Джулия Робинсон и десятая проблема Гильберта

23 проблемы Гильберта

http://www-history.mcs.st-andrews.ac.uk/BigPictures/Hilbert_1900.jpeg

Mathematische Probleme

Vortrag, gehalten auf dem internationalen Mathematiker-Kongress, Paris, 1900

⋮

10. Entscheidung der Lösbarkeit einer diophantischen Gleichung

⋮

Давид Гильберт, *“Математические проблемы”*, [1900]

Давид Гильберт, *"Математические проблемы"*, [1900]

10. Entscheidung der Lösbarkeit einer diophantischen Gleichung. Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoefficienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist*.

Давид Гильберт, *"Математические проблемы"*, [1900]

10. Entscheidung der Lösbarkeit einer diophantischen Gleichung. Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoefficienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist*.

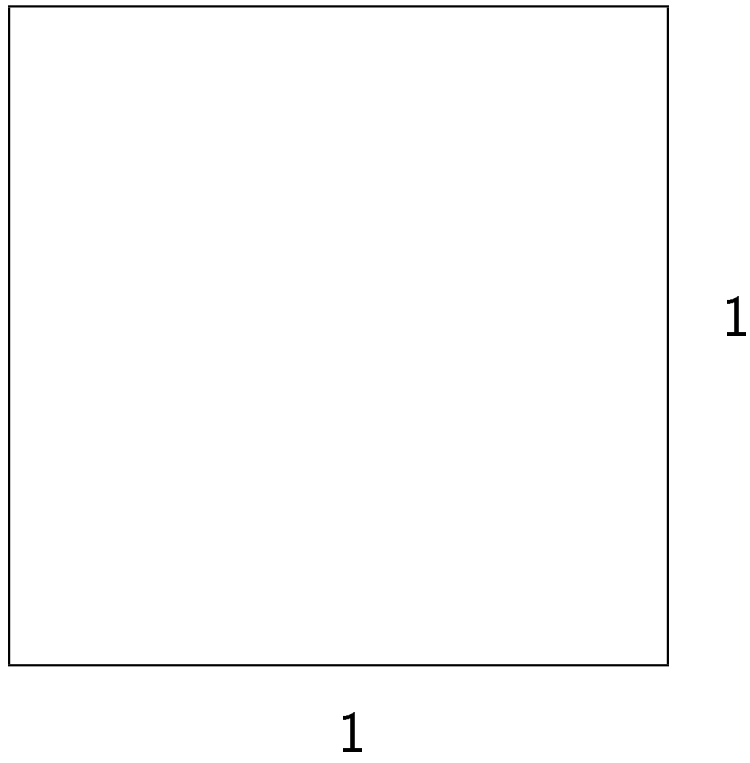
10. Решение проблемы разрешимости для произвольного диофантова уравнения. Пусть дано произвольное диофантово уравнение с произвольным числом неизвестных и целыми рациональными коэффициентами; *требуется указать общий метод, следуя которому можно было бы в конечное число шагов узнать, имеет ли данное уравнение решение в целых рациональных числах или нет*.

Полиномиальные уравнения у древних греков

$$x^2 = 2$$

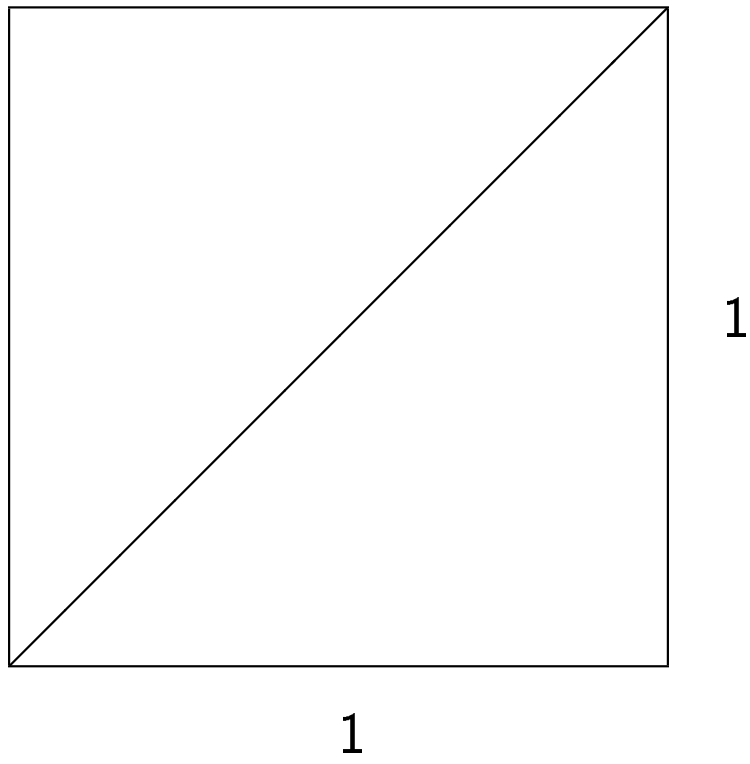
Полиномиальные уравнения у древних греков

$$x^2 = 2$$



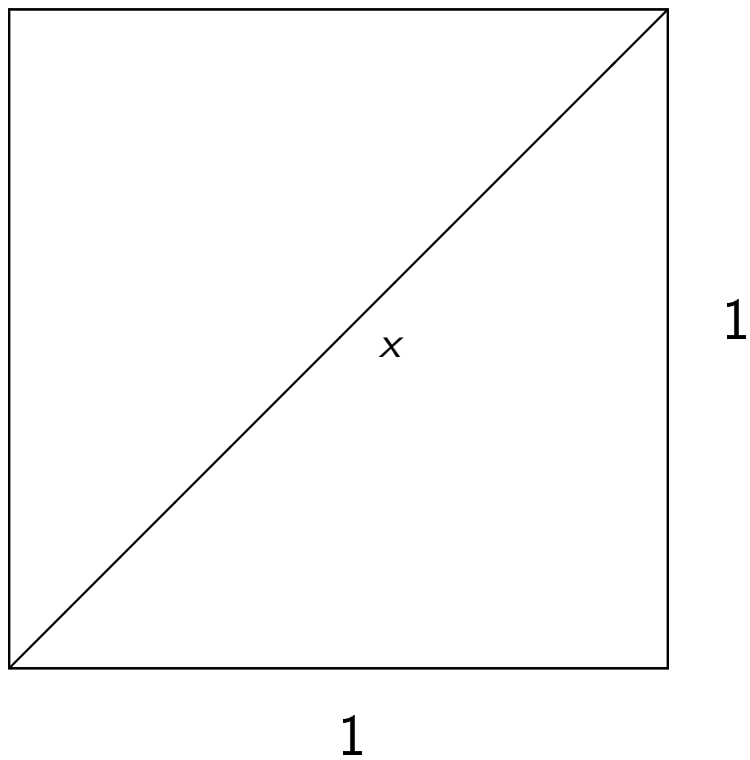
Полиномиальные уравнения у древних греков

$$x^2 = 2$$



Полиномиальные уравнения у древних греков

$$x^2 = 2$$



Диофантовы уравнения

Определение. Диофантово уравнение имеет вид

$$M(x_1, \ldots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами.

Давид Гильберт, *"Математические проблемы"*, [1900]

10. Решение проблемы разрешимости для произвольного диофантова уравнения. Пусть дано произвольное диофантово уравнение с произвольным числом неизвестных и целыми рациональными коэффициентами; *требуется указать общий метод, следуя которому можно было бы в конечное число шагов узнать, имеет ли данное уравнение решение в целых рациональных числах или нет.*

Мы будем расматривать решения диофантовых уравнений в *натуральных числах*

Давид Гильберт, *“Математические проблемы”*, [1900]

10. Решение проблемы разрешимости для произвольного диофантова уравнения. Пусть дано произвольное диофантово уравнение с произвольным числом неизвестных и целыми рациональными коэффициентами; *требуется указать общий метод, следуя которому можно было бы в конечное число шагов узнать, имеет ли данное уравнение решение в целых рациональных числах или нет.*

Мы будем расматривать решения диофантовых уравнений в *натуральных числах* 0, 1, 2, . . .

