Десятая проблема Гильберта

Решение и приложения в информатике

Ю. В. Матиясевич

Санкт-Петербургское отделение
Математического института им. В. А. Стеклова РАН

URL: http://logic.pdmi.ras.ru/~yumat

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*.

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

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

где M – многочлен с целыми коэффициентами.

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

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

где M – многочлен с целыми коэффициентами.

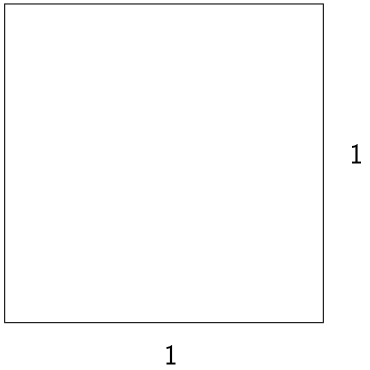
Греческий математик *Диофант* жил, скорее всего, в 3-ем веке нашей эры.

Полиномиальные уравнения у древних греков

$$x^2 = 2$$

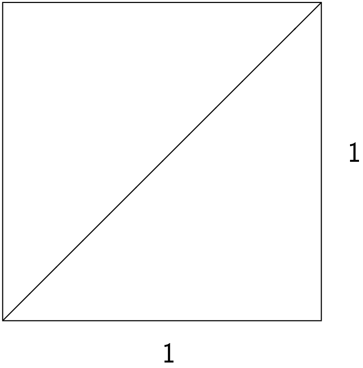
Полиномиальные уравнения у древних греков

$$x^2 = 2$$



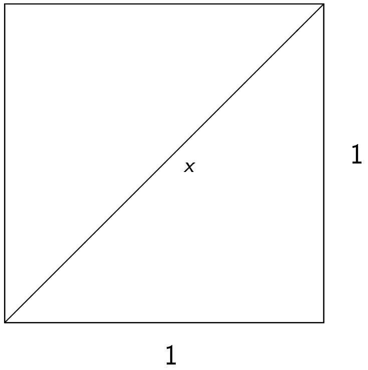
Полиномиальные уравнения у древних греков

$$x^2 = 2$$



Полиномиальные уравнения у древних греков

$$x^2 = 2$$



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.*

Целые рациональные числа что это такое?

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.*

Целые рациональные числа – это числа $0, \pm 1, \pm 2, \pm 3, \ldots$

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

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

где M – многочлен с целыми коэффициентами.

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

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

где M – многочлен с целыми коэффициентами.

Диофант искал решения в (положительных) рациональных числах

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

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

где M – многочлен с целыми коэффициентами.

Диофант искал решения в (положительных) рациональных числах

Гильберт спрашивал про решение диофантовых уравнений в целых числах

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

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

где M – многочлен с целыми коэффициентами.

Диофант искал решения в (положительных) рациональных числах

Гильберт спрашивал про решение диофантовых уравнений в целых числах

Можно также ограничиться только решениями в положительных целых числах или только в неотрицательных целых числах

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

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

где M – многочлен с целыми коэффициентами.

Диофант искал решения в (положительных) рациональных числах

Гильберт спрашивал про решение диофантовых уравнений в целых числах

Можно также ограничиться только решениями в положительных целых числах или только в неотрицательных целых числах

От Диофанта до Гильберта

Диофант жил – когда?

От Диофанта до Гильберта

Диофант жил, скорее всего, в 3-ем веке нашей эры.

От Диофанта до Гильберта

Диофант жил, скорее всего, в 3-ем веке нашей эры.

Гильберт сформулировал проблемы – когда?

От Диофанта до Гильберта

Диофант жил, скорее всего, в 3-ем веке нашей эры.

Гильберт сформулировал проблемы в 1900 году

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.

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.

Ответ

Сегодня мы знаем, что 10-я проблема Гильберта решения не имеет. Это означает, что она неразрешима как массовая проблема:

Ответ

Сегодня мы знаем, что 10-я проблема Гильберта решения не имеет. Это означает, что она неразрешима как массовая проблема:

Теорема (Неразрешимость 10-й проблемы Гильберта) *Не существует алгоритма, который по узнавал бы по произвольному диофантову уравнению, имеет ли оно решения.*

Ответ

Сегодня мы знаем, что 10-я проблема Гильберта решения не имеет. Это означает, что она неразрешима как массовая проблема:

Теорема (Неразрешимость 10-й проблемы Гильберта) *Не существует алгоритма, который по узнавал бы по произвольному диофантову уравнению, имеет ли оно решения.*

В этом смысле говорят об *отрицательном решении* 10-й проблемы Гильберта.

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.

Первая неразрешимая массовая проблема в чистой математике

А. А. Марков (сын)
1903–1979

Emil L. Post
1897–1954

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.

Hilbert's 10th problem "begs for an unsolvability proof"

EMIL L. POST
1897–1954

Хронология

Хронология

- Начало 50-х годов: гипотеза, которую выдвинул Martin Davis.

Хронология

- Начало 50-х годов: гипотеза, которую выдвинул Martin Davis.
- Начало 60-х годов: частичный прогресс, который достигли Martin Davis, Hilary Putnam и Julia Robinson.

Хронология

- Начало 50-х годов: гипотеза, которую выдвинул Martin Davis.
- Начало 60-х годов: частичный прогресс, который достигли Martin Davis, Hilary Putnam и Julia Robinson.
- 1970 год: последний шаг сделал Ю.Матиясевич.

