PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 93, Number 4, April 1985

A DIOPHANTINE PROBLEM FOR LAURENT POLYNOMIAL RINGS

PETER PAPPAS

ABSTRACT. Let R be an integral domain of characteristic zero. We prove that the diophantine problem for the Laurent polynomial ring $R[T, T^{-1}]$ with coefficients in $\mathbf{Z}[T]$ is unsolvable. Under suitable conditions on R we then show that either $\mathbf{Z}$ or $\mathbf{Z}[i]$ is diophantine over $R[T, T^{-1}]$.

1. Introduction. Let R be a commutative ring with identity and let S be a fixed recursive subring of R, i.e. there exists a bijective map $\theta\colon \mathbf{N} \to S$ such that the pre-images of the ring operations are recursive in $\mathbf{N}$ (see, e.g., Rabin [**5**]). The diophantine problem for R with coefficients in S is said to be unsolvable (solvable) if there exists no (an) algorithm to decide whether or not a diophantine equation in several variables with coefficients in S has a solution in R. The diophantine problem for the complex function field $\mathbf{C}(T)$ with coefficients in $\mathbf{Z}[T]$ is very much an open question. Related results are as follows:

THEOREM A (DENEF [**3**]). *Let R be an integral domain of characteristic zero. Then the diophantine problem for $R[T]$ with coefficients in $\mathbf{Z}[T]$ is unsolvable.*

THEOREM B (DENEF [**3**]). *Let K be a formally real field. Then the diophantine problem for $K(T)$ with coefficients in $\mathbf{Z}[T]$ is unsolvable.*

Now let R be an integral domain of characteristic zero with quotient field F. The smallest ring containing R in which T is invertible is the Laurent polynomial ring $R[T, T^{-1}] \subset F(T)$.

Our main theorem is the following:

THEOREM. *Let R be an integral domain of characteristic zero. Then the diophantine problem for $R[T, T^{-1}]$ with coefficients in $\mathbf{Z}[T]$ is unsolvable.*

In light of Theorem A our result is not surprising; in fact, our proof follows the same route. However, there is an interesting difference. We need to consider two cases, namely $\sqrt{-1} \notin R$ and $\sqrt{-1} \in R$.

To handle the first case we use the well-known result of M. Davis, Yu. Matijasevic, H. Putnam and J. Robinson (see, e.g., [**1**]) that Hilbert's tenth problem is unsolvable, and for the second case we rely on a result of Denef which states that the diophantine problem for the ring of Gaussian integers $\mathbf{Z}[i]$ with coefficients in $\mathbf{Z}$ is unsolvable (see [**2**] or his generalization in [**4**]).

Received by the editors March 30, 1984.
1980 *Mathematics Subject Classification*. Primary 03B25, 10N05.
Key words and phrases. Diophantine problems, unsolvable problems, Hilbert's tenth problem.

2. The solution. We shall stay with the notation from [3] and begin by setting up some general terminology. Let $D(x_1,\dots,x_n)$ be a relation on $R[T, T^{-1}]$. We say that $D(x_1,\dots,x_n)$ is diophantine over $R[T, T^{-1}]$ with coefficients in $\mathbf{Z}[T]$ if there exists a diophantine equation $P(x_1,\dots,x_n, y_1,\dots,y_m)$ over $\mathbf{Z}[T]$ such that, for all $x_1,\dots,x_n \in R[T, T^{-1}]$:

$$D(x_1,\dots,x_n) \leftrightarrow \exists y_1,\dots,y_m \in R[T, T^{-1}]: P(x_1,\dots,x_n, y_1,\dots,y_m) = 0.$$

We note that if D_1 and D_2 are diophantine over $R[T, T^{-1}]$ with coefficients in $\mathbf{Z}[T]$, then so are $D_1 \vee D_2$ and $D_1 \wedge D_2$. Indeed, $P_1 = 0 \vee P_2 = 0 \leftrightarrow P_1P_2 = 0$ and $P_1 = 0 \wedge P_2 = 0 \leftrightarrow P_1^2 + TP_2^2 = 0$.

