HILBERT'S 10TH PROBLEM

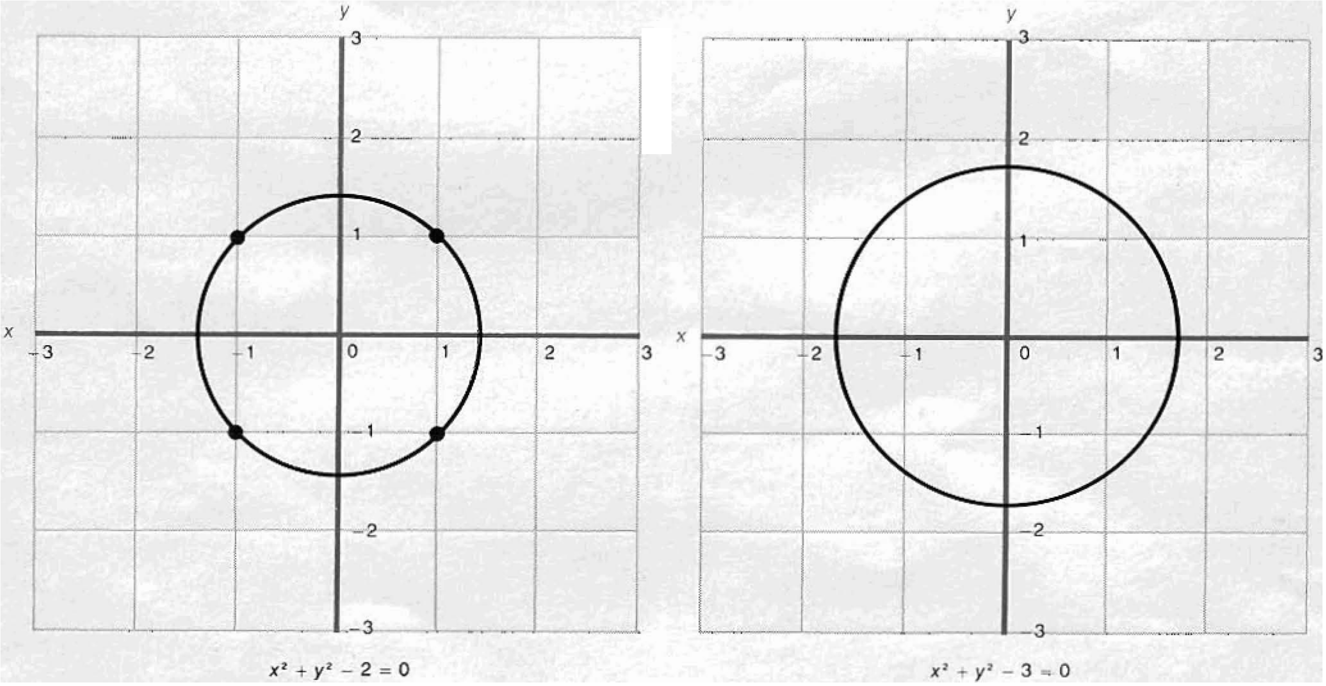
Can a procedure be devised that will indicate if there are solutions to a Diophantine equation (an equation where whole-number solutions are sought)? This question on a famous list has now been answered

by Martin Davis and Reuben Hersh

"We hear within us the perpetual call: there is the problem. Seek its solution. You can find it by pure reason, for in mathematics there is no *ignorabimus* [We shall not know]." So did David Hilbert address the Second International Congress of Mathematicians in Paris on August 8, 1900, greeting the new century by presenting a list of 23 major problems to challenge future mathematicians. Some of Hilbert's problems are still unsolved. Others have inspired generations of mathematical investigators and have led to major new mathematical theories. The most recently conquered of Hilbert's problems is the 10th, which was solved in 1970 by the 22-year-old Russian mathematician Yuri Matyasevich.

David Hilbert was born in Königsberg in 1862 and was professor at the University of Göttingen from 1895 until his death in 1943. After the death of Henri Poincaré in 1912 he was generally regarded as being the foremost mathematician of his time. He made fundamental contributions in several fields, but he is perhaps best remembered for his development of the abstract method as a powerful tool in mathematics.

Hilbert's 10th problem is easily described. It has to do with the simplest and most basic mathematical activity: solving equations. The equations to be solved are polynomial equations, that is, equations such as $x^2 - 3xy = 5$, which are formed by adding and multiplying constants and variables and by using whole-number exponents. Moreover, Hilbert specified that the equations must use only integers, that is, positive or negative whole numbers. No irrational



GRAPHS OF TWO EQUATIONS illustrate the difference between an ordinary equation and a Diophantine equation, for which one is interested only in whole-number solutions; this difference is central to Hilbert's 10th problem. The equations in point are $x^2 + y^2 - 2 = 0$ (*left*) and $x^2 + y^2 - 3 = 0$ (*right*); both are represented by circles with their center at the origin, that is, at the point with coordinates $x = 0$, $y = 0$. In the case of $x^2 + y^2 - 2 = 0$ the circle has a radius of $\sqrt{2}$. If the equation is treated as an ordinary equation, there are infinitely many solutions. If, however, it is treated as a Diophantine equation, there are only four solutions: (1) $x = 1, y = 1$, (2) $x = -1, y = 1$, (3) $x = 1, y = -1$, and (4) $x = -1, y = -1$. These solutions are represented by dots where the graph crosses the four points with those coordinates on the Cartesian grid. In the case of $x^2 + y^2 - 3 = 0$, the circle has a radius of $\sqrt{3}$. As an ordinary equation it has an infinite number of solutions; as a Diophantine equation, however, it has none at all.

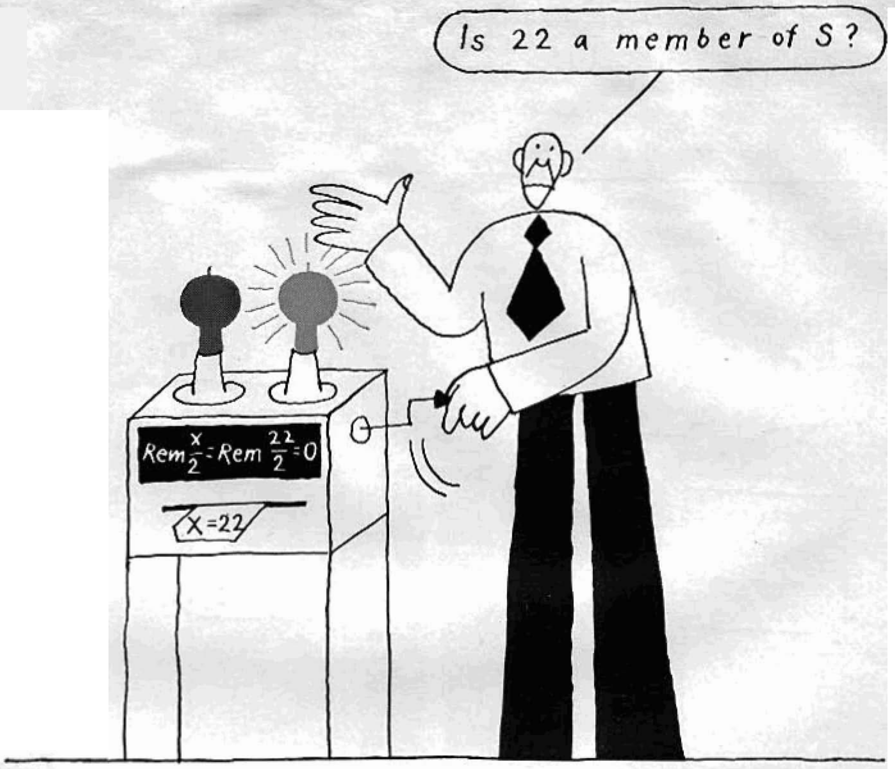
or imaginary numbers or even fractions are allowed in either the equations or their solutions. Problems of this type are called Diophantine equations after Diophantus of Alexandria, who wrote a book on the subject in the third century.