An e-mail

An e-mail

```
Dear Professor,

you are wrong.  I am a brilliant young programmer and
last night I wrote a sophisticated program in Java##.
My program solves Hilbert's tenth problem in the
__positive__ sense.  Namely, for every Diophantine
equation given as input, the program will print 1 or 0
depending on whether the equation has a solution or
not.

The attachment contains my ingenious program.  You can
run it on your favorite Diophantine equations and see
how fast my program works.

Have a fun, Professor!
```

Точка зрения студента

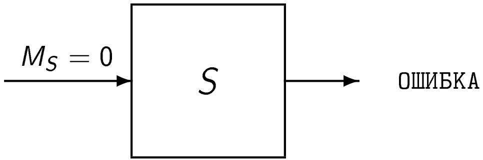
Для любого многочлена M:

$$\xrightarrow{M=0} \boxed{\;S\;} \longrightarrow \begin{cases} 1, & \text{если существует хотя бы одно решение} \\ 0, & \text{если решений вообще не существует} \end{cases}$$

Точка зрения профессора:

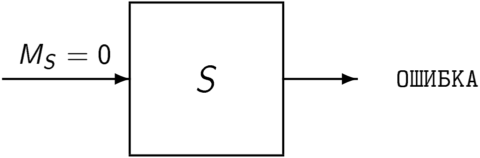
Точка зрения профессора:

Существует многочлен M_S такой, что



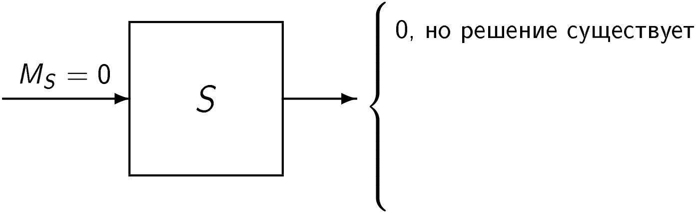
Точка зрения профессора:

Существует многочлен M_S такой, что



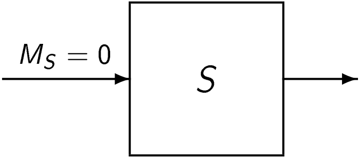
Точка зрения профессора:

Существует многочлен M_S такой, что



Точка зрения профессора:

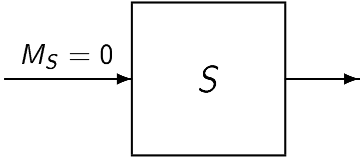
Существует многочлен M_S такой, что



$$\begin{cases} 0, \text{ но решение существует} \\ 1, \text{ но решений не существует} \\ \\ \\ \end{cases}$$

Точка зрения профессора:

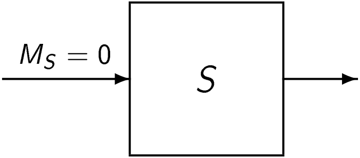
Существует многочлен M_S такой, что



$$\begin{cases} 0, \text{ но решение существует} \\ 1, \text{ но решений не существует} \\ \texttt{ДРУГОЙ ОТВЕТ} \\ \\ \end{cases}$$

Точка зрения профессора:

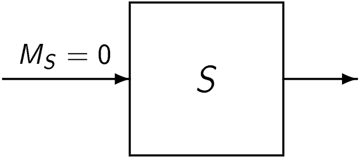
Существует многочлен M_S такой, что



- 0, но решение существует
- 1, но решений не существует
- `ДРУГОЙ ОТВЕТ`
- остановка без ответа

Точка зрения профессора:

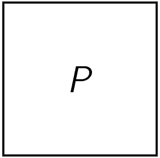
Существует многочлен M_S такой, что



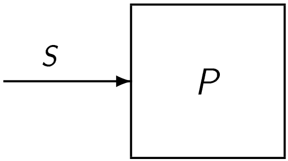
- 0, но решение существует
- 1, но решений не существует
- `ДРУГОЙ ОТВЕТ`
- остановка без ответа
- не останавливается
  и ничего не печатает

