UNSOLVABLE DIOPHANTINE PROBLEMS

JULIA ROBINSON

We shall show that there is no general method of telling whether an arbitrary polynomial $P(x_1, \cdots, x_k)$ with integer coefficients is ever a power of 2 for $x_1, \cdots, x_k$ natural numbers. At present there is no general method known even in the special case with $k=1$.

Actually we shall show directly that the relation given by $r=2^t$ is diophantine in the set $\mathfrak{I}$ of powers of 2. Hence every recursively enumerable set is diophantine in $\mathfrak{I}$ by Corollary 5 of Davis, Putnam, and Robinson [4].

We call a relation $\rho(x_1, \cdots, x_n)$ among natural numbers *diophantine* if there is a polynomial P with integer coefficients such that $\rho(x_1, \cdots, x_n)$ if and only if there are natural numbers $y_1, \cdots, y_k$ with $P(x_1, \cdots, x_n, y_1, \cdots, y_k)=0$. A set $\mathfrak{S}$ (function F) is *diophantine* if $x\in\mathfrak{S}$ (the graph of F) is diophantine. Also, ρ *is diophantine in a set* $\mathfrak{S}$ if there is a polynomial P with integer coefficients such that $\rho(x_1, \cdots, x_n)$ if and only if there are natural numbers $y_1, \cdots, y_k$, $z_1, \cdots, z_l$ with both $P(x_1, \cdots, x_n, y_1, \cdots, y_k, z_1, \cdots, z_l)=0$ and $z_1, \cdots, z_l\in\mathfrak{S}$. In [6], the term "existentially definable" was used instead of "diophantine". The definitions given there are easily seen to be equivalent to these. In both [1] and [4], relations over the positive integers were considered but the definitions and theorems hold for natural numbers with only the obvious modifications.

The logical symbols $\vee$ (there exists), $\wedge$ (and), $\leftrightarrow$ (if and only if) occur in this paper. The variables always range over the natural numbers.

Let $a>1$ and a_n, a_n' be defined by

$$a_n + a_n'(a^2-1)^{1/2} = (a+(a^2-1)^{1/2})^n.$$

LEMMA 1. *Natural numbers x and y satisfy the Pell equation $x^2-(a^2-1)y^2=1$ if and only if there is a natural number n such that $x=a_n$ and $y=a_n'$.*

This is a standard result of elementary number theory.

LEMMA 2. *For $a>1$,*

$$a_n' \equiv n \pmod{a-1}, \qquad a_n - a_n'(a-2) \equiv 2^n \pmod{4a-5}.$$

For proof, see Lemmas 5 and 7 of [6].

Presented to the Society, April 26, 1969; received by the editors September 18, 1968.

LEMMA 3. *There is a binary diophantine relation* $\mathfrak{A}$ *such that* $\mathfrak{A}(t, m)$ *implies* $m > 2^t$ *and if* m *is sufficiently large with respect to* t *then* $\mathfrak{A}(t, m)$ *holds.*

PROOF. Let ψ be the relation of Lemma 8 of [6]. Then the binary relation $\mathfrak{A}$ defined by

$$\mathfrak{A}(t, m) \leftrightarrow (\forall u)(\psi(t + 2, u) \wedge m > u)$$

clearly satisfies the requirements.

LEMMA 4. *A natural number* n *is the sum of two squares if and only if no number of the form* $4t+3$ *divides* n *to an odd power. Hence if* x *and* y *are relatively prime then* xy *is the sum of two squares if and only if* x *and* y *are each the sum of two squares.*

This is again a standard result of elementary number theory.

THEOREM 1. *Let* $\mathfrak{M}$ *be an infinite set of natural numbers and* H *be a diophantine function such that for all* $m \in \mathfrak{M}$,

$$(m, H(m)) = 1, \qquad 2^{H(m)} \equiv 1 \pmod{m}.$$

Then $r = 2^t$ *is diophantine in* $\mathfrak{M}$.

Before proving the theorem, we give two corollaries.

COROLLARY 1. *Every recursively enumerable set is diophantine in any infinite set of numbers* m *such that* $2^{m-1} \equiv 1 \pmod{m}$. *In particular,* $\mathfrak{M}$ *can be any infinite set of primes.*

PROOF. From Theorem 1 with $H(m) = m - 1$ and Corollary 5 of [4]. This result is also proved in [7].

