BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 3, Number 2, September 1980

UNDECIDABLE DIOPHANTINE EQUATIONS

BY JAMES P. JONES

In 1900 Hilbert asked for an algorithm to decide the solvability of all diophantine equations, $P(x_1, \ldots, x_\nu) = 0$, where P is a polynomial with integer coefficients. In special cases of Hilbert's tenth problem, such algorithms are known. Siegel [7] gives an algorithm for all polynomials $P(x_1, \ldots, x_\nu)$ of degree $\leqslant 2$. From the work of A. Baker [1] we know that there is also a decision procedure for the case of homogeneous polynomials in two variables, $P(x, y) = c$.

The first steps toward the eventual negative solution of the entire (unrestricted) form of Hilbert's tenth problem, were taken in 1961 by Julia Robinson, Martin Davis and Hilary Putnam [2]. They proved that every recursively enumerable set, W can be represented in exponential diophantine form

$$x \in W \Leftrightarrow \exists x_1, x_2, \ldots, x_\mu \; P(x, x_1, \ldots, x_\mu, 2^{x_1}, \ldots, 2^{x_\mu}) = 0,$$

where P is a polynomial with integer coefficients and $x_1, \ldots, x_\mu$ range over positive integers.

In 1970 Ju. V. Matijasevič [4] proved that the exponential relation, $y = 2^x$ is diophantine and hence that every r.e. set W can be represented in polynomial (diophantine) form

$$x \in W \Leftrightarrow \exists x_1, x_2, \ldots, x_\nu \; P(x, x_1, x_2, \ldots, x_\nu) = 0,$$

where the unknowns $x_1, \ldots, x_\nu$ range over positive integers.

Since there exist r.e. nonrecursive sets, Matijasevič's Theorem implies the undecidability of Hilbert's tenth problem. There is no algorithm to decide whether an arbitrary diophantine equation has a solution.

Matijasevič's Theorem implies also the existence of particular undecidable diophantine equations. In fact there must exist *universal* diophantine equations, polynomial analogues of the universal Turing machine. This follows from the well-known fact that the r.e. sets, $W_1, W_2, \ldots,$ can be listed in such a way that the binary relation, $x \in W_v$, is r.e. Hence by [2], [4] there exists a universal polynomial $U(x, v, x_1, \ldots, x_\nu)$ with the property

$$x \in W_v \Leftrightarrow \exists x_1, \ldots, x_\nu \; U(x, v, x_1, \ldots, x_\nu) = 0.$$

Thus a single polynomial, in a fixed degree and a fixed number of unknowns, can define every r.e. set, by mere change of a parameter v. The existence of such

Received by the editors March 5, 1980.

AMS (*MOS*) *subject classifications* (1970). Primary 02F25, 10N05; Secondary 10B15.