Давид Гильберт, *“Математические проблемы”*, [1900]

Давид Гильберт, *“Математические проблемы”*, [1900]

10. Решение проблемы разрешимости для произвольного диофантова уравнения. Пусть дано произвольное диофантово уравнение с произвольным числом неизвестных и целыми рациональными коэффициентами; *требуется указать общий метод, следуя которому можно было бы в конечное число шагов узнать, имеет ли данное уравнение решение в целых рациональных числах или нет.*

Массовые проблемы

В современной терминологии 10-я проблема Гильберта является массовой проблемой, то есть проблемой, состоящей из счетного числа вопросов, на каждый из которых требуется дать ответ ДА или НЕТ. Суть массовой проблемы состоит в требовании найти единый универсальный метод, который позволял бы ответить на любой из этих вопросов.

Массовые проблемы

В современной терминологии 10-я проблема Гильберта является массовой проблемой, то есть проблемой, состоящей из счетного числа вопросов, на каждый из которых требуется дать ответ ДА или НЕТ. Суть массовой проблемы состоит в требовании найти единый универсальный метод, который позволял бы ответить на любой из этих вопросов.

Среди двадцати трёх “Математических проблем” Гильберта 10-я является единственной массовой проблемой

Массовые проблемы

В современной терминологии 10-я проблема Гильберта является массовой проблемой, то есть проблемой, состоящей из счетного числа вопросов, на каждый из которых требуется дать ответ ДА или НЕТ. Суть массовой проблемы состоит в требовании найти единый универсальный метод, который позволял бы ответить на любой из этих вопросов.

Среди двадцати трёх “Математических проблем” Гильберта 10-я является единственной массовой проблемой и она может рассматриваться как проблема информатики (которая в 1900 не существовала самостоятельно).

Массовые проблемы

В современной терминологии 10-я проблема Гильберта является массовой проблемой, то есть проблемой, состоящей из счетного числа вопросов, на каждый из которых требуется дать ответ ДА или НЕТ. Суть массовой проблемы состоит в требовании найти единый универсальный метод, который позволял бы ответить на любой из этих вопросов.

Среди двадцати трёх “Математических проблем” Гильберта 10-я является единственной массовой проблемой и она может рассматриваться как проблема информатики (которая в 1900 не существовала самостоятельно).

Алгоритмическая неразрешимость *проблемы тождества слов в конечно определенных полугруппах* (проблема Thue [1914])

А. А. Марков (сын)
1903–1979

Emil L. Post
1897–1954

Hilbert's problem "begs for an unsolvability proof"

Recursively enumerable sets of positive integers and their decision problems. *Bulletin AMS*, **50**, 284–316 (1944); reprinted in: The Collected Works of E. L. Post, Davis, M. (ed), Birkhäuser, Boston, 1994.

Emil L. Post
1897–1954

Уравнения с параметрами

Семейство диофантовых уравнений имеет вид

$$M(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами, переменные которго разделены на две группы:

Уравнения с параметрами

Семейство диофантовых уравнений имеет вид

$$M(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами, переменные которго разделены на две группы:

- параметры $a_1, \ldots, a_n$;

Уравнения с параметрами

Семейство диофантовых уравнений имеет вид

$$M(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами, переменные которго разделены на две группы:

- параметры $a_1, \ldots, a_n$;
- неизвестные $x_1, \ldots, x_m$.

Рассмотрим множество $\mathcal{M}$ такое, что

$$\langle a_1, \ldots, a_n \rangle \in \mathcal{M} \Longleftrightarrow \exists x_1 \ldots x_m \{M(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0\}.$$

Уравнения с параметрами

Семейство диофантовых уравнений имеет вид

$$M(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0,$$

где M – многочлен с целыми коэффициентами, переменные которго разделены на две группы:

- параметры $a_1, \ldots, a_n$;
- неизвестные $x_1, \ldots, x_m$.

Рассмотрим множество $\mathcal{M}$ такое, что

$$\langle a_1, \ldots, a_n \rangle \in \mathcal{M} \Longleftrightarrow \exists x_1 \ldots x_m \{M(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0\}.$$

Множества, имеющие такие представления называются диофантовыми.

Примеры диофантовых множеств

Примеры диофантовых множеств

- Множество всех полных квадратов, представлено уравнением

Примеры диофантовых множеств

- Множество всех полных квадратов, представлено уравнением

$$a - x^2 = 0$$

Примеры диофантовых множеств

- Множество всех полных квадратов, представлено уравнением

$$a - x^2 = 0$$

- Множество всех составных чисел, представлено уравнением

Примеры диофантовых множеств

- Множество всех полных квадратов, представлено уравнением
$$a - x^2 = 0$$
- Множество всех составных чисел, представлено уравнением
$$a - (x_1 + 2)(x_2 + 2) = 0$$

Примеры диофантовых множеств

- Множество всех полных квадратов, представлено уравнением
$$a - x^2 = 0$$
- Множество всех составных чисел, представлено уравнением
$$a - (x_1 + 2)(x_2 + 2) = 0$$
- Множество всех *не*степеней числа 2, представлено уравнением

Примеры диофантовых множеств

- Множество всех полных квадратов, представлено уравнением
$$a - x^2 = 0$$
- Множество всех составных чисел, представлено уравнением
$$a - (x_1 + 2)(x_2 + 2) = 0$$
- Множество всех *не*степеней числа 2, представлено уравнением
$$a - (2x_1 + 3)x_2 = 0$$

Задача Тарского

Доказать, что существуют диофантовы множества, дополнения которых диофантовыми не являются.

Alfred Tarski
1901–1983

Задача Тарского

Доказать, что существуют диофантовы множества, дополнения которых диофантовыми не являются.

Кандидаты:

- множество всех простых чисел
- множество всех степеней числа 2

Alfred Tarski
1901–1983

Теорема Джулии Робинсон [1952]

Julia Robinson
1929–1985

Теорема Джулии Робинсон [1952]

Множество $\{\langle a, b, c\rangle : a^b = c\}$ *является диофантовым при условии, что существует двупараметрическое диофантово уравнение*

$$J(u, v, y_1, \ldots, y_n) = 0$$

обладающее следующими двумя свойствами:

- *в любом решении* $u < v^v$;
- *для каждого* k *существует решение, в котором* $u > v^k$.

Julia Robinson
1929–1985

Теорема Джулии Робинсон [1952]

Множество $\{\langle a, b, c\rangle : a^b = c\}$ *является диофантовым при условии, что существует двупараметрическое диофантово уравнение*

$$J(u, v, y_1, \ldots, y_n) = 0$$

обладающее следующими двумя свойствами:

- *в любом решении* $u < v^v$;
- *для каждого* k *существует решение, в котором* $u > v^k$.

Julia Robinson
1929–1985

Джулия Робинсон назвала отношение между u и v, обладающее этими двумя свойствами, отношением экспоненциального роста

Теорема Джулии Робинсон [1952]

Множество $\{\langle a, b, c\rangle : a^b = c\}$ *является диофантовым при условии, что существует двупараметрическое диофантово уравнение*

$$J(u, v, y_1, \ldots, y_n) = 0$$

обладающее следующими двумя свойствами:

- *в любом решении* $u < v^v$;
- *для каждого* k *существует решение, в котором* $u > v^k$.

Julia Robinson
1929–1985

Джулия Робинсон назвала отношение между u и v, обладающее этими двумя свойствами, отношением экспоненциального роста; позднее они были названы предикатами Джулии Робинсон.

E. Post: Hilbert's problem "begs for an unsolvability proof"

E. Post: Hilbert's problem "begs for an unsolvability proof"

ON THE THEORY OF RECURSIVE
UNSOLVABILITY
by Martin Davis
A DISSERTATION PRESENTED
TO THE FACULTY
OF PRINCETON UNIVERSITY
1950

Martin Davis
Род. 1928

E. Post: Hilbert's problem "begs for an unsolvability proof"

ON THE THEORY OF RECURSIVE
UNSOLVABILITY
by Martin Davis
A DISSERTATION PRESENTED
TO THE FACULTY
OF PRINCETON UNIVERSITY
1950

Martin Davis
Род. 1928

Теорема. *Существуют диофантовы множества с недиофантовыми дополнениями.*

E. Post: Hilbert's problem "begs for an unsolvability proof"

ON THE THEORY OF RECURSIVE
UNSOLVABILITY
by Martin Davis
A DISSERTATION PRESENTED
TO THE FACULTY
OF PRINCETON UNIVERSITY
1950

Martin Davis
Род. 1928

Теорема. *Существуют диофантовы множества с недиофантовыми дополнениями.*
Доказательство. Reductio ad absurdum.

