МАТЕМАТИЧЕСКИЕ ЗАМЕТКИ

т. 12, № 1 (1972), 115—120

ДОКТОРСКИЕ ДИССЕРТАЦИИ

УДК 517.11

Ю. В. Матиясевич. Диофантово представление перечисленных предикатов.

Автореферат диссертации на соискание ученой степени доктора физико-математических наук (печатается с сокращениями). Диссертация защищена 24 февраля 1972 г. на заседании Ученого совета Математического института им В. А. Стеклова АН СССР. Официальные оппоненты: доктор физ.-матем. наук профессор С. И. Адян, член-корреспондент АН СССР Ю. Л. Ершов, член-корреспондент АН СССР Д. К. Фаддеев.

Выступая в 1900 г. на II Международном конгрессе математиков, Давид Гильберт включил в число 23 нерешенных математических проблем, исследование которых могло, по его мнению, значительно стимулировать дальнейшее развитие науки, задачу о разрешимости диофантовых уравнений. Она была сформулирована в его докладе [1] следующим образом:

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.

Многочисленные попытки найти требуемый в проблеме способ не приводили к успеху. Более того, не удавалось найти способа, позволяющего распознавать наличие решений для диофантовых уравнений даже из некоторых довольно узких классов уравнений.

Безуспешность попыток найти требуемый способ естественно наводит на мысль о том, что такого способа не существует. Возможность сформулировать эту гипотезу в виде строгого математического утверждения появилась в 30-х годах после того, как было выработано точное

понятие алгорифма. Тогда же были найдены и первые примеры алгорифмически неразрешимых проблем.

Первые исследования, имеющие своей целью установление алгорифмической неразрешимости 10-й проблемы Гильберта, появились в начале 50-х годов. Крупнейшим достижением в этой области является теорема Мартина Дейвиса, Хилэри Патнама и Джулии Робинсон о том, что проблема распознавания наличия решений у так называемых показательно-диофантовых уравнений является алгорифмически неразрешимой.

Исследовались различные подходы к установлению алгорифмической неразрешимости 10-й проблемы Гильберта. Многие работы связаны с попытками доказать следующее утверждение: каждый перечислимый *) предикат $\mathcal{R}(a_1, \ldots, a_n)$ является *диофантовым*, т. е. представи́м в виде $\exists z_1 \ldots z_k [R(a_1, \ldots, a_n, z_1, \ldots, z_k) = 0]$, где R — некоторый полином (все рассматриваемые нами полиномы имеют лишь целочисленные коэффициенты). Так как существуют перечислимые, но неразрешимые предикаты (это является одним из классических результатов теории алгорифмов), то из справедливости этого утверждения непосредственно следует, что 10-я проблема Гильберта является алгорифмически неразрешимой.

Гипотезу о диофантовости перечислимых предикатов впервые высказал, по-видимому, Мартин Дейвис. В работе [2] он вынужден оставить открытым вопрос о справедливости этой гипотезы, однако там получен один родственный результат. А именно, в [2] показано, что каждый перечислимый предикат $\mathcal{R}(a_1, \ldots, a_n)$ представи́м в виде

$$\exists x \forall y_{\leqslant x} \exists z_1 \ldots z_k [R(a_1, \ldots, a_n, x, y, z_1, \ldots, z_k) = 0],$$

где R — полином.

Используя это представление, Мартин Дейвис, Хилэри Патнам и Джулия Робинсон доказали в [3], что каждый перечислимый предикат $\mathcal{R}(a_1, \ldots, a_n)$ представи́м в виде

$$\exists z_1 \ldots z_k [P(a_1, \ldots, a_n, z_1, \ldots, z_k) = Q(a_1, \ldots, a_n, z_1, \ldots, z_k)],$$

*) Приведем одно из возможных определений понятия «перечислимый предикат»: предикат $\mathcal{R}(a_1, \ldots, a_n)$ называется перечислимым, если можно указать некоторый алгорифм, который, будучи применен к произвольной n-ке чисел, окончит работу в том и только в том случае, когда предикат $\mathcal{R}$ истинен на этой n-ке.

где P и Q — некоторые функции, построенные при помощи суперпозиции сложения, умножения, возведения в степень и конкретных натуральных чисел.

