PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 69, Number 1, April 1978

DIOPHANTINE SETS OVER $\mathbf{Z}[T]$

J. DENEF[1]

ABSTRACT. Let $\mathbf{Z}[T]$ be the ring of polynomials with integer coefficients. We prove that every recursively enumerable subset of $\mathbf{Z}[T]$ is diophantine over $\mathbf{Z}[T]$. This extends a theorem of Davis and Putnam which states that every recursively enumerable subset of $\mathbf{Z}$ is diophantine over $\mathbf{Z}[T]$.

1. Introduction. Let $\mathbf{Z}[T]$ be the ring of polynomials with integer coefficients, in one variable T. M. Davis and H. Putnam [2, Theorem 1.3] proved

PROPOSITION 1. *Every recursively enumerable relation in* $\mathbf{Z}$ *is diophantine over* $\mathbf{Z}[T]$.

We refer to [2] for the definition of diophantine relations over $\mathbf{Z}[T]$.

REMARK. Proposition 1 follows at once from the Main Theorem on diophantine sets [1] (every recursively enumerable relation in $\mathbf{Z}$ is diophantine over $\mathbf{Z}$) and from the fact (see [2, Lemma 3.1]) that $\mathbf{Z}$ is diophantine over $\mathbf{Z}[T]$.

Notice that $\mathbf{Z}[T]$ is a recursive ring (in the sense of Rabin [4]), thus there exists a bijective map $\theta\colon \mathbf{N} \to \mathbf{Z}[T]$ such that the pre-images of addition and multiplication are recursive in $\mathbf{N}$. In what follows we shall denote, for any natural number n, the polynomial $\theta(n)$ by P_n.

It is trivial that every diophantine relation over $\mathbf{Z}[T]$ is recursively enumerable (with respect to the distinguished recursive structure on $\mathbf{Z}[T]$).

In this paper we prove:

PROPOSITION 2. *The relation* "$n \in \mathbf{N} \wedge F = P_n$" *in the variables* n *and* F *is diophantine over* $\mathbf{Z}[T]$.

From Propositions 1 and 2 follows at once the main result of this paper:

THEOREM. *A relation in* $\mathbf{Z}[T]$ *is diophantine over* $\mathbf{Z}[T]$ *if and only if it is recursively enumerable.*

2. Some lemmas. Let F be a polynomial in one variable T and let x be a real number, then we denote the value of F at x by $F \circ x$.

Received by the editors June 28, 1977.

AMS (MOS) subject classifications (1970). Primary 02F50, 10N05, 10B99.

Key words and phrases. Diophantine sets, Hilbert's tenth problem, unsolvable problems, recursively enumerable sets, diophantine equations.

[1] This work has been supported by the "Nationaal Fonds voor Wetenschappelijk Onderzoek". It was done at Harvard University whose generous hospitality I greatly appreciate.

LEMMA 1. *The relation "$x \in \mathbf{Z} \wedge F \in \mathbf{Z}[T] \wedge y = F \circ x$" in the variables x, y and F is diophantine over $\mathbf{Z}[T]$.*

PROOF. For any x in $\mathbf{Z}$ and F in $\mathbf{Z}[T]$ we have

$$y = F \circ x \leftrightarrow \exists G \in \mathbf{Z}[T]\colon F = (T - x)G + y \wedge y \in \mathbf{Z}.$$

This proves the lemma, since $\mathbf{Z}$ is diophantine over $\mathbf{Z}[T]$ by Proposition 1.

We consider the Pell equation

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

over $\mathbf{Z}[T]$. M. Davis and H. Putnam [2, Lemma 2.2] constructed two sequences of polynomials A_m, B_m, $m = 0, 1, 2, \ldots$, such that all solutions of (1) in $\mathbf{Z}[T]$ are given by $X = \pm A_m$, $Y = \pm B_m$, $m = 0, 1, 2, \ldots$. For our purposes we only need to know (see [2, Lemma 2.3]) that

$$\deg B_{m+1} = m \quad (\deg \text{ denotes the degree of the polynomial}), \tag{2}$$

$$B_m \circ 1 = m, \tag{3}$$

for all natural numbers m.

LEMMA 2. *The relation "$m \in \mathbf{N} \wedge F = B_m$" in the variables m and F is diophantine over $\mathbf{Z}[T]$.*

PROOF. By (3) we have for any F in $\mathbf{Z}[T]$

$$\begin{aligned} m \in \mathbf{N} \wedge F = B_m \leftrightarrow \exists X \in \mathbf{Z}[T]\colon & m \in \mathbf{N} \wedge X^2 - (T^2 - 1)F^2 \\ & = 1 \wedge F \circ 1 = m. \end{aligned}$$

Apply now Proposition 1 and Lemma 1.

