ANNALS OF MATHEMATICS
Vol. 74, No. 3, November, 1961
*Printed in Japan*

# THE DECISION PROBLEM FOR EXPONENTIAL DIOPHANTINE EQUATIONS

BY MARTIN DAVIS[1], HILARY PUTNAM[1], AND JULIA ROBINSON

(Received July 26, 1960)

## 1. Introduction

We prove that every recursively enumerable set can be existentially defined in terms of exponentiation. Hence, there is no general algorithm for deciding whether or not an exponential diophantine equation has a solution in positive integers. We also obtain a general theorem about bounds for solutions of diophantine equations with a finite number of solutions[2].

The tenth problem on David Hilbert's famous list (cf., Hilbert [4]) is given as follows:

10. Entscheidung der Lösbarkeit einer diophantischen Gleichung.

Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoeffizienten sei vorgelegt; man soll ein Verfahren angeben, nach welchem sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

Our result provides a negative answer to a closely related problem.

A diophantine equation is an equation of the form $P(x_1, \cdots, x_n) = 0$ where $P$ is a polynomial with integer coefficients and a solution in integers (or sometimes positive integers) is required.

An exponential diophantine equation is an equation which can be put in the form $E(x_1, \cdots, x_n) = F(x_1, \cdots, x_n)$ where $E$ and $F$ are functions built from $x_1, \cdots, x_n$ and particular positive integers by addition, multiplication and exponentiation. Such an equation is clearly equivalent to

[1] The contribution of Martin Davis and Hilary Putnam to this research was supported by the United States Air Force under Contract No. AF 49(638)-527.

[2] The result that every recursively enumerable set can be existentially defined in terms of exponentiation was obtained by Davis and Putnam, basing themselves on their [3], using the unproved number-theoretical hypothesis that there are arbitrarily long arithmetic progressions containing only prime numbers. They wish to acknowledge useful suggestions, made in conversation, by H. S. Shapiro. Their results are contained in the third part of an Airforce report (AFOSRTR 59-124, October 1959) and were presented to the American Mathematical Society, October 31, 1959. Abstract 560-10. Julia Robinson showed that the use of this hypothesis can be avoided. This result was presented to the American Mathematical Society, January 27, 1960. Abstract 564-275. Subsequently, she greatly simplified the entire proof. The theorem concerning bounds for solutions of diophantine equations is also due to Julia Robinson, and was presented to the American Mathematical Society, April 23, 1960. Abstract 569-23.

a system of equations, each of the form $\alpha + \beta = \lambda$, $\alpha\beta = \lambda$, or $\alpha^\beta = \lambda$, where $\alpha$, $\beta$, and $\lambda$ are variables or particular positive integers. Now a system of equations $A_i = B_i$ for $i = 1, \cdots, m$ is equivalent to the single equation $\sum (A_i - B_i)^2 = 0$. Hence every exponential diophantine equation is equivalent to an equation $E'(x_1, \cdots, x_n) = 0$, where $E'$ is a linear combination (with integer coefficients) of products of terms of the form $\alpha^\beta$ and where $\alpha$ and $\beta$ are either variables or particular positive integers. Without loss of generality, we may restrict ourselves to equations which have been reduced to this form. Examples of exponential diophantine equations from the current literature are $x^x y^y = z^z$, $2^y - 7 = x^2$, and $2^x + 11^y = 5^z$. Solutions of exponential diophantine equations are usually required to be positive integers.

An algorithm for determining the solvability of diophantine equations in integers would yield an algorithm for determining the solvability in positive integers and conversely. (See Davis [2, pp. 102 103] or Davis [1, pp. 35–36]). Hence we will limit our discussion to questions of solvability in positive integers. Lower-case Latin letters will always represent positive integers or variables whose range is the positive integers.

