Math-Net.Ru

Общероссийский математический портал

Ю. Матиясевич, Десятая проблема Гильберта, *Квант*, 2021, номер 2, 2–8

DOI: <https://doi.org/10.4213/kvant20210201>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.207.199.55

26 апреля 2023 г., 17:22:28

Десятая проблема Гильберта

(К 50-летию ее решения)

Ю. МАТИЯСЕВИЧ

В 1900 ГОДУ ПРЕДСТАВИТЕЛИ многих стран собрались в Париже для участия во Втором Международном конгрессе математиков. Выдающийся немецкий математик Давид Гильберт выступил там с докладом, который назывался «Математические проблемы» [1]. Во вступительной части доклада Гильберт сказал, что, по его мнению, математика – это наука, которую двигают вперед не решенные еще задачи. Затем он перечислил 23 проблемы, решение которых, по его мнению, важно для дальнейшего прогресса математики.

Проблема под номером 10 посвящена *диофантовым уравнениям*. Эти уравнения названы в честь древнегреческого математика Диофанта Александрийского, который жил в III веке нашей эры.

Математики издавна занимались решением алгебраических уравнений. Древние греки делали это, однако, геометрически. Например, для уравнения

$$x^2 = 2 \quad (1)$$

они давали такое решение: *построить (циркулем и линейкой) квадрат со стороной 1; его диагональ и будет искомым решением уравнения* (по теореме Пифагора; рис.1).

Рис. 1

(точнее, в положительных рациональных числах, ибо отрицательные числа не были ему известны). При таком ограничении

области допустимых значений неизвестных уравнение (1) решений не имеет.

В настоящее время при решении диофантовых уравнений обычно накладывают еще более сильное ограничение на область допустимых значений неизвестных, требуя решать эти уравнения в целых числах или в натуральных, т.е. положительных целых числах. Помимо внутриматематического интереса, это может быть мотивировано решаемой прикладной задачей, например, если неизвестные величины – это количества людей, необходимых для выполнения определенных работ.

Говоря о диофантовых уравнениях, наряду с ограничениями на неизвестные, также подразумевают и специальную форму самих уравнений. Мы под диофантовыми уравнениями будем понимать уравнения вида

$$A(x_1, \dots, x_m) = B(x_1, \dots, x_m), \quad (2)$$

где A и B – многочлены с целыми коэффициентами. Строчные латинские буквы у нас всегда будут использоваться для обозначения натуральных чисел.

За период, прошедший со времени Диофанта, математики нашли решения у огромного количества диофантовых уравнений, а про многие другие доказали, что решений (в целых или натуральных числах) у них нет. Для этого пришлось разработать большое количество разнообразных методов, каждый из которых применим к уравнениям очень специального вида. Ярким примером здесь может служить Великая теорема Ферма, ждавшая своего доказательства более трех столетий. Гильберт считал нужным покончить с разнородными методами решения диофантовых уравнений, найдя единый, универсальный метод,

который можно было бы применить к любому диофантову уравнению и узнать, есть ли у него решения.

В современных терминах можно сказать, что Гильберт просил найти *алгоритм* для решения диофантовых уравнений. В своей формулировке проблемы он, однако, не использовал именно это слово. Дело в том, что в то время в математике еще не было строгого определения алгоритма. Такое определение было выработано гораздо позднее, в 30-е годы XX столетия. В наши дни 10-ю проблему Гильберта можно понимать как следующую задачу: написать на каком-либо языке программирования программу, которая, получив на вход произвольное диофантово уравнение, через конечное время выдавала бы ответ, скажем, печатая число 0, если уравнение решений не имеет, и что угодно, отличное от 0, в противоположном случае.

Сегодня мы знаем, что написать такую программу нельзя. Десятая проблема Гильберта не имеет решения, которое требовал Гильберт, а доказательство этого факта считается *отрицательным решением* этой проблемы.

