HILBERT'S TENTH PROBLEM: What can we do with Diophantine equations?

Yuri Matiyasevich
Steklov Institute of Mathematics at Saint-Petersburg
27 Fontanka, Saint-Petersburg, 191011, Russia
URL: http://logic.pdmi.ras.ru/~yumat

Abstract

This is an English version of a talk given by the author in 1996 at a seminar of *Institut de Recherche sur l'Enseignement des Mathématique* in Paris. More information about Hilbert's tenth problem can be found on WWW site [31].

I have given talks about Hilbert's tenth problem many times but it always gives me a special pleasure to speak about it here, in Paris, in the city where David Hilbert has posed his famous problems [13]. It happened during the *Second International Congress of Mathematicians* which was held in 1900, that is, in the last year of 19th century, and Hilbert wanted to point out the most important unsolved mathematical problems which the 20th century was to inherit from the 19th century.

Usually one speaks about 23 Hilbert's problems and names them the 1st, the 2nd, ... , the 23rd as they were numbered in [13]. In fact, most of these 23 problems are collections of related problems. For example, the 8th problem includes, in particular

- Goldbach's Conjecture,
- the Riemann Hypothesis,
- the infinitude of twin-primes.

The formulation of the 10th problem is so short that can be reproduced here entirely.

> **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.*[1]

A *Diophantine equation* is an equation of the form

$$D(x_1, \ldots, x_m) = 0, \tag{1}$$

where D is a polynomial with integer coefficients. These equations were named after greek mathematician Diophantus who lived in the 3rd century A.C.

So Hilbert's tenth problem can be also viewed as a collection of problems but there are essential differences with the other problems:

- First, these individual subproblems are, so to say, homogeneous, each of them is represented by a particular Diophantine equation.
- Second, there are infinitely (countably) many such problems.
- Third, and most important, is the following. In the 10th problem Hilbert asked for a *single* method which could be applied to *every* equation. In fact, since Diophantus time number-theorists have found solutions for plenty of Diophantine equations and also have proved the unsolvability of a large number of other equations. Unfortunately, for different classes of equations, or even for different individual equations, one had to invent different specific methods. In the 10th problem Hilbert asked for a *universal* method for recognizing the solvability of Diophantine equations.

[1] **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.*

In today's terminology Hilbert's 10th problem is a *decision problem*, i.e. a problem consisting of infinitely many individual problems each of which requires an answer "YES" or "NO". The heart of a decision problem is the demand to find a single universal method which could be applied to each of comprising it *individual problem.*

By the way, the 10th problem is the only decision problem among the 23 Hilbert's problems.

In the 10th problem Hilbert asked about solvability in integers. One can also consider similar problem about solvability in natural numbers. For a given Diophantine equation *the problem of deciding whether it has a solution in integers* and *the problem of deciding whether it has a solution in natural numbers* are in general two rather different problems.

For example, the equation

$$(x+1)^3 + (y+1)^3 = (z+1)^3 \tag{2}$$

clearly has infinitely many integer solutions of the form $x = z, \quad y = -1$. However, the fact that this equation has no solutions in natural numbers is not trivial at all.

On the other hand, let

$$D(x_1, \ldots, x_m) = 0 \tag{3}$$

be an arbitrary Diopnantine equation; suppose that we are looking for its solutions in integers $x_1, \ldots, x_m$. Consider another equation

$$D(p_1 - q_1, \ldots, p_m - q_m) = 0. \tag{4}$$

It is clear that any solution of equation (4) in natural numbers $p_1, \ldots, p_m$, $q_1, \ldots, q_m$ yields the solution

$$\begin{aligned} x_1 &= p_1 - q_1 \\ &\vdots \\ x_m &= p_m - q_m \end{aligned} \tag{5}$$

of equation (3) in integers $x_1, \ldots, x_m$. Moreover, for any $x_1, \ldots, x_m$ forming a solution of equation (3) we can find natural numbers $p_1, \ldots, p_m, q_1, \ldots, q_m$ satisfying (5) and hence yielding a solution of equation (4).

One says that the problem of solvability of equation (3) in integers *reduces* to the problem of solvability of equation (4) in natural numbers. Respectively, one says also 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.

In fact, these two decision problems are *equivalent* in the sence that each of them reduces to the other one, but the reduction in the other direction is less evident. Let

$$D(p_1, \ldots, p_m) = 0 \tag{6}$$

be an arbitrary Diophantine equation for which we are looking for natural number solution. Consider the following equation:

$$D(w_1^2 + x_1^2 + y_1^2 + z_1^2, \ldots, w_m^2 + x_m^2 + y_m^2 + z_m^2) = 0. \tag{7}$$

It is clear that any solution of the latter equation in integers yields a solution of the former equation in natural numbers. Conversely, every solution of (6) in natural numbers $x_1, \ldots, x_m$ can be obtained in this way from some solution of equation (7) in integers $w_1, \ldots, z_m$ because by Lagrange's theorem every natural number is the sum of four squares.

Thus we see that two problems, that of recognizing whether a Diophantine equation has a solution in integers, and that of recognizing whether it has a solution in natural numbers, are in general different problems for a particular equation but they are equivalent when considered as decision problems, i.e. algorithmic problems about the whole class of Diophantine equations.

By some technical reason it is a bit easier to work with variables ranging over natural number, and most of the time I shall suppose that our unknows are natural numbers.