COROLLARY 2. *Every recursively enumerable set is diophantine in the set of numbers of the form* 2^{2^n}.

PROOF. Let $\mathfrak{M} = \{2^{2^n} - 1\}$ and $H(m) = m + 1$. Now

$$2^{2^{2^n}} \equiv 1 \pmod{2^{2^n} - 1}$$

since 2^n divides 2^{2^n}. Hence for $m \in \mathfrak{M}$,

$$2^{m+1} \equiv 1 \pmod{m}.$$

Hence the corollary follows from Theorem 1 as before.

REMARK. R. M. Robinson pointed out this application of the theorem to me.

PROOF OF THEOREM 1. We shall show that $r = 2^t$ if and only if there are natural numbers a, u, v, and m such that

(1) $a>1$, $m\in\mathfrak{M}$, $m\mid(4a-5)$, $H(m)\mid(a-1)$, $m>1$,
(2) $\mathfrak{A}(t, m)$,
(3) $u^2-(a^2-1)v^2=1$,
(4) $\mathrm{Rem}(u-v(a-2), m)=r$,
(5) $\mathrm{Rem}(v, H(m))=t$.

Suppose that a, u, v, and m satisfy (1)–(5). By Lemma 1 and (3), there is a natural number n such that $u=a_n$ and $v=a_n'$. Then by Lemma 2,

$$\begin{aligned} u-v(a-2) &\equiv 2^n \pmod{4a-5} \\ &\equiv 2^n \pmod{m} \end{aligned}$$

since $m\mid(4a-5)$ by (1). Hence by (4),

(6) $r\equiv 2^n \pmod{m}$, $r<m$.

Also by Lemma 2,

$$\begin{aligned} v &\equiv n \pmod{a-1} \\ &\equiv n \pmod{H(m)} \end{aligned}$$

since $H(m)\mid(a-1)$ by (1). Hence by (5),

$$t\equiv n \pmod{H(m)}, \qquad t<H(m).$$

Thus, $n=t+q\cdot H(m)$ for some $q\geqq 0$. But by the hypothesis of the theorem $2^{H(m)}\equiv 1 \pmod{m}$ and by (2), $A(t, m)$ holds so that

$$2^n\equiv 2^t \pmod{m}, \qquad 2^t<m.$$

Hence by (6), $r=2^t$.

On the other hand, suppose $r=2^t$. We need to find a, u, v, and m which satisfy (1)–(5). Choose m in $\mathfrak{M}$ sufficiently large so that $\mathfrak{A}(t, m)$ holds. This is possible by Lemma 3 since $\mathfrak{M}$ is infinite by hypothesis. Now m is odd since $2^{H(m)}\equiv 1 \pmod{m}$ and $H(m)>0$. Hence by the Chinese Remainder Theorem, we can choose $a>1$ so that

$$4a\equiv 5 \pmod{m}, \qquad a\equiv 1 \pmod{H(m)}$$

since m and $H(m)$ are relatively prime. Hence (1) and (2) are satisfied. Now let $u=a_t$ and $v=a_t'$ so that (3) holds. By Lemma 2, we have

$$\begin{aligned} u-v(a-2) &\equiv 2^t \pmod{4a-5} \\ &\equiv 2^t \pmod{m}. \end{aligned}$$

Also since $A(t, m)$ holds, $2^t<m$. Hence $\mathrm{Rem}(u-v(a-2), m)=2^t=r$ so that (4) holds. By Lemma 2,

$$v \equiv t \pmod{a-1}$$
$$\equiv t \pmod{H(m)}$$

since $H(m) \mid (a-1)$. Now $t < H(m)$ since $2^t < m$ and $2^{H(m)} > m$. Hence $\mathrm{Rem}(v, H(m)) = t$ so (5) holds. Since all of the relations occurring in (1)–(5) except $m \in \mathfrak{M}$ are diophantine, the theorem follows.

The following existential definition of the set of numbers of the form 2^{2^n} in terms of $\mathfrak{I}$, the set of powers of 2, was suggested by the work of Davis [3].