A relation $\rho(x_1, \cdots, x_n)$ *is existentially definable in terms of* $\varphi_1, \cdots, \varphi_k$ if there is an equivalence

$$\rho(x_1, \cdots, x_n) \longleftrightarrow \bigvee_{u_1, \cdots, u_m} \psi(x_1, \cdots, x_n, u_1, \cdots, u_m)$$

where $\psi$ is an expression composed of the free variables $x_1, \cdots, x_n$; the bound variables $u_1, \cdots, u_m$; the logical connectives $\wedge$, $\vee$, $=$; $\varphi_1, \cdots, \varphi_k$; and symbols for particular positive integers. Here $\varphi_1, \cdots, \varphi_k$ can be either relations or operations (i.e., positive integer valued functions defined on the positive integers), on any number of variables. Clearly, if $\rho$ can be existentially defined in terms of $\varphi_1, \cdots, \varphi_k$ and $\varphi_k$ can be existentially defined in terms of $\varphi_1, \cdots, \varphi_{k-1}$, then $\rho$ can be existentially defined in terms of $\varphi_1, \cdots, \varphi_{k-1}$.

It is easy to see that a set $\mathcal{S}$ of positive integers (i.e., a relation of one argument) is existentially definable in terms of addition and multiplication if and only if there is a polynomial $P$ with integer coefficients (positive or negative) such that

$$s \in \mathcal{S} \longleftrightarrow \bigvee_{u_1, \cdots, u_m} P(s, u_1, \cdots, u_m) = 0 \ .$$

(See Davis [2, pp. 104–106] or Davis [1, pp. 34–35]). Such a set is also called *diophantine* since it is the set of values of a parameter $s$ for which the diophantine equation $P(s, u_1, \cdots, u_m) = 0$ is solvable in positive integers.

Similarly, a set $\mathcal{S}$ of positive integers is existentially definable in terms

of exponentiation if and only if there is an exponential diophantine equation with one parameter $s$ which is solvable if and only if $s$ belongs to $\mathcal{S}$, and hence such a set is also called *exponential diophantine*. To show that the values of a parameter for which an exponential diophantine equation is solvable do form a set which is existentially definable in terms of exponentiation, we need only check that the relations given by $xy = z$ and $x + y = z$ are existentially definable in terms of exponentiation. But this follows from the equivalences

$$xy = z \longleftrightarrow (2^x)^y = 2^z \longleftrightarrow \mathbf{V}_{u,v}\,(u = 2^x \wedge v = 2^z \wedge v = u^y)$$

and

$$x + y = z \longleftrightarrow 2^x 2^y = 2^z\,.$$

On the other hand, to show that every set which is existentially definable in terms of exponentiation is the set of values of a parameter for which some exponential diophantine equation is solvable, we can use the standard formulas:

$$A = 0 \wedge B = 0 \longleftrightarrow A^2 + B^2 = 0$$

and

$$A = 0 \vee B = 0 \longleftrightarrow AB = 0$$

to combine several equations into a single equation. Thus we can reduce an existential definition in terms of exponentiation to the form

$$s \in \mathcal{S} \longleftrightarrow \mathbf{V}_{u_1,\cdots,u_m} E(s, u_1, \cdots, u_m) = 0$$

where $E = 0$ is an exponential diophantine equation.

Quite similarly, we can speak of *diophantine relations* and *exponential diophantine relations*. For example, the relations given by $x < y$ and $x \mid y$ ($x$ divides $y$) are easily seen to be diophantine.

We now state the main theorem, but we will postpone the proof until § 3.

THEOREM. *Every recursively enumerable set (or relation) is exponential diophantine.*

In other words, every recursively enumerable set $\mathcal{S}$ can be expressed in the form

$$s \in \mathcal{S} \longleftrightarrow \mathbf{V}_{u_1,\cdots,u_m} E(s, u_1, \cdots, u_m) = 0$$

where $E$ is a linear combination (with integer coefficients) of products of terms of the form $\alpha^\beta$ where $\alpha$ and $\beta$ are variables or particular positive integers. Since there are recursively enumerable sets which are not re-

cursive, there is a non-recursive set $\mathcal{N}$ of positive integers which can be expressed in the form

$$n \in \mathcal{N} \longleftrightarrow \mathsf{V}_{u_1,\cdots,u_m} N(n, u_1, \cdots, u_m) = 0$$

where $N = 0$ is an exponential diophantine equation. That is, $n$ belongs to $\mathcal{N}$ if and only if the exponential diophantine equation $N(n, u_1, \cdots, u_m) = 0$ is solvable. Hence, if there were a general algorithm for determining the solvability of exponential diophantine equations, we could determine effectively whether or not $N(n, u_1, \cdots, u_m) = 0$ is solvable for a given $n$ and hence whether or not $n \in \mathcal{N}$. But this is impossible, in general, since $\mathcal{N}$ is a non-recursive set. That is:

COROLLARY 1. *There is no general algorithm for determining whether or not a given exponential diophantine equation is solvable.*

Suppose all exponential diophantine equations are numbered effectively according to some definite scheme, and let $\mathcal{E}_i$ be the $i^{\text{th}}$ equation in this ordering. Also let $x$ be some fixed variable and let $\mathcal{E}_i(u)$ be the equation obtained from $\mathcal{E}_i$ by substituting $u$ for $x$ throughout $\mathcal{E}_i$. We can easily give an effective procedure for listing all exponential diophantine equations which are solvable. Hence the set of positive integers $i$ such that $\mathcal{E}_i$ has a solution is recursively enumerable. Hence, by Corollary 1, the set of positive integers $i$ such that $\mathcal{E}_i$ has no solution is not recursively enumerable. We will now show that there is an effective procedure which, given a proposed effective listing of "unsolvable" exponential diophantine equations, will yield a particular equation which is either on the list (even though it has a solution) or is omitted from the list (even though it has no solution). The argument given is essentially the one used by Post [6] to prove the existence of creative sets.

Let the proposed list of "unsolvable" equations be $\mathcal{F}_1, \mathcal{F}_2, \cdots$. The set $\mathcal{U}$ of positive integers $t$ such that $\mathcal{E}_t(t)$ is "unsolvable" according to the given list is clearly recursively enumerable, since for every $s$ and $t$ we can compare $\mathcal{E}_t(t)$ with $\mathcal{F}_s$ and put $t$ in $\mathcal{U}$ whenever $\mathcal{E}_t(t)$ is $\mathcal{F}_s$. Hence[3], by our main theorem, there is a positive integer $n$ such that $t \in \mathcal{U}$ if and only if $\mathcal{E}_n(t)$ has a solution. Then $\mathcal{E}_n(n)$ is the required counter-example since $\mathcal{E}_n(n)$ is solvable if and only if it is "unsolvable" according to the proposed list.

COROLLARY 2a. *There is a mechanical procedure which, given any*

[3] This argument has a lacuna at this point in that it is tacitly assumed that, from the possession of an algorithm which effectively enumerates $\mathcal{U}$, we can *effectively* obtain the required integer $n$. This difficulty can be overcome by verifying that the *proof* of our main theorem as well as the proof of Theorem B of § 3 is constructive.

*axiomatization*[4] *of number theory, will yield a particular exponential diophantine equation which has no solution, but which cannot be proved to be unsolvable from the given axioms.*

PROOF. We take as the set of "unsolvable" equations those which can be proved unsolvable in the given axiomatization of number theory and list them in order of proof in some systematic way. Then the counter-example corresponding to this list of unsolvable equations must be an equation which is unsolvable but which is not on our list.

COROLLARY 2b. *There is a mechanical procedure which, given any proposed algorithm for testing exponential diophantine equations for solvability, will yield a particular exponential diophantine equation as a counter-example.*

PROOF. Here we take for the list of "unsolvable" equations those equations which are given as "unsolvable" by the proposed algorithm ordered as they appear in the list $\mathcal{E}_1, \mathcal{E}_2, \cdots$.

## 2. Applications to ordinary diophantine equations

We now combine our main theorem with an earlier result of Julia Robinson (Theorem A below) to investigate the relationship of exponential diophantine equations and their decision problem to ordinary diophantine equations and Hilbert's tenth problem. We also obtain a curious theorem about possible bounds for solutions of ordinary diophantine equations.

Let $x * n$ be the $n^{\text{th}}$ super power of $x$. This can be defined recursively by $x * 1 = x$ and $x * (n + 1) = x^{(x*n)}$.

