DIOPHANTINE SETS OVER POLYNOMINAL RINGS[1]

BY

MARTIN DAVIS AND HILARY PUTNAM

Recent work (cf. [1], [2]) on decision problems for Diophantine equations can be generalized to various rings other than the integers. In this paper, we shall prove the recursive unsolvability of the analogue of Hilbert's tenth problem (cf. [2]) for the ring $J[\xi]$ of formal polynomials with integer coefficients.

1. Principal results

We begin with the following notational conventions:

J is the ring of rational integers, R is a *recursive ring* (in the sense of [3]) such that $J \subset R$. The letter ξ with or without a numerical subscript is an indeterminate. Where the contrary is not explicitly stated, capital Latin letters stand for elements of R, lower case Latin letters stand for positive integers, capital Greek letters stand for sets.

DEFINITION. A set Σ is called *Diophantine over R* if for some polynomial form $P(\xi_0, \xi_1, \cdots, \xi_n)$ in the polynomial ring $R[\xi_0, \xi_1, \cdots, \xi_n]$, we have

$$X \in \Sigma \quad \leftrightarrow \quad \bigvee_{Y_1,\cdots,Y_n} P(X, Y_1, \cdots, Y_n) = 0.$$

A similar definition may be given for predicates $R(X_1, \cdots, X_n)$. We have at once

COROLLARY 1.1. *If Σ is Diophantine over R, then Σ is a recursively enumerable[2] set.*

We shall be concerned with the following decision problem which we call the *Diophantine problem over R*:

To determine of a given polynomial form $P(\xi_1, \cdots, \xi_m) \in R[\xi_1, \cdots, \xi_m]$ whether or not the equation $P(\xi_1, \cdots, \xi_m) = 0$ has a solution in R.

For $R = J$, the ring of integers, this is exactly Hilbert's tenth problem. Invoking the Church-Turing identification of recursiveness with effective calculability, and using the fact that there exists a recursively enumerable set which is not recursive, we have at once

COROLLARY 1.2. *If every recursively enumerable set of positive integers is Diophantine over R, then the Diophantine problem over R is unsolvable.*

The main result of the present paper, whose proof we postpone, is

Received November 22, 1961.

[1] This research was supported by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command.

[2] Note that R is recursive, so this concept is defined for sets of elements of R.

THEOREM 1.3. *Every recursively enumerable set of positive integers is Diophantine over* $J[\xi]$.

From Corollary 1.2 and Theorem 1.3 we have

COROLLARY 1.4. *The Diophantine problem over* $J[\xi]$ *is unsolvable.*

Let σ be a homomorphism from $J[\xi]$ to $J[\xi]/(Q(\xi))$ where $(Q(\xi))$ is the principal ideal of all multiples of the polynomial $Q(\xi)$. We write $J[\xi^\sigma]$ for $J[\xi]/(Q(\xi))$. For each polynomial $P(\xi_0, \xi_1, \cdots, \xi_n)$ in $J[\xi]\,[\xi_0, \xi_1, \cdots, \xi_n]$, let $P^\sigma(\xi_0, \xi_1, \cdots, \xi_n)$ be the polynomial over $J[\xi^\sigma]$ obtained by replacing in $P(\xi_0, \xi_1, \cdots, \xi_n)$ each coefficient by its image under σ. Let

$$\Sigma = \{x \mid \bigvee\nolimits_{Y_1,\cdots,Y_n \epsilon J[\xi]} P(x, Y_1, \cdots, Y_n) = 0\}, \tag{1}$$

$$\Sigma^\sigma = \{x \mid \bigvee\nolimits_{Y_1,\cdots,Y_n \epsilon J[\xi^\sigma]} P^\sigma(x, Y_1, \cdots, Y_n) = 0\}. \tag{2}$$

Then, clearly, $\Sigma \subset \Sigma^\sigma$. If in particular we choose for Σ a set which is *simple* in the sense of Post, then either Σ^σ is simple or $\overline{\Sigma^\sigma}$ is finite. Since a simple set is not recursive, we have

COROLLARY 1.5. *Either for every* σ, $\overline{\Sigma^\sigma}$ *is finite, or for some* σ, *the Diophantine problem over* $J[\xi^\sigma]$ *is unsolvable.*

But it is easy to prove

COROLLARY 1.6. *If the Diophantine problem over* J (*i.e., Hilbert's tenth problem*) *is solvable, so is the Diophantine problem over* $J[\xi^\sigma]$, *where* σ *is a homomorphism of* $J[\xi]$ *onto* $J[\xi]/(Q(\xi))$.