Программа профессора

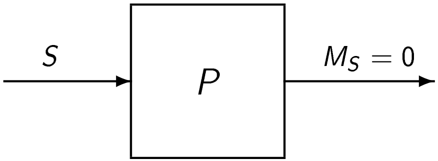
Программа профессора



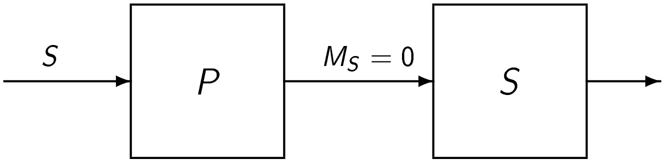
Программа профессора



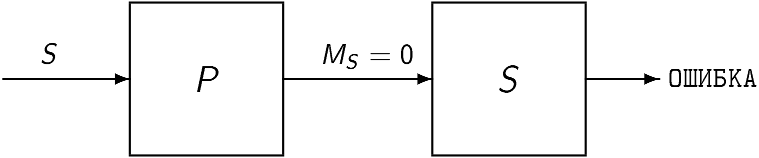
Программа профессора



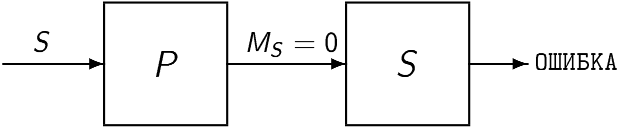
Программа профессора



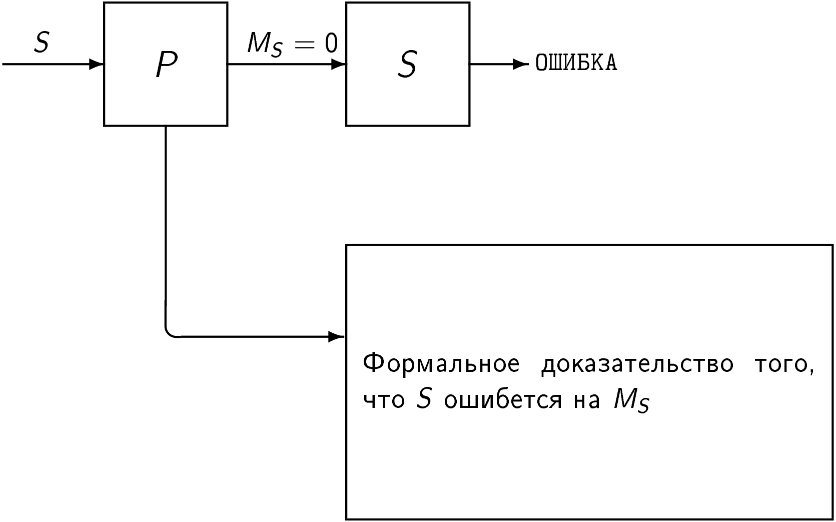
Программа профессора



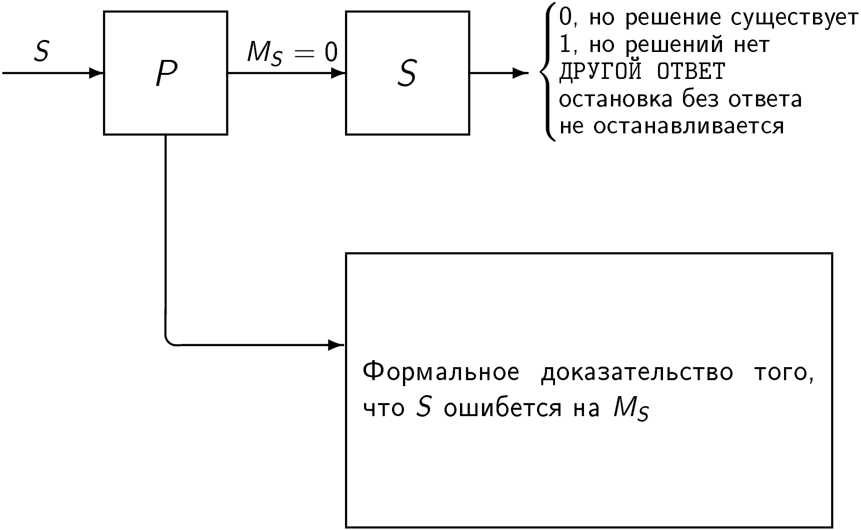
Усовершенствованная программа профессора



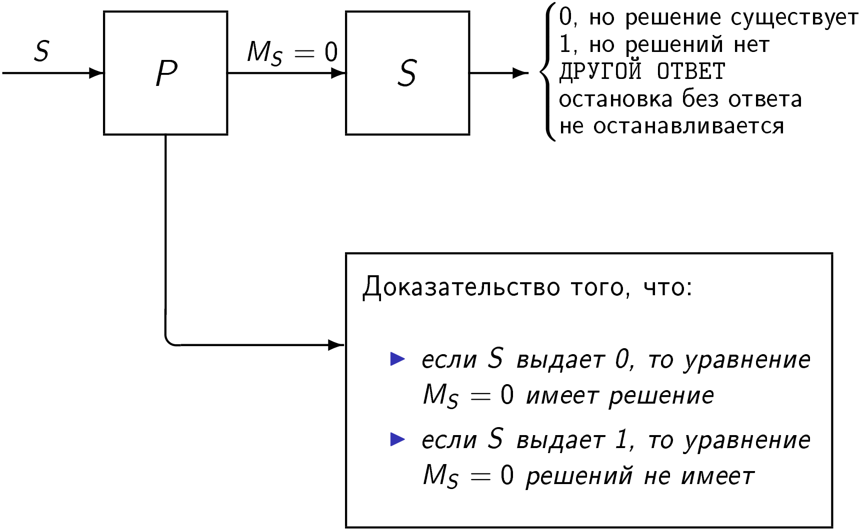
Усовершенствованная программа профессора



Усовершенствованная программа профессора



Усовершенствованная программа профессора



Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

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

где M – многочлен с целыми коэффициентами.

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

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

где M – многочлен с целыми коэффициентами.

Диофант искал решения в (положительных) рациональных числах

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

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

где M – многочлен с целыми коэффициентами.

Диофант искал решения в (положительных) рациональных числах

Гильберт спрашивал про решение диофантовых уравнений в целых числах

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

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

где M – многочлен с целыми коэффициентами.

Диофант искал решения в (положительных) рациональных числах

Гильберт спрашивал про решение диофантовых уравнений в целых числах

Можно также ограничиться только решениями в положительных целых числах или только в неотрицательных целых числах

Диофантовы уравнения

Определение. *Диофантово уравнение* имеет вид

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

где M – многочлен с целыми коэффициентами.

Диофант искал решения в (положительных) рациональных числах

Гильберт спрашивал про решение диофантовых уравнений в целых числах

Можно также ограничиться только решениями в положительных целых числах или только в неотрицательных целых числах

Натуральные числа против целых

$$(x+1)^3 + (y+1)^3 = (z+1)^3$$

Натуральные числа против целых

$$(x+1)^3 + (y+1)^3 = (z+1)^3$$

Имеет ли это уравнение решение в целых числах?

Натуральные числа против целых

$$(x+1)^3 + (y+1)^3 = (z+1)^3$$

Имеет ли это уравнение решение в целых числах?

Да, и это тривиально: $y = -1, \quad z = x.$

Натуральные числа против целых

$$(x+1)^3 + (y+1)^3 = (z+1)^3$$

Имеет ли это уравнение решение в целых числах?
Да, и это тривиально: $y = -1, \quad z = x.$

Имеет ли это уравнение решение в неотрицательных целых числах?

Натуральные числа против целых

$$(x+1)^3 + (y+1)^3 = (z+1)^3$$

Имеет ли это уравнение решение в целых числах?
Да, и это тривиально: $y = -1, \quad z = x$.

Имеет ли это уравнение решение в неотрицательных целых числах?
Нет, не имеет, но это нетривиально (частный случай Великой теоремы Ферма).

От целых чисел к натуральным

Диофантово уравнение

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

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

$$P(p_1 - q_1, \ldots, p_m - q_m) = 0.$$

имеет решение в натуральных числах $p_1, \ldots, p_m$, $q_1, \ldots, q_m$.

От целых чисел к натуральным

Диофантово уравнение

$$P(x_1, \dots, x_m) = 0$$

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

$$P(p_1 - q_1, \dots, p_m - q_m) = 0.$$

имеет решение в натуральных числах $p_1, \dots, p_m$, $q_1, \dots, q_m$.