Hilbert's 10th problem is: Give a mechanical procedure by which any Diophantine equation can be tested to see if solutions exist. In Hilbert's words: "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." Hilbert does not ask for a process to find the solutions but merely for a process to determine if the equation has solutions. The process should be a clear-cut formal procedure that could be programmed for a computing machine and that would be guaranteed to work in all cases. Such a process is known as an algorithm.

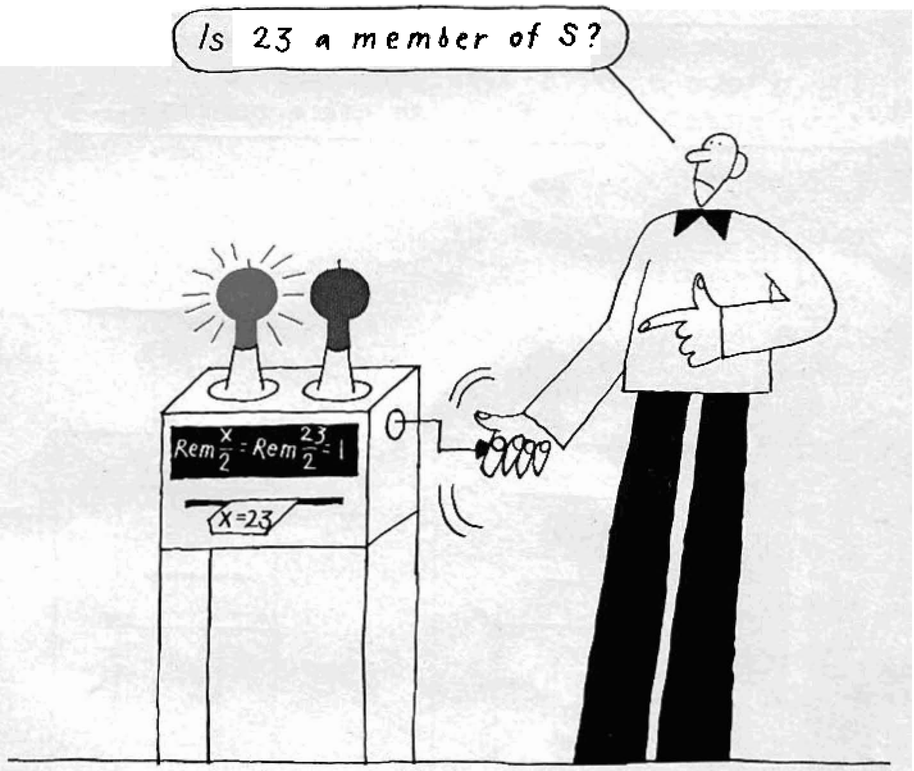
If Hilbert's problem is simply stated, Matyasevich' solution is even more simply stated: No such process can ever be devised; such an algorithm does not exist. Worded in this way, the answer sounds disappointingly negative. Matyasevich' result, however, constitutes an important and useful addition to the understanding of properties of numbers.

Matyasevich' work extended a series of researches by three Americans: one of us (Davis), Julia Robinson and Hilary Putnam. Their work in turn was based on earlier investigations by several founders of modern logic and computability theory: Alan Turing, Emil Post, Alonzo Church, Stephen Kleene and the same Kurt Gödel who is famous for his work on the consistency of axiomatic systems (Hilbert's second problem) and on the continuum hypothesis of Cantor (Hilbert's first problem).

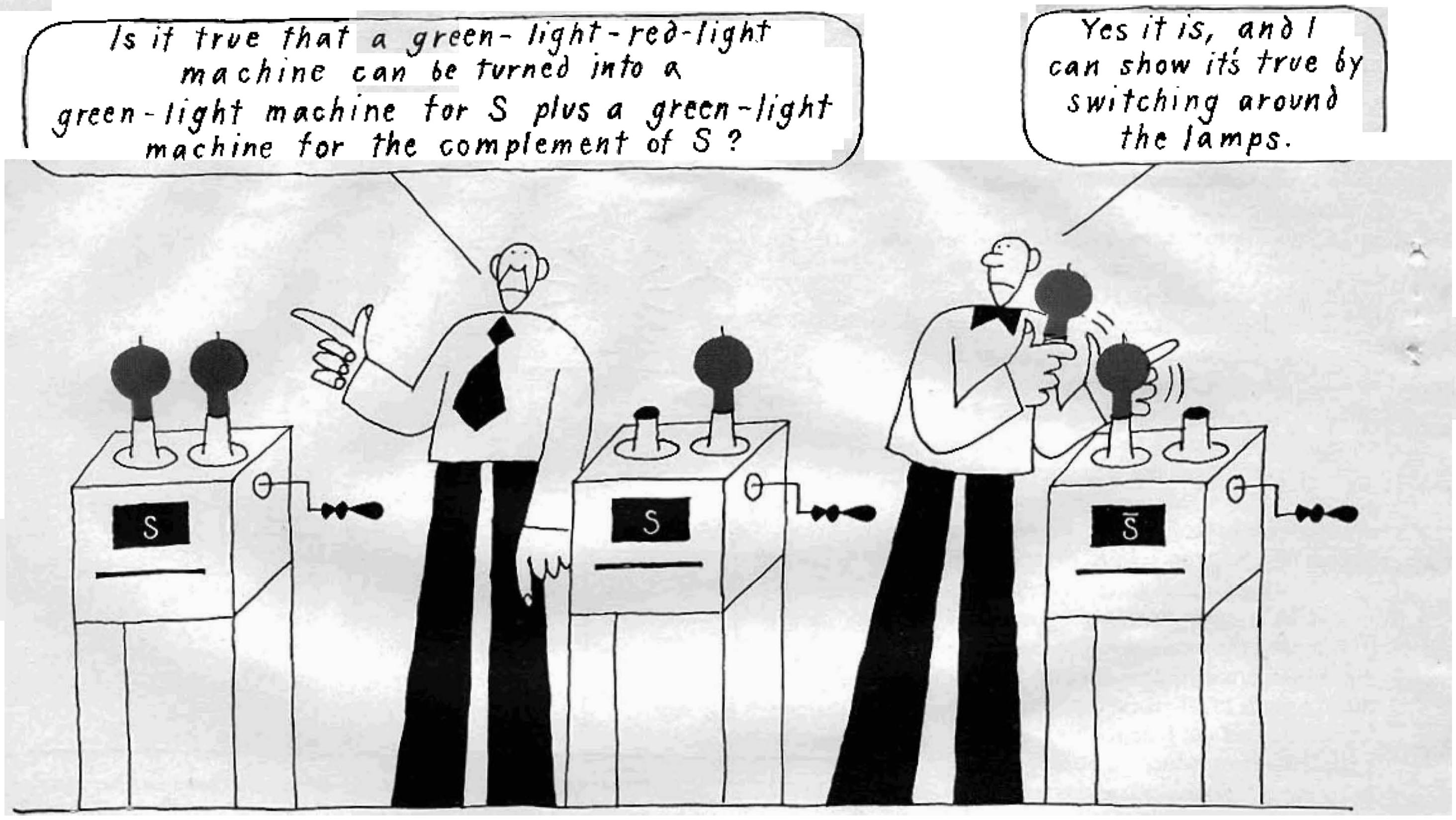
Let us start on Hilbert's 10th problem by looking at a few Diophantine equations. The term "Diophantine equation" is slightly misleading, because it is not so much the nature of the equation that is crucial as the nature of the admissible solutions. For example, the equation $x^2 + y^2 - 2 = 0$ has infinitely many solutions if one does not think of it as a Diophantine equation. The solutions are represented by the graph of the equation, which is a circle in the plane formed by the x axis and the y axis. The center of the circle is at the coordinates $x = 0$, $y = 0$. That point is called the origin; it is abbreviated (0,0). The radius of the circle is $\sqrt{2}$ [*see illustration on opposite page*]. The coordinates of any