Proof. The elements of $J[\xi^\sigma]$ may, as is well known, be taken as elements of $J[\xi]$ of degree less than that of $Q(\xi)$ added and multiplied modulo $Q(\xi)$. Hence

$$\begin{aligned}&\bigvee\nolimits_{Y_1,\cdots,Y_n \epsilon J[\xi^\sigma]} P(Y_1, \cdots, Y_n) = 0 \;\leftrightarrow\\ &\qquad\bigvee\nolimits_{a_0^{(1)},\cdots,a_m^{(1)},\cdots,a_0^{(n)},\cdots,a_m^{(n)} \epsilon J} P(M_1(\xi), \cdots, M_n(\xi)) \equiv 0 \mod Q(\xi),\end{aligned}$$

where $Q(\xi)$ is of degree $m + 1$ and $M_i(\xi) = \sum_{j=0}^m a_j^{(i)}(\xi)$. That is,

$$\begin{aligned}&\bigvee\nolimits_{Y_1,\cdots,Y_n \epsilon J[\xi^\sigma]} P(Y_1, \cdots, Y_n) = 0 \;\leftrightarrow\\ &\qquad\bigvee\nolimits_{a_0^{(1)},\cdots,a_m^{(1)},\cdots,a_0^{(n)},\cdots,a_m^{(n)},b_0,\cdots,b_k \epsilon J} [P(M_1(\xi), \cdots, M_n(\xi))\\ &\qquad\qquad = Q(\xi)\cdot\sum\nolimits_{j=0}^k b_j\, \xi^j],\end{aligned}$$

where $k = q - (m + 1)$ and q is the degree of $P(M_1(\xi), \cdots, M_n(\xi))$, and the last polynomial identity is equivalent to the conjunction of $(m + 1)$ polynomial predicates, which proves the result.

Combining Corollaries 1.5 and 1.6, we have the curious result:

COROLLARY 1.7. *If* Σ *is any simple set expressed in the form* (1), *then either* $\overline{\Sigma^\sigma}$ *is finite for every* σ, *or Hilbert's tenth problem is unsolvable.*

It remains to prove Theorem 1.3.

2. Some lemmas on Pell's equation

In what follows we assume familiarity with the notation and results of [4].

LEMMA 2.1. *$X^2 - 3Y^2 = 1$ has the same solutions in $J[\xi]$ as in J.*

Proof. Let $[P_1(\xi)]^2 - 3[P_2(\xi)]^2 = 1$, where neither $P_1(\xi)$ nor $P_2(\xi)$ is a constant, and where, with no loss in generality, we may assume the leading coefficients of $P_1(\xi)$, $P_2(\xi)$ to be positive. Then, for ξ sufficiently large, say for $\xi \geqq N$, $P_1(\xi)$, $P_2(\xi)$ are positive and increasing. Thus,

$$P_1(N) = a_i \geqq a_0 .$$

$$P_1(N+1) = a_j > a_i \; ; \quad \text{hence} \quad a_j \geqq a_1 .$$

$$P_1(N+2) = a_k > a_j \; ; \quad \text{hence} \quad a_k \geqq a_2 .$$

In general,

$$P_1(N+r) = a_r .$$

Similarly,

$$P_2(N+r) \geqq a_r' .$$

Hence, for $\xi > N$,

$$P_1(\xi) + P_2(\xi)\sqrt{3} \geqq a_{\xi-N} + a_{\xi-N}'\sqrt{3} = (2+\sqrt{3})^{\xi-N}.$$

But for ξ sufficiently large, this inequality is certainly false. Hence, $P_1(\xi)$ or $P_2(\xi)$ must be a constant. But if one is constant, so is the other. This completes the proof.

