PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 35, Number 2, October 1972

ON THE NUMBER OF SOLUTIONS OF DIOPHANTINE EQUATIONS

MARTIN DAVIS[1]

ABSTRACT. For any nontrivial set of cardinal numbers $\leqq\aleph_0$, it is shown that there is no algorithm for testing whether or not the number of positive integer solutions of a given polynomial Diophantine equation belongs to the set.

We consider decision problems concerning the number of distinct solutions in positive integers of polynomial Diophantine equations.

For any polynomial $P(x_1, \cdots, x_m)$ with integer coefficients (not identically zero) we let $\#(P)$ be the number of distinct positive integer solutions of

$$P(x_1, \cdots, x_m) = 0.$$

Thus, $0 \leqq \#(P) \leqq \aleph_0$. Let $C=\{0, 1, 2, 3, \cdots, \aleph_0\}$. Then for given $A \subseteq C$, we may seek algorithms for testing whether or not $\#(P) \in A$. We shall prove:

THEOREM. *For no subset $A \subseteq C$ (except for the trivial cases $A=\varnothing$, $A=C$) is there an algorithm for testing whether or not $\#(P) \in A$.*

In proving the theorem we shall find the following transformations useful:

(i) $T^\infty P = uP$ where u is a variable not occurring in P.

(ii) $T^+P = P \cdot [(x_1-a_1)^2 + \cdots + (x_n-a_n)^2]$ where $P=P(x_1, \cdots, x_n)$ and $(a_1, \cdots, a_n)$ is the first n-tuple of positive integers in some fixed (recursive) ordering which is *not* a solution of $P=0$. Thus,

$$T^+P = 0 \iff P = 0 \vee (x_1, \cdots, x_n) = (a_1, \cdots, a_n).$$

$$\text{(iii)} \qquad T^-P = P^2 + \prod_{i=1}^{n} \left(\sum_{j=1}^{i-1} (x_j - a_j)^2 + ((x_i - a_i)^2 - u)^2 \right)^2,$$

where $P=P(x_1, \cdots, x_n)$ and $(a_1, \cdots, a_n)$ is the first n-tuple of positive

Received by the editors December 1, 1971.

AMS 1970 *subject classifications*. Primary 02F50, 10B99, 10N05, 02E15.

Key words and phrases. Diophantine equations, unsolvable problems, Hilbert's tenth problem, recursive functions.

[1] This work was supported by the National Science Foundation.

© American Mathematical Society 1972

integers (using the same ordering as in (ii)) which is a solution of $P=0$; if $P=0$ has no solutions, $T^{-}P$ is not defined.[2] Thus,

$$T^{-}P = 0 \Leftrightarrow P = 0 \ \& \ (x_1, \cdots, x_n) \neq (a_1, \cdots, a_n).$$

We have at once:

$$\#(T^{\infty}P) = \aleph_0 \Leftrightarrow \#(P) > 0. \tag{1}$$

(For, any solution of $P=0$ gives rise to infinitely many solutions as $u=1, 2, 3, \cdots$.)

$$\#(T^{+}P) = \#(P)+1. \tag{2}$$

$$\#(T^{-}P) = \#(P) - 1 \quad \text{if } \#(P) > 0. \tag{3}$$

Note that T^{∞}, T^{+} are recursive operations and that T^{-} is partial recursive. We set $T^{0}P=P$ and, for $m>0$, $T^{m+1}P=T^{+}(T^{m}P), T^{-m-1}=T^{-}(T^{-m}P)$. Thus, for $m>0$,

$$\#(T^{m}P) = \#(P) + m, \tag{4}$$

$$\#(T^{-m}P) = \#(P) - m \quad \text{if } \#(P) \geqq m. \tag{5}$$

We now proceed with the proof of the theorem:

Case I. $A=\{0\}$. This is just Hilbert's tenth problem, and so it is known that there is no algorithm.[3]

Case II. $A=\{m\}$, $0<m<\aleph_0$. We have, for any polynomial P (using (4)),

$$\#(P) = 0 \Leftrightarrow \#(T^{m}P) = m.$$

Hence an algorithm for this case would yield one for Case I.

Case III. $A=\{\aleph_0\}$. For any polynomial P,

$$\#(P) = 0 \Leftrightarrow \#(T^{\infty}P) \neq \aleph_0.$$

So again an algorithm for this case would yield one for Case I.

Case IV. $\aleph_0 \in A$, $0 \notin A$, $A \neq \{\aleph_0\}$. Let m be the least element of A. Then for any P,

$$\#(P) = m \Leftrightarrow \#(P) \in A \ \& \ \#(T^{\infty}T^{-m}P) \notin A.$$

So an algorithm for this case would yield one for Case II.

---

[2] My original definition of T^{-} was faulty. I am grateful to Yuri Matijasevič for this correction. I am also grateful to N. K. Kosovskiĭ and to the referee for pointing out oversights.

[3] This was shown in Matijasevič [2]. Cf. also [1]. For historical remarks and further references, cf. [3].

Case V. $\aleph_0 \notin A$, $0 \in A$, $A \neq \{0\}$. Then $C-A$ is in Case III or IV.

Case VI. $0 \notin A$, $\aleph_0 \notin A$, A contains at least 2 elements. Let m be the least element of A and let $B=\{x-m|x \in A\}$. Then B is in Case V, and

$$\#(P) \in B \quad \Leftrightarrow \quad \#(T^m P) \in A$$

so that an algorithm for A would yield one for B.

Case VII. $0 \in A$, $\aleph_0 \in A$, $A \neq C$. Then $C-A$ is in Case II or VI.

Since Cases I through VII exhaust all possibilities, this proves the theorem.

REFERENCES

1. Martin Davis, *An explicit Diophantine definition of the exponential function*, Comm. Pure Appl. Math. **24** (1971), 137–145. MR **42** #7632.

2. Ju. V. Matijasevič, *Enumerable sets are Diophantine*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282=Soviet Math. Dokl. **11** (1970), 354–358.

3. Julia Robinson, *Hilbert's tenth problem*, Proc. Sympos. Pure Math., vol. 20, Amer. Math. Soc., Providence, R.I., 1971, pp. 191–194.

COURANT INSTITUTE OF MATHEMATICAL SCIENCES, NEW YORK UNIVERSITY, NEW YORK, NEW YORK 10012