

HILBERT'S TENTH PROBLEM:
WHAT WAS DONE AND WHAT IS TO BE DONE

YURI MATIYASEVICH

Steklov Institute of Mathematics at St.Petersburg, Russia

[http://logic.pdmi.ras.ru/~yumat/Journal/H10history/
H10histe.{ps,pdf}](http://logic.pdmi.ras.ru/~yumat/Journal/H10history/H10histe.{ps,pdf})

Hilbert's Tenth Problem

Range of Unknowns

10. Determination of the Solvability of a Diophantine Equation.

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in **rational integers**.*

Rational integers are nothing else but numbers $0, \pm 1, \pm 2, \dots$ which will be called during my talk just **integers**.

In today's terminology Hilbert's 10th problem is a *decision problem*, i.e. a problem consisting of infinitely many individual questions each of which requires an answer YES or NO.

Hilbert's Tenth Problem

Range of Unknowns

An equation

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

has a solution in integers x_1, \dots, x_m if and only if equation

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

has a solution in natural numbers $p_1, \dots, p_m, q_1, \dots, q_m$.

So one says that the decision problem of recognizing solvability of Diophantine equations in integers *reduces* to the decision problem of recognizing the solvability of Diophantine equations in natural numbers.

Hilbert's Tenth Problem

Range of Unknowns

An equation

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

has a solution in natural numbers if and only if equation

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

has a solution in integers because by Lagrange's theorem every natural number is the sum of four squares.

The decision problem of recognizing solvability of Diophantine equations in integers is *equivalent* to the decision problem of recognizing solvability of Diophantine equations in natural numbers.

We will deal with solving Diophantine equations in natural numbers so all lower-case italic letters will range over $0, 1, 2, \dots$

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

Parametric Equations

Diophantine Sets

A *family* of Diophantine equations:

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

where P is a polynomial with integer coefficients, the variables of which are split into two groups:

- ▶ the *parameters* a_1, \dots, a_n ;
- ▶ the *unknowns* x_1, \dots, x_m .

Consider the set \mathfrak{M} such that

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

Sets having such *representations* are called *Diophantine*.

Examples

Some easy examples of Diophantine sets:

- ▶ *the set of all squares*, represented by equation

$$a - x^2 = 0;$$

- ▶ *the set of all composite numbers*, represented by equation

$$a - (x_1 + 2)(x_2 + 2) = 0;$$

- ▶ *the set of all positive integers which are not powers of 2*, represented by equation

$$a - (2x_1 + 3)(x_2 + 1) = 0.$$

Listable Sets

Given a parametric Diophantine equation

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

we can effectively list all n -tuples from the Diophantine set \mathfrak{M} represented by this equation. Namely, we need only to look over, in some order, all $(n + m)$ -tuples of possible values of all variables $a_1, \dots, a_n, x_1, \dots, x_m$ and check every time whether the equality holds or not. As soon as it does, we put the tuple $\langle a_1, \dots, a_n \rangle$ on the list of elements of \mathfrak{M} . In this way every tuple from \mathfrak{M} will sooner or later appear on the list, maybe many times.

Definition A set \mathfrak{M} of n -tuples of natural numbers is called *listable* or *effectively enumerable*, if there is an algorithm which would print in some order, possibly with repetitions, all elements of the set \mathfrak{M} .

From Evident to Unbelievable

Evident fact. Every Diophantine set is effectively enumerable.

Martin Davis' Conjecture. Every effectively enumerable set is Diophantine.

Corollary of Davis' Conjecture *There is a polynomial Q such that the equation*

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

has a solution if and only if a is a prime number.

Corollary of Davis' Conjecture *There is a polynomial P such that the equation*

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

has a solution if and only if a is a prime number.