Говорят, что массовая проблема распознавания разрешимости диофантовых уравнений в целых числах *сводится* к массовой проблеме распознавания разрешимости диофантовых уравнений в натуральных числах.

От натуральных чисел к целым

Диофантово уравнение

$$P(p_1, \ldots, p_m) = 0$$

имеет решение в натуральных числах тогда и только тогда, когда диофантово уравнение

$$P(w_1^2 + x_1^2 + y_1^2 + z_1^2, \ldots, w_m^2 + x_m^2 + y_m^2 + z_m^2) = 0.$$

имеет решение в целых числах.

От натуральных чисел к целым

Диофантово уравнение

$$P(p_1, \ldots, p_m) = 0$$

имеет решение в натуральных числах тогда и только тогда, когда диофантово уравнение

$$P(w_1^2 + x_1^2 + y_1^2 + z_1^2, \ldots, w_m^2 + x_m^2 + y_m^2 + z_m^2) = 0.$$

имеет решение в целых числах.

Теорема (Joseph-Louis Lagrange [1770], знал и Pierre Fermat, но не опубликовал) *Каждое натуральное число является суммой четырех квадратов.*

От натуральных чисел к целым

Диофантово уравнение

$$P(p_1, \dots, p_m) = 0$$

имеет решение в натуральных числах тогда и только тогда, когда диофантово уравнение

$$P(w_1^2 + x_1^2 + y_1^2 + z_1^2, \dots, w_m^2 + x_m^2 + y_m^2 + z_m^2) = 0.$$

имеет решение в целых числах.

Теорема (Joseph-Louis Lagrange [1770], знал и Pierre Fermat, но не опубликовал) *Каждое натуральное число является суммой четырех квадратов.*

Таким образом, массовая проблема распознавания разрешимости диофантовых уравнений в натуральных целых числах *сводится к* массовой проблеме распознавания разрешимости диофантовых уравнений в целых 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*.

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

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

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

- *параметры* $a_1, \dots, a_n$;

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 $\mathfrak{M}$ такое, что

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

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 $\mathfrak{M}$ такое, что

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

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* нестепеней *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* нестепеней *числа* 2, представлено уравнением
$$a - (2x_1 + 3)x_2 = 0$$

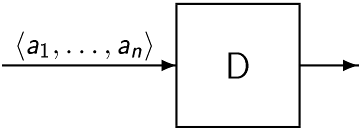
Программа Диофанта

Программа Диофанта

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

Программа Диофанта

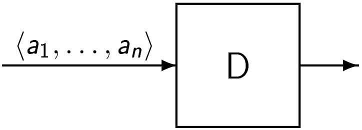
$$\langle a_1, \dots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow \exists x_1 \dots x_m \{ P(a_1, \dots, a_n, x_1, \dots, x_m) = 0 \}$$



$$\begin{cases} \text{остановка, если } \langle a_1, \dots, a_n \rangle \in \mathfrak{M} \\ \text{вечная работа в противном случае} \end{cases}$$

Программа Диофанта

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



$$\begin{cases} \text{остановка, если } \langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \\ \text{вечная работа в противном случае} \end{cases}$$

```
for (y=0;;y++)
  for (x1=0;x1<y;x1++)
   ........................
    for (xm=0;xm<y;xm++)
     if (P(a1,...,an,x1,...,xm)=0) STOP
```

Перечислимые множества

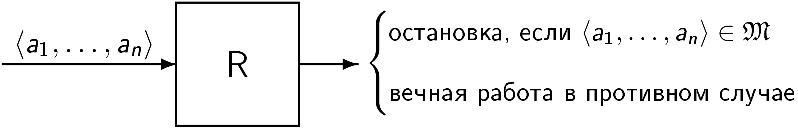
Перечислимые множества

Определение. Множество $\mathfrak{M}$, состоящее из n-ок натуральных чисел называется *перечислимым*, если можно написать программу R, такую что

$$\xrightarrow{\langle a_1, \ldots, a_n \rangle} \boxed{\mathrm{R}} \longrightarrow \begin{cases} \text{остановка, если } \langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \\ \text{вечная работа в противном случае} \end{cases}$$

Перечислимые множества

Определение. Множество $\mathfrak{M}$, состоящее из n-ок натуральных чисел называется *перечислимым*, если можно написать программу R, такую что



Эквивалентное определение. Множество $\mathfrak{M}$, состоящее из n-ок натуральных чисел называется *перечислимым*, если можно написать программу P которая (работая бесконечно долго) будет печатать только элементы множества $\mathfrak{M}$ и напечатает каждое из них, быть может, много раз.

Вторая программа Диофанта

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

Вторая программа Диофанта

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

```
for (y=0;;y++)
  for (a1=0;a1<y;a1++)
   .......................
    for (an=0;an<y;an++)
     for (x1=0;x1<y;x1++)
      ........................
       for (xm=0;xm<y;xm++)
        if (P(a1,...,an,x1,...,xm)=0)
          print(a1,...,an)
```

Пример

$$P(a_1, x_1, x_2) = a_1 - (x_1 + 2)(x_2 + 2)$$

Пример

$$P(a_1, x_1, x_2) = a_1 - (x_1 + 2)(x_2 + 2)$$

```
for y do
  for a1 to y do
    for x1 to y do
      for x2 to y do
        if a1 - (x1 + 2)*(x2 + 2)=0 then
          print(a1) fi
od od od od
```

Пример

$$P(a_1, x_1, x_2) = a_1 - (x_1 + 2)(x_2 + 2)$$

```
for y do
  for a1 to y do
    for x1 to y do
      for x2 to y do
        if a1 - (x1 + 2)*(x2 + 2)=0 then
          print(a1) fi
od od od od
```

4, 4, 4, 6, 6, 4, 6, 6, 4, 6, 6, 8, 8, 4, 6, 6, 8, 8, 9, 4, 6, 6, 8, 8, 9, 10, 10, 4, 6, 6, 8, 8, 9, 10, 10, 4, 6, 6, 8, 8, 9, 10, 10, 12, 12, 12, 12, 4, 6, 6,...