Consider the Pell equation

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

and let U be an element in the algebraic closure of $R[T, T^{-1}]$ satisfying

$$U^2 = T^2 - 1. \tag{2}$$

Then we have

$$(X + UY)(X - UY) = 1. \tag{3}$$

Let $X, Y \in R[T, T^{-1}]$ satisfy (1). As an algebraic function of T, $X + UY$ can be written in the form

$$g(T)/T^r + \sqrt{T^2 - 1}\, f(T)/T^s$$

with $g(T), f(T) \in R[T]$ and $r, s \in \mathbf{N}$. We next parametrize the curve (2) by

$$T = t^2 + 1/t^2 - 1, \qquad U = 2t/t^2 - 1.$$

As rational functions of t, it is easily seen that $X + UY$ and $X - UY$ have poles only at $t = \pm 1, \pm i$. Furthermore, (3) implies that they have zeros only at $t = \pm 1, \pm i$.

Now observe that $(X + UY)(-t) = (X - UY)(t)$ and so we conclude that if $X, Y \in R[T, T^{-1}]$ is a solution of (1), then

$$X + UY = c\left(\frac{t-1}{t+1}\right)^m \left(\frac{t-i}{t+i}\right)^n, \qquad X - UY = c\left(\frac{t-1}{t+1}\right)^{-m} \left(\frac{t-i}{t+i}\right)^{-n},$$

for some $c \in R$ and some $m, n \in \mathbf{Z}$. Substituting these two expressions into (3) yields $c^2 = 1$.

Let us now consider $X + UY$ as an algebraic function of T and suppose for the moment that $c = 1$. (The case $c = -1$ is entirely similar to this one.) We have

$$\begin{aligned} X + UY &= \left(\frac{t-1}{t+1}\right)^m \left(\frac{t-i}{t+i}\right)^n \\ &= (T + U)^m \left(\frac{t^2 - 1}{t^2 + 1} - i\frac{2t}{t^2 + 1}\right)^n = (T + U)^m \left(\frac{1 - iU}{T}\right)^n. \end{aligned}$$

From (2),

$$(T - U)^{-m} = (T + U)^m \quad \text{and} \quad \left(\frac{1 - iU}{T}\right)^{-n} = \left(\frac{1 + iU}{T}\right)^n,$$

and therefore we may rewrite $X + UY$ and $X - UY$ as expressions involving only positive integral exponents.

Thus if $(X, Y) \in R[T, T^{-1}] \times R[T, T^{-1}]$ is a solution to (1), we have one of four possible outcomes, namely

$$\left.\begin{aligned} X + UY &= (T+U)^m \left(\frac{1-iU}{T}\right)^n, \\ X - UY &= (T-U)^m \left(\frac{1-iU}{T}\right)^n, \end{aligned}\right\} \quad \text{some } (m, n) \in \mathbf{N} \times \mathbf{N};$$

$$\left.\begin{aligned} X + UY &= (T+U)^m \left(\frac{1+iU}{T}\right)^n, \\ X - UY &= (T-U)^m \left(\frac{1-iU}{T}\right)^n, \end{aligned}\right\} \quad \text{some } (m, n) \in \mathbf{N} \times \mathbf{N};$$

$$\left.\begin{aligned} X + UY &= (T-U)^m \left(\frac{1-iU}{T}\right)^n, \\ X - UY &+ (T+U)^m \left(\frac{1+iU}{T}\right)^n, \end{aligned}\right\} \quad \text{some } (m, n) \in \mathbf{N} \times \mathbf{N};$$

$$\left.\begin{aligned} X + UY &= (T-U)^m \left(\frac{1+iU}{T}\right)^n, \\ X - UY &= (T+U)^m \left(\frac{1-iU}{T}\right)^n, \end{aligned}\right\} \quad \text{some } (m, n) \in \mathbf{N} \times \mathbf{N}.$$