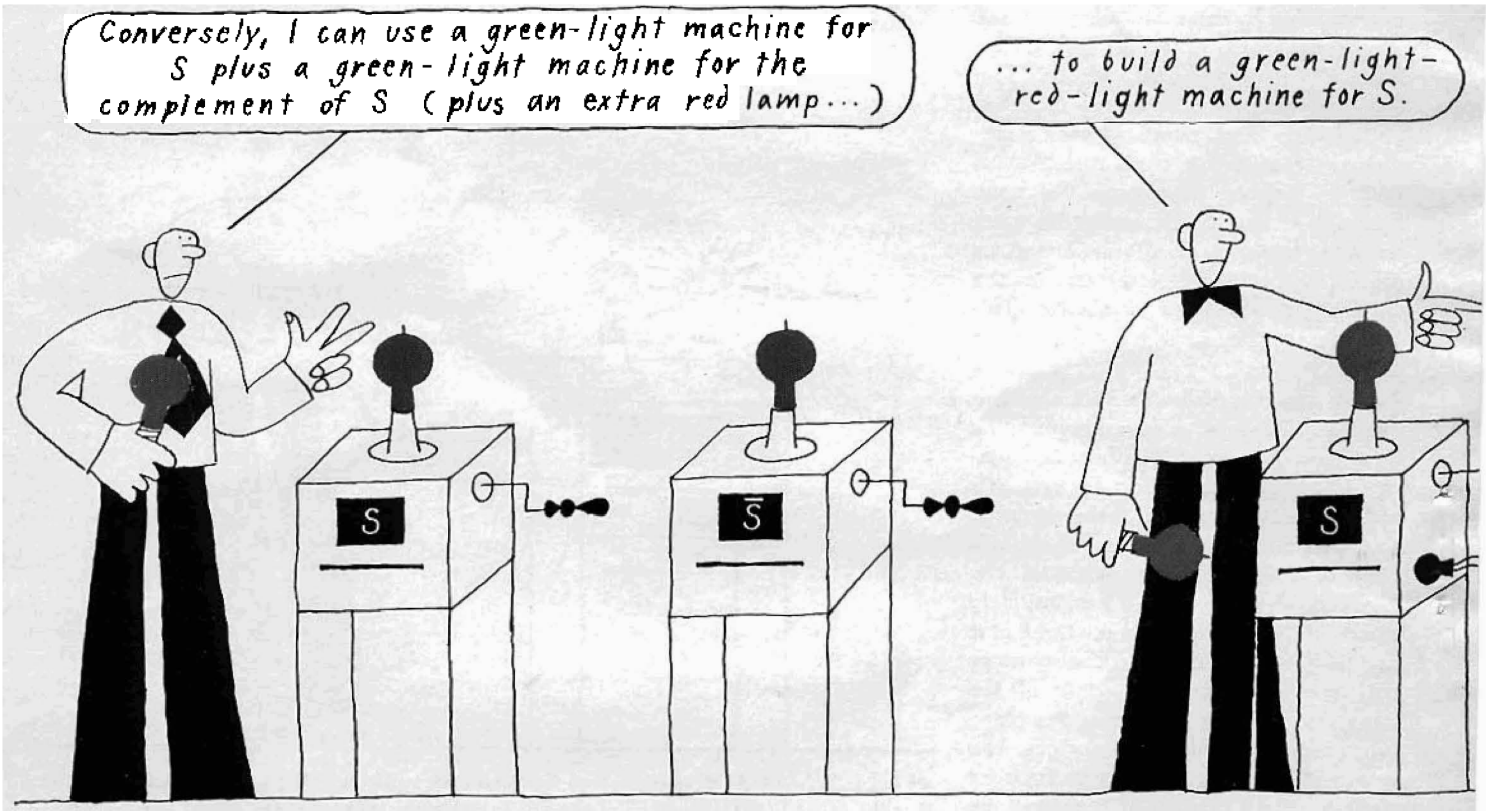
GREEN-LIGHT-RED-LIGHT MACHINE is an imaginary device that tests numbers to determine if they are members of a given set. Hilbert's 10th problem asks if a green-light-red-light "Hilbert machine" can be built to test Diophantine equations to see whether or not they have solutions. In the case of testing numbers for membership in a set, green light goes on if the machine can determine in a finite number of steps that a given input is a member of the set. Say that S is the set of all even numbers. To test inputs one can devise an algorithm for dividing each input x by 2. If the remainder of the division is 0 (written Rem $x/2 = 0$), machine would turn on its green light, signifying that x is a member of S.



RED LIGHT GOES ON on the green-light-red-light machine if the machine can determine that the input is not a member of the set. Suppose the input x is the whole number 23; 2 goes into 23 with a remainder of 1, signifying that 23 is not a member of S. Complement of set S is $\overline{S}$, the set of odd numbers; 23 is a member of $\overline{S}$. Since a green-light-red-light machine can be built to sort members of S from members of $\overline{S}$, the set S is called computable.