Гипотеза Martin'a Davis'a

Гипотеза Martin'a Davis'a

Тривиальный факт. *Каждое диофантово множество является перечислимым.*

Гипотеза Martin'a Davis'a

Тривиальный факт. *Каждое диофантово множество является перечислимым.*

Гипотеза M. Davis'a (начало 50-х). *Каждое перечислимое множество является диофантовым.*

Гипотеза Martin'a Davis'a

Тривиальный факт. *Каждое диофантово множество является перечислимым.*

Гипотеза M. Davis'a (начало 50-х). *Каждое перечислимое множество является диофантовым.*

Гипотеза M. Davis'a была доказана в 1970 году.

DPRM-теорема. Понятия *перечислимое множество* и *диофантово множество* совпадают.

Davis-Putnam-Robinson-Матиясевич

Перечисление диофантовых уравнений

$$M_1(a, \bar{x}) = 0, \qquad \ldots, \qquad M_k(a, \bar{x}) = 0, \qquad \ldots$$

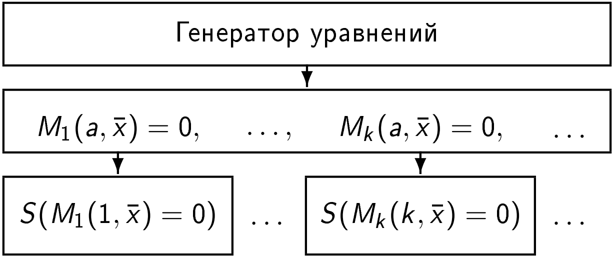
Программа профессора

Генератор уравнений

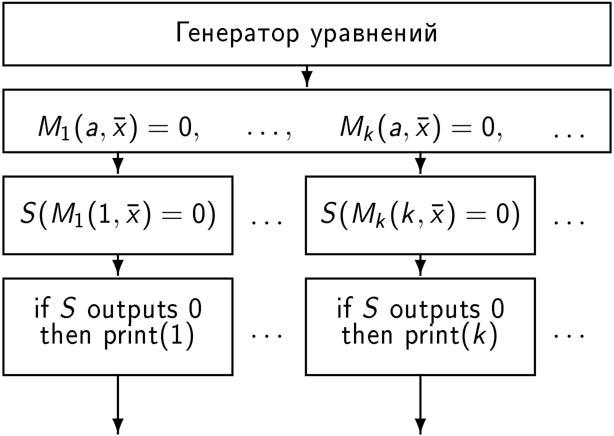
$$\downarrow$$

$$M_1(a,\bar{x})=0, \quad \ldots, \quad M_k(a,\bar{x})=0, \quad \ldots$$