Перечислимые множества

$$M(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$$

Мы можем начать перебирать в каком-либо порядке все наборы из $n + m$ чисел $a_1, \ldots, a_n$, $x_1, \ldots x_m$ и для каждого набора проверять это равенство; если оно выполнено, мы будем помещать набор $\langle a_1, \ldots, a_n \rangle$ в отдельный список. В этот список попадут только элементы множества $\mathcal{M}$, и каждый элемент этого множества рано или поздно появится в нашем списке, быть может, с повторениями.

Перечислимые множества

$$M(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$$

Мы можем начать перебирать в каком-либо порядке все наборы из $n + m$ чисел $a_1, \ldots, a_n$, $x_1, \ldots x_m$ и для каждого набора проверять это равенство; если оно выполнено, мы будем помещать набор $\langle a_1, \ldots, a_n \rangle$ в отдельный список. В этот список попадут только элементы множества $\mathcal{M}$, и каждый элемент этого множества рано или поздно появится в нашем списке, быть может, с повторениями.

Определение. Множество $\mathcal{M}$, состоящее из n-ок натуральных чисел называется *перечислимым*, если существует алгоритм, который (работая бесконечно долго) будет печатать только элементы множества $\mathcal{M}$ и напечатает каждое из них, быть может, много раз.

Гипотеза Мартина Дейвиса

Тривиальный факт. *Каждое диофантово множество является перечислимым.*

Гипотеза Мартина Дейвиса

Тривиальный факт. *Каждое диофантово множество является перечислимым.*

Иными словами, *если множество не является перечислимым, то оно не может быть диофантовым*. Мартин Дейвис предположил, что это является *единственным* препятствием.

Гипотеза Мартина Дейвиса

Тривиальный факт. *Каждое диофантово множество является перечислимым.*

Иными словами, *если множество не является перечислимым, то оно не может быть диофантовым*. Мартин Дейвис предположил, что это является *единственным* препятствием.

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

Следствия гипотезы Мартин Дейвиса

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

Следствия гипотезы Мартин Дейвиса

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

Следствие. *Существует многочлен P с целыми коэффициентами такой, что уравнение*

$$P(a, x_1, \ldots, x_m) = 0$$

имеет решение тогда и только тогда, когда a является простым числом.

Следствия гипотезы Мартин Дейвиса

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

Следствие. *Существует многочлен P с целыми коэффициентами такой, что уравнение*

$$P(x_1, \ldots, x_m) = a$$

имеет решение тогда и только тогда, когда a является простым числом.

Следствия гипотезы Мартин Дейвиса

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

Следствие. *Существует многочлен P с целыми коэффициентами такой, что уравнение*

$$P(x_1, \ldots, x_m) = a$$

имеет решение тогда и только тогда, когда a является простым числом.

Иными словами, множество всех натуральных значений, принимаемых многочленом P, есть в точности множество всех простых чисел.

Следствие гипотезы Мартин Дейвиса

Составим список всех однопараметрических уравнений:

$$M_1(a, x_1, \dots) = 0, \dots, M_k(a, x_1, \dots) = 0, \dots$$

Следствие гипотезы Мартин Дейвиса

Составим список всех однопараметрических уравнений:

$$M_1(a, x_1, \dots) = 0, \dots, M_k(a, x_1, \dots) = 0, \dots$$

Рассмотрим множество $\mathfrak{U}$ такое, что

$$\langle a, k \rangle \in \mathfrak{U} \Leftrightarrow \exists x_1, \dots \{M_k(a, x_1, \dots) = 0\}$$

Следствие гипотезы Мартин Дейвиса

Составим список всех однопараметрических уравнений:

$$M_1(a, x_1, \dots) = 0, \dots, M_k(a, x_1, \dots) = 0, \dots$$

Рассмотрим множество $\mathfrak{U}$ такое, что

$$\langle a, k \rangle \in \mathfrak{U} \Leftrightarrow \exists x_1, \dots \{M_k(a, x_1, \dots) = 0\}$$

Множество $\mathfrak{U}$ перечислимо и (по гипотезе Мартина Дейвиса) диофантово:

$$\langle a, k \rangle \in \mathfrak{U} \ \Leftrightarrow \ \exists y_1 \dots y_N \{U(a, k, y_1, \dots, y_N) = 0\}$$

Следствие гипотезы Мартин Дейвиса

Составим список всех однопараметрических уравнений:

$$M_1(a, x_1, \dots) = 0, \dots, M_k(a, x_1, \dots) = 0, \dots$$

Рассмотрим множество $\mathfrak{U}$ такое, что

$$\langle a, k \rangle \in \mathfrak{U} \Leftrightarrow \exists x_1, \dots \{M_k(a, x_1, \dots) = 0\}$$

Множество $\mathfrak{U}$ перечислимо и (по гипотезе Мартина Дейвиса) диофантово:

$$\langle a, k \rangle \in \mathfrak{U} \ \Leftrightarrow \ \exists y_1 \dots y_N \{U(a, k, y_1, \dots, y_N) = 0\}$$

Таким образом,

$$\exists x_1, \dots \{M_k(a, x_1, \dots) = 0\} \ \Leftrightarrow \ \exists y_1 \dots y_N \{U(a, k, y_1, \dots, y_N) = 0\}$$

Слабая форма гипотезы Мартина Дейвиса

Каждое перечислимое множество $\mathcal{M}$ имеет экспоненциально диофантово представление

$$\langle a_1, \ldots, a_n \rangle \in \mathcal{M} \Longleftrightarrow$$
$$\exists x_1 \ldots x_m \{ E_{\mathrm{L}}(a_1, \ldots, a_n, x_1, \ldots, x_m) \;=\; E_{\mathrm{R}}(a_1, \ldots, a_n, x_1, \ldots, x_m) \}$$

где E_{L} и E_{R} – выражения, построенные по традиционным правилам из конкретных положительных целых чисел и переменных с помощью сложения, умножения и возведения в степень.

Условное доказательство ослабленной гипотезы Дейвиса

Теорема Дейвиса–Патнама.
Каждое перечислимое множество $\mathcal{M}$ имеет экспоненциально диофантово представление

Hilary Putnam
1926–2016

Условное доказательство ослабленной гипотезы Дейвиса

Теорема Дейвиса–Патнама.
Каждое перечислимое множество $\mathcal{M}$ имеет экспоненциально диофантово представление, если существуют сколько угодно длинные арифметические прогрессии, состоящие только из неравных простых чисел.

Hilary Putnam
1926–2016

Условное доказательство ослабленной гипотезы Дейвиса

Теорема Дейвиса–Патнама.
Каждое перечислимое множество $\mathcal{M}$ имеет экспоненциально диофантово представление, если существуют сколько угодно длинные арифметические прогрессии, состоящие только из неравных простых чисел.

Technical Report AFOSR TR59-124

Hilary Putnam
1926–2016

Условное доказательство ослабленной гипотезы Дейвиса

Теорема Дейвиса–Патнама.
Каждое перечислимое множество $\mathcal{M}$ имеет экспоненциально диофантово представление, если существуют сколько угодно длинные арифметические прогрессии, состоящие только из неравных простых чисел.

Technical Report AFOSR TR59-124 of U.S. Air Force, October 1959

Hilary Putnam
1926–2016

Условное доказательство ослабленной гипотезы Дейвиса

Теорема Дейвиса–Патнама.
Каждое перечислимое множество $\mathcal{M}$ имеет экспоненциально диофантово представление, если существуют сколько угодно длинные арифметические прогрессии, состоящие только из неравных простых чисел.

Technical Report AFOSR TR59-124 of U.S. Air Force, October 1959

Hilary Putnam
1926–2016

Теорема Ben Green & Terence Tao M [2004]. Такие арифметические прогрессии действительно существуют.

Письмо Джулии Робинсон

Professor Martin Davis
Rensselaer Polytechnic Institute
Hartford Graduate Division

and

Professor Hilary Putnam
Princeton University
Princeton, New Jersey

Dear Martin,

Thank you for the copies of your report. I am very pleased, surprised, and impressed with your results on Hilbert's Tenth Problem. Quite frankly, I did not think your methods could be pushed further than in your paper in the Journal but I'm very glad to have been wrong.