Неразрешимость 10-й проблемы Гильберта означает, что если мы зафиксируем некоторый язык программирования $\mathcal{Y}$, то для любой программы P на этом языке, которая гипотетически решает эту проблему, найдется конкретное диофантово уравнение

$$A_P(x_1, \dots, x_m) = B_P(x_1, \dots, x_m), \quad (3)$$

на котором программа ошибется. А именно,

- либо программа напечатает 0, а уравнение имеет решение,
- либо уравнение решений не имеет, а программа печатает нечто, отличное от нуля, или же не печатает ничего (просто остановившись или работая неограниченно долго).

Многочлены в уравнении (3) не зря имеют индекс P , они действительно должны зависеть от программы P . Невозможно указать одно «очень трудное» уравнение, для которого ни одна программа не дала бы правильный ответ. Действительно, есть две очень простые программы (одна, которая всегда печатает ноль, и другая, которая всегда

печатает единицу), и для каждого конкретного уравнения одна из этих двух программ неизбежно даст правильный ответ.

Неразрешимость 10-й проблемы Гильберта доказана в следующем сильном смысле: *можно написать программу H такую, что какова бы ни была программа P на выбранном нами языке $\mathcal{Y}$, если подать ее на вход программы H , то через конечное время программа H напечатает некоторое диофантово уравнение (3), на котором программа P ошибается* (рис.2).

Можно также написать вторую программу, которая, получив на вход программу P , напечатает формальное доказательство

Рис. 2

того, что программа P действительно не дает правильного ответа для уравнения (3), найденного программой H .

Мы видим, что существует тесная связь между программами и диофантовыми уравнениями: программы можно преобразовывать в уравнения со специальными свойствами. Гипотезу о существовании подобной связи высказал в конце 40-х годов прошлого столетия молодой американский математик Мартин Дейвис (Martin Davis, род. в 1928 г.). Он рассматривал диофантовы уравнения с параметрами:

$$A(a_1, \dots, a_n, x_1, \dots, x_m) = B(a_1, \dots, a_n, x_1, \dots, x_m). \quad (4)$$

При одних значениях параметров $a_1, \dots, a_n$ уравнение (4) может иметь решение в неизвестных $x_1, \dots, x_m$ (принимаящих целые неотрицательные значения), а при других значениях параметров решений может и не быть. Мы можем рассмотреть множество M , состоящее из тех и только тех значений параметров, для которых хотя бы одно решение существует. В символической записи это выглядит так:

$$\begin{aligned} \langle a_1, \dots, a_n \rangle \in M &\Leftrightarrow \\ &\Leftrightarrow \exists x_1, \dots, x_m \{ A(a_1, \dots, a_n, x_1, \dots, x_m) = \\ &= B(a_1, \dots, a_n, x_1, \dots, x_m) \}. \end{aligned} \quad (5)$$

Множества, которые можно определить таким образом, Мартин Дейвис назвал *диофантовыми*, а формулы такого вида стали называться *диофантовыми представлениями* таких множеств.

Вот простые примеры диофантовых множеств:

- *множество квадратов всех натуральных чисел*, задаваемое уравнением

$$x^2 = a;$$

- *множество всех составных чисел*, задаваемое уравнением

$$(x_1 + 1)(x_2 + 1) = a;$$

- *множество всех натуральных чисел, не являющихся степенями числа 2*, задаваемое уравнением

$$(2x_1 + 1)x_2 = a.$$

В качестве упражнения попробуйте доказать, что диофантовым является и дополнение к множеству из первого из этих трех примеров, т.е. множество всех натуральных чисел, отличных от полных квадратов. Аналогичные вопросы для второго и третьего примеров (про множество всех простых чисел и про множество всех степеней числа 2) оказались гораздо более трудными.

Для произвольного диофантова множества M , задаваемого представлением (5), можно написать несложную программу, которая будет перебирать в некотором порядке всевозможные значения параметров и неизвестных и проверять, не выполнено ли равенство (4); каждый раз, когда это произойдет, программа будет вывести на печать набор значений параметров. Работая неограниченно долго, эта программа напечатает все элементы множества M (быть может, с повторениями), и только их.