Is it true that a green-light-red-light machine can be turned into a green-light machine for S plus a green-light machine for the complement of S ?
Yes it is, and I can show it's true by switching around the lamps.
S
S
$\bar{S}$

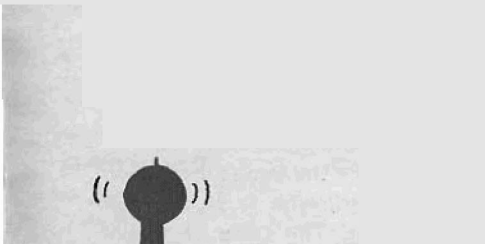
GREEN-LIGHT-RED-LIGHT MACHINE FOR THE SET *S* can be transformed into a green-light machine for *S* (that is, a machine that simply lights up when the input is a member of *S*) plus a green-light machine for $\bar{S}$, the complement of *S*. The proof is simple. To build a green-light machine for *S*, unscrew the red lamp of the green-light-red-light machine. To build a green-light machine for $\bar{S}$, unscrew the green lamp of the green-light-red-light machine and put it into the socket that held the red lamp. This fact can be stated in another way. If a set (such as *S*) is computable, then both the set and its complement (such as $\bar{S}$) are listable, that is, the members of *S* (in this case the set of even numbers) can be listed separately and sorted from the members of $\bar{S}$ (the set of odd numbers).


Conversely, I can use a green-light machine for S plus a green-light machine for the complement of S (plus an extra red lamp...)
... to build a green-light-red-light machine for S.
S
$\bar{S}$
S

GREEN-LIGHT MACHINE FOR EACH OF *S* AND $\bar{S}$ can be used to construct a green-light-red-light machine for the set *S*. This statement is the converse of the one for the top illustration on this page. In the green-light machine for $\bar{S}$ replace the green lamp with a red lamp. Then hook the machines in parallel so that the input goes into both simultaneously. The result is clearly a green-light-red-point on the circle satisfy the equation, and there are an infinite number of such points. If we consider the problem as a Diophantine equation, however, there are only four solutions: (1) $x = 1, y = 1$; (2) $x = -1, y = 1$; (3) $x = 1, y = -1$, and (4) $x = -1, y = -1$.

Suppose the equation is changed to $x^2 + y^2 - 3 = 0$. There are still an infinite number of solutions if it is treated as an ordinary equation but no solutions at all if it is treated as a Diophantine equation. The reason is that now the graph is a circle with radius equal to $\sqrt{3}$, and no points on this curve have both coordinates simultaneously equal to whole numbers.

A famous family of Diophantine equations has the form $x^n + y^n = z^n$, where n may equal 2, 3, 4 or any larger integer. If n is equal to 2, the equation is satisfied by the lengths of the sides of any right triangle and is called the Pythagorean theorem. One such solution is the set of numbers $x = 3$, $y = 4$, $z = 5$. If n is equal to or greater than 3, the equation is what is known as Fermat's equation. The 17th-century French mathematician Pierre de Fermat thought he had proved that these equations have no positive whole-number solutions. In the margin of his copy of Diophantus' book he wrote that he had found a "marvelous proof" that was unfortunately too long to be written down in that space. The proof (if indeed Fermat had one) has never been found. Known as Fermat's last theorem, it is probably the oldest and most famous unsolved problem in mathematics. These examples show that Diophantine equations are easy to write down but hard to solve. They are hard to solve because we are so exclusive about the kind of numbers we accept as solutions.



light machine. This assertion can be stated differently: If both a set and its complement are listable, then the set is computable.

For first-degree equations, that is, equations in which unknowns are not multiplied together and all exponents are equal to 1, such as $7x + 4y - 3z - 99t + 13u - 10 = 0$, the existence of solutions can be determined by a technique of division known since ancient times as Euclid's algorithm. For second-degree equations with two unknowns, such as $3x^2 - 5y^2 + 7 = 0$ or $x^2 - xy - y^2 = 1$, a theory developed early in the 19th century by the great Karl Friedrich Gauss enables one to determine whether there are any solutions. Recent work by the young British mathematician Alan Baker has shed considerable light on equations greater than the second degree that have two unknowns. For equations greater than the first degree that have more than two unknowns, there exist only some special cases that can be handled by special tricks, and a vast sea of ignorance.

Why is it so difficult to find a process such as the one Hilbert called for? The most direct approach would be to simply test all possible sets of values of the unknowns, one after another, until a solution is found. For example, if the equation has two unknowns, one could make a list of all pairs of integers. Then one would simply go through the list trying one pair after another to see if it satisfies the equation. This is certainly a clear-cut, mechanical procedure that a machine could carry out. What will be the result?

If the equation is the first one we mentioned, $x^2 + y^2 - 2 = 0$, one would test (0,0), (0,1), (1,0), (0,−1), (−1,0) and reject them all. The next candidate, (1,1), is a solution. We were lucky: only six pairs had to be considered. If, on the other hand, the equation were $x^2 + y^2 = 20{,}000$, one would have to test thousands of pairs of numbers before a solution was found. Still, it is clear that if a solution exists, it will be found in a finite number of steps.

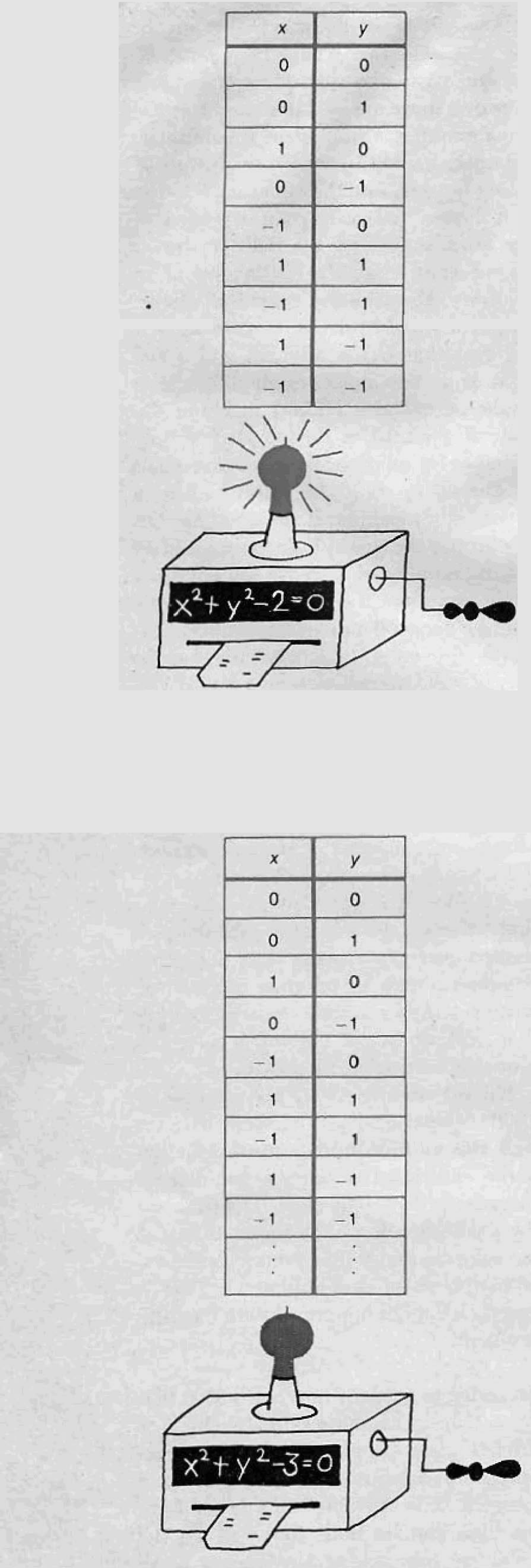
On the other hand, what about the second equation: $x^2 + y^2 - 3 = 0$? One can try pairs of integers from now till eternity, and all that will ever be known is that a solution has not been found yet. One would never know whether or not the next pair tried would be a solution. For this particular example it is possible to prove there are no solutions. But the proof requires a new idea; it cannot be obtained merely by successively substituting integers into the equation.