Listing Listable Sets

A list of all listable sets:

$$\mathfrak{M}_0, \mathfrak{M}_1, \dots, \mathfrak{M}_k, \dots$$

Formally, for every n there exists a listable set \mathfrak{U}_n of $(n + 1)$ -tuples such that

$$\langle a_1, \dots, a_n \rangle \in \mathfrak{M}_k \iff \langle a_1, \dots, a_n, k \rangle \in \mathfrak{U}_n.$$

Being listable, \mathfrak{U}_n has a Diophantine representation:

$$\langle a_1, \dots, a_n, a_{n+1} \rangle \in \mathfrak{U}_n \iff \\ \exists y_1 \dots y_M \{ U_n(a_1, \dots, a_n, a_{n+1}, y_1, \dots, y_M) = 0 \}.$$

Universal Equations

Collapse of Diophantine Hierarchy

Corollary of Martin Davis Conjecture *For every n there exist an equation*

$$U_n(a_1, \dots, a_n, k, y_1, \dots, y_M) = 0 \quad (1)$$

which is universal in the following sense: For every Diophantine equation

$$P(a_1, \dots, a_n, x_1, \dots, x_m) = 0 \quad (2)$$

one can effectively find a particular number k_P such that, for given value of the parameters a_1, \dots, a_n , equation (2) has a solution in x_1, \dots, x_m if and only if equation

$$U_n(a_1, \dots, a_n, k_P, y_1, \dots, y_M) = 0$$

has a solution in y_1, \dots, y_M .

First Step

Theorem (Martin Davis [1950]) *Every listable set \mathfrak{M} has a representation of the form*

$$\langle a_1, \dots, a_n \rangle \in \mathfrak{M} \iff \\ \exists z \forall y \leq z \exists x_1 \dots x_m \{ P(a_1, \dots, a_n, x_1, \dots, x_m, y, z) = 0 \}.$$

Such representations have become known as *Davis normal form*.

A Milestone

Theorem (Martin Davis, Hilary Putnam, Julia Robinson [1961])

Every listable set \mathfrak{M} has an *exponential Diophantine representation*, i.e., a representation of the form

$$\langle a_1, \dots, a_n \rangle \in \mathfrak{M} \iff$$

$$\exists x_1 \dots x_m \{ E_L(a_1, \dots, a_n, x_1, \dots, x_m) = E_R(a_1, \dots, a_n, x_1, \dots, x_m) \}$$

where E_L and E_R are expressions constructed by traditional rules from the variables and particular positive integers by addition, multiplication and exponentiation.

A Milestone

and Final Proof

Theorem (Martin Davis, Hilary Putnam, Julia Robinson [1961])

Every listable set \mathfrak{M} has an *exponential Diophantine representation*, i.e., a representation of the form

$$\langle a_1, \dots, a_n \rangle \in \mathfrak{M} \iff$$

$$\exists x_1 \dots x_m \{ E_L(a_1, \dots, a_n, x_1, \dots, x_m) = E_R(a_1, \dots, a_n, x_1, \dots, x_m) \}$$

where E_L and E_R are expressions constructed by traditional rules from the variables and particular positive integers by addition, multiplication and exponentiation.

DPRM-Theorem [1970]) Every listable set \mathfrak{M} has an Diophantine representation.

Current Records

Solving an arbitrary parametric Diophantine equation can be reduced to solving another Diophantine equation (with the same parameters) of degree D in M unknowns where $\langle D, M \rangle$ is any of the following pairs:

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

Equations with Finitely Many Solutions

Problem of Effectivization

Suppose that we have a Diophantine equation

$$P(a, x_1, \dots, x_m) = 0, \quad (*)$$

which for every value of the parameter a has at most finitely many solutions in x_1, \dots, x_m .

This fact can be expressed in two ways:

1. The equation $(*)$ has at most $\nu(a)$ solutions;
2. For every solution of $(*)$ we have

$$x_1 < \sigma(a), \dots, x_m < \sigma(a)$$

Here ν and σ should be some suitable functions defined for every a .

Equations with Finitely Many Solutions

Impossibility of Effectivization

Theorem One can construct an exponential Diophantine equation

$$E_L(a, x_1, x_2, \dots, x_m) = E_R(a, x_1, x_2, \dots, x_m) \quad (**)$$

with the following properties:

1. for every value of the parameter a , the equation $(**)$ has at most one solution in x_1, \dots, x_m ;
2. for every total effectively computable function σ there is a value of a for which the equation $(**)$ has a solution x_1, \dots, x_m such that $x_1 > \sigma(a)$.