I believe I have succeeded in eliminating the need for P. A. P. by extending and modifying your proof. I have this written out for my own satisfaction but it is not yet in shape for anyone else.

Слабая форма гипотезы Мартина Дейвиса доказана

J. Robinson
The undecidability of exponential Diophantine equations
Notices AMS, vol. 75, issue 1, p. 1, 1960.

Слабая форма гипотезы Мартина Дейвиса доказана

J. Robinson
The undecidability of exponential Diophantine equations
Notices AMS, vol. 75, issue 1, p. 1, 1960.

M. Davis, H. Putnam, and J. Robinson
The decision problem for exponential diophantine equations
Ann. Math., vol. 74, issue 3, pp. 425-436, 1961.

Слабая форма гипотезы Мартина Дейвиса доказана

J. Robinson
The undecidability of exponential Diophantine equations
Notices AMS, vol. 75, issue 1, p. 1, 1960.

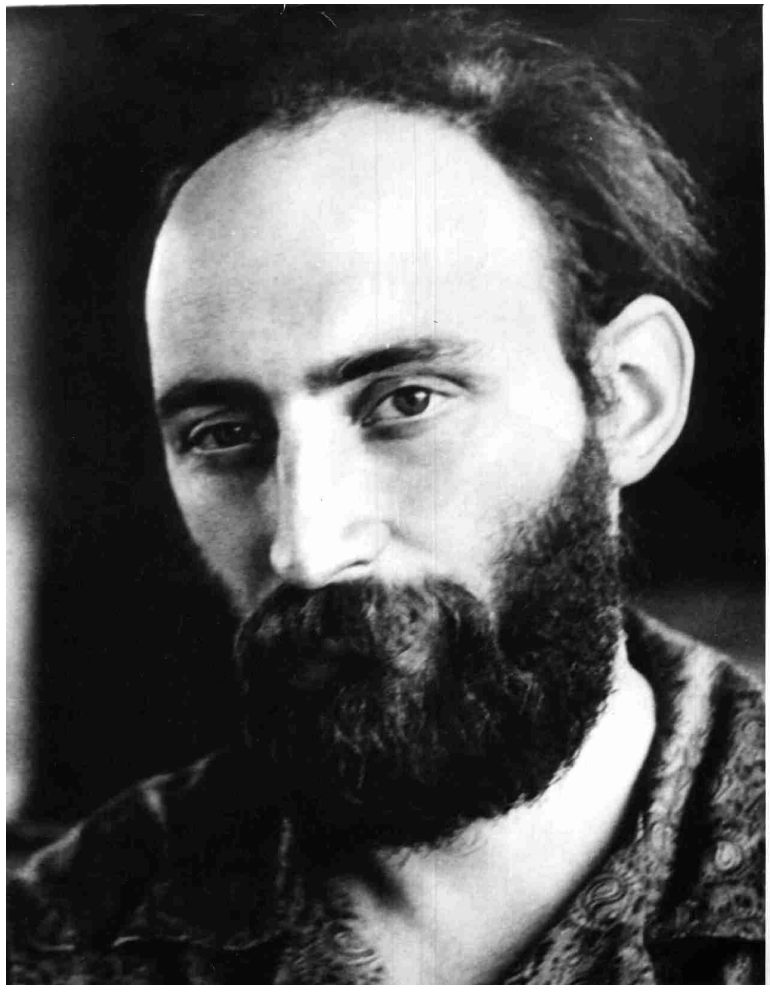
M. Davis, H. Putnam, and J. Robinson
The decision problem for exponential diophantine equations
Ann. Math., vol. 74, issue 3, pp. 425-436, 1961.

DPR-теорема. *Каждое перечислимое множество $\mathcal{M}$ имеет экспоненциально диофантово представление, т.е. представление вида*

$$\langle a_1, \ldots, a_n \rangle \in \mathcal{M} \Longleftrightarrow$$
$$\Longleftrightarrow \exists x_1 \ldots x_m \{ E_{\mathrm{L}}(x_1, x_2, \ldots, x_m) \;=\; E_{\mathrm{R}}(x_1, x_2, \ldots, x_m) \}$$

где E_{L} и E_{R} – выражения, построенные по обычным правилам из переменных и конкретных натуральных чисел с помощью сложения, умножения и возведения в степень.

Сергей Юрьевич Маслов



1939–1982

Mathematical Reviews 1962, 24A, page 574, review A3061:

Davis, Martin; Putnam, Hilary; Robinson, Julia. The decision problem for exponential Diophantine equations. Ann. Math. (2), **74** 425–436 (1961).

> *. . . These results are superficially related to Hilbert's tenth problem on (ordinary, i.e., non-exponential) Diophantine equations. The proof of the authors'results, though very elegant, does not use recondite facts in the theory of numbers nor in the theory of r.e. [recursively enumerable] sets, and so it is likely that the present result is not closely connected with Hilbert's tenth problem. . .*

Mathematical Reviews 1962, 24A, page 574, review A3061:

Davis, Martin; Putnam, Hilary; Robinson, Julia. The decision problem for exponential Diophantine equations. Ann. Math. (2), **74** 425–436 (1961).

> *. . . These results are superficially related to Hilbert's tenth problem on (ordinary, i.e., non-exponential) Diophantine equations. The proof of the authors'results, though very elegant, does not use recondite facts in the theory of numbers nor in the theory of r.e. [recursively enumerable] sets, and so it is likely that the present result is not closely connected with Hilbert's tenth problem. . .*
>
> G.Kreisel

Что сделать?

После DPR-теоремы для того, чтобы доказать, что *каждое* перечислимое множество является диофантовым было достаточно показать, что диофантовым является одно *конкретное* множество, а именно, множество (с помощью диофантова представления этого множества

$$a^b = c \iff \exists z_1 \dots z_m \{A(a, b, c, w_1, \dots, w_m) = 0\}$$

мы могли бы преобразовывать любое экспоненциально диофантово представление любого множества в диофантово представление того же множества).

Что сделать?

После DPR-теоремы для того, чтобы доказать, что *каждое* перечислимое множество является диофантовым было достаточно показать, что диофантовым является одно *конкретное* множество, а именно, множество (с помощью диофантова представления этого множества

$$a^b = c \iff \exists z_1 \dots z_m \{A(a, b, c, w_1, \dots, w_m) = 0\}$$

мы могли бы преобразовывать любое экспоненциально диофантово представление любого множества в диофантово представление того же множества).

По теореме Джулии Робинсон для этого достаточно доказать, что существует двупараметрическое диофантово уравнение

$$J(u, v, y_1, \dots, y_w) = 0$$

обладающее следующими двумя свойствами:

- в любом решении $u < v^v$;
- для каждого k существует решение, в котором $u > v^k$.

Новая работа Джулии Робинсон

J. Robinson
Unsolvable Diophantine problems
Proceedings of the American Mathematical Society, 22(2), 534–538, 1969.

Последний шаг в доказательстве гипотезы Дейвиса

Теорема (Ю. Матиясевич [1970]) *Для того, чтобы v было $2u$-м числом Фибоначчи, необходимо и достаточно, чтобы существовали числа g, h, ℓ, m, x, y, z такие, что*

$$u \leq v < \ell,$$
$$\ell^2 - lz - z^2 = 1,$$
$$g^2 - 2gh - 4h^2 = 1,$$
$$\ell^2 | g,$$
$$\ell | m - 2,$$
$$(2h + g) | (m - 3)$$
$$x^2 - myx + y^2 = 1,$$
$$\ell | x - u,$$
$$(2h + g) | (x - v).$$

Последний шаг в доказательстве гипотезы Дейвиса

Теорема (Ю. Матиясевич [1970]) *Для того, чтобы v было $2u$-м числом Фибоначчи, необходимо и достаточно, чтобы существовали числа g, h, ℓ, m, x, y, z такие, что*

$$u \leq v < \ell,$$
$$\ell^2 - lz - z^2 = 1,$$
$$g^2 - 2gh - 4h^2 = 1,$$
$$\ell^2 | g,$$
$$\ell | m - 2,$$
$$(2h + g) | (m - 3)$$
$$x^2 - myx + y^2 = 1,$$
$$\ell | x - u,$$
$$(2h + g) | (x - v).$$