A solution to a decision problem should be given in the form of an algorithm which for given input would always produce the required answer "YES" or "NO". However, at the end of the 19th century when Hilbert posed his problems, there was no rigouroues mathematical definition of what is an algorithm. All what was known were different examples of mathematical algorithms starting from the famous Euclid's algorithm for finding GCD of two integers. That is why Hilbert, instead of the notion of an algorithm, uses a bit vague terminology asking for "*a process according which it can be determined by finite number of operations ...*".

The absense of a general definition of an algorithm was not by itself an obstacle for a positive solution of the 10th problem. If somebody invented the required "*process*" it should be clear that in fact this process does the job.

The situation is essentially different if there is no required algorithm as it turned out to be the case with Hilbert's 10th problem. To prove this fact, or even to state it rigorously, one need a definition of an algorithm. Such a definition was developed much later, only in the 30's of this century in the work of Kurt Gödel, Alan Turing, Emil Post, Alonzo Church and other logicians. Different tools were introduced to describe computational processes: λ-calculus, recursive function, Turing machines an so on. Alonso Church was the first who understood that each of these rather specific particular definitions adequately reflects our intutive idea about general notion of algorithms. This assertion is now known as *Church thesis*.

Today we know that Hilbert's 10th problem has no solution. That means that it is undecidable as a decision problem.

Theorem (Undecidability of Hilbert's tenth problem) There is no algorithm which, for a given arbitrary Diophantine equation, would tell whether the equation has a solution or not.

In fact, the undecidability of Hilbert's 10th problem can be stated in a stronger form than the above one. To prove the mere non-existence of the required algorithm one could just suppose its existence and then deduce a contradiction. In such a case we would have nothing but this deduction of contradiction.

However, for Hilbert's 10th problem we can do a bit more. The non-existence of the algorithms for Hilbert's 10th problem means that any given algorithm $\mathcal{A}$ (supposed to solve Hilbert's 10th problem) fails for some particular equation

$$D_{\mathcal{A}}(x_1, \ldots, x_m) = 0. \tag{8}$$

That is, for this *counter-example* either the algorithm never stops or its output, if any, is wrong.

Theorem (**A stronger form of the undecidability of Hilbert's 10th problem**) There is an algorithm which for given algorithm $\mathcal{A}$ produces a counter-example to the assumption that $\mathcal{A}$ solves Hilbert's tenth problem.

Here the algorithm $\mathcal{A}$ can be represented in any standard form: as a Turing machine, as a recursive function, as a Pascal program and so on.

This form of the undecidability of Hilbert's 10th problem indicates that there is a close relationship between algorithms and Diophantine equations. The existence of such a relation was conjectured in the begining of 50's by american mathematician Martin Davis [6]. To be able to state his hypothesis we need to introduce some more terminology.

Besides *individual* Diophantine equations we can consider also *families* of Diophantine equations. Such a family is defined by a Diophantine equation of the form

$$D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0, \tag{9}$$

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

- the *parameters* $a_1, \ldots, a_n$;
- the *unknowns* $x_1, \ldots, x_m$.

I will suppose that the parameters can assume, as the unknowns does, positive integer values only.

For some choice of the values of the parameters $a_1, \ldots, a_n$ the equation can have a solution in the unknowns $x_1, \ldots, x_m$, for other choices of the values of the parameters it can have no solution. We can consider the set $\mathfrak{M}$ of all n-tuples $\langle a_1, \ldots, a_n \rangle$ for which our parametric equation has a solution, that is

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow \exists x_1 \ldots x_m \{D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0\}. \tag{10}$$

Sets having such representations are called *Diophantine*. An equivalence of the form (10) is called *Diophantine representation* of the set $\mathfrak{M}$. With an abuse of language, one can say that the equation

$$D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0 \tag{11}$$

itself is a representation of the set.

An easy examples of Diophantine sets are the following:

- *the set of all squares* represented by equation

$$a - x^2 = 0; \tag{12}$$

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

$$a - (x_1 + 2)(x_2 + 2) = 0; \tag{13}$$

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

$$a - (2x_1 + 3)x_2 = 0. \tag{14}$$

It is a bit less evident that *the set of all numbers which are* not *squares* is also Diophantine; it is represented by equation

$$(a - z^2 - x - 1)^2 + ((z + 1)^2 - a - y - 1)^2 = 0. \tag{15}$$

However, if we ask about the complements of the other two sets, the answers are not clear at all.

- Is *the set of all prime numbers* Diophantine?

- Is *the set of all powers of 2* Diophantine?

It is natural to ask about a characterization of the whole class of Diophantine sets or, at least, about finding some necessary or some sufficient conditions for a set to be Diophantine. One necessary condition arises if we look at Diophantine sets from computational point of view. Namely, as soon as we are given a parametric Diophantine equation

$$D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0 \tag{16}$$

we can effectively list all n-tuples from the Diophantine set $\mathfrak{M}$ represented by this equation. Namely, we need only to look in some order over all $(n + m)$-tuples of possible values of all the variables $a_1, \ldots, a_n$, $x_1, \ldots x_m$ and check every time whether the equality holds or not. As soon as is does, we put the

n-tuple $\langle a_1, \ldots, a_n \rangle$ on the list of elements of $\mathfrak{M}$. In this way every n-tuple from $\mathfrak{M}$ will sooner or later appear on the list, maybe many times.

The above described algorithms for listing Diophantine sets have a very special form. Allowing arbitrary algorithms, we arrive to the following notion studed in the computability theory. 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 the elements of the set $\mathfrak{M}$.