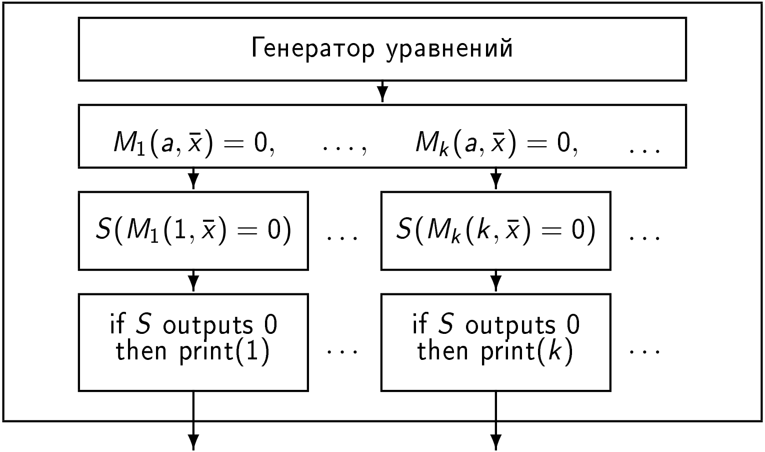
Программа профессора



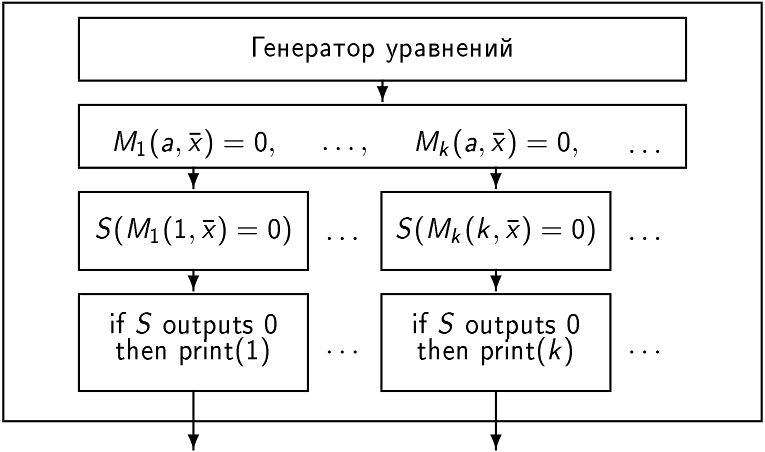
Программа профессора



Программа профессора

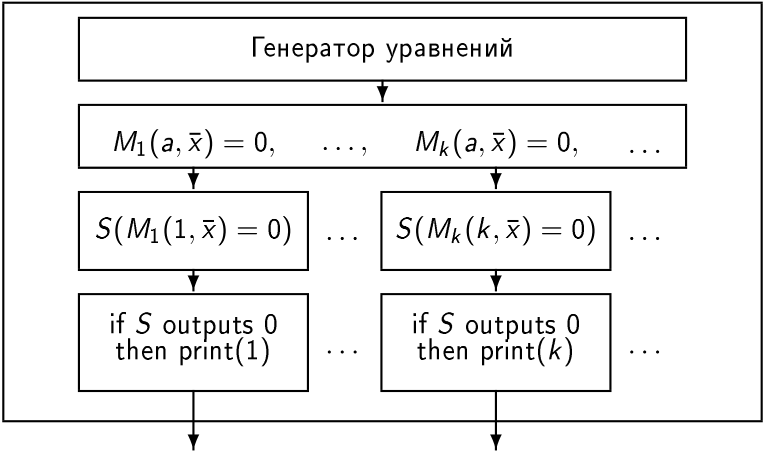


Программа профессора



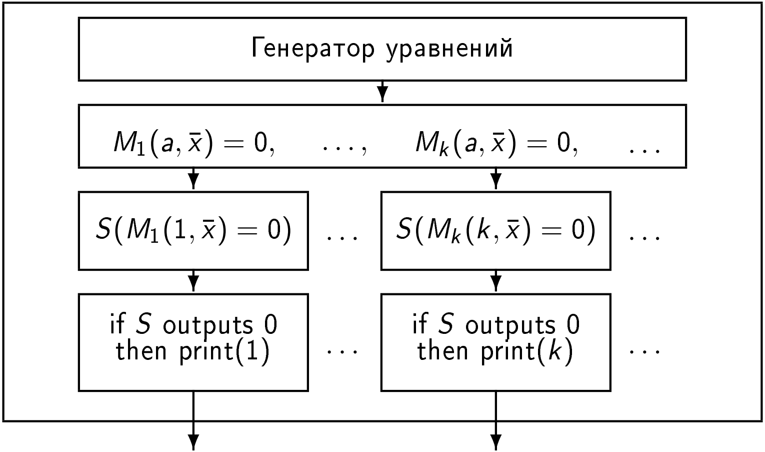
$$S(M_k(k, \bar{x}) = 0) = 0 \;\Leftrightarrow\; k \in \mathfrak{M}_S$$

Программа профессора



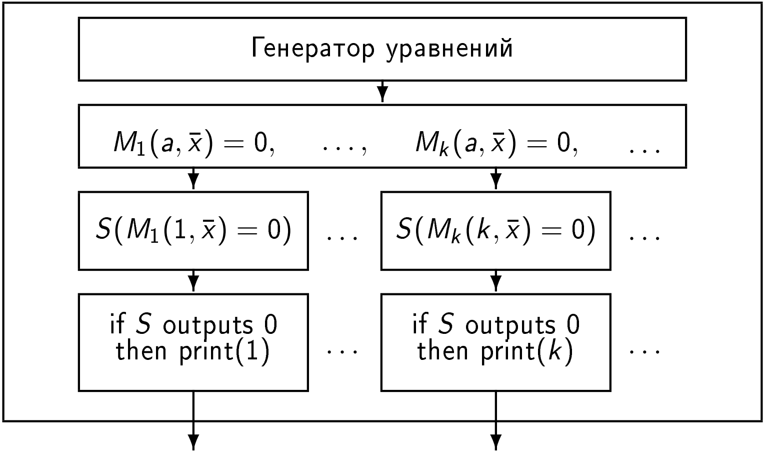
$$S(M_k(k, \bar{x}) = 0) = 0 \;\Leftrightarrow\; k \in \mathfrak{M}_S$$

Программа профессора



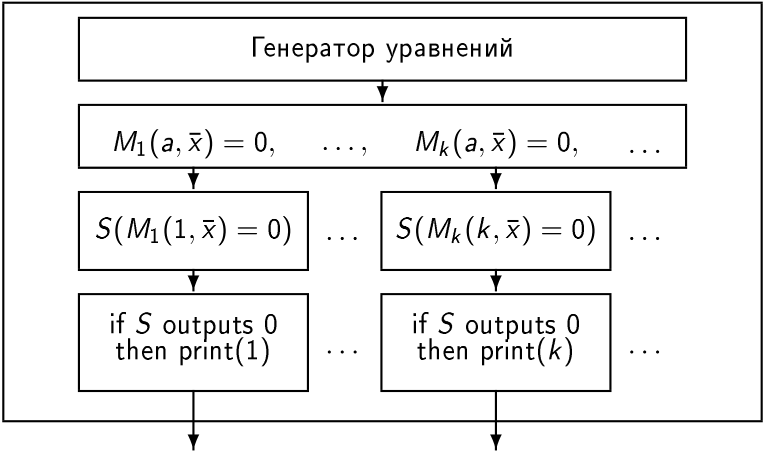
$$S(M_k(k, \bar{x}) = 0) = 0 \;\Leftrightarrow\; k \in \mathfrak{M}_S \;\Leftrightarrow\; \exists \bar{x} \{ M_S(k, \bar{x}) = 0 \}$$

Программа профессора



$$S(M_k(k,\bar{x})=0)=0 \;\Leftrightarrow\; k\in\mathfrak{M}_S \;\Leftrightarrow\; \exists\bar{x}\{M_{k_S}(k,\bar{x})=0\}$$

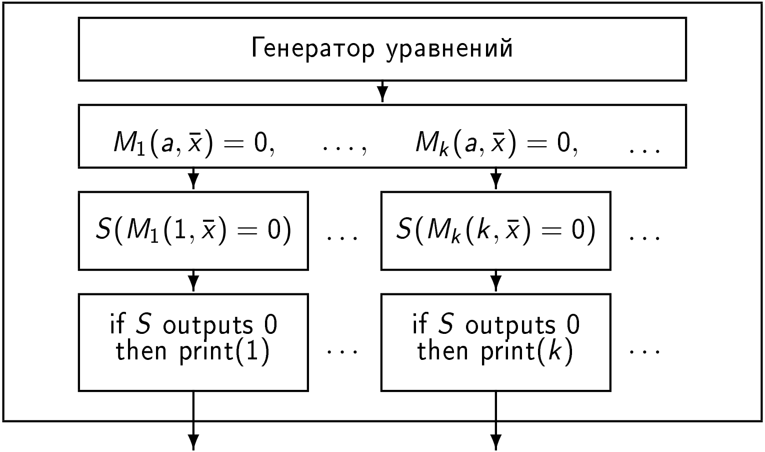
Программа профессора



$$S(M_k(k,\bar{x})=0)=0 \;\Leftrightarrow\; k\in\mathfrak{M}_S \;\Leftrightarrow\; \exists\bar{x}\{M_{k_S}(k,\bar{x})=0\}$$