A device that carries out a process of the kind suggested by Hilbert should accept as an input the coefficients of an arbitrary Diophantine equation. As an output it should turn on a green light if the equation has a solution and a red light if it has none. Such a machine might be called a Hilbert machine. By way of contrast a device that simply searches for solutions by successive trials *ad infinitum* could be described as a green-light machine. If the equation has a solution, the green light goes on after a finite number of steps. If the equation has no solution, the computation simply goes on forever; unlike the Hilbert machine, the green-light machine has no way of knowing when to give up.

It is easy to build a green-light machine for Diophantine equations. The question is, can we do better and build a Hilbert machine, that is, a green-light-red-light machine that will always stop after a finite number of steps and give a definite yes or no answer? What Matyasevich proved is that this can never be done. Even if we allow the machine unlimited memory storage and unlimited computing time, no program can ever be written and no machine can ever be built that will do what Hilbert wanted. A Hilbert machine does not exist.

Hilbert continued in his address of 1900: "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." That is exactly what has happened with the 10th problem.

In order to explain how we know that no Hilbert machine exists, we have to discuss some simple ideas about computability. Suppose S stands for a set of integers. S is "listable" if a green-light machine can be built that will do the following job: accept any integer as an input, and as an output turn on a green light after a finite number of steps if and only if the input (the integer) belongs to S. For example, the set of even numbers is listable. In this case the machine would divide the input by 2 and turn on a green light if the remainder is 0. In mathematical literature such sets are called recursively enumerable; the word



x	y
0	0
0	1
1	0
0	−1
−1	0
1	1
−1	1
1	−1
−1	−1

x	y
0	0
0	1
1	0
0	−1
−1	0
1	1
−1	1
1	−1
−1	−1
⋮	⋮

PAIRS OF INTEGERS can be individually tested by green-light machines to see if they are solutions to Diophantine equations. Trial and error comes up with a solution for the equation $x^2 + y^2 - 2 = 0$ on the sixth try (*top*). Green-light machine testing equation $x^2 + y^2 - 3 = 0$ has no way of knowing when to give up, however, because there are no whole-number solutions (*bottom*). All it knows is that it has found no solutions yet.

"listable" is our informal equivalent.

The set S is "computable" if a green-light-red-light machine (similar to the Hilbert machine for Diophantine equations) can be built to do a more difficult job: accept any integer as input and, after a finite number of steps, turn on a green light if the integer is in S and a red light if the integer is not in S. For example, the set of even numbers is computable. The machine would divide the input by 2; if the remainder is 0, it turns on a green light, and if the remainder is 1, it turns on a red light [*see illustrations on page 85*].

There is a close connection between these two definitions. For the purposes of explanation, let $\bar{S}$ denote the complement of S, that is, the set of all integers that do not belong to S. If in the two examples S is the set of even integers, then $\bar{S}$ is the set of odd integers. We can prove that if S is computable, S and $\bar{S}$ are both listable. To put that statement another way: If a green-light-red-light machine exists for S, then there exists a green-light machine for S and a green-light machine for $\bar{S}$. The proof is simple. To build a green-light machine for S, just unscrew the red bulb of the green-light-red-light machine. To build a green-light machine for $\bar{S}$, unscrew the green bulb of the Hilbert machine and put it into the socket that held the red bulb.

The converse is also true: If S and $\bar{S}$ are listable, then S is computable. The equivalent of this statement is: If a green-light machine exists for each of S and $\bar{S}$, then a green-light-red-light machine can be built for S. This is easily done. In the green-light machine for $\bar{S}$, replace the green bulb with a red bulb. Then hook up the two machines in parallel, so that the input goes into both simultaneously. The result is clearly a green-light-red-light machine.

Knowing all of this, we can now state one of the crucial facts in computability theory, one that plays a central role in the solution of Hilbert's 10th problem: There is a set K that is listable but not computable! That is, there exists a green-light machine for K, but it is impossible to build a green-light machine for $\bar{K}$, the complement of K.