For example, it is easy to write a Pascal program which would, working infinitly long, print all prime numbers or all powers of 2, so the corresponding sets are listable.

We saw that for a set $\mathfrak{M}$ to be Diophantine it is *necessary* that $\mathfrak{M}$ is listable. Martin Davis conjectured that this condition is also *sufficient*.

M. Davis's conjecture The notions of Diophantine set and listable set coincides, i.e. a set is Diophantine if and only if it is listable.

It was a rather bald conjecture because it had many striking consequence. For example, it implied the existence of a particular polynomial P such that the equation

$$P(a, x_1, \ldots, x_m) = 0 \tag{17}$$

had a solution if and only if a is a prime number. It was noted by Hilary Putnam [26] that such an equation can be rewritten in the following form:

$$a = (x_0 + 1)(1 - P^2(x_0, x_1, \ldots, x_n) - 1. \tag{18}$$

In fact, every solution of equation (17) can be extended to a solution of equation (18) by putting

$$x_0 = a. \tag{19}$$

On the other hand, in any solution of equation (18) with non-negative a, the product in the left-hand side should be positive, which is possible only if

$$P(x_0, \ldots, x_n) = 0, \tag{20}$$

which implies (19) and respectively (17).

Thus Davis's conjecture implies the existence of a particular polynomial P (namely, the right-hand side in (18)) such that the set of all its non-negative values is exactly the set of all prime numbers. This corollary was considered by many researches as an informal argument against Davis's conjecture.

There was another striking corollary of Davis's conjecture. We can list all listable sets:

$$\mathfrak{M}_0, \mathfrak{M}_1, \ldots, \mathfrak{M}_k, \ldots \tag{21}$$

Formally, for given n we can consider the set $\mathfrak{U}_n$ of $(n+1)$-tuples such that

$$\langle a_1, \ldots, a_n, k \rangle \in \mathfrak{U}_n \Longleftrightarrow \langle a_1, \ldots, a_n \rangle \in \mathfrak{M}_k. \tag{22}$$

It is not difficult to select a listing of listable sets such that the set $\mathfrak{U}_n$ be listable itself and then, by Davis's conjecture, it should have a Diophantine representation:

$$\begin{aligned} &\langle a_1, \ldots, a_n, a_{n+1} \rangle \in \mathfrak{U}_n \iff \\ &\quad \exists y_1 \ldots y_w \{U_n(a_1, \ldots, a_n, a_{n+1}, y_1, \ldots, y_w) = 0\}. \end{aligned} \tag{23}$$

Now (22) implies that a Diophantine representation of *arbitrary* listable set of n-tuples can be obtained from *single* polynomial U_n just by fixing the value of one of its variables.

Universal listable sets and other similar objects, like universal Turing machines, have been studed for a long time in the computability theory. Now Davis's conjecture implied the existence of similar universal object in number theory, namely, the existence for every n of a *universal Diophantine equation*. Namely, it follows from (22) and (23) that the equation

$$U_n(a_1, \ldots, a_n, k, y_1, \ldots, y_w) = 0. \tag{24}$$

is universal in the following sense:

for every Diophantine equation (16) *one can effectively find a particular number* k_D *such that equation* (16) *has a solution for given value of the parameters* a_1, ..., a_n *if and only if equation* (24) *has a solution for the same values of parameters* a_1, ..., a_n *and* k_D *as the value of parameter* k:

$$\begin{aligned} &\forall D \exists k_D \forall a_1 \ldots a_n \\ &\quad [\exists x_1 \ldots x_m \{D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0\} \Longleftrightarrow \\ &\qquad \exists y_1 \ldots y_w \{U_n(a_1, \ldots, a_n, k_D, y_1, \ldots, y_w) = 0\}]. \end{aligned}$$

Nothing like this has been known in number theory before: *one can effectively reduce the problem of solving a parametric Diophantine equation of arbitrary large degree with arbitrary many unknowns to the problem of solving of another equation with the same parameters but having fixed degree and fixed number of unknowns.*

In the case $n = 1$ we can apply the above described trick of Putnam and find a *universal polynomial* $V(k, y_0, \ldots, y_w)$. For every listable set $\mathfrak{M}$ of intergers there is a particular number $k_{\mathfrak{M}}$ such that $\mathfrak{M}$ is exactly the set of all non-negative values assumes by V for $k = k_{\mathfrak{M}}$ and arbitrary non-negative integer values of $y_0, \ldots, y_w$. In particular, for some value of k, polynomial V represents in this sense the set of all primes, for another value of k represents the set of all power of 2 and so on.

Martin Davis's [6] made the first step to proving his conjecture. Namely, he proved that every listable set $\mathfrak{M}$ has an almost Diophantine representation.

Theorem (Martin Davis) Every listable set $\mathfrak{M}$ has a representation of the form

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow$$
$$\exists z \forall y_{\leq z} \exists x_1 \ldots x_m \{D(a_1, \ldots, a_n, x_1, \ldots, x_m, y, z) = 0\}.$$

Representation of this type became known as *Davis normal form.* They were a quantitive improvement over the classical result of Kurt Gödel [12] who demonstrated the existence of similar arithmetical representations with arbitrary number of universal quantifiers. All what remained to prove Davis's conjecture was to eliminate the last universal quantifier, but this last step took 20 years.