Now let S denote the ring $\mathbf{Z}[i][T, T^{-1}]$. By (2), $S[U]$ defines a quadratic ring extension of S. For each $j = 1, 2, 3, 4$ define two sequences $X^{(j)}_{(m,n)}$, $Y^{(j)}_{(m,n)}$, $(m, n) \in \mathbf{N} \times \mathbf{N}$, of elements of S by

$$X^{(1)}_{(m,n)} + UY^{(1)}_{(m,n)} = (T+U)^m \left(\frac{1-iU}{T}\right)^n, \tag{4}$$

$$X^{(2)}_{(m,n)} + UY^{(2)}_{(m,n)} = (T+U)^m \left(\frac{1+iU}{T}\right)^n, \tag{5}$$

$$X^{(3)}_{(m,n)} + UY^{(3)}_{(m,n)} = (T-U)^m \left(\frac{1-iU}{T}\right)^n, \tag{6}$$

$$X^{(4)}_{(m,n)} + UY^{(4)}_{(m,n)} = (T-U)^m \left(\frac{1+iU}{T}\right)^n. \tag{7}$$

Applying the ring automorphism $S[U] \to S[U]$, which fixes S elementwise and sends U to $-U$, together with (2) yields

$$X^{(1)}_{(m,n)} - UY^{(1)}_{(m,n)} = (T-U)^m \left(\frac{1+iU}{T}\right)^n = (T+U)^{-m} \left(\frac{1-iU}{T}\right)^{-n},$$

$$X^{(2)}_{(m,n)} - UY^{(2)}_{(m,n)} = (T-U)^m \left(\frac{1-iU}{T}\right)^n = (T+U)^{-m} \left(\frac{1-iU}{T}\right)^{-n},$$

$$X^{(3)}_{(m,n)} - UY^{(3)}_{(m,n)} = (T+U)^m \left(\frac{1+iU}{T}\right)^n = (T-U)^{-m} \left(\frac{1-iU}{T}\right)^{-n},$$

$$X^{(4)}_{(m,n)} - UY^{(4)}_{(m,n)} = (T+U)^m \left(\frac{1-iU}{T}\right)^n = (T-U)^{-m} \left(\frac{1+iU}{T}\right)^{-n},$$

and hence, for every $(m, n) \in \mathbf{N} \times \mathbf{N}$ and each $j = 1,2,3,4$, the pair $(X^{(j)}_{(m,n)}, Y^{(j)}_{(m,n)}) \in \mathbf{S} \times \mathbf{S}$ is a solution to (1).

LEMMA 1. (a) *If $i \in R$, then the solutions of* (1) *in $R[T, T^{-1}]$ are of the form*

$$\left(X^{(j)}_{(m,n)}, Y^{(j)}_{(m,n)}\right), \qquad (m, n) \in \mathbf{N} \times \mathbf{N}, j = 1,2,3,4.$$

(b) *If $i \notin R$, then the solutions of* (1) *in $R[T, T^{-1}]$ are of the form*

$$\left(X^{(j)}_{(m,0)}, Y^{(j)}_{(m,0)}\right), \qquad m \in \mathbf{N}, j = 1,2,3,4.$$

PROOF. By the foregoing discussion, it remains only to show that if $i \notin R$, then for every $(m, n) \in \mathbf{N} \times \mathbf{N}^{>0}$ and $j = 1,2,3,4$,

$$\left(X^{(j)}_{(m,n)}, Y^{(j)}_{(m,n)}\right) \notin R[T, T^{-1}] \times R[T, T^{-1}].$$

Fix $x = X^{(j)}_{(m,n)}$, $y = Y^{(j)}_{(m,n)}$ for some $(m, n) \in \mathbf{N} \times \mathbf{N}^{>0}$, $j \in \{1,2,3,4\}$, and assume $(x, y) \in R[T, T^{-1}] \times R[T, T^{-1}]$. Let σ: $S[U] \to S[U]$ be the ring automorphism which fixes T and U and sends i to $-i$. Then $\sigma(x + Uy) = x + Uy$, which by (4)–(7) implies

$$\left(\frac{1 + iU}{T}\right)^n = \left(\frac{1 - iU}{T}\right)^n.$$

Since this is impossible for $n > 0$, we obtain the desired contradiction, and the lemma is complete.