В теоретической информатике есть более общее понятие *эффективно перечислимого множества*. Для того чтобы некоторое множество было таковым, должна существовать программа, которая перечисляет все его элементы; при этом на структуру и сложность такой программы никаких ограничений не налагается. Примерами эффективно перечислимых множеств могут

служить множество всех простых чисел и множество всех степеней числа 2.

Из сказанного выше видно, что все диофантовы множества эффективно перечислимы. Это можно перефразировать так: если множество не является эффективно перечислимым, то оно не может быть диофантовым – неперечислимость множества является *препятствием* для его диофантовости. Мартин Дейвис высказал предположение, что это препятствие является единственным.

Гипотеза Дейвиса. *Каждое эффективно перечислимое множество является диофантовым.*

Иными словами, Мартин Дейвис предположил, что по каждой программе, перечисляющей элементы какого-то множества, можно найти параметрическое диофантово уравнение, задающее то же самое множество.

Гипотеза Дейвиса была очень смелой, поскольку имела много следствий, которые казались невероятными. Вот одно из них: программу, перечисляющую все простые числа, можно преобразовать в диофантово уравнение с одним параметром

$$A(a, x_1, \dots, x_m) = 0, \quad (6)$$

которое разрешимо тогда и только тогда, когда значением параметра a является простое число. Специалисты по теории чисел считали, что такого уравнения быть не может. Их скептицизм еще более возрос, когда американский математик (философ по основному образованию) Хилари Патнэм (Hilary Putnam, 1926–2016) заметил, что таким же свойством будет обладать и уравнение

$$x_0(1 - A^2(x_0, x_1, \dots, x_m)) = a \quad (7)$$

(докажите это!). Иными словами, если гипотеза Дейвиса верна, то множество всех простых чисел должно быть множеством всех положительных значений, принимаемых одним конкретным многочленом при произвольных натуральных значениях его переменных.

В 1960 году Дейвис и Патнэм почти доказали гипотезу Дейвиса. Это «почти» было вызвано двумя причинами.

Во-первых, Дейвис и Патнэм были вынуждены расширить класс рассматриваемых уравнений. А именно, они разрешили использовать при построении правых и левых частей в уравнениях (4) и (5) операции сложения, умножения и *возведения в степень*, применяемые к конкретным натуральным числам и переменным. Получающиеся при этом уравнения получили название *экспоненциально диофантовых*, а формулы вида (5) – *экспоненциально диофантовых представлений*. В экспоненциально диофантовых уравнениях использование отрицательных чисел не разрешается – объясните, почему.

Во-вторых, Дейвис и Патнэм использовали предположение, что для любого n существует арифметическая прогрессия, состоящая из n неравных простых чисел. Эта гипотеза считалась правдоподобной, но доказана была Б.Грином и Т.Тао только в 2004 году.

К счастью, Дейвису и Патнэму не пришлось ждать так долго, чтобы их доказательство избавилось от недоказанного предположения. Другой американский математик, Джулия Робинсон (Julia Robinson, 1919–1985), усилила их аргументы, и в 1961 появилась статья этих трех авторов с доказательством следующей ослабленной формы гипотезы Дейвиса.

ДПР-теорема. *Каждое эффективно перечислимое множество является экспоненциально диофантовым.*

После этого для доказательства первоначальной гипотезы Дейвиса было достаточно доказать один ее частный случай, а именно, найти трехпараметрическое диофантово уравнение, выражающее возведение в степень через сложение и умножение:

$$a = b^c \Leftrightarrow$$

$$\Leftrightarrow \exists x_1, \dots, x_m \{E(a, b, c, x_1, \dots, x_m) = 0\}. \quad (8)$$

Используя нужное количество копий этого уравнения с новыми неизвестными, мы можем преобразовать произвольное параметрическое экспоненциально диофантово уравнение в диофантово уравнение, разрешимое при тех же значениях параметров.