$$S(M_{k_S}(k_S,\bar{x})=0)$$

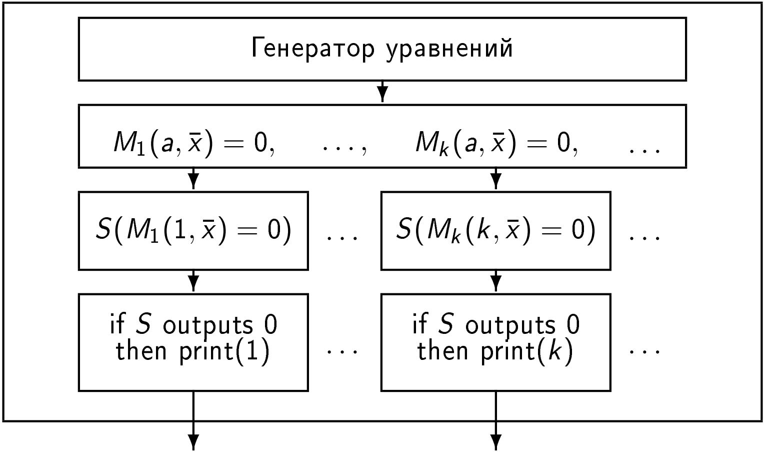
Программа профессора



$$S(M_k(k,\bar{x}) = 0) = 0 \;\Leftrightarrow\; k \in \mathfrak{M}_S \;\Leftrightarrow\; \exists \bar{x}\{M_{k_S}(k,\bar{x}) = 0\}$$

$$S(M_{k_S}(k_S,\bar{x}) = 0) =?$$

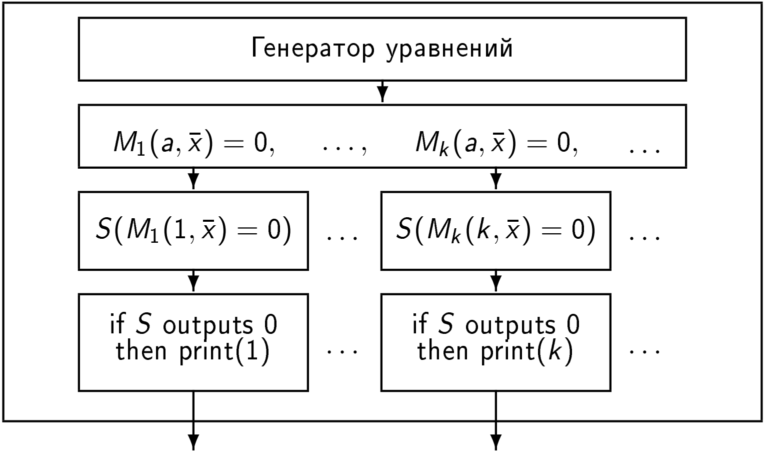
Программа профессора



$$S(M_k(k, \bar{x}) = 0) = 0 \;\Leftrightarrow\; k \in \mathfrak{M}_S \;\Leftrightarrow\; \exists \bar{x} \{ M_{k_S}(k, \bar{x}) = 0 \}$$

$$S(M_{k_S}(k_S, \bar{x}) = 0) = 0$$

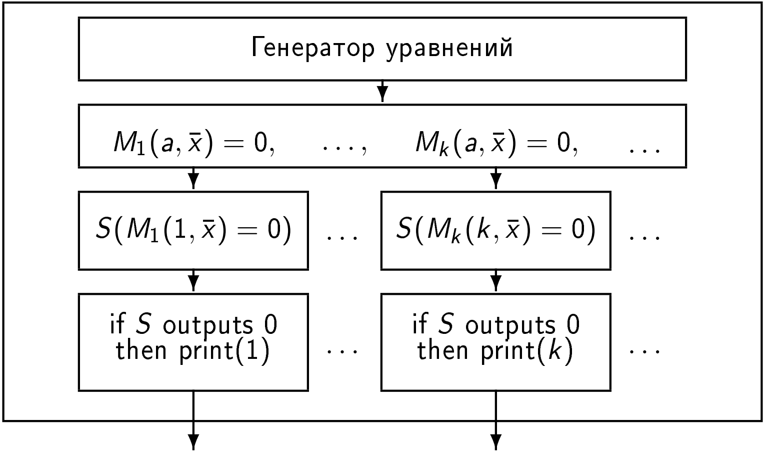
Программа профессора



$$S(M_k(k,\bar{x}) = 0) = 0 \;\Leftrightarrow\; k \in \mathfrak{M}_S \;\Leftrightarrow\; \exists \bar{x}\{M_{k_S}(k,\bar{x}) = 0\}$$

$$S(M_{k_S}(k_S,\bar{x}) = 0) = 0 \;\Rightarrow\; k_S \in \mathfrak{M}_S$$

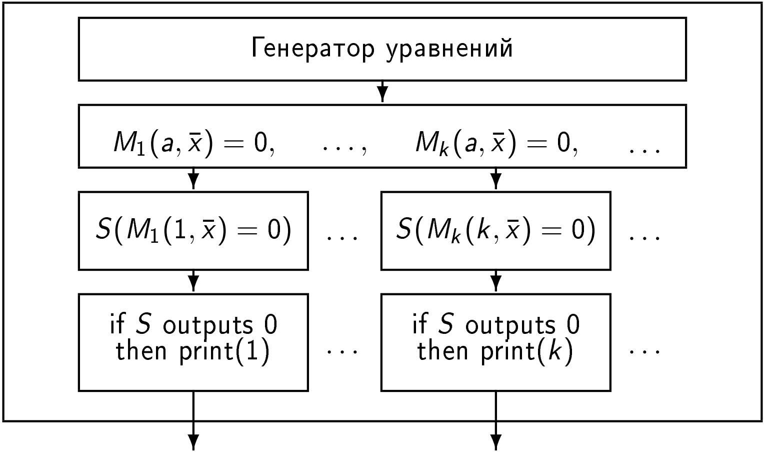
Программа профессора



$$S(M_k(k,\bar{x}) = 0) = 0 \;\Leftrightarrow\; k \in \mathfrak{M}_S \;\Leftrightarrow\; \exists \bar{x}\{M_{k_S}(k,\bar{x}) = 0\}$$

$$S(M_{k_S}(k_S,\bar{x}) = 0) = 0 \;\Rightarrow\; k_S \in \mathfrak{M}_S \;\Rightarrow\; \exists \bar{x}\{M_{k_S}(k_S,\bar{x}) = 0\}$$

