paris J., Dimitracopoulos C.)

[1988] On parameter free induction schemas // J. Symbolic Logic.- V. 53, N 4.- P. 1082-1097.

Капланский (Kaplansky I.)

[1977] Hilbert's problems // Math. Dept. Lect. Notes. Univ. Chicago.

Карстенс (Carstens H. G.)

[1977] The theorem of Matijasevič is provable in Peano's arithmetic by finitely many axioms // Logique et anal.- V. 20, N 77-78.- P. 116-121.

Касами и Токура (Kasami T., Tokura N.)

[1971] Equivalence problem of programs without loops // Systems-Computers-Controls.- V. 2, N 4.- P. 83-84.

Кент и Ходжсон (Kent C. F., Hodgson B. R.)

[1982] An arithmetical characterization of NP // Theor. Computer Sci.- V. 21.- P. 255-267.

Клейман Ю. Г.

[1979] Тождества и некоторые алгоритмические проблемы в группах // Докл. АН СССР.- Т. 244, № 4.- С. 814-818.

Колмогоров А. Н. и Успенский В. А.

[1958] К определению алгоритма // Успехи мат. наук.- Т. 13, № 4(82).- С. 3-28.

Конвей и Джонс (Conway J. H., Jones A. J.)

[1976] Trigonometric Diophantine equations // Acta Arithm.- V. 30, N 3.- P. 229-240.

Косовский Н. К.

[1967] Достаточные условия неполноты для формализаций частей арифметики // Зап. научн. семинар. Ленингр. отд. Мат. ин-та АН СССР.- Т. 4.- С. 44-57.

[1971] О диофантовых представлениях последовательности решений уравнения Пелля // Зап. научн. семинар. Ленингр. отд. Мат. ин-та АН СССР.- Т. 20.- С. 49-59.

Крайзель (Kreisel G.)

[1958] Mathematical significance of consistency proofs // J. Symbolic Logic.- V. 23, N 2.- P. 155-182.

[1962] [Реферат работы Девиса, Патнама и Робинсон [1961]] // Mathem Reviews.- V. 24, N A3061.- P. 573.

Кряучюкас В. Ю.

[1979] Диофантово представление совершенных чисел // Зап. научн. семинар. Ленингр. отд. Мат. ин-та АН СССР.- Т. 88.- С. 78-89.

Куммер (Kummer E. E.)

[1852] Über die Ergänzungssätze zu den Allgemeinen Reziprozitätsgesetzen // J. Reine Angew. Math.- Bd 44.- S. 93-144.

Л а г р а н ж (Lagrange J. L.)

[1772] Démonstration d'un théorème d'arithmétique // Nouv. Mem. Acad. Roy. Sc. de Berlin, 1770.- P. 123-133.

Л а м б е к (Lambek J.)

[1961] How to program an infinite abacus // Canadian Math. Bull.- V. 4.- P. 295-302.

Л е в и ц (Levitz H.)

[1985] Decidability of some problem petraining to base 2 exponential Diophantine equations // Z. math. Logik Grundl. Math.- Bd 31, N 2.- S. 109-115.

Л и н д о н и Ш у п п (Lindon R. C., Schupp P.E.)

[1977] Combinatorial group theory.- Berlin, Heidelburg, New York: Springer.- Русский перевод: Линдон Р. К., Шупп П. Е. Комбинаторная теория групп.- М: Мир, 1980.

Л и п ш и ц (Lipshitz L.)

[1977] Undecidable existential problem for addition and divisibility in algebraic number rings. II // Proc. Amer. Math. Soc.- V. 64, N 1.- P. 122-128.

[1978a] The diophantine problem for addition and divisibility // Trans. Amer. Math. Soc.- V. 235.- P. 271-283.

[1978б] Undecidable existential problem for addition and divisibility in algebraic number rings // Trans. Amer. Math. Soc.- V. 241.- P. 121-128.

[1979] Diophantine correct models of arithmetic // Proc. Amer. Math. Soc.- V. 73, N 1.- P. 107-108.

Л ь ю и Р о з е н б е р г (Lew J. S., Rosenberg A. L.)

[1975] Polynomial mappings from N×N into N.- IBM Report RC-5761.

М а й х и л (Myhill J.)

[1953] Three contributions to recursive function theory // Actes XI Congrès Intern. Phylos. (Brussels, 1953).- V. 24.- P. 50-59.

М а к а л у н (McAloon K.)

[1978] Completeness theorems, incompletenss theorems and models of arithmetic // Trans. Amer. Math. Soc.- V. 239, N 5.- P. 235-277.

М а к г е т р и к (McGettrick A. D.)

[1977] Teaching mathematics by computer // Comput. J.- V. 20, N 3.- P. 263-268.

Макинтайр и Симмонс (Macintyre A., Simmons H.)

[1973] Gödel's diagonalization technique and related propeties of theories // Colloq. math.- V. 28, N 2.- P. 165.

Мальцев А. И.

[1968] О некоторых пограничных вопросах алгебры и логики // Труды Международного конгресса математиков (Москва, 1966).- М.: Мир.- С. 217-231.

[1986] Алгоритмы и рекурсивные функции.- М.: Наука.

Манас (Mănas M.)

[1971] Nekonvexní úlohy matematického programování // Economicko-matematický Obzor.- V. 7, N 4.- P. 390-405.

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

[1978] NP-complete decision problems for binary quadratics // J. Comput. and Syst. Sci.- V. 16.- P. 168-184.- Русский перевод с добавлением переводчика: Киб. сб., нов. сер.- 1980.- вып. 17.- С. 124-163.

Маневиц (Manevitz L. M.)

[1976a] Robinson forcing is not absolute // Isr. J. Math.- V. 25, N 3-4.- P. 211.

[1976б] Internal end-extentions of Peano arithmetic and a problem of Gaifman // J. London Math. Soc.(2).- V. 13, N 1.- P. 80-82.

Манин Ю. И.

[1973] Десятая проблема Гильберта // Современные проблемы математики.- Т. 1.- М.: ВИНИТИ.- С. 5-37.

[1977] A course in Mathematical Logic.- New York; Heidelberg; Berlin: Springer.