Вопрос о существовании диофантова представления возведения в степень Джулия Робинсон начала изучать еще в начале 50-х годов прошлого столетия. Первоначально она пыталась доказать, что это невозможно, но не смогла это сделать. Вместо этого она нашла достаточное условие для существования представления вида (8). Оказалось, что достаточно найти двухпараметрическое диофантово уравнение

$$J(u, v, x_1, \dots, x_m) = 0, \quad (9)$$

лишь очень отдаленно напоминающее возведение в степень. А именно, достаточно, чтобы

- для любого решения уравнения (9) было выполнено неравенство $v < u^u$,

- для любого k должно существовать решение уравнения (9), в котором $v > u^k$.

Выяснилось, что ни одно из сотен диофантовых уравнений, рассмотренных специалистами по теории чисел со времен Диофанта, не обладало обоими этими свойствами, и встала задача построить такое уравнение. Это удалось сделать автору этой статьи в 1970 году. Существенную роль при этом сыграли *числа Фибоначчи*. Они названы в честь итальянского математика Леонардо Пизанского (которого позднее стали называть Фибоначчи). В его книге, опубликованной в 1202 году, эти числа дают решение задачи о размножающихся кроликах (еще гораздо раньше, до нашей эры, числа Фибоначчи возникали при решении других задач индийскими математиками).

Числа Фибоначчи, обладающие многими замечательными свойствами, задаются рекуррентным соотношением

$$F_1 = 1, F_2 = 1, F_{k+2} = F_{k+1} + F_k. \quad (10)$$

Но какое отношение они имеют к диофантовым уравнениям? Вы легко докажете (это сделал Ж.-Д.Кассини еще в 1680 году), что $x = F_{k+1}$, $y = F_k$ для любого k дают решение уравнения

$$(x^2 - xy - y^2)^2 = 1. \quad (11)$$

Гораздо позднее, в 1902 году, Дж.Вастилс доказал и обратное (попробуйте и вы это

сделать) – любое решение уравнения (11) состоит из двух последовательных чисел Фибоначчи.¹

Числа Фибоначчи растут примерно как экспонента – можно доказать, что

$$F_n = \frac{\varphi^n + \varphi^{-n}}{\sqrt{5}}, \quad (12)$$

где $\varphi = (1 + \sqrt{5})/2 = 1,618\dots$ – *золотое сечение*. Тем не менее, уравнение (11) – это не совсем то, что требовалось для выполнения условия Джулии Робинсон. Дело в том, что уравнение (11) задает множество чисел Фибоначчи, а не *последовательность* этих чисел, ибо в него не входят индексы чисел Фибоначчи, составляющих решение уравнения.

Автору этой статьи удалось построить требуемое диофантово уравнение со многими неизвестными, которое связывает число Фибоначчи с его порядковым номером. Это стало возможным благодаря найденному им следующему свойству чисел Фибоначчи:

F_n делится на F_m^2 тогда и только тогда, когда n делится на mF_m . (13)

Доказать это свойство не слишком трудно (сделайте это!) *после того, как оно сформулировано*. Удивительно то, что это красивое свойство чисел Фибоначчи было обнаружено только более чем через семь столетий после их появления в книге Фибоначчи.

Первоначальное доказательство автора было основано на одной теореме, которую ленинградский математик Николай Николаевич Воробьев (1925–1995) доказал во время войны, в 1942 году. Опубликовал же он эту теорему гораздо позднее, только в 1969 году, причем не в научном журнале, а в 3-м издании своей книги [2] из серии «Популярные лекции по математике». Таким неожиданным образом публикация, рассчитанная на школьников, внесла свой вклад в решение важной математической проблемы.

¹ Это обращение теоремы Кассини было ключом к решению одной задачи, предложенной на Международной математической олимпиаде в 1981 году [9].

Основной технический результат работы [3] таков.

