HILBERT'S 10^{TH} PROBLEM

JASON MEDCOFF

1. Diophantine Equations and General Satisfiability

At the turn of the twentieth century, German mathematician David Hilbert gave a lecture to the International Congress of Mathematicians in Paris, France. The paper outlined 23 unsolved problems. The tenth problem 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 in a finite number of operations whether the equation is solvable in rational integers."

By "rational integers", we understand that the numbers in question belong to $\mathbb{Z}$. A process that makes a decision in a finite number of operations is informally the definition of an algorithm in modern mathematical vernacular. So, the problem statement asks for an algorithm that takes as an input some Diophantine equation, and outputs YES if there exists a solution in integers, and NO otherwise. Note that the problem statement asks nothing about the solutions themselves, but only about their existence.

A Diophantine equation is a polynomial with integer coefficients of the form

$$D(x_1, x_2, \ldots, x_n) = 0 \tag{1}$$

such that only integral solutions are considered; some $\langle x_1, x_2, \ldots, x_n \rangle$ satisfying (1) must also satisfy

$$\langle x_1, x_2, \ldots, x_n \rangle \in \mathbb{Z}^n$$

to be considered a solution to (1).

2. What it means to be Diophantine

From Diophantine equations, we can devise new terminology to associate with these equations other mathematical objects, namely sets and functions.

Definition 2.1. A set S is said to be Diophantine if there exists a polynomial

$$D(x_1, \ldots, x_n, y_1, \ldots, y_m)$$

with integer coefficients where an n-tuple $\langle x_1, \ldots, x_n \rangle$ belongs to S if and only if there exists $y_1, \ldots, y_m$ such that

$$D(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0.$$

Equivalently, we can say

$$\langle x_1, \ldots, x_n \rangle \in S \iff \exists y_1, \ldots, y_m : D(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0.$$

Now, the notion of Diophantine equations has been extended to sets as well. Intuitively, if we have a Diophantine equation with some parameters, the parameters belong to a Diophantine set if the equation is satisfiable under them.

As an example, consider the set

$$S = \{\langle x_1, x_2, x_3 \rangle : x_3 = x_1 + x_2; x_1, x_2 \in \mathbb{N}\}.$$

We can say with certainty that this set is Diophantine. By the definition, $\langle x_1, x_2, x_3 \rangle$ is in S if and only if there exist y_1, y_2, y_3 that satisfy $D(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$ for some polynomial D with integer coefficients. It is easy to show that if we take D to be

$$x_1 y_1 + x_2 y_2 - x_3 y_3,$$

the above equation is satisfied for every $\langle x_1, x_2, x_3 \rangle$ in S.

It is also possible to extend the notion of "being Diophantine" to functions.

Definition 2.2. A function f is considered Diophantine if the set of solutions to the function is Diophantine; namely, f is Diophantine if the set

$$\{\langle x_1, \ldots, x_n, y \rangle : y = f(x_1, \ldots, x_n)\}$$

is Diophantine.

As a simple example, consider $f : \mathbb{N} \to \mathbb{N}$ such that

$$f(n) = n(n-1)(n-2)\ldots(2)(1) = n!$$

This function is Diophantine because the set of solutions to $m = f(n)$ is Diophantine. Specifically, we have

$$\{\langle m, n \rangle : m = n(n-1)(n-2)\ldots(2)(1)\}$$

and we know that for every n, m is a natural number, since the product of natural numbers is a natural number. We can construct a polynomial equation

$$my_1 - ny_2 = 0$$

which is satisfied for any y_1, y_2 with m and n as described by the above set.

Proposition 1. *The function*

$$expt(a, b) = a^b$$

is Diophantine.

Proof. □