DEFINITION. Write $V \sim W$ if the elements $V, W \in R[T, T^{-1}]$ take on the same value at $T = 1$.

LEMMA 2. *The relation $Z \sim 0$ is diophantine over $R[T, T^{-1}]$ with coefficients in* $\mathbf{Z}[T]$.

PROOF. $Z \sim 0 \Leftrightarrow \exists X \in R[T, T^{-1}]$: $Z = (T - 1)X$.

LEMMA 3. (a) *If $i \in R$, then* $\{Y(1)\colon (X, Y) \in X^2 - (T^2 - 1)Y^2 = 1,\ X, Y \in R[T, T^{-1}]\} = \mathbf{Z}[i]$.

(b) *If $i \notin R$, then* $\{Y(1)\colon (X, Y) \in X^2 - (T^2 - 1)Y^2 = 1, X, Y \in R[T, T^{-1}]\} = \mathbf{Z}$.

PROOF. We shall give the explicit form of $Y^{(j)}_{(m,n)}$. We begin by noting

$$Y^{(j)}_{(m,n)} = \frac{\left(X^{(j)}_{(m,n)} + UY^{(j)}_{(m,n)}\right) - \left(X^{(j)}_{(m,n)} - UY^{(j)}_{(m,n)}\right)}{2U}, \tag{8}$$

from which it follows that $Y^{(3)}_{(m,n)} = -Y^{(2)}_{(m,n)}$ and $Y^{(4)}_{(m,n)} = -Y^{(1)}_{(m,n)}$. Using the binomial theorem and (8), we have:

For $(m, n) \in \mathbf{N}^{>0} \times N^{>0}$,

$$T^n Y^{(1)}_{(m,n)} = T^n Y^{(2)}_{(m,n)} = \left(\sum_{\substack{j=0\\ j\text{-odd}}}^{m} \binom{m}{j} T^{m-j} U^{j-n}\right)\left(\sum_{\substack{j=0\\ j\text{-even}}}^{n} \binom{n}{j} (iU)^j\right)$$

$$-\left(\sum_{\substack{j=0\\ j\text{-even}}}^{m} \binom{m}{j} T^{m-j} U^{j}\right)\left(\sum_{\substack{j=0\\ j\text{-odd}}}^{n} \binom{n}{j} (i)^j U^{j-1}\right).$$

For $(m, n) \in \mathbf{N} \times \{0\}$,

$$Y^{(1)}_{(m,n)} = Y^{(2)}_{(m,n)} = \sum_{\substack{j=0\\ j\text{-odd}}}^{m} \binom{m}{j} T^{m-j} U^{j-1}.$$

For $(0, n) \in \{0\} \times \mathbf{N}$,

$$T^n Y^{(1)}_{(0,n)} = \sum_{\substack{j=0\\ j\text{-odd}}} \binom{n}{j} (-i)^j U^{j-1}$$

and

$$T^n Y^{(2)}_{(0,n)} = \sum_{\substack{j=0\\ j\text{-odd}}} \binom{n}{j} (i^j) U^{j-1}.$$

Using (2) and Lemma 1, and setting $T = 1$ and $c = \pm 1$ yields the desired result.

DEFINITION. $\mathrm{Imt}(Y) \Leftrightarrow Y \in R[T, T^{-1}] \wedge \exists X \in R[T, T^{-1}]\colon\ X^2 - (T^2 - 1)Y^2 = 1$.