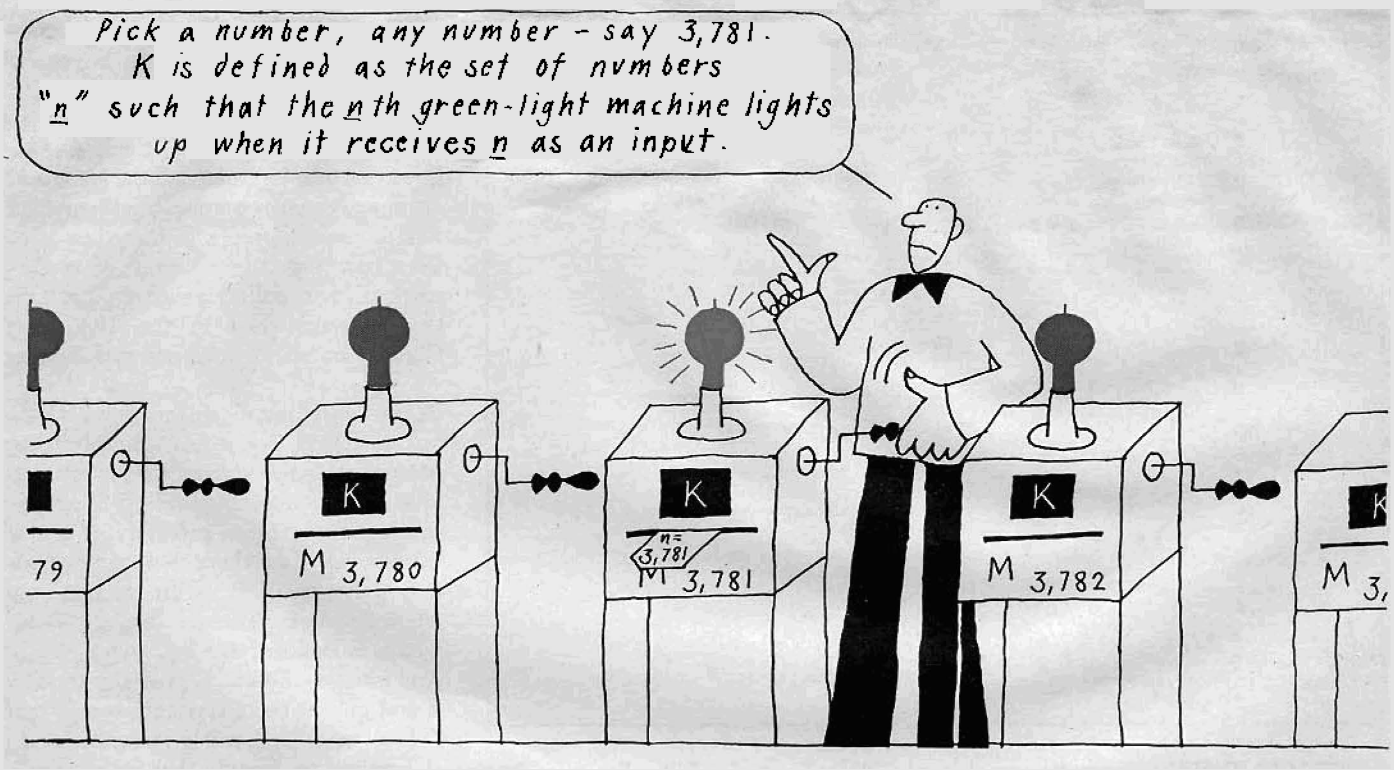
To prove this seemingly strange fact, let each green-light machine be specified by a detailed "customer's manual" in the English language. The customer's manual describes exactly how the machine is constructed. The customer's manuals can be set in order and numbered sequentially 1, 2, 3 and so on. In that way all green-light machines are numbered; M_1 is the first machine, M_2 is the second and so on. There is a subtle point hidden here. Such an ordered list of customer's manuals would not be possible for green-light-red-light machines. The difficulty is that one cannot tell from the manual whether the red light or the green light will turn on for any input to the corresponding machine.

The set K is defined as the set of numbers n such that the nth machine lights up when it receives n itself as an input. In other words, the number 1 belongs to K if and only if M_1 turns on its green light when "1" is entered into its input. The number 2 belongs to K if and only if M_2 eventually lights up when "2" is entered into its input, and so on [*see top illustration on opposite page*].

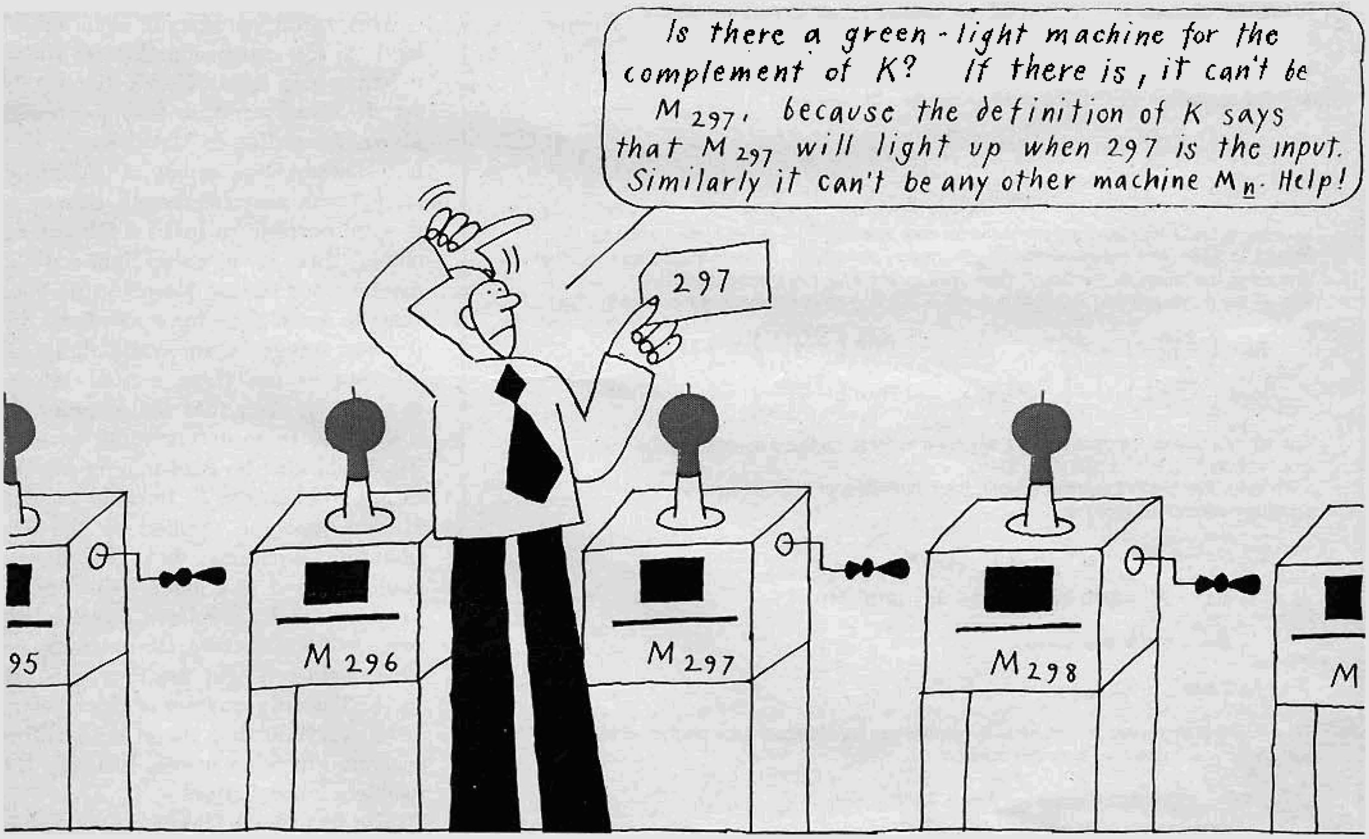
In order to build a green-light machine for K we need, along with the library of customer's manuals, a little man who can read them and carry out their instructions. He should perhaps be a wise old man, but he must be an obedient man who does exactly what he is told. We give the little man a number, say 3,781. The little man looks into customer's manual No. 3,781. Reading the manual, he is able to build the green-light machine $M_{3,781}$. Once this is done, he inserts the integer 3,781 as input into green-light machine $M_{3,781}$. If the green light goes on, the number 3,781 belongs to K. Thus we have a green-light machine for K.

What about $\bar{K}$? How can we be sure there is no green-light machine for it? Well, suppose there were such a machine. Then since $\bar{K}$ is the complement of K, this machine should light up for any input, say for 297, if and only if M_{297} does *not* light up for 297. (If M_{297} lit up, it would mean that the integer 297 belongs to K and not to $\bar{K}$.) Thus the machine for $\bar{K}$ certainly is not the same as M_{297} [*see bottom illustration on opposite page*]. By the same token, however, it is not the same as M_n for any other value of n. The same argument would apply to any other number just as well as to 297, and it shows that no green-light machine for $\bar{K}$ appears anywhere in the library of customer's manuals. Since every possible green-light machine eventually turns up in our list, it follows that no green-light machine for $\bar{K}$ can possibly exist. That is to say, $\bar{K}$ is not listable.

