Diophantine set

Canonical name	DiophantineSet
Date of creation	2013-03-22 18:02:50
Last modified on	2013-03-22 18:02:50
Owner	CWoo (3771)
Last modified by	CWoo (3771)
Numerical id	13
Author	CWoo (3771)
Entry type	Definition
Classification	msc 03D99
Classification	msc 03D80
Defines	Diophantine function

A set S is said to be *Diophantine* if

- it is a subset of $\mathbb{N}^n$, the set of all n-tuples of positive integers, and
- there is a polynomial p over $\mathbb{Z}$ in $n+k$ variables, $k \geq 0$, such that $x \in S$ iff there is some $y \in \mathbb{N}^k$, such that $p(x, y) = 0$.

So S can be thought of as a set such that, there is a Diophantine equation $p = 0$ and a non-negative integer k, so that when each element in S is "combined" with some k-tuple, makes up a solution to a Diophantine equation $p = 0$. In other words, if $f_n^{n+k} : \mathbb{N}^{n+k} \to \mathbb{N}^n$ is a projection function given by $f_n^{n+k}(x, y) = x$ where $x \in \mathbb{N}^n$ and $y \in \mathbb{N}^k$, then S is a Diophantine set iff $S = f_n^{n+k}(Z)$, where Z is the zero set of some Diophantine equation $p = 0$. Equivalently, a set $S \in \mathbb{N}^n$ is Diophantine if there is a $p \in \mathbb{Z}[X_1, \ldots, X_{n+k}]$, such that

$$S = \{x \in \mathbb{N}^n \mid \exists y \in \mathbb{N}^k \; p(x, y) = 0\}.$$

For example, $\mathbb{N}$ itself is Diophantine, for the polynomial $p(x, y) = x - y$ works. Another trivial example: the set of all positive integers divisible by 3 is Diophantine, for the polynomial $p(x, y) = x - 3y$ works.

For a less trivial example, let us show that the set of all triples (a, b, c) such that $a \leq b \leq c$ is Diophantine. For the inequality $a \leq b$, let $p(x_1, x_2, y) = x_2 - x_1 - (y - 1)$. Then the sentence $\exists y \; p(x_1, x_2, y) = 0$ is equivalent to $x_1 \leq x_2$. Similarly, for the inequality $b \leq c$, we have the same polynomial p. Putting the two inequality together amounts to setting $q(x_1, x_2, x_3, y_1, y_2) = p(x_1, x_2, y_1)^2 + p(x_2, x_3, y_2)^2$. Thus, the sentence $\exists(y_1, y_2) \; q(x, y) = 0$, where $x = (x_1, x_2, x_3)$ and $y = (y_1, y_2)$ is the same as the inequality $x_1 \leq x_2 \leq x_3$.

Some other Diophantine sets are:

- the set $A = B \cup C$, where B and C are Diophantine
- the set $A = B \cap C$, where B and C are Diophantine
- the set $\{a \mid a \equiv b \pmod{n}\}$
- the set of composite numbers
- the set of prime numbers
- the set of powers of a positive integer $\{m^n \mid n = 0, 1, \ldots\}$

Remark. Associated with the concept of a Diophantine set is that of a *Diophantine function*: a function f is said to be *Diophantine* if its graph $\{(x, f(x)) \mid x \in \mathrm{dom}(f)\}$ is a Diophantine set. Some well-know Diophantine functions are the exponential functions $f(x) = n^x$ and the factorial function $f(x) = x!$, where n, x are positive integers.

It turns out that a function is Diophantine iff it is recursive. From this, it is possible to prove that Hilbert's 10th problem is unsolvable.

The idea behind using Diophantine sets to prove the unsolvability of Hilbert's 10th problem comes from Yuri Matiyaseviĉ, and hence the theorem is known as Matiyaseviĉ's theorem.

References

[1] M Davis, *Computability and Unsolvability*. Dover Publications, Inc. New York, 1982