Этот результат открывает один из многих возможных подходов к доказательству гипотезы Дейвиса. А именно, согласно этому результату для доказательства диофантовости произвольного перечислимого предиката достаточно установить диофантовость трехместного отношения, задаваемого формулой

$$q = p^{k}. \tag{1}$$

Вопрос о том, является ли это отношение диофантовым, исследовала Джулия Робинсон в работе [4]. Она нашла ряд достаточных условий. В частности, в [4] получен следующий результат: *отношение* (1) *является диофантовым, если существует диофантово отношение* $\mathcal{D}(u, v)$, *обладающее следующими свойствами*:

$$\forall uv\,[\mathcal{D}(u, v) \Rightarrow v \leqslant u^{u}], \tag{2}$$

$$\forall k \exists uv\,[\mathcal{D}(u, v)\ \&\ u^{k} < v]. \tag{3}$$

Про отношение $\mathcal{D}(u, v)$, обладающее свойствами (2) и (3), говорят, что оно *имеет экспоненциальный рост*.

Вопрос о существовании диофантова отношения, имеющего экспоненциальный рост, оказался трудным. Ни одно из многочисленных двупараметрических семейств диофантовых уравнений, уже изученных в теории чисел (см., например, [5]), не дает непосредственной возможности указать такое отношение. Тем не менее, диофантовы отношения, имеющие экспоненциальный рост, существуют. Построение примера такого отношения и является основным техническим результатом диссертации. Этот пример завершает доказательство того, что справедлива

ОСНОВНАЯ ТЕОРЕМА. *Каждый перечислимый предикат является диофантовым.*

Нетрудно показать, что справедливо обратное утверждение: каждый диофантов предикат является перечислимым. Таким образом, свойство «быть перечислимым предикатом», имеющее алгорифмический характер, эквивалентно свойству «быть диофантовым предикатом», имеющему арифметический характер.

Из основной теоремы (и теоремы о существовании перечислимых, но неразрешимых предикатов) следует, что

10-я проблема Гильберта является алгорифмически неразрешимой. Более того, если использовать еще один результат Хилэри Патнама из [6], то можно для некоторого конкретного полинома $T(z_1, \ldots, z_k)$ показать, что невозможен алгорифм, позволяющий узнавать по произвольному натуральному значению параметра a, разрешимо ли в целых (или натуральных) числах уравнение $T(z_1, \ldots, z_k) = a$.

Диссертация состоит из введения и четырех параграфов. В первом параграфе дан краткий обзор результатов, полученных Мартином Дейвисом, Хилэри Патнамом и Джулией Робинсон, а также приведены некоторые следствия основной теоремы. Приведем здесь лишь одно из них: каждый перечислимый предикат $\mathcal{R}(a_1, \ldots, a_n)$ представим в виде $\exists z_1 \ldots z_k [Q(z_1, \ldots, z_k) = D_n(a_1, \ldots, a_n)]$, где Q и D_n — некоторые полиномы, причем полином D_n зависит лишь от числа аргументов предиката $\mathcal{R}$ и $D_1(x) = x$.

Второй параграф является центральным в диссертации. В нем приведен пример диофантова отношения, имеющего экспоненциальный рост. Этот пример строится на основе изучения свойств известной последовательности чисел Фибоначчи 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ..., задаваемой рекуррентным соотношением $\varphi_0 = 0$, $\varphi_1 = 1$, $\varphi_{k+1} = \varphi_k + \varphi_{k-1}$. Приведем одну из ключевых лемм и основную теорему второго параграфа.

ЛЕММА 10. *Каковы бы ни были числа s и q, если $\varphi_s^2 \mid \varphi_q$, то $\varphi_s \mid q$.*

ТЕОРЕМА 1. *Каковы бы ни были натуральные числа u и v, для того чтобы*

$$v = \varphi_{2u}, \tag{4}$$

необходимо и достаточно, чтобы существовали натуральные числа l, g, h, m, x, y, z такие, что

$$\begin{array}{ll} u < l, & v < l, \\ l^2 - lz - z^2 = 1, & g^2 - gh - h^2 = 1, \\ l^2 \mid g, & x^2 - mxy + y^2 = 1, \\ l \mid m - 2, & 2h + g \mid m - 3, \\ l \mid x - u, & 2h + g \mid x - v. \end{array}$$

Как показали впоследствии Н. К. Косовский [7] и М. Дейвис [8], основываясь на идеях, позволивших дать диофантово представление отношения (4), можно указать

диофантово представление отношения

$$v = \alpha_u \,\&\, w = \beta_u, \tag{5}$$

где $\langle \alpha_u, \beta_u \rangle$ — u-е (в порядке возрастания) решение уравнения Пелля $\alpha^2 - (a^2 - 1)\beta^2 = 1$. Диофантово представление отношения (5) указал также Г. В. Чудновский в [9].