Маргенштерн (Margenstern M.)

[1981] Le Théorèm de Matiyassévitch et résultats connexes // Lect. Notes Math.- V. 890.- P. 198-241.

Мартин-Лёф (Martin-Löf P.)

[1970] Notes on constructive mathematics.- Stockholm: Almqvist and Wiksell.- Русский перевод: Мартин-Лёф П. Очерки по конструктивной математике.- М.: Мир, 1975.

Маслов С. Ю.

[1967] Понятие строгой представимости в общей теории исчислений // Тр. мат. ин-та АН СССР.- Т. 93.- С. 3-42.

Матиясевич Ю. В.

[1968а] Связь систем уравнений в словах и длинах с 10-й проблемой Гильберта // Зап. науч. семинар. Ленингр. отд. Мат. ин-та АН СССР.- Т. 8.- С. 132-144.

[1968б] Две редукции 10-й проблемы Гильберта // Зап. науч. семинар. Ленингр. отд. Мат. ин-та АН СССР.- Т. 8.- С. 145-158.

[1968в] Арифметические представления степеней // Зап. науч. семинар. Ленингр. отд. Мат. ин-та АН СССР.- Т. 8.- С. 159-165.

[1970] Диофантовость перечислимых множеств // Докл. АН СССР.- Т. 191, № 2.- С. 278-282.

[1971а] Диофантово представление множества простых чисел // Докл. АН СССР.- Т. 196, № 4.- С. 770-773.- Английский перевод с добавлением: Soviet Math. Doklady, 1971.- V. 12, N 4.- P. 249-254.

[1971б] Диофантово представление перечислимых предикатов // Изв. АН СССР. Сер. мат.- Т. 35, № 1.- С. 3-30.

[1971в] Diophantine representation of recursively enumerable predicates // Actes Congres intern. math. (Nice, 1970).- Paris: Gauthier-Villars.- P. 235-238 = Диофантово представление перечислимых предикатов // Межд. конгр. матем. в Ницце. 1970. Доклады сов. матем.- М.: Наука, 1972.- С. 203-206.

[1972а] Диофантовы множества // Успехи мат. наук.- Т. 27, № 5(167).- С. 185-222.

[1972б] Арифметические представления перечислимых множеств с небольшим числом кванторов // Зап. научн. семинар. Ленингр. отд. Мат. ин-та АН СССР.- Т. 32.- С. 77-84.

[1973] On recursive unsolvability of Hilbert's tenth problem // Studies in Logic and Found. of Math.- V. 74.- Amsterdam: North Holland.- P. 89-110.

[1974] Существование неэффективизируемых оценок в теории экспоненциально диофантовых уравнений // Зап. науч. семинар. Ленингр. отд. Мат. ин-та АН СССР.- Т. 40.- С. 77-93.

[1976] Новое доказательство теоремы об экспоненциально диофантовом представлении перечислимых предикатов // Зап. науч. семинар. Ленингр. отд. Мат. ин-та АН СССР.- Т. 60.- С. 75-92.

[1977а] Простые числа перечисляются полиномом от 10 переменных // Зап. науч. семинар. Ленингр. отд. Мат. ин-та АН СССР.- Т. 68.- С. 62-82.

[1977б] Some purely mathematical results inspired by mathematical logic // Proc. Fifth Intern. Congr. Logic, Methodology and Philos. of Sci.(London, Ont., 1975).- Dordrecht: Reidel.- P. 121-127.

[1979] Алгорифмическая неразрешимость экспоненциально диофантовых уравнений с тремя неизвестными // Исследования по теории алгорифмов и мат. логике.-М.: ВЦ АН СССР.- С. 69-78.

[1984] Об исследованиях по некоторым алгорифмическим проблемам алгебры и теории чисел // Тр. мат. ин-та АН СССР.- Т. 168, С. 218-235.

[1988] Диофантова сложность // Зап. научн. семинар. Ленингр. отд. Мат. ин-та АН СССР.- Т. 174.- С. 122-131.

Матиясевич Ю. В. и Робинсон (Robinson J.)

[1974] Два универсальных трёхкванторных представления перечислимых множеств // Теория алгорифмов и мат. логика.- М.: ВЦ АН СССР.- С. 112-123.

[1975] Reduction of an arbitrary diophantine equation to one in 13 unknowns // Acta Arithm.- V.- 27.- P. 521-553.

Мельзак (Melzak Z. A.)

[1961] An informal arithmetical approach to computability and computation // Canadian Math. Bull.- V. 4.- P. 279-294.

Миллер (Miller C. F. III)

[1973] Some connection between Hilbert's 10th problem and the theory of groups // Word Probl. Decis. Probl. Group. Theory.- Amsterdam; London.- P. 483-506.

Минский (Minsky M. L.)

[1961] Recursive unsolvability of Post's problem of tag and other topics in the theory of Turing machines // Ann. Math. (2).- V. 74.- P. 437-455.

[1967] Computation: finite and infinite machines // Englewood Cliffs; New York: Prentice Hall.- Русский перевод: Минский М. Вычисления и автоматы.- М.: Мир, 1971.

Минц Г. Е.

[1975] Теория доказательств (арифметика и анализ) // Итоги науки и техники. Сер. Алгебра. Топология. Геометрия.- Т. 13.- М.: ВИНИТИ.- С. 5-49.

Мияйлович, Маркович и Дошен (Mijajlović Ž., Marković Z., Došen K.)

[1986] Hilbertovi problemi i logika.- Beograd: Zavod udžben i nastavna sredstva.

Мозес (Moses J.)

[1971] Algebraic simplification: A guide for the perplexed // Commun. ACM.- V. 14, N 8.- P. 527-537.

Мясников А. Г., Ремесленников В. Н.

[1986] Elementary group equivalence with the integral length function // Illinois J. Math.- V. 30, N 2.- P. 335-354.

Нильсен (Nielsen J.)

[1924] Die Gruppe der dreidimensionalen Gittertransformationen // Danke Vid. Selsk. Math.-fys. Medd.- V. 5, N 12.- P. 1-29.

Папас (Pappas P.)

