HILBERT'S TENTH PROBLEM

C. T. Chong
National University of Singapore

At the International Congress of Mathematicians held in Paris in the year 1900, David Hilbert presented twenty three mathematical problems whose solutions he believed would greatly advance twentieth century mathematics. The professor from the University of Göttingen in Germany was at this time considered one of the world's two leading mathematicians (the other being Henri Poincaré of France), and it was therefore not surprising that all of the problems were taken very seriously by his and subsequent generations. Indeed the mathematical community has since often used the state of knowledge of the Hilbert problems as a yardstick to appraise the advances of contemporary mathematics. A number of these problems have been satisfactorily solved, among which is the Tenth Problem.

Hilbert's Tenth Problem is quite easily stated. Given an equation $x^2 + y^2 = 1$, it is not difficult to see that this is the equation of a circle with radius 1 centered at the origin. Any point (x, y) lying on the circle is a solution to the equation. But suppose that we require x and y to be both integers. Then there are only four solutions, namely (1, 0), (0, 1), (−1, 0), (0, −1). Now consider the equation $x^2 + y^2 = 3$. This is the equation of a circle with radius $\sqrt{3}$ centered at the origin. Again any point (x, y) lying on the circle is a solution to the equation. But it is not difficult to see that there are no integers x and y for which (x, y) solves $x^2 + y^2 = 3$. One argues as follows: since x, y must be integers and the square of an integer is always non-negative, we know that the following are the only possibilities:

$$x^2 = 0 \qquad y^2 = 3 \qquad (1)$$
$$x^2 = 1 \qquad y^2 = 2 \qquad (2)$$
$$x^2 = 2 \qquad y^2 = 1 \qquad (3)$$
$$x^2 = 3 \qquad y^2 = 0 \qquad (4)$$

As there are no integers whose squares are 2 or 3, there does not exist integral solution to (1), (2), (3) or (4), and so $x^2 + y^2 = 3$ has no solution in integers. Thus asking for integral solutions is a more demanding question, and the answer may be either yes or no, even though the equation given may have solutions in real numbers. A polynomial equation whose coefficients are integers is called a Diophantine equation. This is named after the Greek mathematician Diophantus who wrote a book treating this subject. Thus for example $x^2 + y^2 = 3$, $4x^5 - 2x^2 + 3 = 0$ are Diophantine equations, whereas $x^3 + \sqrt{2}\, y^2 + y = 0$ is not, since the coefficient $\sqrt{2}$ is not an integer. A Diophantine equation can have any number of variables, e.g.

$$2x_1^7 + 3x_2 x_3^5 + x_4^2 + x_5^{100} + x_6 x_7 + 3 = 0$$

has seven variables. Notice that Diophantine equations can get fairly complicated, since one can multiply constants with variables, variables with variables, and raise variables to any (integral) power. Furthermore from the examples given earlier we know that Diophantine equations may or may not have solutions in integers. Is there a way that allows one to decide whether a given Diophantine equation

has integral solutions? Hilbert's Tenth Problem asks: Devise a process according to which, for a given Diophantine equation, "it can be determined by a finite number of operations whether the equation is solvable in integers" (cf. David Hilbert, Mathematical Problems, in: Mathematical Developments Arising from Hilbert Problems, American Mathematical Society, 1976).

It is important to note that in retrospect the problem as stated did not permit an early solution. The reason is clear: it is a problem closely related to a subject in mathematical logic called recursion theory which was not developed until the 1930's. In the year 1900 the only area in logic which was being closely studied was set theory, largely through the influence of Georg Cantor. It is then reasonable to assume that Hilbert kept his wording purposely vague since it was not clear then what constituted a 'procedure', although 'one knows it when one sees it'. But perhaps such a procedure does not exist? In order to fully appreciate this possibility one has to have a clear notion of what a 'procedure' is. That was however lacking in 1900.

In our present day terminology, we can state Hilbert's Tenth Problem in the following way: write a computer programme so that, given the coefficients of a Diophantine equation as input, the programme prints 1 as output if the equation has integral solutions, and prints 0 as output if the equation has no integral solutions. The time factor is completely irrelevant in our consideration. Thus the procedure required is one which is effective, in the sense that it can be carried out by a computing machine.

The readers familiar with computer programming will find numerous examples to illustrate the notion of a procedure. There is, for a start, a programme which outputs 1 if the given input integer is a square, and outputs 0 otherwise. There is also a programme which outputs 1 if the given input integer is a prime number, and outputs 0 otherwise. Now it is true that one can write a programme so that, given the coefficients of a Diophantine equation as input, outputs 1 if the equation has integral solutions. This is done by testing the Diophantine equation successively wih integers. If and when a solution is found, output 1. The problem is that this programme works only when the given equation has a solution. If the equation has no solutions, the programme will instruct the computer to continue with its computations and never yields an output, i.e. the programme never halts (we imagine that there is an unlimited supply of computer time).