At first, the single remaining universal quantifier was eliminated in a famous joint paper of Martin Daivis, Hilary Putnam and Julia Robinson [10] published in 1961. However, the cost of this elimination was rather high. Namely, Davis, Putnum and Robinson were forced to consider a broader class of equations, so called *exponential Diophantine equation.* These are equations of the form

$$E_{\mathrm{L}}(x_1, x_2, \ldots, x_m) \;=\; E_{\mathrm{R}}(x_1, x_2, \ldots, x_m) \tag{25}$$

where E_{L} and E_{R} are so called *exponential polynomials*, i.e. expression constructed by traditions rules from the variables and particular positive integers by addition, multiplication and exponentiations. An example of exponential Diophantine equation is

$$(x+1)^{y+2} + x^3 = y^{(x+1)^x} + y^4. \tag{26}$$

Respectively, Davis, Putnam and Robinson obtained an *exponential Diophantine representation* for every listable set.

Theorem (Martin Davis, Julia Robinson, Hilary Putnam) For every listable set $\mathfrak{M}$ of n-tuples of non-negative integers there is a representation of the form

$$\begin{aligned} &\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow \\ &\exists x_1 \ldots x_m E_{\mathrm{L}}(a_1, \ldots, a_n, x_1, x_2, \ldots, x_m) = \\ &\qquad\qquad E_{\mathrm{R}}(a_1, \ldots, a_n, x_1, x_2, \ldots, x_m) \end{aligned}$$

where E_{L} and E_{R} are exponential polynomials.

It was a great breakthrough because here we have purely existential representation and thus we have immediate corollaries about equations. In particular, one can construct *a universal exponential Diophantine equation*

$$E_{\mathrm{L}}(a_1, \ldots, a_n, k, x_1, x_2, \ldots, x_m) \;=\; E_{\mathrm{R}}(a_1, \ldots, a_n, k, x_1, x_2, \ldots, x_m) \tag{27}$$

and hence solving any arbitrary exponential Diophantine equation can be reduced to solving an exponential Diophantine equation with fixed number of unknowns. Today we know that this number can be as low as 3 unknows only (the original proof of this estimate was given in [22] and was reproduced also in [23, 30]).

Such a reduction of the number of unknowns is purely number-theoretical in its statement but it seems to be never even suspected by number-theorists. At first, it was found by logician with the use of notions from the computability theory. Today one can [24] construct a universal exponential Diophantine equation by purely number-theoretical tools.

But even after this remarkable result of Davis, Putnam and Robinson even for some logicians the existence of a universal Diophantine equation was implausible. The following was said by George Kreisel in the review [16] of the above mentioned celebrated paper of Davis, Putnam and Robinson [10] written by him for *Mathematical Reviews*:

> 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. sets, and so it is likely that the present result is not closely connected with Hilbert's tenth Problem. Also it is not altogether plausible that all (ordinary) Diophantine problems are uniformly reducible to those in a fixed number of variables of fixed degree, which would be the case if all r.e. sets were Diophantine.

After the work of Davis, Putnam and Robinson in order to prove Davis's conjecture it was sufficient to show that the set $\mathfrak{M}$ of all triples of the form $\langle a, b, a^b\rangle$ is Diophantine. In fact, suppose that this is so and let

$$\begin{aligned} \langle a, b, c\rangle \in \mathfrak{M} &\Leftrightarrow a^b = c \\ &\Leftrightarrow \exists z_1 \ldots z_m \{A(a, b, c, z_1, \ldots, z_m) = 0\} \end{aligned} \tag{28}$$

be coresponding Diophantine representation. With the aid of such a polynomial A we can transform an arbitrary exponential Diophantine equation into an equivalent Diophantine equation with extra unknowns. Consider as an example again equation (26). Here we have three exponentiations and we can use three copies of Diophantine equation from (28) to transform equation (26) into equivalent Diophantine equation

$$\begin{aligned} A^2(x+1, x+2, s', z'_1, \ldots, z'_m) &+ \\ A^2(x+1, x, s'', z''_1, \ldots, z''_m) &+ \\ A^2(y, s'', s''', z'''_1, \ldots, z'''_m) &+ \\ (s' + x^3 - s''' - y^4)^2 &= 0. \end{aligned}$$

In other words, in order to prove that *every* listable set is Diophantine it was sufficient to prove that *one particular* set of triples has a Diophantine representation (28). In fact, the study of this problem was began by Julia Robinson [28] much earlier, at the begining of 50's, i.e. at the same time when M. Davis posed his conjecture.

Julia Robinson failed to find a Diophantine representation for exponentiation. However she found in [28] a condition sufficient for the existence of such a representation.

Theorem (Julia Robinson) There is a polynomial $A(a, b, c, z_1, \ldots, z_m)$ such that

$$a^b = c \quad \Leftrightarrow \quad \exists z_1 \ldots z_w \{A(a, b, c, z_1, \ldots, z_m) = 0\}$$

provided that there is an equation

$$J(u, v, y_1, \ldots, y_w) = 0 \tag{29}$$

such that

- in every solution of equation we have $u < v^v$;
- for every k there is a solution such that $u > v^k$.

The equation (29) defines a relation between u and v which hold if and only if the equation has a solution. Julia Robinson called relations satisfying the above two inequalities *relations of exponential growth*, they also became known in the literature as *Julia Robinson relation*.

Now to prove Davis's conjecture remainded to find a single relation of exponential growth defined by a Diophanting equation. Surprisingly, among numerous two-parameter equation studied in the number theory since Diophantus up to the end of 60's years of the 20th century no equation was known to define a relation of exponential growth.