Теорема. Для того чтобы v было $(2u)$ -м числом Фибоначчи, необходимо и достаточно, чтобы существовали числа g, h, l, t, x, e, z , такие, что:

$$u \leq v < l, \quad (14)$$

$$l^2 - lz - z^2 = 1, \quad (15)$$

$$g^2 - gh - h^2 = 1, \quad (16)$$

$$g \text{ делится на } l^2, \quad (17)$$

$$m - 2 \text{ делится на } l, \quad (18)$$

$$m - 3 \text{ делится на } 2h + g, \quad (19)$$

$$x^2 - txu + y^2 = 1, \quad (20)$$

$$x - u \text{ делится на } l, \quad (21)$$

$$x - v \text{ делится на } 2h + g. \quad (22)$$

Не все из условий (14)–(22) являются диофантовыми уравнениями, но все они легко могут быть приведены к такому виду за счет введения дополнительных неизвестных.² Все получающиеся уравнения можно объединить в одно диофантово уравнение (как это сделать?), которое согласно (12) будет удовлетворять условию Джулии Робинсон. Построение этого уравнения и стало последним шагом в доказательстве гипотезы Дейвиса, которая теперь известна как

ДПРМ-теорема. Каждое эффективно перечислимое множество является диофантовым.

Эта теорема говорит, что два понятия, возникшие в разных разделах математики (диофантово множество из теории чисел и перечислимое множество из теоретической информатики) удивительным образом совпадают друг с другом.

Немедленным следствием ДПРМ-теоремы является неразрешимость 10-й пробле-

² Вы теперь понимаете, что условия (15) и (16) говорят, что l и g должны быть числами Фибоначчи, $l = F_i$ и $g = F_j$, причем согласно (17) j делится на iF_i . Попробуйте установить, какому рекуррентному соотношению удовлетворяют последовательные решения уравнения (20), считая m параметром, а x и y – неизвестными.

мы Гильберта. Дело в том, что давно было установлено существование перечислимого множества N натуральных чисел, дополнение которого (до множества всех натуральных чисел) перечислимым не является.³ Рассмотрим диофантово представление этого множества:

$$a \in N \Leftrightarrow$$

$$\Leftrightarrow \exists x_1, \dots, x_m \{Q(a, x_1, \dots, x_m) = 0\}. \quad (23)$$

Если бы у нас был алгоритм, требуемый в 10-й проблеме Гильберта, то мы могли бы перечислить все элементы дополнения множества N , беря по очереди все возможные значения a и узнавая, есть ли решение у уравнения

$$Q(a, x_1, \dots, x_m) = 0. \quad (24)$$

Таким образом, имеет место неразрешимость 10-й проблемы Гильберта в следующем более сильном смысле: *уже для одного конкретного однопараметрического семейства уравнений (24) не существует алгоритма, который позволял бы по произвольному значению параметра узнать, имеет ли соответствующее диофантово уравнение решения или нет.*

Интересно отметить, что Гильберт в принципе допускал подобные «отрицательные» решения математических проблем. В своем докладе [1] он привел в качестве примера неразрешимой задачи решение алгебраических уравнений произвольной степени в радикалах, а также задачи о трисекции произвольного угла и квадратуре круга, которые нельзя решить при помощи циркуля и линейки.

Гильберт там же указал на «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 удастся получить

ответ на поставленный вопрос, или же в том смысле, что будет установлена невозможность ее решения и вместе с тем доказана неизбежность неудачи всех попыток ее решить». Однако дальнейшее развитие математики не оправдало этой надежды Гильберта — никто не доказал, что каждая математическая проблема допускает решение, положительное или отрицательное, а Курт Гёдель своими знаменитыми *теоремами о неполноте* (см., например, [8]) показал, что для этого не хватит средств никакой одной фиксированной логической системы.