When $\xi = a$, a positive integer, the solutions of

$$X^2 - (\xi^2 - 1)Y^2 = 1$$

in positive integers are the numbers a_n, a_n' of [4], both of which are solutions of the second order difference equation

$$U_{n+2} = 2\xi \cdot U_{n+1} - U_n . \tag{3}$$

We now define sequences $A_n(\xi)$, $A_n'(\xi)$ of elements of $J[\xi]$ by the requirements that each sequence satisfies (3), and that

$$A_0(\xi) = 1, \qquad A_0'(\xi) = 0,$$

$$A_1(\xi) = \xi, \qquad A_1'(\xi) = 1.$$

Then we have

LEMMA 2.2. *The solutions of*

$$X^2 - (\xi^2 - 1)Y^2 = 1 \tag{4}$$

are given precisely by

$$X = \pm A_n(\xi), \qquad Y = \pm A_n'(\xi).$$

Proof. For each integer value of ξ the values $X = A_n(\xi)$, $Y = A'_n(\xi)$ satisfy (4). Thus, the polynomial

$$P(\xi) = [A_n(\xi)]^2 - (\xi^2 - 1)[A'_n(\xi)]^2 - 1$$

is equal to 0 on the integers and hence vanishes identically, i.e., the polynomials $X = A_n(\xi)$, $Y = A'_n(\xi)$ satisfy (4).

Conversely, let

$$[U(\xi)]^2 - (\xi^2 - 1)[V(\xi)]^2 = 1,$$

where $U(\xi)$, $V(\xi)$ are ultimately positive. Let N be chosen so that $\xi > N$ implies $U(\xi) > 0$, $V(\xi) > 0$. Then, for each $a > N$,

$$U(a) = a_{f(a)}, \qquad V(a) = a'_{f(a)}.$$

Thus,

$$U(a) + V(a)\sqrt{(a^2 - 1)} = a_{f(a)} + a'_{f(a)}\sqrt{(a^2 - 1)} = (a + \sqrt{(a^2 - 1)})^{f(a)}.$$

Hence, as $a \to \infty$,

$$f(a) = \frac{\log(U(a) + V(a)\sqrt{(a^2 - 1)})}{\log(a + \sqrt{(a^2 - 1)})} = \frac{O(\log a)}{\log a + O(1)} = O(1).$$

Thus, for a suitable K, $f(a) < K$ for all positive integers, and we may conclude that for some integer q, $f(a) = q$ for infinitely many values of a, so that, for these values of a,

$$U(a) + V(a)\sqrt{(a^2 - 1)} = A_q(a) + A'_q(a)\sqrt{(a^2 - 1)}.$$

Finally, the equations

$$U(a) = A_q(a), \qquad V(a) = A'_q(a)$$

must hold for infinitely many values of a and hence identically.

DEFINITION. If $P(\xi) = Q(\xi)(\xi - a) + m$, we write

$$m = \operatorname{Rem}(P(\xi), \xi - a).$$

LEMMA 2.3. $\operatorname{Rem}(A'_n(\xi), \xi - 1) = n$; $\operatorname{Rem}(A_n(\xi), \xi - 2) = 2_n = A_n(2)$.

Proof. By the remainder theorem, $\operatorname{Rem}(A_n, \xi - 2) = A_n(2)$. But clearly $A_n(2) = 2_n$. Also, $\operatorname{Rem}(A'_n, \xi - 1) = A'_n(1) = 1'_n$. But a trivial induction using the recurrence (3) suffices to show that $1'_n = n$.

3. Proof of the main result

LEMMA 3.1. *The set Π of all positive integers is Diophantine over $J[\xi]$.*

Proof. We claim that

$$X \in \Pi \leftrightarrow \bigvee_{A,B,C,D,U,V,W,Z,Y,R} [(Y^2 - 3R^2 = 1)$$
$$\wedge (X = A^2 + B^2 + C^2 + D^2 + 1) \wedge (Y = X + U^2 + V^2 + W^2 + Z^2)].$$

For, if X is a positive integer, we can represent it as $A^2 + B^2 + C^2 + D^2 + 1$. For Y, R we select a solution of the Pell equation $Y^2 - 3R^2 = 1$, where $Y > X$, and finally represent $Y - X$ as the sum, $U^2 + V^2 + W^2 + Z^2$, of four squares.