This fact, together with unbelievable corollaries of Davis's conjecture produced serious doubts in the existence of Julia Robinson relation. At some

point she herself lost believe in it and began to look for a positive solution of Hilbert's 10th problem.

Finally, in 1970 I [19] was able to construct the requied equation defining a relation with exponential growth. It was precisely the relation

$$v = F_{2u} \tag{30}$$

where F_0, F_1, ... is the well-known sequence of Fibonacci numbers:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$$

This celabrated sequence has been extensively studied since the time of Fibonacci but nevertheless I was able to find its new property which rest unknown to number-theorists for centuries, namely

$$F_n^2 \mid F_m \Longrightarrow F_n \mid m. \tag{31}$$

It is not difficult to prove this property of Fibonacci numbers *after* it has been stated.

The whole construction of a Diophantine representation for (30) did not use any deep achievement of 20th century number theory and could be found in last century as well. What was then missing was a motivation.

Now such a motivation was a proof of Davis's conjecture. My construction of a relation of exponential growth turned out to be chronologically the last step in the proof of Davis's conjecture which is often refered to as *DPRM-theorem* after Davis-Putnam-Robinson-Matiyasevich. Nowadays detailed and simplified proofs of this theorem can be found in many publications, in particular, in [1, 3, 5, 7, 8, 14, 17, 18, 20, 23, 30].

DPRM-Theorem Every listable set $\mathfrak{M}$ of n-tuples of non-negative integers has a Diophantine representation, that is

$$\begin{aligned} &\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow \\ &\quad \exists x_1 \ldots x_m \{ D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0 \} \end{aligned} \tag{32}$$

for some polynomial with integer coefficients.

With the proof of Davis's conjecture we have got all the implausible corollories.

The whole proof was constructive in the sense that given any standard representation of a listable set we can actually found its Diophantine representation. For example, you can look at a particular polynomial representing the set of prime number.

Theorem (J.P.Jones, D.Sato, H.Wada, D.Wiens [15]) The set of all prime numbers is equal to the set of all positive values of the polynomial

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

assumed for positive values of 26 variables $a,\ldots,z$.

Today one can [21] construct a prime number representing polynomial in 10 variables.

Let us return to Hilbert's 10th problem. Davis's conjecture implied its undecidability even in a stronger sense. A classical result in the computability theory is the existence of an undecidable listable set $\mathfrak{W}$ of non-negative integers. For this set there is no algorithm to determing, for given natural

number a, whether it belongs to the set or not. Because $\mathfrak{W}$ is listable, we can find its Diophantine representation

$$a \in \mathfrak{W} \Longleftrightarrow \exists x_1 \ldots x_m \{W(a, x_1, \ldots, x_m) = 0\}. \tag{33}$$

The undecidebility of $\mathfrak{W}$ implies that there is no algorithm to determine for which values of the parameter a the equation in (33) has a solution and for which it has not.

Theorem (**Another strong form of the undecidability of Hilbert's 10th problem**) There is a particular one-parameter Diophantine equation

$$W(a, x_1, \ldots, x_m) = 0 \tag{34}$$

such that there is no algorithm to determing for given value of a, whether this equation has a solution in non-negative integers $x_1, \ldots, x_m$.

Thus to get the undecidability we need not consider the whole class of Diophantine equations, it suffies to consider only equations of bounded degree with bounded number of unknowns, moreover, only those which arise from a particular polynomial W by fixing the value of one of its variables.

The above stated two strong forms of the undicidability of Hilbert's 10th problemcan be combined together.

Theorem (Yet stronger form of the undecidability of Hilbert's 10th problem) There is a particular one-parameter Diophantine equation

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

and an algorithm which, for given algorithm $\mathcal{A}$, produces a number $a_{\mathcal{A}}$ such that the algorithm $\mathcal{A}$ fails to give the correct answer for the question whether equation $W(a_{\mathcal{A}}, x_1, \ldots, x_m) = 0$ has s solution in $x_1, \ldots, x_m$.

The algorithmic undecidability of Hilbert's 10th problem is considered today as its *negative solution*. But would Hilbert himself accept it as a "solution" at all? I think "YES". To support this point of view I wish to cite a part of Hilbert's famous lecture *Mathematical Problems* [13]:

> Occasionally it happens that we seek the solution under insufficient hypotheses or in an incorrect sense, and for this reason do not succeed. The problem then arises: to show the impossibility of the solution under the given hypotheses, or in the sense contemplated. Such proofs of impossibility were effected by the ancients, for instance when they showed that the ratio of the hypotenuse to the side of an isosceles triangle is irrational. In later mathematics, the question as to the impossibility of certain solutions plays a preëminent part, and we perceive in this way that old and difficult problems, such as the proof of the axiom of parallels, the squaring of circle, or the solution of equations of the fifth degree by radicals have finally found fully satisfactory and rigorous solutions, although in another sense than that originally intended. It is probably this important fact along with other philosophical reasons that gives rise to conviction (which every mathematician shares, but which no one has as yet supported by a proof) that every definite mathematical problem must necessary be susceptible of an exact settlement, either in the form of an actual answer to the question asked, or by the proof of the impossibility of its solution and therewith the necessary failure of all attempts.

So, most likely, Hilbert would be satisfied with the "negative solution" of the 10th problem. But now we can ask another question: *would Hilbert be satisfied with the statement of the problem itself if he new it would be "solved" in this way*? I think "NO".

