Computation Paradigms in Light of Hilbert’s Tenth Problem

Yuri Matiyasevich

Steklov Institute of Mathematics, St. Petersburg 191023, Russia
yumat@pdmi.ras.ru
http://logic.pdmi.ras.ru/~yumat

Summary. This is a survey of a century-long history of interplay between Hilbert’s tenth problem (about solvability of Diophantine equations) and different notions and ideas from Computability Theory. The present paper is an extended version of [83].

1 Statement Of The Problem: Intuitive Notion Of Algorithm

In the year 1900, the prominent German mathematician D. Hilbert delivered to the Second International Congress of Mathematicians (held in Paris) his famous lecture titled Mathematische Probleme [41]. There he put forth 23 (groups of) problems that were, in his opinion, the most important open problems in mathematics that the pending 20th century would inherit from the passing 19th century. Problem number 10 was stated as follows:

Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoeffizienten sei vorgelegt: man soll ein Verfahren angeben, nach welchem sich mittels einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist. ²

* The author is very grateful to Martin Davis and Grant Olney Passmore for their comments that corrected English and improved the presentation. Support from the Council for Grants of the President of the Russian Federation under grant NSh-8464.2006.1 is also acknowledged.
² 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: Devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.
A Diophantine equation is an equation of the form

\[ P(x_1, \ldots, x_m) = 0 \]  

(1)

where \( P \) is a polynomial with integer coefficients. Hilbert raised the question about solving Diophantine equations in "rational integers" that were nothing else but numbers \( 0, \pm 1, \pm 2, \ldots \), which we will call just integers. In the last section of the paper, we will investigate a more general version of the problem in which solutions are allowed to be arbitrary "algebraic integers."

A method demanded by Hilbert would allow us to recognize also solvability of Diophantine equations in natural numbers \( 0, 1, 2, \ldots \), namely, equation (1) has a solution in natural numbers if and only if equation

\[ P(p_1^2 + q_1^2 + r_1^2 + s_1^2, \ldots, p_m^2 + q_m^2 + r_m^2 + s_m^2) = 0 \]  

(2)

has a solution in arbitrary integers. Without lost of generality in this paper, we will deal with solving Diophantine equations in natural numbers, and respectively, all italic lowercase Latin letters will range over \( 0, 1, 2, \ldots \) (unless otherwise specified).

Since Diophantus’s time (3rd century A.D.), number-theorists have found solutions for plenty of Diophantine equations and have proved the unsolvability of a large number of other equations. However, for different classes of equations, or even for different individual equations, one had to invent different specific methods. In the tenth problem, Hilbert asked for a universal method for recognizing the solvability of Diophantine equations; i.e., in modern terminology, the tenth problem is a decision problem (the only one among the 23 problems).

Note that Hilbert did not use the word “algorithm” in his statement of the tenth problem. Instead, he used the rather vague wording “a process according to which it can be determined by a finite number of operations ...”. Although he could have used the word “algorithm,” it would not really have helped much to clarify the statement of the problem because, at that time, there was no rigorous definition of the general notion of an algorithm. What existed was a number of examples of particular mathematical algorithms (such as the celebrated Euclidean algorithm for finding the greatest common divisor of two integers) and an intuitive conception of an algorithm in general.

Does this imply that Hilbert’s tenth problem was ill-posed? Not at all. The absence of a general definition of an algorithm was not in itself an obstacle to finding a positive solution of Hilbert’s tenth problem. If somebody invented the required “process,” it would presumably be clear that in fact this process does the job, so an intuitive conception of an algorithm would be sufficient for positive solution of the tenth problem, which was, most likely, Hilbert’s expectation.

It took 70 years before Hilbert’s tenth problem was solved in the negative sense: There exists no algorithm (i.e., no Turing Machine, no recursive function, and so