The result is certainly remarkable. It deserves contemplation and appreciation. We know perfectly well what the set K is; in principle we can produce as much of it as we wish with a computer printout. Nevertheless, there can never be a formal procedure (an algorithm or a machine program) for sorting K from


Pick a number, any number - say 3,781. K is defined as the set of numbers "n" such that the nth green-light machine lights up when it receives n as an input.
79
K
M 3,780
K
n= 3,781
M 3,781
K
M 3,782
K
M 3,

THE SET K IS LISTABLE, that is, a green-light machine for K exists. Let all conceivable green-light machines be numbered: M_1 is the first machine, M_2 is the second machine, M_3 is the third machine and so forth up to the nth machine. K is defined as the set of numbers n such that the nth machine lights up when it receives n itself as an input. In the illustration a little man has entered the number 3,781 as an input to $M_{3,781}$ and the green light has turned on, indicating that the whole number 3,781 is a member of set K.


Is there a green-light machine for the complement of K? If there is, it can't be M 297, because the definition of K says that M 297 will light up when 297 is the input. Similarly it can't be any other machine M n. Help!
297
95
M 296
M 297
M 298
M

THE SET K IS NOT COMPUTABLE, that is, no green-light machine exists for $\overline{K}$, the complement of K. Suppose there was such a green-light machine for $\overline{K}$. Since $\overline{K}$ is the complement of K, this machine should light up for any input, say for 297, if and only if M_{297} does not light up for 297. Thus the machine for $\overline{K}$ is certainly not the same as M_{297}. By the same token, it is not the same as M_n for any other value of n. Thus no green-light machine exists for $\overline{K}$, meaning that $\overline{K}$ is not listable. A listable set whose complement is not listable is not computable; no green-light-red-light machine can be built for it. Thus there is no algorithm for sorting K from $\overline{K}$.

1. 1

2. 1

3. $1 + 1 = 2$

4. $1 + 2 = 3$

5. $2 + 3 = 5$

6. $3 + 5 = 8$

7. $5 + 8 = 13$

8. $8 + 13 = 21$

9. $13 + 21 = 34$

10. $21 + 34 = 55$

11. $34 + 55 = 89$

12. $55 + 89 = 144$

13. $89 + 144 = 233$

.
.
.

$\underline{n}$ $\approx \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^{\underline{n}}$

FIBONACCI NUMBERS were discovered in A.D. 1202 by Leonardo of Pisa, known as Fibonacci. The sequence is obtained by starting with 1 and 1 and successively adding the last two numbers to get the next one. The sequence grows exponentially: the *n*th number in the sequence is approximately proportional to the *n*th power of the real number $[(1 + \sqrt{5})/2]^n$.

PROBLEM: To find the smallest number *n* that has the remainders of 4, 2, 3 and 1 when it is divided by 10, 3, 7 and 11.

SOLUTION: Let *x* be the number sought. "Rem" will be the abbreviation for "The remainder of . . . ." The problem can then be rewritten:

$$\text{Rem}\left(\frac{x}{10}\right) = 4 \qquad \text{Rem}\left(\frac{x}{7}\right) = 3$$

$$\text{Rem}\left(\frac{x}{3}\right) = 2 \qquad \text{Rem}\left(\frac{x}{11}\right) = 1$$

In order to find *x* four auxiliary problems for new unknowns y_1, y_2, y_3 and y_4 must be solved. In each case the numerator is obtained by multiplying three of the divisors together and using the fourth as the denominator. For example, in the first equation with y_1 the numerator 231 is equal to $3 \times 7 \times 11$, and 10 is put in the denominator:

$$\text{Rem}\left(\frac{231y_1}{10}\right) = 4, y_1 < 10 \qquad \text{Rem}\left(\frac{330y_3}{7}\right) = 3, y_3 < 7$$

$$\text{Rem}\left(\frac{770y_2}{3}\right) = 2, y_2 < 3 \qquad \text{Rem}\left(\frac{210y_4}{11}\right) = 1, y_4 < 11$$

The set of smallest integers that are solutions to these auxiliary equations is $y_1 = 4$, $y_2 = 1$, $y_3 = 3$ and $y_4 = 1$.

To get *x* (the original number sought) the numerators of the four auxiliary equations are added together:

$$x = (231y_1) + (770y_2) + (330y_3) + (210y_4)$$

$$= (231 \times 4) + (770 \times 1) + (330 \times 3) + (210 \times 1)$$

$$= 924 + 770 + 990 + 210$$

$$= 2{,}894$$

Thus 2,894 is one value of *x*. A smaller number can be obtained if the product of all four divisors is subtracted from this solution:

$$2{,}894 - (10 \times 3 \times 7 \times 11) = 2{,}894 - 2{,}310 = 584.$$

Therefore 584 is the smallest solution to the problem

CHINESE REMAINDER THEOREM is used in the solution to Hilbert's 10th problem. In this case the theorem is employed to find a number whose remainders, when divided by the numbers 10, 3, 7 and 11, are respectively 4, 2, 3 and 1. Integer 584 is the smallest solution.

K. Thus here is an example of a precisely stated problem that can never be solved by mechanical means.

This discussion has of course been informal and nonrigorous. It is possible, however, to reformulate all the ideas and arguments with precise mathematical definitions and proofs. In fact, they have been formulated in a branch of mathematical logic called recursive function theory, established in the 1930's by Gödel, Church, Post, Kleene and Turing.

Now, what has all this to do with Diophantine equations? Simply this. Matyasevich has proved that every listable set has a corresponding Diophantine equation. More precisely, if *S* is a listable set, then there is a corresponding polynomial *P*, with integer coefficients and variables $x, y_1, y_2, \ldots, y_n$, which is denoted by $P_S(x, y_1, y_2, \ldots, y_n)$. Any integer, such as 17, belongs to set *S* if and only if the Diophantine equation $P(17, y_1, y_2, \ldots, y_n) = 0$ has a solution.

It might be thought that for some sets we would have to resort to inconceivably complicated polynomials, but this is not the case. The degree of *P* need not exceed the fourth power; the number of variables $y_1, y_2, \ldots, y_n$ need not exceed 14. (No one knows yet if both of these bounds can be achieved simultaneously.)