Let me explain my point of view. Hilbert's lecture took 2 and a half hours but still this was not enough to present all the 23 problems so some of them, including the 10th, were not presented oralement but were just included in the printed version of the lecture. The 10th problem occupies there less space than any other problem. In particular, Hilbert gave no motivation for the 10th problem. We can only guess why he asked about

solutions only in *rational integers*. We saw that this is equivalent to asking for an algorithm for solving Diophantine equations in non-negative integers. But in fact, Diophantus himself was solving equations neither in integers nor in non-negative integers, he was looking for solutions in rational numbers. So why Hilbert did not ask about a procedure to determine the existence of solution in rational numbers?

The answer is more or less evident. Hilbert was an optimist and believed in the existence of an algorithm for solving Diophantine equations in integers. Such an algorithm would allow us to solve equations in rational numbers as well. Namely, solving an equation

$$D(\chi_1, \ldots, \chi_m) = 0 \tag{35}$$

in rational $\chi_1, \ldots, \chi_m$ is equivalent to solving equation

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

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

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

where d is the degree of D.

There is a less evident reduction of solving Diophantine equations in rational numbers to solving homogenous Diophantine equations in integers. We start by transforming (35) into

$$D\left(\frac{x_1}{z}, \ldots, \frac{x_m}{z}\right) = 0$$

and then into

$$z^d D\left(\frac{x_1}{z}, \ldots, \frac{x_m}{z}\right) = 0$$

but an additional trick (see, for example, [23, 30]) is required to guarantee that $z \neq 0$.

So asking *explicitely* about solving Diophantine equations in integers, Hilbert asked *implicitely* 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 similar problem about solution in rational numbers.

However, we have got a negative solution of the original statement of the 10th problem. What does it imply for solving Diophantine equations in rational numbers? Nothing. In fact, the decision problem of determing the solvability an arbitrary Diophantine equation in rational numbers is equivalent to the decision problem of solving homogenous Diophantine equations in integers. Such equations form only a subclass of all Diophantine equations and it is quite possible that for this narrower class there is corresponding algorithm.

So it is rather likely that, if Hilbert previewed non-existence of the algorithms for solving Diophantine equations in integers, he would include into the 10th problem the case of solving equations in rational numbers as well. Thus we can understand the 10th problem in two senses.

- *narrower sense*, i.e. literally as the problem was stated;
- *broader sense*, including other problem solutions of which would easily follow from a positive solution of the 10th problem as it was stated.

In the narrow sense the 10th problem is closed but in the broder sense is still open.

Solving equations in rational numbers remains one of the most important open cases of Hilbert's 10th problem taken in broader sense. The progress in this direction is rather small.

Some of other open cases are as follows. Besides solving Diophantine equations in rational integers, we can be interested in solving them in rings of integers of an algebraic extensions of the field of rational numbers. For example, we can be interested in solving Diophantine equation in *Gaussian numbers*, i.e. in numbers of the form $a + bi$ where $a, b \in Z$. Clearly, equation

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

has a solution in Gaussian numbers if and only if equation

$$D(x_1 + y_1 i, \ldots, x_m + y_m i) = 0 \tag{36}$$

has a solution in rational integers. Now we can separate the real and the imaginary parts by writing

$$D(x_1 + y_1 i, \ldots, x_m + y_m i) =$$

$$D_{\mathrm{R}}(x_1,\ldots,x_m,y_1,\ldots,y_m)+D_{\mathrm{I}}(x_1,\ldots,x_m,y_1,\ldots,y_m)i$$

and rewrite (36) as a genuine Diophantine equation

$$D^2_{\mathrm{R}}(x_1,\ldots,x_m,y_1,\ldots,y_m)+D^2_{\mathrm{I}}(x_1,\ldots,x_m,y_1,\ldots,y_m)=0.$$

So we can consider solving Diophantine equations in Gaussian number as part of Hilbert's 10th problem in the broader sense.

This problem was shown indecidable by J. Denef [11]. Namely, he found a reduction in the opposite direction, i.e., he showed how solving a Diophantine equation

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

in integers can be reduced to solving another Diophantine equation

$$G(\chi_1,\ldots,\chi_w)=0$$

in Gaussian numbers. Thanks to this reduction, the undecidability of Hilbert's 10th problem in the narrower sense implied the undecidability of its counterpart for Gaussian numbers.

Similar reductions were found by different reseachers (for references see survey [25]) for rings of integers from some other algebraic extensions of the field of rational number, which constitute a progress for the 10th problem in the broader sense. However, this was done only for certain specific extensions, the general case of an arbitrary extensions still remains an important open case of the 10th problem in the broader sense.

Introducing the problem in the broader sense, I spoke about problems solutions of which would *easily follow* from a positive solution of the 10th problem in as it was stated. Thus the scope of the 10th problem in the broader sense depends on what we understand by *easily follow*. Certainly, solving Diophantine equations in rational or in Gaussian numbers would follow easily. Strikingly, ther are many other problems reductions of which to the 10th problem is not difficult but just much less evident. Now I am to present several examples of such problems which could be considered as cases of the 10th problem in the broader sense.

Let us start from the famous Fermat's Last theorem a proof of which we had recently witnessed. Hilbert did not include *explicitely* Fermat's Last theorem in his Problems. Formally, the problem is about unsolvability of an infinite series of Diophantine equation

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

and thus it is not a case of the 10th problem in which Hilbert ask for solving only single Diophantine equation rather than infinite series of them.