[1985] A diophantine problem for Laurent polynomial rings // Proc. Amer. Math. Soc.- V. 93, N 4.- P. 713-718.

Парис и Димитракопулос (Paris J., Dimitracopoulos C.)

[1982] Truth definitions for Δ_0 formulae // Monogr. Enseign. Math.- V. 30.- P. 317-329.

Патнам (Putnam H.)

[1960] An unsolvable problem in number theory // J. Symbolic Logic.- V. 25, N 3.- P. 220-232.- Русский перевод: Математика, 1964.- Т.8, № 5.- С. 55-67.

Пензин Ю. Г.

[1978] Неразрешимые теории кольца непрерывных функций // Алгоритмические вопросы алгебраических систем.- Иркутск: С. 142-147.

Пост (Post E. L.)

[1936] Finite combinatory processes. Formulation I // J. Symbolic Logic.- V. 1, N 3.- P. 103-105.- Русский перевод в книге Успенского [1979], С. 89-95.

Рабин (Rabin M. O.)

[1957] Effective computability of winning strategies // Ann. Math. Stud.- V. 39.- P. 147-157.

Ремесленников В. Н.

[1979] Об одной алгоритмической задаче для нильпотентных групп и колец // Сиб. мат. ж.- Т. 20, № 5.- С. 1077-1081.

Репин Н. Н.

[1983] Уравнения с одной неизвестной в нильпотентных группах // Мат. заметки.- Т. 34, № 2.- С. 201-206.

Рид (Reid C.)

[1970] Hilbert.- Berlin; Heideberg; New York: Springer.- Русский перевод: Рид К. Гильберт.- М.: Наука, 1977.

[1986] The autobiography of Julia Robinson // The College Mathematics Journal.- V. 17, N 1.- P. 3-21.

Ричардсон (Richardson D.)

[1968] Some undecidable problems involving elementary functions of a real variable // J. Symbol. Log.- V. 33, N 4.- P. 514-520.

Робинсон А. (Robinson A.)

[1973] Nonstandard arithmetic and generic arithmetic // Proc. IV Int. Congress Logic, Method. and Phil. of Sci.. (Bucharest, 1971).- Amsterdam: North-Holland.- P. 137-154.

Робинсон Дж. (Robinson J.)

[1952] Existential definability in arithmetic // Trans. Amer. Math. Soc.- V. 72, N 3.- P. 437-449.- Русский перевод: Математика, 1964.- Т. 8, № 5.- С. 3-14.

[1960] The undecidability of exponential diophantine equations // Notices Amer. Math. Soc.- V. 7, N 1.- P. 75.

[1962] The undecidability of exponential diophantine equations // Proc. I Int. Congr. Logic, Method., Philos. Sci. (Stanford, 1960).- Stanford: Stanford University Press.- P. 12-13.- Русский перевод: Матем. логика и её применения.- М.: Мир, 1965.- С. 7-8.

[1969a] Unsolvable diophantine problems // Proc. Amer. Math. Soc.- V. 22, N 2.- P. 534-538.

[1969б] Diophantine decision problems // Studies in number theory. Studies in Math.- V. 6.- Englewood Cliffs: Math. Assoc. of America.- P. 76-116

[1971] Hilbert's tenth problem // Proc. Sympos. Pure Math.- V. 20.- P. 191-194.

[1973] Solving Diophantine equations // Studies in Logic and Foundation of Math - V. 74.- Amsterdam: Noth-Holland.- P. 63-67.

Робинсон Р. М. (Robinson R. M.)

[1951] Arithmetical definitions in the ring of integers // Proc. Amer. Math. Soc.- V. 2, N 2.- P. 279-284.

[1956] Arithmetical representation of recurcively enumerable sets // J. Symbol. Log.- V. 21, N 2.- P. 162-186.- Русский перевод: Математика.- 1964.- Т. 8, № 5.- С. 23-47.

[1972] Some representation of diophantine sets // J. Symbolic Logic.- V. 37, N 3.- P. 572-578.

Розенблат Б. В.

[1985] Диофантовы теории свободных инверсных полугрупп // Сиб. мат. ж.- Т 26, № 6.-С. 101-107.

Романьков В. А.

[1977] О неразрешимости проблемы эндоморфной сводимости в свободных нильпотентных группах и в свободных кольцах // Алгебра и логика.- Т. 16, № 4.- С. 457-471.

[1979] Об универсальной теории нильпотентных групп // Мат. заметки.- Т. 25, № 4.- С. 487-495.

Р у м л и (Rumely R. S.)

[1986] Arithmetic over the ring of all algebraic integers // J. reine angew. Math.- Bd 368, N 5.- S. 127-133.

Р у о х о н е н (Ruohonen K.)

[1972] Hilbertin Kymmenes probleema // Arkhimedes.- N 1-2.- P. 71-100.

[1980] Hilbert tionde problem // Normat.- V. 28, N 4.- P. 145-154.

С а л о м а а (Salomaa A.)

[1985] Computation and Automata // Encyclopedia of Mathematics and its applications.- V. 25.- Cambridge: Cambridge University Press.

С а п и р М. В.

[1989] Минимальное многообразие ассоциативных алгебр с неразрешимой проблемой равенства // Мат. сб.- № 12.- С. 1391-1408.

С а п и р М. В. и Х а р л а м п о в и ч О. Г.

[1989] Проблема равенства в многообразиях ассоциативных алгебр и алгебр Ли // Изв. вузов. Мат.- № 6(325).- С. 76-84.

С к а р п е л л и н и (Scarpellini B.)

[1963] Zwei unentscheidbare Probleme der Analysis // Z. math. Logik Grundl. Math.- Bd 9, N 4.- S. 265-289.

С к у л е м (Skolem Th.)

[1934] Über die Nicht-charakterisierbarkeit der Zahlenreihe mittels endlich oder abzählbar unendlich vieler Aussagen mit ausschliesslich Zahlenvariablen // Fund. Math.- Bd 23.- S. 150-161.

С м о р и н ь с к и й (Smoryński C.)

[1977] A note on the number of zeros of polynomials and exponential polynomials // J. Symbolic Logic.- V. 42, N 1.- P. 99-106.