Notice that Imt is diophantine over $R[T, T^{-1}]$ with coefficients in $\mathbf{Z}[T]$.

PROOF OF THE THEOREM.

Case (a). $i \in R$. There exists an algorithm to find for any diophantine equation $P \in \mathbf{Z}[X_1, \ldots, X_N]$ a diophantine equation $P^* \in \mathbf{Z}[T][X_1, \ldots, X_N]$ satisfying

$$\begin{aligned} &\exists z_1, \ldots, z_N \in \mathbf{Z}[i]\colon P(z_1, \ldots, z_N) = 0 \\ &\quad \leftrightarrow Z_1, \ldots, Z_N \in R[T, T^{-1}]\colon P^*(Z_1, \ldots, Z_N) = 0. \end{aligned} \tag{9}$$

Indeed, by Lemma 3 we have

$$\begin{aligned} &\exists z_1, \ldots, z_N \in \mathbf{Z}[i]\colon P(z_1, \ldots, z_N) = 0 \\ &\leftrightarrow Z_1, \ldots, Z_N \in R[T, T^{-1}]\colon \big(\mathrm{Imt}(Z_1) \wedge \cdots \wedge \mathrm{Imt}(Z_N)\big) \wedge P(Z_1, \ldots, Z_N) \sim 0. \end{aligned}$$

Since Imt and $\sim$ are diophantine over $R[T, T^{-1}]$ with coefficients in $\mathbf{Z}[T]$, (9) follows. Thus if the diophantine problem for $R[T, T^{-1}]$ with coefficients in $\mathbf{Z}[T]$ would be solvable, then so would the diophantine problem for $\mathbf{Z}[i]$ with coefficients in $\mathbf{Z}$, contradicting Denef's result in [**2**].

Case (b). $i \notin R$. In exactly the same way we see that if the diophantine problem for $R[T, T^{-1}]$ with coefficients in $\mathbf{Z}[T]$ would be solvable, then so would Hilbert's tenth problem.

As in [**3**], we obtain the following corollary.

COROLLARY. (a) *Let R be an integral domain of characteristic zero with $i \in R$. Suppose there exists a subset S of R which contains $\mathbf{Z}[i]$ and which is diophantine over $R[T, T^{-1}]$; then $\mathbf{Z}[i]$ is diophantine over $R[T, T^{-1}]$. In particular, this is true where R contains $\mathbf{Q}(i)$.*

(b) *Let R be an integral domain of characteristic zero with $i \notin R$. Suppose there exists a subset S of R which contains $\mathbf{Z}$ and which is diophantine over $R[T, T^{-1}]$; then $\mathbf{Z}$ is diophantine over $R[T, T^{-1}]$. In particular, this is true when R contains $\mathbf{Q}$.*

PROOF. We prove only (a) since (b) follows similarly. If S satisfies the conditions of the corollary, then

$$z \in \mathbf{Z}[i] \leftrightarrow \exists Z \in R[T, T^{-1}](\mathrm{Imt}(Z) \wedge Z \sim z \wedge \in S).$$

Moreover, if R contains $\mathbf{Q}(i)$, then we define S by

$$x \in S \leftrightarrow x \in R[T, T^{-1}]$$
$$\wedge (x = 0 \vee x = 1 \vee \exists y_1, y_2\, xy_1 = 1 \wedge (x-1)y_2 = 1).$$

REFERENCES

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

2. J. Denef, *Hilbert's tenth problem for quadratic rings*. Proc. Amer. Math. Soc. **48** (1975), 214–220.

3. ______, *The diophantine problem for polynomial rings and fields of rational functions*, Trans. Amer. Math. Soc. **242** (1978), 391–399.

4. ______, *Diophantine sets over algebraic integer rings*. II, Trans. Amer. Math. Soc. **257** (1980), 227–236.

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

DEPARTMENT OF MATHEMATICS, VASSAR COLLEGE, POUGHKEEPSIE, NEW YORK 12601