Let us summarise what we have obtained thus far. There are programmes which accept integers as inputs. These programmes contain instructions according to which the computer will do its computations. Let us order these programmes as Programme No. 1 (p_1), Programme No. 2 (P_2), . . ., Programme No. n (P_n), . . . Depending on the instructions given by P_n on input integer m, the computer may do one of the following: (a) It outputs 1; (b) it outputs 0; (c) it does not give an output. Let us call the programme P_n perfect if on any given input either (a) or (b) occurs. For each n, let C_n be all the integers m which when given as inputs for P_n, outputs 1. Now if P_n is perfect, it is possible to decide in finite amount of time whether any m is in C_n, namely make m the input and run the programme P_n. If the output is 1, then m is in C_n. If the output is 0, then m is not in C_n. We can then say that the programme P_n gives a procedure for deciding whether a given number is in C_n. Now

it is possible that for a given n, P_n is not perfect but C_n is equal to C_k for some k where P_k is perfect, (hence $n \neq k$). This may happen for example when both P_n and P_k test the divisibility of numbers by 2 with the following instructions:

P_n: If input is 2, give no output.
Otherwise, see if input is even.
If yes, output 1; otherwise output 0.

P_k: If input is 2, give output 0.
Otherwise, see if input is even.
If yes, output 1; otherwise output 0.

Notice that P_k is perfect but P_n is not. Both of them, however, do virtually the same thing. In fact $C_n = C_k$.

Let us call C_n decidable if it is equal to a C_k where P_k is perfect. We now ask the fundamental question: Is every C_n decidable? The answer is a resounding no. Let us write a programme P which does exactly the following things: Given input n, output 1 when n is in C_n. Then $P = P_k$ for some k. We claim that C_k is not decidable. For suppose that it is. Then $C_k = C_s$ for some s such that P_s is perfect. Introduce a new programme P_j such that for a given input r, P_j outputs 1 if P_s outputs 0, and P_j outputs 0 if P_s outputs 1. Is j in C_j? If j is in C_j, then by the instructions given for P_k, we know j is in C_k. And therefore, since $C_k = C_s$, j is in C_s. But then j is not in C_j. Conversely, if j is not in C_j, then j is not in C_n, and so j is not in C_s. But then j is in C_j. Hence either way we get a contradiction. We conclude that C_k is not decidable. In other words, there is a set C_k of integers for which no procedure exists to decide whether a given integer belongs to the set. Furthermore, this set C_k has the property that programme P_k yields output 1 on each input integer m in C_k.

But what do all of these have to do with Hilbert's Tenth Problem? Simply this: Firstly, given a Diophantine equation (of one variable say), one can associate with it a programme P_n so that C_n is precisely the set of integral solutions of the equation (this P_n may say: given m, if m is a solution of the equation, output 1. Otherwise output nothing). Note that it is not necessary to restrict one's attention to Diophantine equations of one variable only. Programmes can be written to accommodate Diophantine equations of several variables. And secondly, and this is the most significant point in our discussion, every C_n is the set of solutions of some Diophantine equation.

The answer to the Hilbert problem is now clear: since each C_n is the solution set of some Diophantine equation, we know that there is a procedure to decide if a given Diophantine equation has integral solutions if, and only if, there is a procedure to decide if a given number m belongs to a given set C_n. But we already know that there is a C_k which is undecidable. It follows that Hilbert's Tenth Problem is undecidable, i.e. no such decision procedure exists.

The solution to the Tenth Problem was found in 1970 by the Russian mathematician Matiasevič, building on the earlier results of M. Davis, H. Putnam and J. Robinson of the United States. It is exciting to note that the solution was based on the pioneering work of Gödel, Turing, Church and Kleene in the 1930's in the field of recursion theory, a subject which laid the foundation for modern day computer science. One could only marvel at Hilbert's penetrating insight in antici-

pating thirty years ahead of time the advent of a new branch of mathematics from which the solution to his Tenth Problem emerged seventy years after it was stated.

Of course the story of the Tenth Problem does not end here. It is known that there is a Diophantine equation with degree four where the solution set is undecidable. There is on the other hand a decision procedure for equations of degree two (work of C.L. Siegel of West Germany in 1972). Whether or not a decision procedure exists for degree three is unknown.

As for the number of variables in a Diophantine equation, it is known that no decision procedure exists for testing the solvability of equations with 13 variables. It is not difficult to come up with an algorithm to test equations with one unknown. For two variables, a decision method has been obtained by A. Baker of England and others for a wide class of Diophantine equations. Again nothing is known about three variables.

Finally, one of the interesting offshoots of the solution of Hilbert's Tenth Problem is the discovery that many sets of numbers are found to have Diophantine character. For example, there is a Diophantine equation whose set of solutions in positive integers is precisely the set of prime numbers. Before the proof it was thought highly unlikely that this was true, and this feeling had often been used as evidence against the correctness of the approach taken then to prove the unsolvability of Hilbert's Tenth Problem.