[1987] Diophantine encoding // Preprint N 455, Univ. Utrecht, Dept. of Math.

С т е т м е н (Statman R.)

[1981] On the existence of closed terms in the typed λ-calculus. II. Transformations of unification problems // Theor. Comput. Sci.- V. 15, N 3.- P. 329-338.

Сусман (Sussman H.J.)

[1971] Hilbert's tenth problem // Revista Colombiana de Matemáticas, Monografías Matemáticas, V. 9, Bogotá: Sociedad Colombiana de Matemáticas.

Такахаши (Takahashi S.)

[1974] Méthodes logiques en géométrie diophantienne.- Montreal: Univ de Montreal.

Тарасов С. П. и Хачиян Л. Г.

[1980] Границы решений и алгоритмической сложности систем выпуклых диофантовых неравенств // Докл. АН СССР.- Т. 255, № 2.- С. 296-300.

Тунг (Tung Shih-Ping)

[1988] Definability on formulas with single quantifier // Z. math. Logik Grundl. Math.- Bd 34, N 2.- S. 105-108.

Туракайнен (Turakainen P.)

[1978] A note on noncontext-free rational stochastic languages // Inform. Control.- V. 39, N 1.- P. 225-226.

[1981] On some bounded semiAFLs and AFLs // Information Sciences.- V. 23, N 1.- P. 31-48.

Тьюринг (Turing A. M.)

[1936] On computable numbers with an application to the Entscheidungsproblem // Proc. London Math. Soc., Ser. 2.- V. 42.- P. 230-265.

[1937] On computable numbers with an application to the Entscheidungsproblem. A correction // Proc. London Math. Soc., Ser. 2.- V. 43.- P. 544-546.

[1939] Systems of logic based on ordinals // Proc. London Math. Soc. (2).- V. 45.- P. 161-228.

Уилки (Wilkie A.)

[1975] On models of arithmetic - answers to two problems raised by H. Gaifman // J. Symbolic Logic.- V. 40, N 1.- P. 41-47.

Уилмерс (Wilmers G.)

[1985] Bounded existential induction // J. Symbol. Log.- V. 50, N 1.- P. 72-90.

Успенский В. А.

[1979] Машина Поста.- М.: Наука.

Успенский В. А. и Семёнов А. Л.

[1987] Теория алгоритмов: основные открытия и применения.- М.: Наука.

Фейдас (Pheidas T.)

[1987a] An undecidability results for power series rings of positive characteristic // Proc. Amer. Math. Soc.- V. 99, N 2.- P. 364-366.

[1987б] An undecidability results for power series rings of positive characteristic.II // Proc. Amer. Math. Soc.- V. 100, N 3.- P. 526-530.

[1988] Hilbert's tenth problem for a class of rings of algebraic integers // Proc. Amer. Math. Soc.- V. 104, N 2.- P. 611-620.

Фенстад (Fenstad J. E.)

[1971] Hilberts 10. Problem // Nordisk Matematisk Tidskift.- V. 19.- P. 5-14.

Фич (Fitch J. P.)

[1973] On algebraic simplification // Comput. J.- V. 16, N 1.- P. 23-27.

Фридрихсдорф (Friedrichsdorf U.)

[1976] Einige Bemerkungen zur Peano-Arithmetik // Z. math. Logik Grundl. Math.- Bd 22, N 5.- S. 431-436.

Хавел (Havel I.)

[1973] O desátém Hilbertově problemu // Pokr. mat. fys. a astron.- V. 18, N 4.- P. 185-192.

Хавел, Пнуели и Стави (Havel D., Pnueli A., Stavi J.)

[1983] Propositional dynamic logic of nonregular programs // J. Comp. Syst.- V. 26, N 2.- P. 222-243.

Харлампович О. Г.

[1989a] Проблема равенства для разрешимых алгебр Ли и групп // Мат. сб.- Т. 180, № 8.- С. 1033-1066.

[1989б] Конечноопределённые разрешимые группы и алгебры Ли с неразрешимой проблемой равенства // Мат. зам.- Т. 46, № 3.- С. 80-92.

Хек (Hack M.)

[1976] The equality problem for vector addition system is undecidable // Theor. Comput. Sci.- V. 2, N 1.- P. 77-95.

Х е р м а н (Herrman O.)

[1971] A nontrivial solution of the Diophantine equation $9(u^2+7v^2)^2-7(r^2+7s^2)^2=2$ // Computers in number theory.- London: Academic Press.- P. 207-212.

Х е т ч е р и Х о д ж с о н (Hatcher W. S., Hodgson B. R.)

[1981] Complexity bounds on proofs // J. Symbol. Log.- V. 46, N 2.- P. 255-258.

Х и р о с е (Hirose K.)

[1973] Вокруг 10-й проблемы Гильберта (яп.) // Sûgaku.- V. 25, N 1.- P. 1-9.

Х и р о с е и И и д а (Hirose K. Iida S.)

[1973] A proof of negative answer to Hilbert's 10th problem // Proc. Jap. Acad.- V. 49.- P. 10-12.

Х и р ш ф е л ь д (Hirschfeld J.)

[1975] Models of arithmetic and recursive functions // Isr. J. Math.- V. 20, N 2.- P. 111-126.

Х и р ш ф е л ь д и У и л е р (Hirschfeld J., Wheeler W.)

[1975] Forcing, arithmetic, division rings // Lect. Notes Math.- V. 454.- P. 266

Х о д ж с о н и К е н т (Hodgson B. R., Kent C. F.)

[1983] A normal form for arithmetical representation of NP-sets // J. Comput. Syst.- V. 27, N 3.- P. 378-388.

Ч е й т и н (Chaitin G. J.)

[1974] Information-theoretic limitations of formal systems // J. Assoc. Comput. Mach.- V. 21, N 3.- P. 403-424.

[1987] Algorithmic information theory // Cambridge Tracts in Theoretical Computer Sci.- V. 1.- Cambridge: Cambridge University Press.

Ч ё р ч (Church A.)