$0, 1, 1, 2, 3, 5, \ldots, \quad \phi(k+1) = \phi(k) + \phi(k-1)$

Последний шаг в доказательстве гипотезы Дейвиса

Теорема (Ю. Матиясевич [1970]) *Для того, чтобы v было $2u$-м числом Фибоначчи, необходимо и достаточно, чтобы существовали числа g, h, ℓ, m, x, y, z такие, что*

$$u \leq v < \ell,$$
$$\ell^2 - lz - z^2 = 1,$$
$$g^2 - 2gh - 4h^2 = 1,$$
$$\ell^2 | g,$$
$$\ell | m - 2,$$
$$(2h + g) | (m - 3)$$
$$x^2 - myx + y^2 = 1,$$
$$\ell | x - u,$$
$$(2h + g) | (x - v).$$

$0, 1, 1, 2, 3, 5, \ldots, \quad \phi(k+1) = \phi(k) + \phi(k-1) \quad \phi(n)^2 | \phi(m) \Rightarrow \phi(n) | m$

Хронология

- 4 января 1970: Построено требуемое двупараметрическое диофантово уравнение с экспоненциальным ростом

Хронология

- 4 января 1970: Построено требуемое двупараметрическое диофантово уравнение с экспоненциальным ростом
- 29 января 1970: моё первое публичное представление доказательства на семинарн ЛОМИ

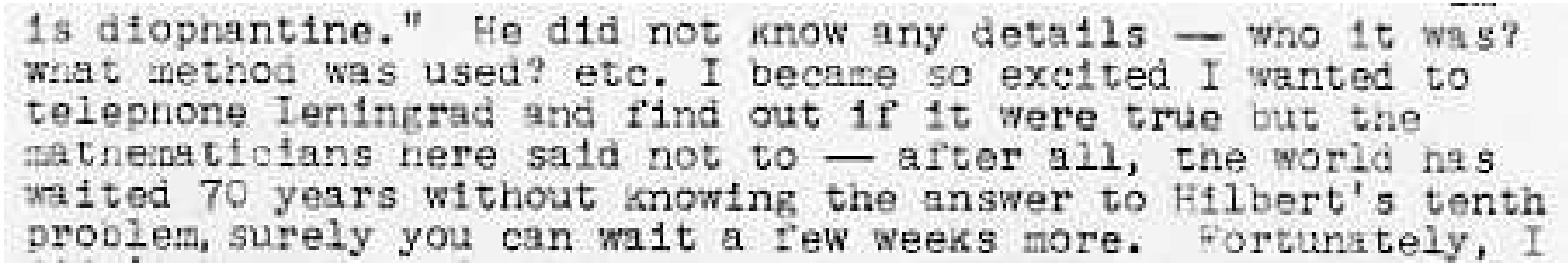
Хронология

- 4 января 1970: Построено требуемое двупараметрическое диофантово уравнение с экспоненциальным ростом
- 29 января 1970: моё первое публичное представление доказательства на семинарн ЛОМИ
- 15 февраля: Мартин Дейвис звонит Джулии из Нью-Йорка и сообщает что “some Russian had proved the existence of Diophantine relation of exponential growth”

Хронология

- 4 января 1970: Построено требуемое двупараметрическое диофантово уравнение с экспоненциальным ростом
- 29 января 1970: моё первое публичное представление доказательства на семинарн ЛОМИ
- 15 февраля: Мартин Дейвис звонит Джулии из Нью-Йорка и сообщает что “some Russian had proved the existence of Diophantine relation of exponential growth”

Из первого письма Джулии Робинсон ко мне от 22 февраля 1970 года:


is diophantine." He did not know any details — who it was? what method was used? etc. I became so excited I wanted to telephone Leningrad and find out if it were true but the mathematicians here said not to — after all, the world has waited 70 years without knowing the answer to Hilbert's tenth problem, surely you can wait a few weeks more. Fortunately, I

Хронология

- 4 января 1970: Построено требуемое двупараметрическое диофантово уравнение с экспоненциальным ростом
- 29 января 1970: моё первое публичное представление доказательства на семинаре ЛОМИ.

Хронология

- 4 января 1970: Построено требуемое двупараметрическое диофантово уравнение с экспоненциальным ростом
- 29 января 1970: моё первое публичное представление доказательства на семинаре ЛОМИ. Среди слушателей: Григорий Самуилович Цейтин

Хронология

- 4 января 1970: Построено требуемое двупараметрическое диофантово уравнение с экспоненциальным ростом
- 29 января 1970: моё первое публичное представление доказательства на семинаре ЛОМИ. Среди слушателей: Григорий Самуилович Цейтин
- 9 февраля 1970г. Цейтин рассказывает про моё доказательство участникам конференции в Новосибирске.

Хронология

- 4 января 1970: Построено требуемое двупараметрическое диофантово уравнение с экспоненциальным ростом
- 29 января 1970: моё первое публичное представление доказательства на семинаре ЛОМИ. Среди слушателей: Григорий Самуилович Цейтин
- 9 февраля 1970г. Цейтин рассказывает про моё доказательство участникам конференции в Новосибирске. Среди слушателей: John McCarthy, делающий записи

Хронология

- 4 января 1970: Построено требуемое двупараметрическое диофантово уравнение с экспоненциальным ростом
- 29 января 1970: моё первое публичное представление доказательства на семинаре ЛОМИ. Среди слушателей: Григорий Самуилович Цейтин
- 9 февраля 1970г. Цейтин рассказывает про моё доказательство участникам конференции в Новосибирске. Среди слушателей: John McCarthy, делающий записи
- February 21: Джулия Робинсон получает записи McCarthy

Lecture by Taitin on Unsolvability of Hilbert's 10th problem

9 Feb 1970

Матиясевич
Юрий Владимирович

diophantine predicate

$\exists y_1 \cdots \exists y_n . P(x_1 \cdots x_m, y_1 \cdots y_n) = 0$

can take y's positive
by replacing a y by enumerable $z_1^2 + z_2^2 + z_3^2 + z_4^2 + 1$

Every recursively enumerable predicate is Diophantine

$U(p,q)$ a Diophantine universal predicate exists. For any r.e. set can get p s.

$q(1 - (P(p, x, y \cdots y_n))^2)$ another consequence

first every r.e. and is exponentially D

The first page of the notes by John McCarthy (1927) on the lecture he heard in Novosibirsk about the solution of Hilbert's tenth problem by a young Russian, Yuri Matijasevich (1947).

Давид Гильберт, *"Математические проблемы"*, [1900]

Вместе с тем бывает и так, что мы добиваемся ответа при недостаточных предпосылках, или идя в неправильном направлении, и вследствии этого не достигаем цели. Тогда возникает задача доказать неразрешимость данной проблемы при принятых предпосылках и выбранном направлении. Такие доказательства невозможности проводились еще 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 все 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 удается 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.

Непростой многочлен для простых чисел

Теорема (J.P.Jones, D.Sato, H.Wada, D.Wiens, [1976])
Множество всех простых чисел – это в точности множество всех положительных значений, принимаемых многочленом

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

при натуральных значениях 26 переменных $a, b, c, \ldots, x, y, z$.

Следствия гипотезы Дейвиса (=DPRM-теоремы)

Нахождение решений любого параметрического диофантова уравнения можно эффективно свести к нахождению решений другого диофантова уравнения с теми же параметрами, имеющего m неизвестных, где m – "абсолютная" константа, не зависящая ни от уравнения, ни от количества параметров.

Сколь малым такое m может быть?

Следствия гипотезы Дейвиса (=DPRM-теоремы)

Нахождение решений любого параметрического диофантова уравнения можно эффективно свести к нахождению решений другого диофантова уравнения с теми же параметрами, имеющего m неизвестных, где m – "абсолютная" константа, не зависящая ни от уравнения, ни от количества параметров.

Сколь малым такое m может быть?

- Моя первоначальная оценка: $m = 200$

Следствия гипотезы Дейвиса (=DPRM-теоремы)

Нахождение решений любого параметрического диофантова уравнения можно эффективно свести к нахождению решений другого диофантова уравнения с теми же параметрами, имеющего m неизвестных, где m – "абсолютная" константа, не зависящая ни от уравнения, ни от количества параметров.