Improving this result to the case of Diophantine equations remains a challenge.

Back to Diophantus

Solving an equation

$$P(\chi_1, \dots, \chi_m) = 0$$

in rational numbers χ_1, \dots, χ_m is equivalent to solving the equation

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

in non-negative integers $x_1, \dots, x_m, y_1, \dots, y_m, z$. The latter equation is equivalent to the Diophantine equation

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

where d is the degree of P .

So asking *explicitly* about solving Diophantine equations in integers, Hilbert asked *implicitly* about solving Diophantine equations in rational numbers. A positive solution of the 10th problem, as it was stated, would give immediately a positive solution to the similar problem about solutions in rational numbers.

Broad Understanding

We can understand Hilbert's 10th problem in two senses:

- ▶ the *narrower sense*, i.e. literally as the problem was stated originally;
- ▶ the *broader sense*, including other problems, solutions of which would **easily** follow from a positive solution of the problem as it was stated originally.

In the narrow sense Hilbert's 10th problem is closed but in the broader sense is open.

Solving equations in rational numbers remains one of the most important open cases of Hilbert's 10th problem taken in the broader sense.

Hilbert's 10th problem in the broader sense

Gaussian integers

Gaussian integers are complex numbers of the form $a + bi$ where $a, b \in \mathbb{Z}$. Clearly, an equation

$$P(\chi_1, \dots, \chi_m) = 0$$

has a solution in Gaussian integers if and only if the equation

$$P(x_1 + y_1i, \dots, x_m + y_mi) = 0$$

has a solution in rational integers.

A reduction in the opposite direction was found by J.Denef [1975]. Thanks to this reduction, the undecidability of Hilbert's 10th problem (in the original formulation) implied the undecidability of its analogue for Gaussian integers.

Hilbert's 10th problem in the broader sense.

Fermat's Last Theorem

$$x^n + y^n = z^n$$

$$x^n + y^n = z^n \iff \exists u_1 \dots u_m \{F(n, x, y, z, u_1, \dots, u_m) = 0\}$$

Fermat's Last Theorem (reformulation) *Diophantine equation*

$$F(w + 3, x + 1, y + 1, z, u_1, \dots, u_m) = 0$$

has no solution in non-negative unknowns.

While it was not included *explicitly* among Hilbert's problems, Fermat's Last Theorem is *implicitly* present as a very particular case of the tenth problem.

Hilbert's 10th problem in the broader sense.

Goldbach's conjecture

Every even integer greater than 2 is the sum of two prime numbers.

The set \mathfrak{M} of counter examples to Goldbach's conjecture (i.e., even numbers greater than 2 not being the sum of two primes) is listable and hence Diophantine

$$a \in \mathfrak{M} \iff \exists x_1 \dots x_m \{G(a, x_1, \dots, x_m) = 0\}$$

Hence, Goldbach's conjecture is equivalent to the statement that the Diophantine equation

$$G(x_0, x_1, \dots, x_m) = 0$$

has no solution.

Thus a positive solution of Hilbert's 10th problem in its original form would allow us to know whether Goldbach's conjecture is true or not.

Hilbert's 10th problem in the broader sense

The Riemann hypothesis

In the original formulation RH is a statement about complex zeros of Riemann's Zeta function which is the analytical continuation of the series

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

which converges for $\Re(z) > 1$.

We can also construct a particular Diophantine equation

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

which has no solution if and only if the Riemann hypothesis is true.

Thus a positive solution of Hilbert's tenth problem would give us principal possibility to prove or disprove the Riemann hypothesis.

Hilbert's 10th problem in the broader sense.

The 4 color conjecture

Since 1976 the 4CC is a theorem due to K. Appel and W. Haken

We can construct a particular Diophantine equation

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

which has no solutions if and only if the 4 color conjecture is true.

Again a problem which was not included by Hilbert into his problems, appears in a disguise in the 10th problem.

Famous Problems

Four outstanding mathematical problems:

- ▶ Fermat's last theorem
- ▶ Goldbach's conjecture
- ▶ The Riemann hypothesis
- ▶ The four color conjecture

each can be restated as an assertion that particular Diophantine equation has no solutions.