[1936] An unsolvable problem of elementary number theory // Amer. J. Math.- V. 58.- P. 345-363.

Ч у д н о в с к и й Г. В. (Chudnovsky G. V.)

[1970] Диофантовы предикаты // Успехи мат наук.- Т. 25, № 4.- С. 185-186.

[1971] Некоторые арифметические проблемы // Препринт ИМ-71-3.- Киев: Ин-т матем. АН УССР.

[1984] Contributions to the theory of transcendental numbers // Providence: Amer. Math. Soc.

Шапиро и Шлапентох (Shapiro H., Shlapentokh A.)

[1989] Diophantine relationship between algebraic number fields // Commun. Pure Appl. Math.- V. 42.- P. 1113-1122.

Шенкс (Shanks D.)

[1972] Five number-theoretic algorithms // Proc. Second Manitoba Conf. on Numerical Math.- P. 51-70.

Шёнфельд (Schönfeld L.)

[1976] Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II // Math. Comput.- V. 30, N 134.- P. 337-360; Corrigendum: Ibid., N 136.- P. 900.

Шепердсон и Стёргис (Shepherdson J.C., Sturgis H.E.)

[1963] Computability of recursive funcions // J. ACM.- V. 10.- P. 217-255.

Шлапентох (Shlapentokh A.)

[1989] Extentions of Hilbert's tenth problem to some algebraic number fields // Commun. Pure Appl. Math.- V. 42.- P. 939-962.

[1990] Diophantine definitions for some polynomial rings // Commun. Pure Appl. Math.- V. 43.- P. 1055-1066.

Юкна С.

[1982a] Арифметические представления классов машинной сложности // Мат. логика и ее применения. Вып. 2. Вильнюс: Ин-т матем. и кибернет. АН ЛитССР.- С. 92-107.

[1982б] Об арифметизации вычислений // Мат. логика и её применения.- Вып. 3. Вильнюс: Ин-т матем. и кибернет. АН ЛитССР.- С. 117-125.

УКАЗАТЕЛЬ ОБОЗНАЧЕНИЙ

ADD 74
Add 48
and 68
APPEND 74
arem 18

$\mathbf{B}_n$ 48
Bernoulli 48
BIN 89

Cantor 39
Cantor$_n$ 39
Card 117
Code 42
Concat 43
COPY 74

D 147
DEC 73
DECODE 75
Deg 102
DELETE 73
div 18
do 68
DOUBLE 89

e 109
E 155
ECard 136
ECode 55
Elem 42
Elem$_{n,m}$ 39
Elema 39
Elemb 39
Eq 44
EQUAL 75
Equal 44

erank 142
erankiter 142
ERASE 89
Even 17
explog 109

F 34
$\mathfrak{F}_0$ 153
$\mathfrak{F}_1$ 157
$\mathfrak{F}_2$ 158
$\mathfrak{F}_3$ 161
FIND 72
Format 54

$\mathbb{G}$ 126
G 107
GCD 18
GElem 41
grem 131

H 155
$\mathfrak{H}_0$ 60
$\mathfrak{H}_1$ 60

i 126
if 68
INC 73
iter 142
itererank 142

JUMP 72

LAST 73
LCM 18
LEFT 70
Less 48
Li 108

MARK 74
Min 49
MULT 75
Mult 48

$\mathbb{N}$ 127
NEVERSTOP 72
NEW 73
NEXT 75
NOTEQUAL 75
NOTGREATER 75
NotGreater 44
NotGreater$_p$ 122
NP 147

od 68
Odd 17
oper 140
operord 141
operordrank 141
operrank 141
ord 139
ordoper 141
ordrank 139
ordrankoper 141
Ortnorm 47

P 107
P$_k$ 111
PNotGreater 45
Prime 44, 106
Primenth 49
PSmall 45
PSmall$_p$ 122

$\mathbb{Q}$ 120

$\mathbb{R}$ 150
rank 139
rankoper 141
rankord 139
rankordoper 141
READ 71
READNOT 72
Real 112
rem 17
Repeat 45
RESTORE 74
RIGHT 70

SCod 56
SCode 56
Small 44
Solution 58
sqrt 48, 126
STAR 72
STOP 71
Sum 48

then 68
THEREIS 74
THEREWAS 74

U 59
U$_0$ 59
U$_1$ 59
U$_n$ 59
unit 100

VACANT 72

while 68
WRITE 70

Z 127
$\mathbb{A}$ 23
α 22
β 22
γ 35
$\mathbb{E}$ 23
ζ 107
θ 100
Ξ 23
$\pi(a)$ 48
φ 37
ψ 108

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Алфавит машины Тьюринга 66

Гипотеза Гольдбаха 107
— Девиса 91
— Римана 107
Граница универсальная
количества операций 141
— — порядка 140
— — ранга 140
— — — экспоненциального 142
— — сложности 140

Дзета-функция Римана 107
Длина позиционного
кода кортежа 42

Закон простых чисел 108

Игра диофантова 164
Изображение кортежа 69
— — двоичное 89
— — каноническое 69
— числа 69
— — двоичное 89
Инструкция машины регистровой 89
— — Тьюринга 66
— — шахматной 169
Код конфигурации 78
— кортежа гёделев 41
— — позиционный 42
— множества 52
— полинома 55
— уравнения 59
— — без параметров 59
— — расширенный 54, 56
Коды эквивалентные 44
Количество операций
относительное 141

Конкатенация 42
Конфигурация 78
Кортеж 39
— пустой 41
— характеристический 46

Машина диофантова 148
— регистровая 89
— Тьюринга 65
— — недетерминированная 149
— шахматная 169
Множество диофантово 13
— (A, C, X)-диофантово 127
— — универсальное 52
— двоично полуразрешимое
по Тьюрингу 89
— достижимости 167
— полуразрешимое
в интуитивном смысле 87
— — на регистровой машине 90
— — по Тьюрингу 77
— простое 113
— разрешимое
в интуитивном смысле 87
— — по Тьюрингу 84
— трассирующее 165

Неизвестная 12
Номер кортежа канторов 39
— уравнения 112
Нуль дзета-функции
нетривиальный 108
— — тривиальный 108