Сколь малым такое m может быть?

- Моя первоначальная оценка: $m = 200$
- Джулия и Рафаель Робинсон: $m = 35$

Следствия гипотезы Дейвиса (=DPRM-теоремы)

Нахождение решений любого параметрического диофантова уравнения можно эффективно свести к нахождению решений другого диофантова уравнения с теми же параметрами, имеющего m неизвестных, где m – "абсолютная" константа, не зависящая ни от уравнения, ни от количества параметров.

Сколь малым такое m может быть?

- Моя первоначальная оценка: $m = 200$
- Джулия и Рафаель Робинсон: $m = 35$
- мое улучшение: $m = 33$

Следствия гипотезы Дейвиса (=DPRM-теоремы)

Нахождение решений любого параметрического диофантова уравнения можно эффективно свести к нахождению решений другого диофантова уравнения с теми же параметрами, имеющего m неизвестных, где m – "абсолютная" константа, не зависящая ни от уравнения, ни от количества параметров.

Сколь малым такое m может быть?

- Моя первоначальная оценка: $m = 200$
- Джулия и Рафаель Робинсон: $m = 35$
- мое улучшение: $m = 33$

Джулия Робинсон: *"I consider it in the range of 'practical' number theory, since Davenport once wrote a paper on cubic forms in 33 variables."*

Дальнейшие оценки требуемого количества неизвестных

- моя первоначальная оценка: $m = 200$
- Джулия и Рафаель Робинсон: $m = 35$
- мое улучшение: $m = 33$

Дальнейшие оценки требуемого количества неизвестных

- моя первоначальная оценка: $m = 200$
- Джулия и Рафаель Робинсон: $m = 35$
- мое улучшение: $m = 33$
- февраль 1971 г.: $m = 26$

Дальнейшие оценки требуемого количества неизвестных

- моя первоначальная оценка: $m = 200$
- Джулия и Рафаель Робинсон: $m = 35$
- мое улучшение: $m = 33$
- февраль 1971 г.: $m = 26$

Джулия Робинсон: *“breaking the ‘alphabetical’ barrier”*

Дальнейшие оценки требуемого количества неизвестных

- моя первоначальная оценка: $m = 200$
- Джулия и Рафаель Робинсон: $m = 35$
- мое улучшение: $m = 33$
- февраль 1971 г.: $m = 26$

Дальнейшие оценки требуемого количества неизвестных

- моя первоначальная оценка: $m = 200$
- Джулия и Рафаель Робинсон: $m = 35$
- мое улучшение: $m = 33$
- февраль 1971 г.: $m = 26$
- август 1971 г.: $m = 14$ (доложено мною на IV International Congress on Logic, Methodology and Philosophy of Science в Бухаресте)

Дальнейшие оценки требуемого количества неизвестных

- моя первоначальная оценка: $m = 200$
- Джулия и Рафаель Робинсон: $m = 35$
- мое улучшение: $m = 33$
- февраль 1971 г.: $m = 26$
- август 1971 г.: $m = 14$ (доложено мною на IV International Congress on Logic, Methodology and Philosophy of Science в Бухаресте)

Джулия Робинсон: *"With just 14 variables we ought to be able to know every variable personally and why it has to be there"*

Дальнейшие оценки требуемого количества неизвестных

- моя первоначальная оценка: $m = 200$
- Джулия и Рафаель Робинсон: $m = 35$
- мое улучшение: $m = 33$
- февраль 1971 г.: $m = 26$
- август 1971 г.: $m = 14$ (доложено мною на IV International Congress on Logic, Methodology and Philosophy of Science в Бухаресте)

Дальнейшие оценки требуемого количества неизвестных

- моя первоначальная оценка: $m = 200$
- Джулия и Рафаель Робинсон: $m = 35$
- мое улучшение: $m = 33$
- февраль 1971 г.: $m = 26$
- август 1971 г.: $m = 14$ (доложено мною на IV International Congress on Logic, Methodology and Philosophy of Science в Бухаресте)
- март 1972 г.: $m = 15$

Кто виноват?

Джулия Робинсон:

I was completely flabbergasted by your letter of May 11. I wanted to crawl under a rock and hide from myself! Somehow I had never questioned that

$$\binom{a}{c} \equiv \binom{b}{c} \pmod{a-b}.$$

I usually know enough not to divide by zero. I had even mentioned (asserted) it to Raphael several times and he had not objected. He said he would have said 'no' if I had asked if it were true. I guess I would have myself if I had asked!

Кто виноват?

Джулия Робинсон:

I was completely flabbergasted by your letter of May 11. I wanted to crawl under a rock and hide from myself! Somehow I had never questioned that

$$\binom{a}{c} \equiv \binom{b}{c} \pmod{a-b}.$$

I usually know enough not to divide by zero. I had even mentioned (asserted) it to Raphael several times and he had not objected. He said he would have said 'no' if I had asked if it were true. I guess I would have myself if I had asked!

I am very glad you sent a way around the mistake at the same time you told me about it.

Кто виноват?

Джулия Робинсон:

> *I was completely flabbergasted by your letter of May 11. I wanted to crawl under a rock and hide from myself! Somehow I had never questioned that*
>
> $$\binom{a}{c} \equiv \binom{b}{c} \pmod{a-b}.$$
>
> *I usually know enough not to divide by zero. I had even mentioned (asserted) it to Raphael several times and he had not objected. He said he would have said 'no' if I had asked if it were true. I guess I would have myself if I had asked!*
>
> *I am very glad you sent a way around the mistake at the same time you told me about it.*

- $m = 13$

ACTA ARITHMETICA
XXVII (1975)

Reduction of an arbitrary diophantine equation to one in 13 unknowns

by

YURI MATIJASEVIČ (Leningrad) and JULIA ROBINSON (Berkeley, Calif.)

A diophantine equation is a polynomial equation in some *parameters* $a_1, \ldots, a_\mu$ and some *unknowns* $x_0, \ldots, x_\nu$. That is, an equation of the form

$$P(a_1, \ldots, a_\mu, x_0, \ldots, x_\nu) = 0 \tag{1}$$

where P is a polynomial with integer coefficients (μ and ν are particular natural numbers). Both parameters and unknowns will be restricted to

Встречи с Ю. В. Линником

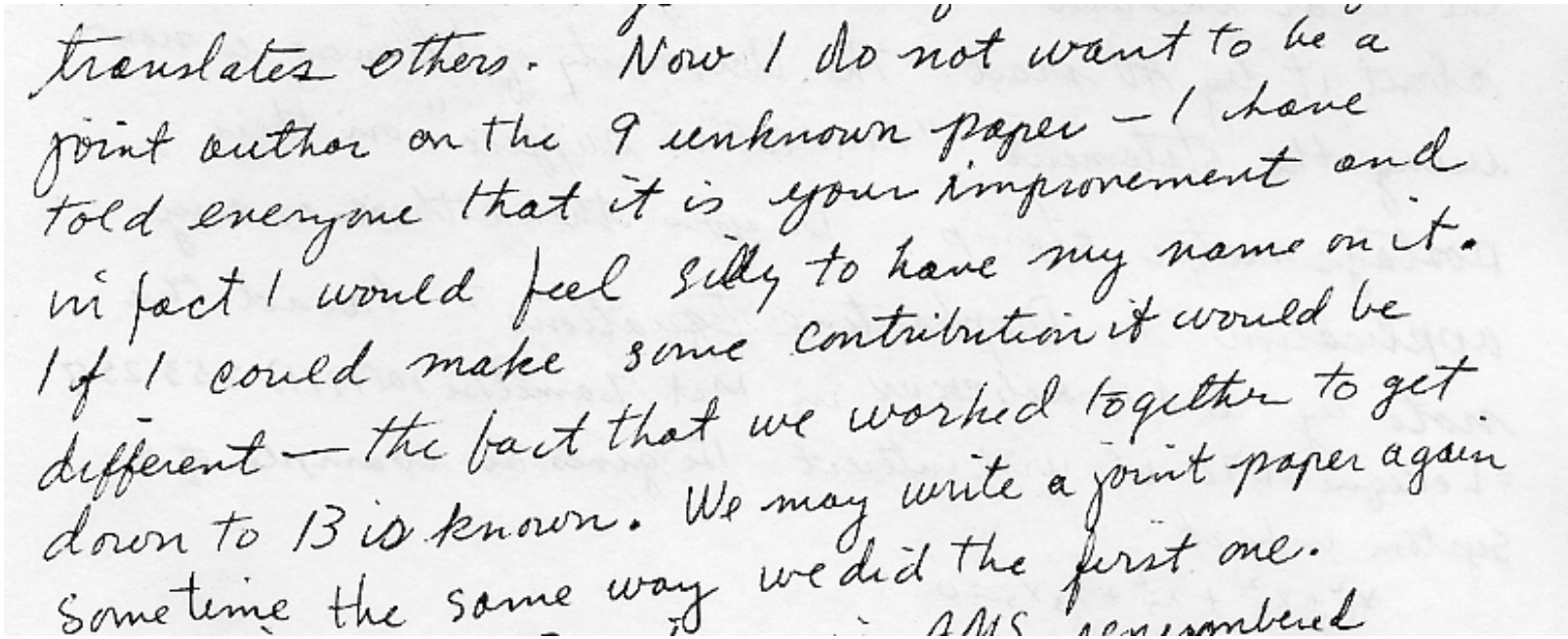
to hear of his passing. We got to know him some
when he was in Berkeley. Of course I will always
remember how in Stockholm in 1962 he came
up to me, introduced himself, and then said I
was the second most famous Robinson in the Soviet
Union right after Robinson Crusoe. It wasn't
true but it was very nice to hear him say so. He has
certainly built a great deal of mathematics during
his life and it will always last.