Fermat's equation is a Diophantine equation in x, y, z for a fixed value of n but is an exponential Diophantine equation if viewed as an equation in four unknown n, x, y, z. But now we know how to transform an arbitrary exponential Diophantine equation into genuine Diophantine equation with extra unknows and we are able (and this was actually done in [29, 4]) to construct a particular polynomial F with integer coefficients such that equation

$$F(n, x, y, z, u_1, \ldots, u_m) = 0$$

has a solution in u_1, $\ldots$,u_m if and only if n, x, y and z are solution of Fermat's equation. So Fermat's Last theorem is equivalent to the statement that particular genuine Diophantine equation

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

has no solution in non-negative unknows. Thus, a positive solution of the 10th problem in its original formulation should give us a tool to proof or disproof Fermat's Last theorem. So, while Fermat's Last theorem is not presented *explicitely* among Hilbert's problems, it is presented there *implicitely* as a very particular case of the 10th problem.

In spite of the fact that such a reduction of Fermat's Last theorem to a fixed Diophantine equations was not known before 1970, is not too striking because the Fermat's theorem is about Diophantine equations. As a less evident example we can consider another famous problem, *Goldbach's conjecture*, which was included by Hilbert into the 8th problem and still remains open.

Goldbach's conjecture states that every even integer greater than 4 is the sum of two prime numbers. We can consider the set $\mathfrak{G}$ of even numbers which are greater than 2 but still are not the sum of two primes. For any particular number a we can easily check whether it is a counterexample to Goldbach's conjecture or not. Thus this set $\mathfrak{G}$ of counterexamples is listable and hence Diophantine. Respectively, we can find a particular Diophantine equation

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

which has a solution if and only if a a spoils the conjecture. In other words, Goldbach's conjecture is equivalent to the statement that the set $\mathfrak{G}$ is empty,

and hence to the statement that Diophantine equation

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

has no solution at all.

Thus we again see that positive solution of the 10th problem in it original form would allow us to know whether Goldbach's conjecture is true or not.

The reduction of Goldbach's conjecture to particular Diophantine equation is less evident and requires more techniques than the reduction of Fermat's Last theorem because now we have to deal with primality. Still, is it not unbelievable because Goldbach's conjecture is about integers.

Besides Goldbach's conjecture, Hilbert included into the 8th problem another outstanding conjecture, the famous *Riemann hypothesis*. In its original formulation is its a statement about complex zeros of Riemann's zeta function which is the analitical continuation of the series

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}. \tag{37}$$

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

Nevertheless, we can [9, 23] also construct a particular Diophantine equation

$$\mathfrak{R}(x_1, \ldots, x_m) = 0$$

which has no solution if and only if the Riemann hypothesis is true. Such a reduction requires either the use of the theory of complex variable or the use of the fact that the Riemann Hypothesis can be reformulated as a statement about distribution of prime numbers.

Thus once again we see that an ontstanding mathematical problem is a specific case of Hilbert's tenth problem in its original formulation.

The above considered three famous problems, i.e. Fermat's Last Theorem, Goldbach's conjecture and Riemann Hypothesis were about numbers and so their reductions to Diophantine equations while not obvious are still imaginable. However, in mathematical logic there is a powerful tool, *arithmetization*, which allows one to reduce to numbers many problems which are not about numbers at all.

As my last example I am to consider yet another famous challenge to mathematicians, the Four Color Conjecture which since 1976 is a theorem of

K. Appel and W. Haken [2]. This is a problem about coloring planar maps but again we can construct a particular Diophantine equation

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

which has no solution if and only if the Four Color Conjecture is true. Again a problem which was not included by Hilbert into his Problems, appears in a masked form in the 10th problem.

I have discribed reductions to Diophantine equation of 4 famous problems:

- Fermat's Last theorem,
- Goldbach conjecture,
- Riemann hypothesis,
- Four color conjecture.

Two of this problem are now solved, the two others remain open. The reductions of these problems may be considered as striking, amazing, amusing but could these reductions be useful? The 10th problem is indecidable so we do not have any universal method to solve all this problem at once. Hardly we can solve any of these problem by looking at particular corresponding Diophantine equations because they are rather complicated.

But we can reverse the order of things. The 10th problem is indecidable and we need to invent more and more *ad hoc* methods to solve more and more Diophantine equation. Now we can view the proof of the Fermat's Last Theorem and that of the Four Color Conjecture as a very deep tools for treating particular Diophantine equations and we can try to extend these techniques to other equations.

References

[1] Adamowicz Zofia, Zbierski Paweł. *Logic of Mathematics.* John Wiley & Sons, New York a. o., 1997.

[2] K. Appel, W. Haken. Every planar map is four colorable. Part I. Discharging. *Illinois J. of Mathematics*, **21**(3):429–490 (1977).

[3] J.-P. Azra, Relations Diophantiennes et la solution négative du 10e problème de Hilbert. volume 244 of *Lecture Notes in Mathematics*, 244:11–28, 1971.

[4] C. Baxa A note on Diophantine representations. *The American Mathematical Monthly*, 100(2):138–143, 1993.

[5] E. Börger. *Computability, Complexity, Logic.* North-Holland, Amsterdam, 1989.

[6] M. Davis. Arithmetical problems and recursively enumerable predicates. *J. Symbolic Logic*, 18(1):33–41, 1953.

[7] M. Davis. Hilbert's tenth problem is unsolvable. *Amer. Math. Monthly*, 80(3):233–269, 1973.