Помимо отрицательного решения 10-й проблемы Гильберта, ДПРМ-теорема имеет много других интересных следствий, в том числе «положительных». В частности, можно явно выписать многочлен, задающий простые числа. Вот один них:

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

Дж.Джонс, Д.Сато, Х.Вада и Д.Вьенс доказали, что множество всех простых чисел — это в точности множество всех положительных значений, принимаемых этим многочленом при целых неотрица-

³ Такое множество можно построить с помощью диагональной конструкции, аналогичной той, с которой Кантор установил несчетность множества вещественных чисел (см., например, [8]).

тельных значениях его 26 переменных. Ровно столько букв имеется в латинском алфавите, и авторы решили обойтись без нижних индексов, используя все эти буквы, включая *o* – не примите эту букву за ноль, здесь это переменная!

Указанный выше многочлен, представляющий простые числа, обладает парадоксальным свойством: он сам является произведением двух многочленов (объясните, почему такое возможно).

С основной идеей построения многочленов для простых чисел можно познакомиться по статье [4]. Доказательство неразрешимости 10-й проблемы Гильберта также доступно школьникам, серьезно интересующимся математикой. Например, они могут попробовать свои силы, решая цепочку задач, предложенных (с подсказками и решениями) в [7]. Тот, кто хочет пойти более легким путем, может прослушать лекции [6]. Старшеклассникам также доступны первые пять глав книги [5], дающие подробное доказательство ДПРМ-теоремы.

Литература

1. Проблемы Гильберта. Под ред. П.С.Александрова. – М.: Наука, 1969. <https://math.ru/lib/377>

2. Н.Н.Воробьев. Числа Фибоначчи. Популярные лекции по математике, выпуск 6. – М.: Наука, 3-е издание, 1969. https://www.mathedu.ru/text/vorobjev_chisla_fibonachchi_1984/p9/

3. Ю.В.Матиясевич. Диофантовость перечислимых множеств. – Доклады АН СССР, том 191, вып. 2, с. 279–282, 1970. <http://www.mathnet.ru/links/de8fdd3514a2645f67701f9257553c20/dan35274.pdf>

4. Ю.В.Матиясевич. Формулы для простых чисел. – «Квант», 1975, № 5. http://kvant.mccme.ru/1975/05/formuly_dlya_prostykh_chisel.htm

5. Ю.В.Матиясевич. Десятая проблема Гильберта. – М.: Наука, 1993.

6. Ю.В.Матиясевич. Десятая проблема Гильберта: что можно и что нельзя делать с диофантовыми уравнениями. – Летняя школа «Современная математика», Дубна, 2011. http://www.mathnet.ru/php/presentation.phtml?option_lang=rus&presentid=3578

7. Ю.В.Матиясевич, Я.Абрамов, А.Я.Белов-Канель, И.А.Иванов-Погодаев, А.С.Малистов. Задача 2. Десятая проблема Гильберта. – 19-я летняя конференция международного математического Турнира городов. <https://olympiads.mccme.ru/ltkg/2007/2/>

8. В.А.Успенский. Теорема Гёделя о неполноте. – Популярные лекции по математике, вып. 57: – М.: Наука, 1982. <https://math.ru/lib/plm/57>

9. Задача 3 Международной математической олимпиады 1981 года. https://artofproblemsolving.com/wiki/index.php/1981_IMO_Problems/Problem_3

НАША ОБЛОЖКА

На первой странице обложки приведена иллюстрация Леонардо да Винчи к трактату Луки Пачоли «О божественной пропорции». Представлены пять платоновых тел, входивших в число девяти правильных многогранников – объемных тел, все грани

которых одинаковые правильные многоугольники. Додекаэдр имеет 12 пятиугольных граней, икосаэдр – 20 треугольных граней, октаэдр – 8 треугольных граней, тетраэдр – 4 треугольные грани, куб (или гексаэдр) – 6 квадратных граней.

Тетраэдр олицетворял огонь, поскольку его вершина устремлена вверх, как у разгоревшегося пламени; икосаэдр, как самый обтекаемый, – воду; куб, как самая устойчивая из фигур, – землю; октаэдр – воздух. Додекаэдр символизировал весь мир и почитался главным.