HILBERT'S 10TH PROBLEM

JASON MEDCOFF

Diophantine equations are of major interest in elementary number theory; for example, Bézout's identity

$$ax + by = d$$

relates multiples of a and b to their greatest common divisor, d, and is clearly a linear Diophantine equation. Finding solutions to such equations is the central study of Diophantine analysis. For many Diophantine equations, however, solutions do not exist. As a simple example, take $x^2 + 1 = 0$. It is easily seen that no solution to this equality exists in $\mathbb{Z}$. Therefore, the Diophantine equation has no solution. Given more complex examples, verifying the existence of a solution to an equation becomes increasingly difficult.

In 1900, mathematician David Hilbert proposed a list of 23 unsolved problems varying wildly in precision and topic. Problem 10 in this list asks about Diophantine equations:

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

"Rational integers" are interpreted to mean the familiar integers $\mathbb{Z}$. We can also infer that by asking for a "process", Hilbert wanted an algorithm. So, the problem asks for a general algorithm to decide whether an arbitrary Diophantine equation has solutions. Note that we are not concerned with finding the solutions themselves. We would only like to know whether solutions exist.

A related concept to Diophantine equations is the Diophantine set. Given an equation written as $p(x_1, x_2, ..., x_i, a_1, a_2, ..., a_j) = 0$, a Diophantine set S is a subset of $\mathbb{N}^i$ such that

$$\bar{x} \in S \iff \exists \bar{a} \in \mathbb{N}^j : p(\bar{x}, \bar{a}) = 0.$$

In other words, the Diophantine set gives the values of x for which an associated Diophantine equality holds true. From the definition, we can see that if the Diophantine set is empty, the associated equation is unsatisfiable. So, we can restate Hilbert's tenth problem succinctly by asking whether a certain Diophantine set is empty.

We can also introduce recursively enumerable sets. A set is said to have this property if there exists an algorithm that enumerates the elements of the set. In other words, given a recursively enumerable set E, we can write a program that

outputs every element e_1, e_2, ... in the set. There is little other restriction on E; it can be a countably infinite set and our program would still work. Such a program is said to be undecidable.

Hilbert's tenth problem has been proven impossible. Yuri Matiyasevich showed in 1972 that every recursively enumerable set is Diophantine. Since we can create examples of the former that are countably infinite, there are Diophantine sets that are countably infinite. Then we have Diophantine sets which are undecidable, and thus there cannot be a decidable algorithm that determines the satisfiability of any arbitrary Diophantine equation.

Since Matiyasevich's paper, some interesting further work has been done in the area. Hilbert's original postulation can be asked not only for integers, but for other rings of interest in algebraic number theory. The tenth problem has been shown unsolvable for some algebras. In addition, Matiyasevich went on to show that by increasing the degree of the polynomial, Diophantine equations can be reduced to eleven unknowns in the integers, and nine unknowns in the natural numbers.