[8] M. Davis. *Computability and Unsolvability.* Dover Publications, New York, 1982.

[9] Martin Davis, Yuri Matijasevich and Julia Robinson, Hilbert's tenth problem. Diophantine equations : positive aspects of a negative solution, *Proc. Symp. Pure Math.* 28 (1976), 323-378.

[10] Martin Davis, Hilary Putnam and Julia Robinson, The decision problem for exponential Diophantine equations, *Ann. Math.* (2) 74 (1961), 425-436.

[11] J.Denef, Hilbert's Tenth Problem for quadratic rings. *Proceedings of the American Mathematical Society*, (1975) 48(1):214–220.

[12] K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme. I. *Monatsh. Math. und Phys.*, 38(1):173–198, 1931.

[13] David Hilbert, Mathematische Probleme. Vortrag, gehalten auf dem internationalen Mathematiker Kongress zu Paris 1900, *Nachr. K. Ges. Wiss., Göttingen, Math.-Phys.Kl.* (1900), 253-297. See also *Arch. Math. Phys.* (1901) 44-63, 213-237. See also David Hilbert, *Gesammelte Abhandlungen*, Berlin : Springer, vol. 3 (1935), 310 (Reprinted: New York : Chelsea (1965)). French translation with corrections and

additions : *Compte rendu du Deuxième Congrès International des Mathématiciens tenu à Paris du 6 au 12 août 1900*, Gauthier-Villars, 1902, pp.58-114 (réédition : Editions Gabay, Paris 1992). English translation : *Bull. Amer. Math. Soc.* (1901-1902) 437-479. Reprinted in : *Mathematical Developments arising from Hilbert problems*, Proceedings of symposia in pure mathematics, vol.28, American Mathematical Society, Browder Ed., 1976, pp.1-34.

[14] J. P. Jones, Y. V. Matijasevič. Proof of recursive unsolvability of Hilbert's tenth problem. *Amer. Math. Monthly* 98(8):689–709, 1991.

[15] James P. Jones, Daihachiro Sato, Hideo Wada, and Douglas Wiens, Diophantine representation of the set of prime numbers. *The American Mathematical Monthly*, 83(6):449–464, 1976.

[16] G. Kreisel, "Davis, Martin; Putnam, Hilary; Robinson, Julia. The decision problem for exponential Diophantine equations." *Mathematical Reviews*, 24#A3061:573, 1962.

[17] Yu. I. Manin. *A Course in Mathematical Logic.* Springer, New York; Heidelberg; Berlin, 1977.

[18] M. Margenstern. Le théorèm de Matiyassévitch et résultats connexes. In C. Berline, K. McAloon, and J.-P. Ressayre, editors, *Model Theory and Arithmetic*, volume 890 of *Lecture Notes in Mathematics*, pages 198–241. Springer-Verlag, 1981.

[19] Yu. V. Matiyasevich. Diofantovost' perechislimykh mnozhestv. *Dokl. AN SSSR*, 191(2):278–282, 1970. Translated in: *Soviet Math. Doklady*, 11(2):354-358, 1970.

[20] Yu. Matiyasevich. Diofantovy mnozhestva. *Uspekhi Mat. Nauk*, 27:5(167),185–222,1972. Translated in: *Russian Mathematical Surveys*, 27(5):124–164, 1972.

[21] Yu. Matiyasevich. Prostye chisla perechislyayutsya polinomom ot 10 peremennykh. *Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR* , 68:62–82, 1977. (Translated as Yu. V. Matijasevič. Primes are nonnegative values

of a polynomial in 10 variables. *Journal of Soviet Mathematics*, 15(1):33–44, 1981.)

[22] Yu. V. Matiyasevich. Algorifmicheskaya nerazreshimost' eksponentsial'no diofantovykh uravneniĭ s tremya neizvestnymi. *Issledovaniya po teorii algorifmov i matematicheskoĭ logike*, A. A. Markov and V. I. Homich, Editors, Akademiya Nauk SSSR, Moscow 3:69–78,1979. Translated in: *Selecta Mathematica Sovietica*, 3(3):223–232, 1983/84.

[23] Matiyasevich Yu. *Desyataya Problema Gilberta.* Moscow, Fizmatlit, 1993. English translation: Hilbert's tenth problem. MIT Press, 1993. French translation: Le dixième problème de Hilbert, Masson, 1995

[24] Les equations-bricoleurs. *Revue de Mathematiques Speciales*, 5:305–309, 1994.

[25] Thanases Pheidas, Extensions of Hilbert's tenth problem. J. Symbolic Logic 59:2(1994), 372–397.

[26] H. Putnam. An unsolvable problem in number theory. *J. Symbolic Logic*, 25(3):220–232, 1960.

[27] Constance Reid, The autobiography of Julia Robinson, in *More Mathematical People*, Academic Press, 1990, 262–280; reprinted in: Constance Reid *JULIA. A life in mathematics*, The mathematical Association of America, 1996, ISBN 0-88385-520-8.

[28] Julia Robinson, Existential definability in arithmetic, *Trans. Amer. Math. Soc.* 72 (1952), 437-449.

[29] K. Ruohonen. Hilbertin kymmenes probleema (Finnish). *Arkhimedes*, no. 1–2:71–100, 1972.

[30] C.Smoryński. *Logical number theory* I*: An Introduction*, Berlin, Springer-Verlag, 1991.

[31] URL: `http://logic.pdmi.ras.ru/Hilbert10`.