Conversely, suppose X is a polynomial satisfying the condition on the right. Then, by Lemma 2.1, $Y, R \in \Pi$. But $X(\xi) < Y$ for all ξ. But, since $X(\xi)$ is one plus the sum of squares, it is positive definite, and hence if it is not constant, it will assume arbitrarily large values. Thus, $X(\xi)$ must be a constant, i.e., $X \in \Pi$.

Definition. A predicate $\rho(u, v)$ is called a *Julia Robinson predicate* if
(1) $\rho(u, v) \quad \rightarrow \quad v \leqq u^u$,
(2) for each k, there are u, v for which

$$\rho(u, v) \wedge v > u^k.$$

Lemma 3.2. *If there is a Julia Robinson predicate which is Diophantine over $J[\xi]$, then every recursively enumerable set is Diophantine over $J[\xi]$.*

Proof. By [1], for each recursively enumerable set Σ of positive integers, we may write

$$x \in \Sigma \quad \leftrightarrow \quad \bigvee_{t_1, \cdots, t_k, u, v} [P(t_1, \cdots, t_k, u, v, x) = 0 \wedge \rho(u, v)],$$

where P is a polynomial and $\rho(u, v)$ is any Julia Robinson predicate. Suppose that

$$\rho(u, v) \quad \leftrightarrow \quad \bigvee_{U_1, \cdots, U_m} Q(u, v, U_1, \cdots, U_m) = 0$$

for some polynomial Q, and let Π be the set of positive integers. Then

$$X \in \Sigma \quad \leftrightarrow \quad \bigvee_{T_1, \cdots, T_k, U, V, U_1, \cdots, U_m} [P(T_1, \cdots, T_k, U, V, X) = 0$$
$$\wedge\, Q(U, V, U_1, \cdots, U_m) = 0 \wedge T_1 \in \Pi \wedge \cdots \wedge T_k \in \Pi \wedge X \in \Pi$$
$$\wedge\, U \in \Pi \wedge V \in \Pi].$$

Lemma 3.3. *Let $\rho(u, v) \quad \leftrightarrow \quad v = 2_u \wedge u > 3$. Then $\rho(u, v)$ is a Julia Robinson predicate and is Diophantine over $J[\xi]$.*

Proof. By [4, Lemma 4], $2^u < 2_u < 4^u$. Hence, for $u > 3$, $2_u < 4^u < u^u$. Suppose $2_u < u^k$ for some k and all $u > 3$. Then $2^u < u^k$ for all $u > 3$, which is certainly false. Hence, $\rho(u, v)$ is a Julia Robinson predicate.

Next, by Lemmas 2.2 and 2.3,

$$v = 2_u \quad \leftrightarrow \quad \bigvee_{A, A'} \{[A^2 - (\xi^2 - 1)(A')^2 = 1]$$
$$\wedge \bigvee_{Q_1} [A = Q_1 \cdot (\xi - 2) + v] \wedge \bigvee_{Q_2} [A' = Q_2 \cdot (\xi - 1) + u]\}.$$

Finally,

$$u > 3 \quad \leftrightarrow \quad \bigvee_{A, B, C, D} u = 4 + A^2 + B^2 + C^2 + D^2.$$

Hence $\rho(u, v)$ is Diophantine over $J[\xi]$.

Theorem 1.3 follows at once from Lemmas 3.2 and 3.3.

References

1. Martin Davis, *Extensions and corollaries of recent work on Hilbert's tenth problem*, Illinois J. Math., vol. 7 (1963), pp. 246–250.

2. Martin Davis, Hilary Putnam, and Julia Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2), vol. 74 (1961), pp. 425–436.

3. M. O. Rabin, *Computable algebra, general theory and theory of computable fields*, Trans. Amer. Math. Soc., vol. 95 (1960), pp. 341–360.

4. Julia Robinson, *Existential definability in arithmetic*, Trans. Amer. Math. Soc., vol. 72 (1952), pp. 437–449.

Yeshiva University
New York, New York
Massachusetts Institute of Technology
Cambridge, Massachusetts