Лучший современный результат

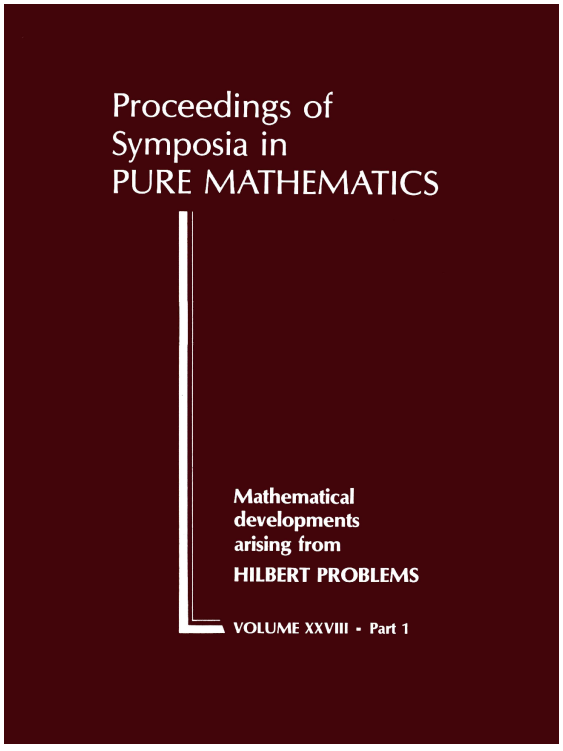
- $m = 9$

Лучший современный результат

- $m = 9$

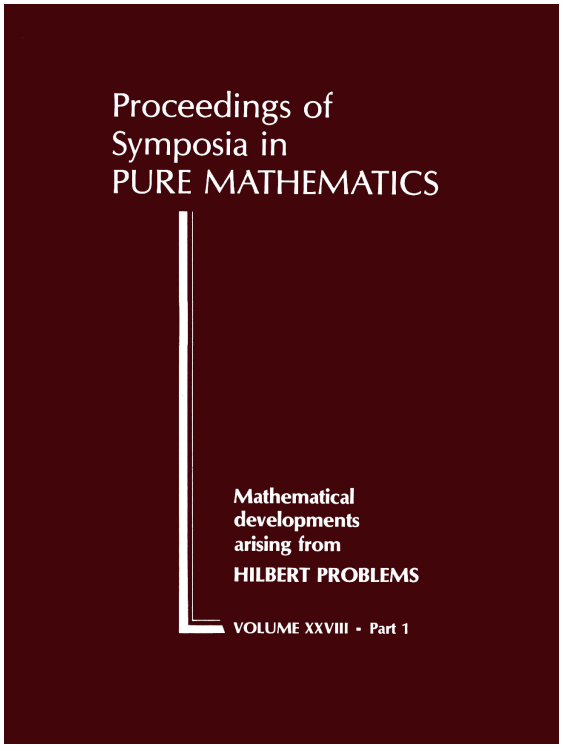

translates others. Now I do not want to be a
joint author on the 9 unknown paper — I have
told everyone that it is your improvement and
in fact I would feel silly to have my name on it.
If I could make some contribution it would be
different — the fact that we worked together to get
down to 13 is known. We may write a joint paper again
sometime the same way we did the first one.

AMS, DeKalb, Illinois, 1974



Mathematical developments arising from Hilbert problems

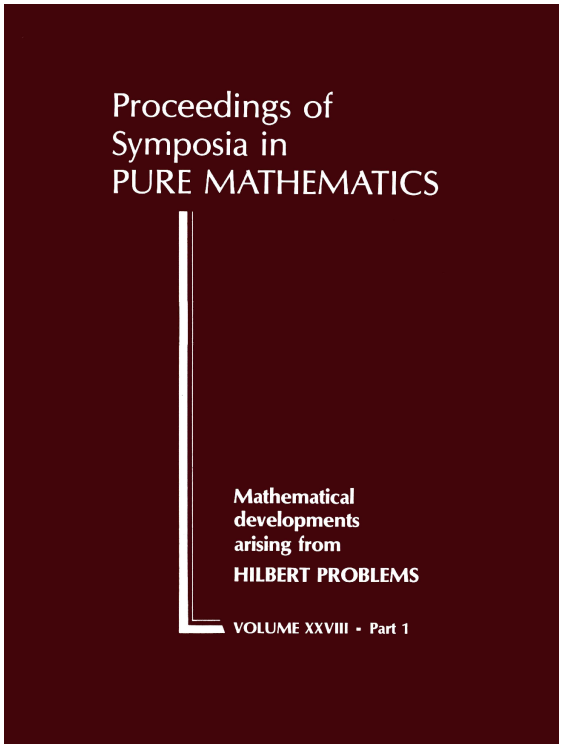
AMS, DeKalb, Illinois, 1974



Mathematical developments arising from Hilbert problems

Proceedings of Symposia in Pure Mathematics, v. 28, 1976

AMS, DeKalb, Illinois, 1974

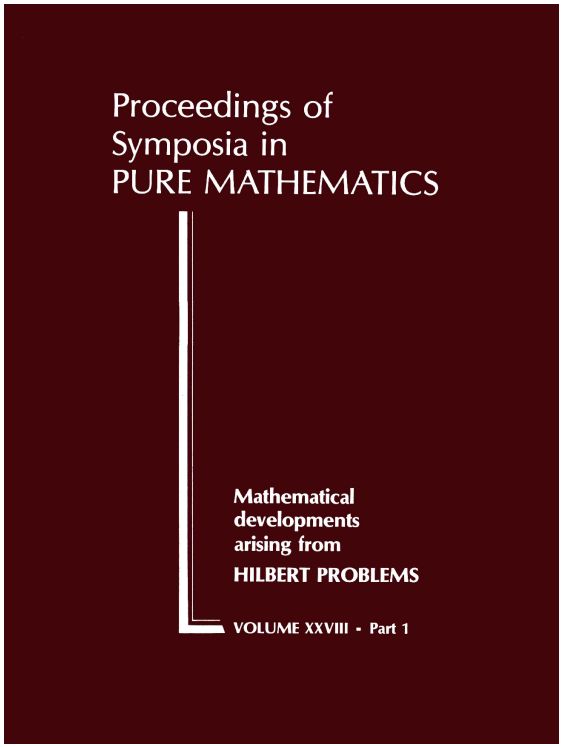


Mathematical developments arising from Hilbert problems

Proceedings of Symposia in Pure Mathematics, v. 28, 1976

Martin Davis, Yuri Matijasevič, and Julia Robinson

AMS, DeKalb, Illinois, 1974



Mathematical developments arising from Hilbert problems

Proceedings of Symposia in Pure Mathematics, v. 28, 1976

Martin Davis, Yuri Matijasevič, and Julia Robinson

Proceedings of Symposia in Pure Mathematics
Volume 28, 1976

HILBERT'S TENTH PROBLEM. DIOPHANTINE EQUATIONS: POSITIVE ASPECTS OF A NEGATIVE SOLUTION

Martin Davis[1], Yuri Matijasevič, and Julia Robinson

ABSTRACT

Applications (including the negative solution of Hilbert's tenth problem) and extensions are surveyed of the Main Theorem on Diophantine sets: Every listable (recursively enumerable) set is Diophantine. Key steps in the proof of the Main Theorem are outlined and applied to obtain prime representing polynomials, a universal Diophantine equation, and a sharp form of Gödel's incompleteness theorem. Many famous problems are reduced to the solvability of Diophantine equations. The number, size and effectiveness of solutions are discussed. Relationships are explored with the theory of algorithms (recursion theory), model theory, and algebraic number theory.