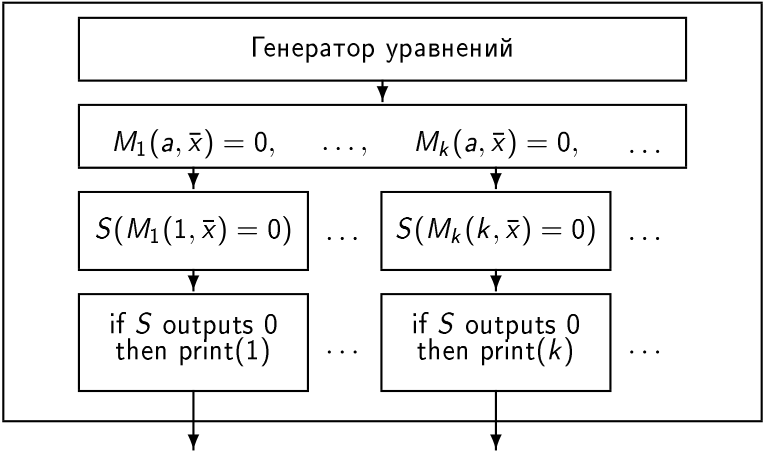
Программа профессора



$$S(M_k(k, \bar{x}) = 0) = 0 \;\Leftrightarrow\; k \in \mathfrak{M}_S \;\Leftrightarrow\; \exists \bar{x}\{M_{k_S}(k, \bar{x}) = 0\}$$

$$S(M_{k_S}(k_S, \bar{x}) = 0) = 1$$

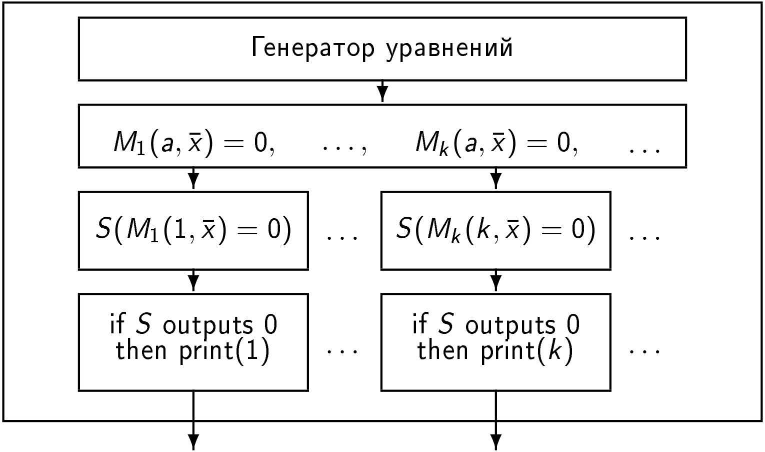
Программа профессора



$$S(M_k(k,\bar{x}) = 0) = 0 \;\Leftrightarrow\; k \in \mathfrak{M}_S \;\Leftrightarrow\; \exists \bar{x}\{M_{k_S}(k,\bar{x}) = 0\}$$

$$S(M_{k_S}(k_S,\bar{x}) = 0) = 1 \;\Rightarrow\; k_S \notin \mathfrak{M}_S$$

Программа профессора



$$S(M_k(k,\bar{x}) = 0) = 0 \;\Leftrightarrow\; k \in \mathfrak{M}_S \;\Leftrightarrow\; \exists \bar{x}\{M_{k_S}(k,\bar{x}) = 0\}$$

$$S(M_{k_S}(k_S,\bar{x}) = 0) = 1 \;\Rightarrow\; k_S \notin \mathfrak{M}_S \;\Rightarrow\; \neg\exists \bar{x}\{M_{k_S}(k_S,\bar{x}) = 0\}$$

Универсальное уравнение

Универсальное уравнение

Список всех однопараметрических уравнений:

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

Универсальное уравнение

Список всех однопараметрических уравнений:

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

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

Универсальное уравнение

Список всех однопараметрических уравнений:

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

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

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

Универсальное уравнение

Список всех однопараметрических уравнений:

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

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

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

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

Текущие рекорды

Задача о решении произвольного параметрического диофантова уравнения может быть сведена к решению эквивалентного диофантова уравнения, имеющего степень D и N неизвестных, где в качестве $\langle D, N \rangle$ можно взять любую из следующих пар:

$$\langle 4, 58\rangle,\ \langle 8, 38\rangle,\ \langle 12, 32\rangle,\ \langle 16, 29\rangle, \langle 20, 28\rangle,\ \langle 24, 26\rangle,\ \langle 28, 25\rangle,\ \langle 36, 24\rangle,$$
$$\langle 96, 21\rangle,\ \langle 2668, 19\rangle,\ \langle 2\times 10^5, 14\rangle, \langle 6.6\times 10^{43},\ 13\rangle,\ \langle 1.3\times 10^{44}, 12\rangle,$$
$$\langle 4.6\times 10^{44}, 11\rangle,\ \langle 8.6\times 10^{44}, 10\rangle,\ \langle 1.6\times 10^{45}, 9\rangle.$$

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

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

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

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.

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.