Основание позиционного
кода кортежа 42
Отношение грубо
экспоненциального роста 35

Отношение диофантово 15
— достижимости 167
— экспоненциального роста 35
Оценка неэффективная 119

Параметр 12
Параметр-код 52
Параметр-элемент 52
Порядок множества 139
— — относительный 139, 141
Последовательность полиномов
универсальная 111
Предикат Джулии Робинсон 36
Представление диофантово
множества 13
— — отношения 15
— — свойства 15
— — функции 16
— однократное 120
— экспоненциально диофантово
множества 33
— — отношения 33
— — свойства 33
— — функции 33
Принцип Дирихле,
мультипликативная форма 114
Проблема индивидуальная 8
— массовая 8

Размерность множества 13
Ранг множества 139
— — относительный 139, 141
— — экспоненциальный 142
— — — относительный 142
Реализация последовательности
полиномов 112
Регистр машины регистровой 89
— — шахматной 169
— — — входной 170
— — — выходной 170
Решение тривиальное однородного
уравнения 133

Свойство диофантово 15
— полиномиальное 115
Семейство диофантовых уравнений 12
Состояние машины Тьюринга 66
Состояние машины Тьюринга
заключительное 66
начальное 66
— — шахматной 169
— — — заключительное 170
— — — начальное 170
Степень уравнения относительно
всех неизвестных 7
— — — — переменных 13
— — — данной неизвестной 7

Тезис Тьюринга 91
— Чёрча 88
Теорема арифметики основная 49
Терм диофантов 16
Тождество Эйлера 107, 180

Уравнение диофантово 7
— — параметрическое 12
— — тригонометрическое 20
— Пелля 184
— универсальное 52
— экспоненциально диофантово 33
— — — унарное 34
— — — — с фиксированным
основанием 34
Уровень итерированности
множества 142
— — — относительный 142
— — уравнения 142

Шифр позиционного кода кортежа 42
— полинома 55

Форма нормальная Девиса 91
Функция, вычислимая по Тьюрингу 89
— диофантова 16
— тестирующая 141
— Чебышева 108

Числа Мерсенна 51
— Ферма 51
— Фибоначчи 37
Число гауссово 126
— диофантово вещественное 150
— натуральное 11
— треугольное 184

ИМЕННОЙ УКАЗАТЕЛЬ

Адлеман (Adleman L.) 149, 194, 204
Адлер (Adler A.) 138, 163, 178, 191, 193, 194
Азра (Azra J. P.) 4, 194
Айвазян С. В. 178, 194
Амик (Amic Y.) 185, 194
Аник (Anick D. J.) 178, 194
Бакстер (Baxter L. D.) 178, 194
Бартон (Barton D.) 163, 195
Баур (Baur W.) 178, 195
Бейкер (Baker A.) 119, 195
Бек (Beck H) 179, 195
Белл (Bell J. L.) 4, 195
Бернулли (Bernoulli J.) 48
Блюм (Blum M.) 192, 195
Бокуть Л. А. 178, 195
Больман (Bollman D.) 186, 195
Бриттон (Britton J. L.) 21, 195
Вада (Wada H.) 51, 195, 200
Важенин Ю. М. 178, 196
Валиев М. К. 178, 196
Ванг П. (Wang P.) 163, 196
Вьенс (Wiens D.) 51, 200
Виноградов А. К. 149, 196
Вольстенхольм (Wolstenholme J.) 49, 196
Гайфман (Gaifman H.) 178, 196
Гёдель (Gödel K.) 3, 49, 92, 97, 115, 196
Германо (Germano G.) 178, 196
Гермес (Hermes H.) 4, 197
Гжегорчик (Grzegorczyk A.) 149
Гильберт (Hilbert D.) 3–5, 7–11, 13, 20, 21, 34, 38, 49, 50, 60, 63–65, 83, 85, 86, 89, 91, 93, 106, 107, 111, 115–117, 126, 127, 133, 135, 137, 138, 147, 153, 154, 158, 163, 174, 178, 186, 197
Гольдбах (Goldbach C.) 107
Гольдфарб (Goldfarb W.D.) 178, 197
Гуаспари (Guaspari D.) 178, 197
Губер-Дайсон (Huber-Dyson V.) 178, 197, 198
Гудстейн (Goodstein R. L.) 179, 197
Гурари (Gurari E. M.) 179, 197
Гэри (Garey M. R.) 147, 197
Дайзель (Deizell C. N.)
Дайсон (Dyson V. H.) 178, 197, 198
Данько (Dańko W.) 179, 198
Девис (Davis M.) 4, 21, 36–38, 50, 63, 64, 91, 92, 115, 116, 138, 146, 148, 178, 186, 190–192, 198, 199, 202
Денеф (Denef J.) 137, 138, 163, 191, 199
Джозеф (Joseph D.) 178, 199
Джонс А. Дж. (Jones A. J.) 185, 202
Джонс Дж. П. (Jones J. P.) 51, 63, 92, 148, 177, 178, 187, 189, 190, 192, 193, 198–200
Джонсон (Johnson D. S.) 147, 197
Димитракопулос (Dimitracopoulos C.) 178, 201, 207
Диофант (Διοφαντος) 8, 9, 21, 133, 200
Дирихле (Dirichlet P. G. L.) 38, 114, 191
Дошен (Došen K.) 4, 206
Дурнев В. Г. 178, 179, 200
Евклид (Εὐκλειδης) 87
Ерослов (Jeroslow R.G.) 179, 200
Захаров Д. А. 4, 201
Зикман (Siekmann J.) 178, 201
Зигель (Siegel K. L.) 21, 201
Зингер (Singer M. F.) 163, 178, 201
Ибарра (Ibarra O. H.) 179, 193, 201
Иида (Iida S.) 115, 191, 212
Кавинес (Caviness B.F.) 163, 201