LEMMA 3. *The relation "$F \in \mathbf{Z}[T] \wedge \forall x \in \mathbf{R}\colon F \circ x \geqslant 0$" in the variable F is diophantine over $\mathbf{Z}[T]$.*

PROOF. For any F in $\mathbf{Z}[T]$ we have:

$$\begin{aligned} (\forall x \in \mathbf{R}\colon F \circ x \geqslant 0) \leftrightarrow \exists G_1, G_2, \ldots, G_5, h_1, h_2, \ldots, h_4 \in \mathbf{Z}[T]\colon \\ (1 + h_1^2 + h_2^2 + h_3^2 + h_4^2)F = G_1^2 + G_2^2 + \cdots + G_5^2. \end{aligned}$$

This follows from a theorem of Pourchet [3]: Every positive definite polynomial in $\mathbf{Q}[T]$ can be expressed as a sum of five squares of polynomials in $\mathbf{Q}[T]$. Notice that we can write the common denominator of these polynomials as $1 + h_1^2 + h_2^2 + h_3^2 + h_4^2$, since every natural number is the sum of four squares of natural numbers.

3. Proof of Proposition 2. Let us define the relation $\mathrm{Par}(n, d, c, b, v)$ by

$$\begin{aligned} \mathrm{Par}(n, d, c, b, v) \leftrightarrow \{ & n \in \mathbf{N} \wedge d \in \mathbf{N} \wedge c \in \mathbf{N} \wedge b \in \mathbf{N} \wedge v \in \mathbf{Z} \wedge \\ & d = \deg P_n \wedge && (4) \\ & \forall x \in \mathbf{R}\colon P_n^2 \circ x \leqslant B_{d+2}^2 \circ x + c \wedge && (5) \\ & \forall x \in \mathbf{Z}\colon 0 \leqslant x \leqslant d \to b > B_{d+2}^2 \circ x \wedge && (6) \\ & v = P_n \circ (2b + 2c + d)\}. && (7) \end{aligned}$$

Notice that Par is a recursive relation in $\mathbf{Z}$ (indeed $\mathbf{R}$ is a decidable field), hence Par is diophantine over $\mathbf{Z}[T]$ by Proposition 1. We prove (see (i) and (ii)) for any n and F in $\mathbf{Z}[T]$ that:

$$n \in \mathbf{N} \wedge F = P_n \leftrightarrow \exists d, c, b, v \in \mathbf{Z}[T]:$$

$$\{\mathrm{Par}(n, d, c, b, v) \wedge \tag{8}$$

$$\forall x \in \mathbf{R}: F^2 \circ x \leqslant B_{d+2}^2 \circ x + c \wedge \tag{9}$$

$$F \circ (2b + 2c + d) = v\}. \tag{10}$$

This proves Proposition 2, since the right-hand side of the equivalence is diophantine over $\mathbf{Z}[T]$ by Lemmas 2, 3 and 1.

(i) Suppose $F = P_n$. Set $d = \deg P_n$. From (2) follows $\deg P_n < \deg B_{d+2}$, thus we can choose a natural number c satisfying (5). Take a natural number b which satisfies (6), and set $v = P_n \circ (2b + 2c + d)$. So there exist d, c, b and v in $\mathbf{Z}[T]$ satisfying (8), (9) and (10).

(ii) Suppose there are d, c, b and v in $\mathbf{Z}[T]$ which satisfy (8), (9) and (10). From (8) follows $n \in \mathbf{N}$, $c \in \mathbf{N}$, $b \in \mathbf{N}$ and $d = \deg P_n$. By (10) and (7) we have

$$(F - P_n) \circ (2b + 2c + d) = 0. \tag{11}$$

From (2) and (9) follows $\deg F \leqslant d + 1$, hence

$$\deg(F - P_n) \leqslant d + 1. \tag{12}$$

For every integer x satisfying $0 \leqslant x \leqslant d$ we have by (9), (5) and (6):

$$|F \circ x| \leqslant F^2 \circ x < b + c, \quad |P_n \circ x| \leqslant P_n^2 \circ x < b + c, \quad \text{and} \quad |(F - P_n) \circ x| < 2b + 2c. \tag{13}$$

But from (11), (12) and (13) follows $F = P_n$. Indeed suppose $F - P_n$ is not identically zero, then by (11) we can write

$$F - P_n = (2b + 2c + d - T)S,$$

with $S \in \mathbf{Z}[T]$, $S \neq 0$ and $\deg S \leqslant d$. There exists an integer k satisfying $0 \leqslant k \leqslant d$ and $S \circ k \neq 0$, otherwise S would have more than d zeroes. Hence $|(F - P_n) \circ k| \geqslant 2b + 2c + d - k \geqslant 2b + 2c$. Since this is in contradiction with (13), we conclude $F = P_n$.

References

1. Martin Davis, *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly **80** (1973), 233–269.

2. Martin Davis and Hilary Putnam, *Diophantine sets over polynomial rings*, Illinois J. Math. **7** (1963), 251–256.

3. Y. Pourchet, *Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques*, Acta Arith. **19** (1971), 89–104.

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

Department of Mathematics, University of Leuven, Celestijnenlaan 200 B, 3030 Heverlee, Belgium