THEOREM 2. *$x = 2^{2^n}$ for some $n > 0$ if and only if x is a power of 2 and there are natural numbers u and v such that $x = 1 + 3(u^2 + v^2)$.*

PROOF. Let m be positive and k be odd. Then

$$2^{2^m \cdot k} - 1 = (2^{2^{m-1} \cdot k} + 1)(2^{2^{m-2} \cdot k} + 1) \cdots (2^{2k} + 1)(2^{2k} - 1).$$

Hence $(2^{2^m \cdot k} - 1)/3$ is the sum of two squares if and only if $(2^k - 1)(2^k + 1)/3$ is the sum of two squares by Lemma 4. (Note that $3 \mid (2^k + 1)$ for k odd.) Now for $k \geqq 3$, $2^k - 1$ is of the form $4t + 3$ and is prime to $(2^k + 1)/3$ so the product is not the sum of two squares; while for $k = 1$, it is. In the case $m = 0$ and k odd, $2^k - 1$ is not divisible by 3. Hence for odd k, $2^{2^m \cdot k} = 1 + 3(u^2 + v^2)$ has a solution for u and v if and only if $m > 0$ and $k = 1$.

THEOREM 3. *To every recursively enumerable set $\mathfrak{S}$, there is a polynomial P with integer coefficients such that*

$$\mathfrak{S} = \{x : P(x, y_1, \cdots, y_k) = 2^t \text{ for some } y_1, \cdots, y_k, \text{ and } t\}.$$

PROOF. Since $\mathfrak{S}$ is diophantine in $\mathfrak{I}$ by Corollary 2 and Theorem 2, there is a polynomial F such that

$$x \in \mathfrak{S} \leftrightarrow$$
$$(\forall u_1, \cdots, u_m, v_1, \cdots, v_n)\ (F(x, u_1, \cdots, u_m, 2^{v_1}, \cdots, 2^{v_n}) = 0).$$

Hence

$$x \in \mathfrak{S} \leftrightarrow (\forall u_1, \cdots, u_m, w_1, \cdots, w_n, v)$$
$$(F(x, u_1, \cdots, u_m, w_1, \cdots, w_n) = 0 \wedge w_1 \mid 2^v \wedge \cdots \wedge w_n \mid 2^v).$$

We can now combine the conditions into a single polynomial in more variables in the usual way (see Davis [1, p. 104]). Thus,

$$x \in \mathfrak{S} \leftrightarrow (\forall z_1, \cdots, z_r, v)(G(x, z_1, \cdots, z_r, 2^v) = 0)$$

for a suitable choice of G. Finally, we see that

$$x \in S \leftrightarrow (\forall z_1, \cdots, z_r, w, v)(w(1 + 2G(x, z_1, \cdots, z_r, w)^2) = 2^v).$$

Hence we can take $w(1+2G^2)$ for P.

REMARK. The arguments here are derived from those of Putnam [5] and Davis [2].

Since not every recursively enumerable set is recursive, Theorem 3 shows that there can be no general method of telling whether an arbitrary polynomial assumes a power of 2 as value.

OPEN QUESTIONS. Is every recursively enumerable set diophantine in the set of powers of 3? of n? Is there a general method of telling whether an arbitrary polynomial P with positive integer coefficients assumes a power of 2 as value? (In this case, there is an obvious method of telling whether P assumes a particular power of 2.)

BIBLIOGRAPHY

1. Martin Davis, *Computability and unsolvability*, McGraw-Hill, New York, 1958.

2. ———, *Extensions and corollaries of recent work on Hilbert's tenth problem*, Illinois J. Math. **7** (1963), 246–250.

3. ———, *One equation to rule them all*, Memorandum RM-5494-PR, The RAND Corporation, Santa Monica, Calif., 1968.

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

5. Hilary Putnam, *An unsolvable problem in number theory*, J. Symbolic Logic **25** (1960), 220–232.

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

7. ———, "Diophantine decision problems" in *Studies in number theory*, Studies in Math., vol. 6, Math. Assoc. of America; Prentice-Hall, Englewood Cliffs, N. J., 1969, pp. 76–116.

UNIVERSITY OF CALIFORNIA, BERKELEY