В третьем параграфе указано диофантово представление отношения (1). Это представление является более простым, чем получающееся в результате непосредственного применения метода Джулии Робинсон [4] к построенному во втором параграфе примеру диофантова отношения, имеющего экспоненциальный рост (ср. с [10]).

Кроме того, в третьем параграфе указан метод, позволяющий находить (минуя основную теорему) диофантовы представления для широкого класса последовательностей натуральных чисел, задаваемых линейными рекуррентными соотношениями.

Так как предикат «a — простое число» является перечислимым, то, согласно указанному выше следствию основной теоремы, можно указать такой полином Q, множество всех положительных значений которого есть в точности множество всех простых чисел. Конкретный пример такого полинома 21 степени от 21 переменной построен в четвертом параграфе.

Основное содержание диссертации отражено в работе [11]. Введение и первые три параграфа совпадают с работой [12], предложенная в четвертом параграфе конструкция полинома, представляющего множество простых чисел, является модификацией конструкции, изложенной в [13]. Результаты диссертации были доложены в январе 1970 г. на Ленинградском семинаре по конструктивной математике, в июне 1970 г.— на II Скандинавском симпозиуме по логике (см. [14]), в сентябре 1970 г.— на Международном конгрессе математиков в Ницце (см. [15]), в октябре 1970 г.— на Всесоюзной конференции «Исследования по теории чисел», в августе 1971 г.— на IV Международном конгрессе по логике, методологии и философии науки.

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] Гильберт Д., Математические проблемы, Доклад, прочитанный 8 августа 1900 г. на II Международном конгрессе математиков в Париже, Сб. «Проблемы Гильберта», М., 1969.

[2] Дэвис М., Арифметические проблемы и рекурсивно-перечислимые предикаты, Сб. «Математика», 8, № 5 (1964), 15—22.
[3] Дэвис М., Путнам Х., Робинсон Дж., Проблема разрешимости для показательно-диофантовых уравнений, Сб. «Математика», 8, № 5 (1965), 69—79.
[4] Робинсон Дж., Экзистенциальная выразимость в арифметике, Сб. «Математика», 8, № 5 (1964), 3—14.
[5] Dickson L. E., History of Theory of Numbers, 2, New York, 1952.
[6] Путнам Х., Об одной неразрешимой проблеме арифметики, Сб. «Математика», 8, № 5 (1954), 55—68.
[7] Косовский Н. К., О диофантовых представлениях последовательности решений уравнения Пелля, Записки научных семинаров Ленингр. отд. Матем. ин-та АН СССР, **20**, (1971), 60—66.
[8] Davis M., An explicit Diophantine definition of the exponential function, Communications on Pure and Applied Mathematics, **24**, № 2 (1971), 137—145.
[9] Чудновский Г. В., Диофантовы предикаты, Успехи матем. наук, **25**, № 4, (1970), 185—186.
[10] Robinson J., Diophantine decision problems, Studies in Mathematics, **6** (1969), 76—116.
[11] Матиясевич Ю. В., Диофантовость перечислимых множеств, Докл. АН СССР, **191**, № 2 (1970), 279—282.
[12] Матиясевич Ю. В., Диофантово представление перечислимых предикатов, Изв. АН СССР, Сер. матем., **35**, № 1 (1971), 3—30.
[13] Матиясевич Ю. В., Диофантово представление множества простых чисел, Докл. АН СССР, **196**, № 4 (1971), 770—773.
[14] Matijasevič Yu. V., Diophantine representation of recursively enumerable predicates, Proceedings of the 2nd Nordic Logic Symposium, North-Holland Publ. Comp., 1971, 171—177.
[15] Matijasevič Yu. V., Diophantine representation of recursively enumerable predicates, Actes. Congres intern. math., I, 1970, 235—238.

Математические заметки, том **12**, выпуск **1** (1972)

Редактор *Н. К. Осколкова*
Техн. редакторы *С. Я. Шкляр*, *Е. Н. Земская* Корректор *М. Л. Медведская*

Сдано в набор 25/IV 1972 г. Подписано к печати 20/VI 1972 г. Бумага 84×108/32
Физ. печ. л. 3,75. Условн. печ. л. 6,30. Уч.-изд. л. 6,06
Тираж 1230 экз. Т-10550 Цена 60 коп. Заказ № 477

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

2-я типография издательства «Наука». Москва, Шубинский пер., 10