10-я и 8-я проблемы Гильберта

Гипотеза Riemann'a в оригинальной формулировке является утверждением о комплексных нулях дзета-функции Римана, определяемая при $\Re(z) > 1$ рядом

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}.$$

10-я и 8-я проблемы Гильберта

Гипотеза Riemann'a в оригинальной формулировке является утверждением о комплексных нулях дзета-функции Римана, определяемая при $\Re(z) > 1$ рядом

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}.$$

DPRM-теорема позволяет построить конкретное диофантово уравнение

$$R(x_1, \ldots, x_m) = 0$$

которое не имеет решений в если и только если гипотеза Riemann'a верна.

Назад к Диофанту

Поиск решений уравнения

$$M(\chi_1, \ldots, \chi_m) = 0$$

в рациональных числах $\chi_1, \ldots, \chi_m$ эквивалентен поиску решений уравнения

$$M\left(\frac{x_1 - y_1}{z+1}, \ldots, \frac{x_m - y_m}{z+1}\right) = 0$$

в натуральных числах $x_1, \ldots, x_m$, $y_1, \ldots, y_m$, z.

Назад к Диофанту

Поиск решений уравнения

$$M(\chi_1, \ldots, \chi_m) = 0$$

в рациональных числах $\chi_1, \ldots, \chi_m$ эквивалентен поиску решений уравнения

$$M\left(\frac{x_1 - y_1}{z+1}, \ldots, \frac{x_m - y_m}{z+1}\right) = 0$$

в натуральных числах $x_1, \ldots, x_m$, $y_1, \ldots, y_m$, z. В свою очередь это уравнение эквивалентно диофантову уравнению

$$(z+1)^d M\left(\frac{x_1 - y_1}{z+1}, \ldots, \frac{x_m - y_m}{z+1}\right) = 0,$$

где d – степень многочлена M.

Назад к Диофанту

Поиск решений уравнения

$$M(\chi_1, \ldots, \chi_m) = 0$$

в рациональных числах $\chi_1, \ldots, \chi_m$ эквивалентен поиску решений уравнения

$$M\left(\frac{x_1 - y_1}{z+1}, \ldots, \frac{x_m - y_m}{z+1}\right) = 0$$

в натуральных числах $x_1, \ldots, x_m$, $y_1, \ldots, y_m$, z. В свою очередь это уравнение эквивалентно диофантову уравнению

$$(z+1)^d M\left(\frac{x_1 - y_1}{z+1}, \ldots, \frac{x_m - y_m}{z+1}\right) = 0,$$

где d – степень многочлена M.

Таким образом, спрашивая *явно* только о методе для решения диофантовых уравнений в целых числах, Гильберт *неявно* спрашивал и о методе для решения диофантовых уравнений в рациональных числах.

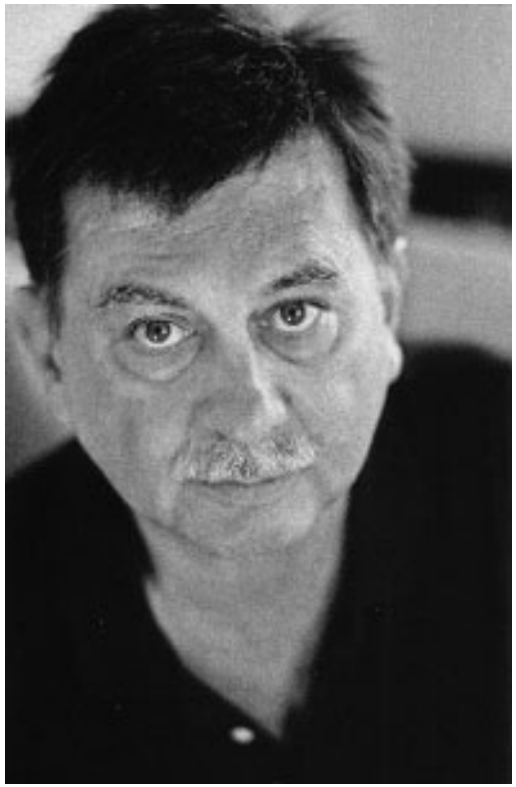
Компьютерная проверка DPRM-теоремы

Karol Pąk
The Matiyasevich Theorem. Preliminaries
Formalized Mathematics, 25(4):315–322, 2017.
Diophantine sets. Preliminaries
Formalized Mathematics, 26(1):81–90, 2018.

Benedikt Stock, Abhik Pal, Maria Antonia Oprea, Yufei Liu, Malte Sophian Hassler, Simon Dubischar, Prabhat Devkota, Yiping Deng, Marco David, Bogdan Ciurezu, Jonas Bayer and Deepak Aryal
Hilbert Meets Isabelle: Formalisation of the DPRM Theorem in Isabelle
EasyChair Preprint no. 152, May 22, 2018

Dominique Larchey-Wendling and Yannick Forster
Hilbert's Tenth Problem in Coq
4th International Conference on Formal Structures for Computation and Deduction (FSCD 2019)
Leibniz International Proceedings in Informatics, No.27, 2019

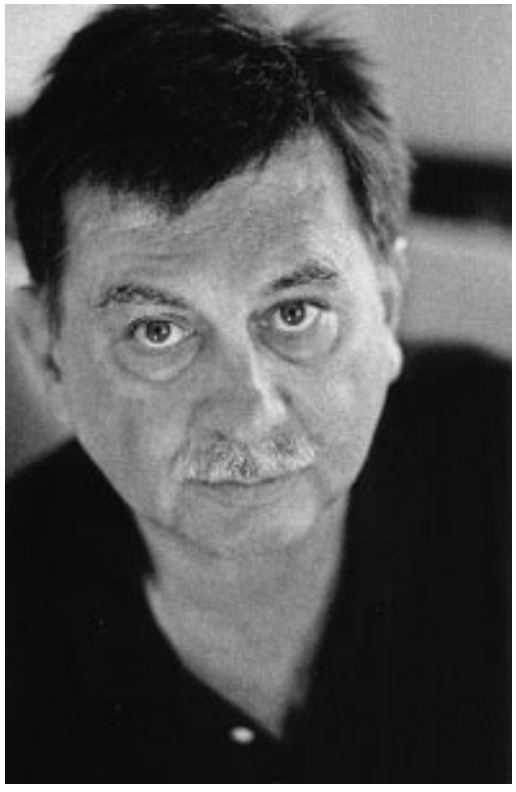
ZALA films



George Paul Csicsery
"a writer and independent filmmaker"

- Secrets of the Surface The Mathematical Vision of Maryam Mirzakhani (2020)
- Erdős 100 Plus (2018)
- Navajo Math Circles (2016)
- Counting from Infinity: Yitang Zhang and the Twin Prime Conjecture (2015)
- Erdős 100 (2013)
- Taking the Long View: The Life of Shiing-shen Chern (2011)
- I Want To Be a Mathematician: A Conversation With Paul Halmos (2009)
- Julia Robinson and Hilbert's Tenth Problem (2008)

ZALA films



George Paul Csicsery
"a writer and
independent filmmaker"

- Hard Problems: The Road To the World's Toughest Math Contest (2008)
- Porridge pulleys and Pi: two mathematical journeys (2004)
- Invitation to Discover (2002) (about MSRI)
- N is a Number: A Portrait of Paul Erdös (1993)
- To Prove and Conjecture: Excerpts from Three Lectures by Paul Erdös (1993)