This result of Matyasevich' quickly leads to the conclusion that no Hilbert machine can exist. Recall the listable set *K* constructed a few paragraphs above. According to Matyasevich, there is a Diophantine equation, $P_K(x, y_1, y_2, \ldots, y_n) = 0$, associated with this set. If it were possible to build a Hilbert machine, that is, a green-light-red-light machine for testing Diophantine equations to see if they have solutions, then for any integer *x* we could determine whether or not there existed integers $y_1, y_2, \ldots, y_n$ such that the equation has a solution. In so determining, however, we would also be determining whether or not *x* belongs to *K*. In other words, a Hilbert machine applied to the Diophantine equation that describes *K* could be used as a green-light-red-light machine for *K*. We have proved, however, that *K* is not computable, so that no green-light-red-light machine can exist for *K*. The only way out of this dilemma is to conclude that there is no Hilbert machine. In other words, Hilbert's 10th problem is unsolvable!

The fact that a Diophantine equation is associated with every listable set is a positive result that is of great interest in itself, quite aside from its application to Hilbert's 10th problem. A particularly important and interesting set of integers is the set of prime numbers. A prime number is one that is factorable (divisible) only by 1 and by itself. Some examples are 2, 3, 5, 7, 11, 13 and 17. That they are listable is rather obvious. An algorithm for listing them has come down from the Greeks with the name of "the sieve of Eratosthenes." Combining Matyasevich' result with a device developed by Putnam, we obtain a Diophantine equation $Q(y_1,y_2,\ldots,y_n) = z$ such that a positive number z is a prime if and only if this equation has a positive integer solution $y_1,y_2,\ldots,y_n$. (The exact form of the polynomial Q is a bit too complicated to fully write out here.)

Another remarkable result can be proved by combining Matyasevich' theorem with Gödel's work on undecidability. If there is any system of axioms whatsoever from which information can be deduced about Diophantine equations, one can always obtain a particular Diophantine equation that has the following properties: (1) the equation has no positive integer solutions and (2) the fact that it has no positive integer solutions cannot be logically deduced from the given set of axioms. Of course, once the Diophantine equation is obtained we can make up a new set of axioms from which one can prove that the Diophantine equation has no solution. But then this new set of axioms will give rise to another Diophantine equation for which the same can be asserted.

What went into the proof of Matyasevich' theorem? In addition to the results from classical and even ancient number theory that we have already mentioned, there is a key result known as the Chinese remainder theorem. It will be helpful to illustrate the Chinese remainder theorem by a numerical example.

Suppose one wishes to find a number whose remainders, when divided by the numbers 10, 3, 7 and 11, are respectively 4, 2, 3 and 1 [*see bottom illustration on opposite page*]. The Chinese remainder theorem assures us that there must be such a number. (In fact, in this case 584 is such a number.) All that is required for the Chinese remainder theorem to work is that no pair of the divisors used have any common factor (except, of course, 1). There can be any number of divisors, and the desired remainders can be any positive integers whatsoever.

In 1931 Gödel showed how to use the Chinese remainder theorem as a coding trick, in which an arbitrary finite sequence of numbers can be encoded as a single number. From the code number one recovers the sequence in the same way that 4, 2, 3 and 1 are obtained from 584 in the example—as remainders in successive divisions. The divisors can be chosen to be in arithmetic progression.

The first attempt to prove that a Hilbert machine cannot exist was made by one of us (Davis) in his doctoral dissertation in 1950. Gödel's technique of using the Chinese remainder theorem as a coding device was applied to associate a Diophantine equation, $P_S(k,x,z,y_1,y_2,\ldots,y_n) = 0$, with every listable set S. Unfortunately the relation between the set and the equation turned out to be more complicated than what was needed for Hilbert's 10th problem. Specifically, the relation was: A positive integer x belongs to the set S if and only if for some positive integer value of z it is possible to find a solution for every one of the Diophantine equations obtained by substituting $k = 1$, then $k = 2$ and so on up to z into the equation $P_S(k,x,z,y_1,y_2,\ldots,y_n) = 0$. Although the result seemed tantalizingly close to what was needed, it was only a beginning.

At about the same time Robinson began her own investigations of sets that can be defined by Diophantine equations. She developed various ingenious techniques for dealing with equations whose solutions behaved like exponentials (grew like a power). In 1960 she, Davis and Putnam collaborated in proving another result. They made use of both her work and Davis' result to show that to any listable set there corresponded a Diophantine equation of an "extended" kind, extended in the sense that variables in the equation were allowed to occur as exponents. An example of such an equation is $2^t + x^2 = z^3$. Davis, Robinson and Putnam combined their work with some of Robinson's earlier results and discovered the following: If even one Diophantine equation could be found whose solutions behaved exponentially in an appropriate sense, then it would be possible to describe every listable set by a Diophantine equation. This would in turn show that Hilbert's 10th problem is unsolvable.

It took a decade to find a Diophantine equation whose solutions grow exponentially in the appropriate sense. In 1970 Matyasevich found such an equation by using what are known as the Fibonacci numbers. These celebrated numbers were discovered in A.D. 1202 by Leonardo of Pisa, who was also known as Fibonacci. He found them by computing the total number of pairs of descendants of one pair of rabbits if the original pair and each offspring pair reproduced itself once a month. The Fibonacci series is obtained by starting with 1 and 1 and successively adding the preceding two numbers to get the next: the first Fibonacci number is 1, the second is 1, the third is 1 + 1 = 2, the fourth is 1 + 2 = 3, the fifth is 2 + 3 = 5 and so on. The property that is important for Hilbert's 10th problem is that the Fibonacci numbers grow exponentially. That is, the nth Fibonacci number is approximately proportional to the nth power of a certain fixed real number.

I. $u + w - v - 2 = 0$

II. $l - 2v - 2a - 1 = 0$

III. $l^2 - lz - z^2 - 1 = 0$

IV. $g - bl^2 = 0$

V. $g^2 - gh - h^2 - 1 = 0$

VI. $m - c(2h + g) - 3 = 0$

VII. $m - fl - 2 = 0$

VIII. $x^2 - mxy + y^2 - 1 = 0$

IX. $(d - 1)l + u - x - 1 = 0$

X. $x - v - (2h + g)(e - 1) = 0$

MATYASEVICH' SOLUTION to Hilbert's 10th problem involves a Diophantine equation that is obtained by squaring each of these 10 equations and then adding them together and setting the resulting complicated polynomial equal to zero. In these equations the values u and v in the solutions are related in such a way that v is the $2u$th Fibonacci number. From the solution it followed that for every listable set there is an associated Diophantine equation. Since there exist listable sets whose complements are not listable, then not every listable set can have a green-light-red-light machine. Since having a green-light-red-light machine for a set is equivalent to having a Hilbert machine for Diophantine equations, Matyasevich' result means that no Hilbert machine can be built to test Diophantine equations.

If one could find a Diophantine equation whose solutions relate n to the nth Fibonacci number, it would be the desired example of a Diophantine equation whose solutions behave exponentially. The solution of Hilbert's 10th problem would follow from this example. What Matyasevich did was to construct such a Diophantine equation [*see illustration above*]. Once he had shown that the set of Fibonacci numbers is associated in this way with a Diophantine equation, it followed immediately from the theorem of Davis, Robinson and Putnam that for every listable set there is an associated Diophantine equation, including in particular the set K, which is not computable. And so ends the story of Hilbert's 10th problem.