Кай (Kaye R.) 178, 201
Кантор (Cantor G.) 39, 64
Капланский (Kaplansky I.) 4, 201
Карстенс (Carstens H. G.) 178, 202
Касами (Kasami T.) 179, 202
Кент (Kent C. F.) 149, 202, 212
Клейман Ю. Г. 178, 202
Клаузен (Clausen T.) 187
Колмогоров А. Н. 91, 202
Конвей (Conway J. H.) 185, 202
Кораблёва Н. Б. 179, 200
Косовский Н. К. 37, 38, 149, 178, 186, 189, 196, 202
Кочен (Kochen P. J) 37
Крайзель (Kreisel G.) 63, 115, 116, 202
Кряучюкас В. Ю. 51, 202
Куммер (Kummer E. E.) 45, 49, 50, 102, 122, 182, 202
Лагранж (Lagrange J. L.) 180, 203
Ламбек (Lambek J.) 92, 203
Лаплаза (Laplaza M.) 186, 195
Левиц (Levitz H.) 148, 200, 203
Лейнингер (Leininger B. S.) 179, 193, 201
Линдон (Lindon R. C.) 178, 203
Ли (Lee R. D.) 179,
Липшиц (Lipshitz L.) 137, 138, 163, 178, 191, 199, 203
Лью (Lew J. S.) 186, 203
Майхил (Myhill J.) 21, 203
Макалун (McAloon K.) 178, 203
Макгетрик (McGettrick A. D.) 163, 203
Макинтайр (Macintyre A.) 178, 204
Мальцев А. И. 91, 201, 204
Манас (Mănas M.) 179, 204
Мандерс (Manders K.) 149, 194, 204
Маневиц (Manevitz L. M.) 178, 204
Манин Ю. И. 4, 204
Маргенштерн (Margenstern M.) 4, 204
Маркович (Marković Z) 4, 206
Мартин-Лёф (Martin-Löf Per) 162, 204
Маслов С. Ю. 91, 204
Матиясевич Ю. В. 4, 21, 37, 38, 50, 51, 63, 92, 93, 115, 138, 148, 186–192, 198, 200, 205, 206
Маховер (Machover M) 4, 195
Мельзак (Melzak Z. A.) 92, 206
Мерсенн (Mersenne M) 51
Миллер (Miller C. F. III) 178, 206
Минский (Minsky M. L.) 92, 206
Минц Г. Е. 178, 206
Мияйлович (Mijajlović Ž.) 4, 206
Мозес (Moses J.) 163, 206
Мясников А. Г. 178, 206
Нильсен (Nielsen J.) 188, 206
Папас (Pappas P.) 163, 207
Парис (Paris J.) 178, 201, 207
Патнам (Putnam H.) 21, 50, 63, 92, 115, 138, 187, 190, 199, 202, 207
Пелль (Pell J.) 35, 184, 186
Пензин Ю. Г. 163, 207
Петри (Petri C.) 178
Пнуели (Pnueli A.) 179, 211
Пост (Post E. L.) 90, 116, 207
Рабин (Rabin M. O.) 177, 178, 207
Ремесленников В. Н. 178, 206, 207
Репин Н. Н. 178, 207
Рид (Reid C.) 21, 137, 207
Риман (Riemann G. F. B.) 107–111, 115, 116
Ричардсон (Richardson D.) 163, 207
Робинсон А. (Robinson A.) 178, 208
Робинсон Дж. (Robinson J.) 21, 36, 37, 38, 50, 63, 92, 115, 116, 148, 178, 185–187, 190–192, 198, 199, 202, 206, 208
Робинсон Р. М. (Robinson R. M.) 138, 148, 191, 192, 208
Розенберг (Rosenberg A. L.) 186, 203
Розенблат Б. В. 178, 208
Романьков В. А. 178, 208
Румли (Rumely R. S.) 137, 209
Руохонен (Ruohonen K.) 4, 38, 209
Сабо (Szabo P) 178, 201
Саломаа (Salomaa A.) 4, 209
Сапир М. В. 178, 209
Сато (Sato D.) 51, 200
Семёнов А. Л. 90, 211
Симмонс (Simmons H.) 178, 204
Скарпеллини (Scarpellini B.) 163, 209
Скулем (Skolem Th.) 21, 209
Смориньский (Smoryński C.) 4, 138, 191, 209
Стави (Stavi J) 179, 211
Стёргис (Sturgis H.E.) 92, 213
Стетмен (Statman R.) 179, 209
Сусман (Sussman H.J.) 4, 210

Такахаши (Takahashi S.) 4, 210
Тарасов С. П. 179, 210
Тарский (Tarski A.) 21, 36, 153, 185
Токура (Tokura N.) 179, 202
Тунг (Tung Shih-Ping) 148, 210
Туракайнен (Turakainen P.) 179, 210
Туэ (Thue A.) 119
Тьюринг (Turing A. M.) 3, 63, 65, 67–69, 76–80, 83–94, 115, 117, 120–123, 149, 150, 162, 169, 189–191, 210
Уилер (Wheeler W.) 179, 212
Уилки (Wilkie A.) 148, 178, 200, 210
Уилмерс (Wilmers G.) 178, 210
Успенский В. А. 90, 91, 207, 210, 211
Фейдас (Pheidas T.) 137, 138, 211
Фенстад (Fenstad J. E.) 4, 37, 211
Ферма (Fermat P.) 34, 38, 51, 106
Фибоначчи (Leonardo Pisano, Fibonacci) 37
Фич (Fitch J. P.) 163, 195, 211
Фридрихсдорф (Friedrichsdorf U.) 178, 211
Хавел Д. (Havel D.) 179, 211
Хавел И. (Havel I.) 4, 211
Харлампович О. Г. 178, 209, 211
Хачиян Л. Г. 179, 210
Хек (Hack M.) 178, 179, 211
Херман (Herrman O.) 37, 212
Хетчер (Hodgson B. R.) 178, 212
Хиросе (Hirose K.) 4, 115, 191, 212
Хиршфельд (Hirschfeld J.) 179, 212
Ходжсон (Hodgson B. R.) 149, 179, 202, 212
Чеб[illegible]ев П. Л. 108
Чейтин (Chaitin G. J.) 179, 212
Чёрч (Church A.) 3, 85, 88–90, 94, 118, 120, 167, 212
Чудновский Г. В. 37, 38, 212
Шапиро (Shapiro H.) 137, 213
Шенкс (Shanks D.) 37, 213
Шёнфельд (Schönfeld L.) 116, 213
Шепердсон (Shepherdson J. C.) 92, 178, 198, 213
Шинцель (Schinzel A.) 116
Шляпентох (Shlapentoch A.) 137, 138, 213
Штауд (Staud K. G. C.) 187
Штурм (Sturm J. C. F.) 153, 185
Шупп (Schupp P.E.) 178, 203
Шютте (Schütte K.) 37
Эйлер (Euler L.) 107, 180, 181
Юкна С. 149, 213
Ютила (Jutila M.) 116
Янг (Young P) 178, 199

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ 3

ГЛАВА 1. ОСНОВНЫЕ ПОНЯТИЯ 7

§ 1.1. Разрешимость диофантовых уравнений как массовая проблема 7
§ 1.2. Системы диофантовых ураанений 9
§ 1.3. Решения в натуральных числах 10
§ 1.4. Диофантовы множества 12
§ 1.5. Логическая терминология 14
§ 1.6. Простейшие примеры диофантовых множеств, свойств, отношений и функций 17
Упражнения 18
Комментарии 21

ГЛАВА 2. ДИОФАНТОВОСТЬ ВОЗВЕДЕНИЯ В СТЕПЕНЬ 22

§ 2.1. Специальные рекуррентные последовательности аторого порядка 22
§ 2.2. Диофантовость специальных рекуррентных последовательностей (основные идеи) 24
§ 2.3. Диофантовость специальных рекуррентных последовательностей (доказательство) 27
§ 2.4. Диофантовость возведения в степень 31
§ 2.5. Экспоненциально диофантовы уравнения 32
Упражнения 34
Комментарии 36

ГЛАВА 3. ДИОФАНТОВО КОДИРОВАНИЕ 39

§ 3.1. Канторова нумерация 39
§ 3.2. Гёделево кодирование 40
§ 3.3. Позиционное кодирование 41
§ 3.4. Диофантовость биномиальных коэффициентов, факториала и простых чисел 43
§ 3.5. Сравнение кортежей 44
§ 3.6. Расширение функций на кортежи 46
Упражнения 48
Комментарии 49

ГЛАВА 4. УНИВЕРСАЛЬНЫЕ ДИОФАНТОВЫ УРАВНЕНИЯ 52

§ 4.1. Основные определения 52
§ 4.2. Кодировка уравнений 54
§ 4.3. Кодировка потенциальных решений 56
§ 4.4. Вычисление значений полиномов 57
§ 4.5. Универсальные диофантовы уравнения 59
§ 4.6. Диофантовы множества с недиофантовыми дополнениями . . . 60
Упражнения 61
Комментарии 63

ГЛАВА 5. АЛГОРИТМИЧЕСКАЯ НЕРАЗРЕШИМОСТЬ 10-Й ПРОБЛЕМЫ ГИЛЬБЕРТА 65

§ 5.1. Машина Тьюринга 65
§ 5.2. Композиция машин 67
§ 5.3. Базисные машины 69
§ 5.4. Распознавание диофантовых множеств машинами Тьюринга . . 76
§ 5.5. Диофантово моделирование машин Тьюринга 77
§ 5.6. Неразрешимость 10-й проблемы Гильберта на машинах Тьюринга 83
§ 5.7. Тезис Чёрча 85
Упражнения 89
Комментарии 90

ГЛАВА 6. ОГРАНИЧЕННЫЕ КВАНТОРЫ ОБЩНОСТИ 94

§ 6.1. Первая конструкция: машины Тьюринга 94
§ 6.2. Вторая конструкция: гёделево кодирование 95
§ 6.3. Третья конструкция: суммирование 99
§ 6.4. Связи между 8-й и 10-й проблемами Гильберта 106
§ 6.5. Ещё одно универсальное уравнение 111
§ 6.6. Ещё одно диофантово множество с недиофантовым дополнением 113
Упражнения 114
Комментарии 115

ГЛАВА 7. МАССОВЫЕ ПРОБЛЕМЫ ТЕОРИИ ЧИСЕЛ 117

§ 7.1. Количество решений у диофантовых уравнений 117
§ 7.2. Неэффективизируемые оценки в теории экспоненциально диофантовых уравнений 119
§ 7.3. Аналог 10-й проблемы Гильберта для гауссовых чисел . . 126
§ 7.4. Однородные уравнения и рациональные решения 133
Упражнения 136
Комментарии 137

ГЛАВА 8. ДИОФАНТОВА СЛОЖНОСТЬ 139

§ 8.1. Основные понятия 139
§ 8.2. Оценка количества неизвестных в экспоненциально диофантовых представлениях 142
Упражнения 146
Комментарии 147

ГЛАВА 9. МАССОВЫЕ ПРОБЛЕМЫ МАТЕМАТИЧЕСКОГО АНАЛИЗА 150

§ 9.1. Диофантово вещественные числа 150
§ 9.2. Уравнения, неравенства и тождества с вещественными переменными 153
§ 9.3. Системы обыкновенных дифференциальных уравнений . . . 158
§ 9.4. Интегрируемость 160
Упражнения 162
Комментарии 162

ГЛАВА 10. ДРУГИЕ ПРИЛОЖЕНИЯ ДИОФАНТОВЫХ ПРЕДСТАВЛЕНИЙ . . . 164

§ 10.1. Диофантовы игры 164
§ 10.2. Обобщённые кони на многомерной шахматной доске . . . 167
Упражнения 176
Комментарии 177

ПРИЛОЖЕНИЯ 180

1. Теорема о четырёх квадратах 180
2. Китайская теорема об остатках 181
3. Теорема Куммера 182
4. Суммирование обобщённой геометрической прогрессии 182

УКАЗАНИЯ К УПРАЖНЕНИЯМ 184

СПИСОК ЛИТЕРАТУРЫ 194

УКАЗАТЕЛЬ ОБОЗНАЧЕНИЙ 214

ПЕРЕДМЕТНЫЙ УКАЗАТЕЛЬ 216

ИМЕННОЙ УКАЗАТЕЛЬ 218