THEOREM A. *The relation given by $z = x^y$ can be defined existentially in terms of addition, multiplication and any relation $\varphi(u, v)$ satisfying the following two conditions:*

(1) *For some $n$, $\varphi(u, v)$ implies $v < u * n$.*

(2) *There is no $n$, such that $\varphi(u, v)$ implies $v < u^n$.*

For the proof of this theorem, see Julia Robinson [8]. Now Theorem A implies that if any relation $\varphi(u, v)$ which satisfies (1) and (2) is diophantine, then the relation given by $z = x^y$ is itself diophantine. This would mean that every exponential diophantine equation could be transformed mechanically into an ordinary diophantine equation with more variables. Hence there could be no algorithm for determining whether or not an arbitrary diophantine equation is solvable. On the other hand, if we could show that some particular recursively enumerable set is not diophantine,

[4] We use here only the two properties: (1) the axiomatization yields an algorithm for proving number-theoretic statements and (2) every exponential diophantine equation proved unsolvable has in fact no solution.

then we would obtain remarkable bounds on every diophantine relation. Corollaries 3 and 4 summarize these remarks and are immediate consequences of our main theorem and Theorem A.

COROLLARY 3. *If any diophantine relation $\varphi(u, v)$ satisfies* (1) *and* (2), *then every recursively enumerable set is diophantine and Hilbert's tenth problem is unsolvable* (i.e., *no algorithm exists for determining the solvability of an arbitrary diophantine equation*).

COROLLARY 4. *If there is any recursively enumerable set which is not diophantine, then given any diophantine equation $P(x, y, u_1, \cdots, u_m) = 0$, either for every $n$ there is a solution with $y > x * n$ or there is an $n$ such that every solution satisfies $y < x^n$.*

Clearly, the relation given by $v = 2^u \wedge u > 1$ satisfies (1) and (2). Hence the relation $z = x^y$ can be existentially defined in terms of addition, multiplication, and this relation. Since a conjunction or a disjunction of equations can be combined into a single equation using only addition and multiplication, we obtain a polynomial $Q(x, y, z, u_1, \cdots, u_k, v_1, \cdots, v_k)$ with integer coefficients such that

$$z = x^y \longleftrightarrow \bigvee_{u_1, \cdots, u_k} Q(x, y, z, u_1, \cdots, u_k, 2^{u_1}, \cdots, 2^{u_k}) = 0 .$$

Then $Q$ can be used to eliminate the general exponential function $x^y$ in terms of addition, multiplication, and the special exponential function $2^x$. Hence we obtain the following reduction of exponential diophantine equations.

COROLLARY 5. *Every recursively enumerable set $\mathcal{S}$ can be given as the set of values of a parameter $s$ for which an equation of the form $P(s, x_1, \cdots, x_k, 2^{x_1}, \cdots, 2^{x_k}) = 0$, where $P$ is a polynomial with integer coefficients, is solvable in positive integers.*

By a straightforward use of the methods of Putnam [7], we have furthermore:

COROLLARY 6. *For every recursively enumerable set $\mathcal{S}$, there is a polynomial $R(x_1, \cdots, x_n, y_1, \cdots, y_n)$ with integer coefficients such that the range of the function $R(x_1, \cdots, x_n, 2^{x_1}, \cdots, 2^{x_n})$ for positive integral values of $x_1, \cdots, x_n$ consists of the members of $\mathcal{S}$ and all non-positive integers.*

PROOF. If $\mathcal{S}$ is the empty set, we can take $R = 1 - x_1$. Otherwise let $P(s, x_1, \cdots, x_k, 2^{x_1}, \cdots, 2^{x_k})$ be chosen by Corollary 5 so that

$$s \in \mathcal{S} \longleftrightarrow \bigvee_{x_1, \cdots, x_k} P(s, x_1, \cdots, x_k, 2^{x_1}, \cdots, 2^{x_k}) = 0 .$$

Let $Q(s, t, u, x_1, \cdots, x_k) = s(1 - P^2) - (t - 1)(s + u - 1)$. Since $Q$ is a function of the desired form (with $n = k + 3$), it is sufficient to check

that the range of $Q$ is the union of $\mathcal{S}$ and the non-positive integers. For $Q > 0$, we must have $P = 0$ and $t = 1$; in which case, $Q = s$ where $s \in \mathcal{S}$. Conversely, if $s \in \mathcal{S}$ and we take $t = 1$, $u$ arbitrary, and $x_1, \cdots, x_k$ so that $P = 0$, then $Q = s$. Finally, choose $s, x_1, \cdots, x_k$ so that $P = 0$ and take $t = 2$, then $Q = 1 - u$ which assumes all non-positive integers.

A rather amusing variation of Corollary 6 is obtained by considering the natural numbers (the non-negative integers) as the domain of the variables:

COROLLARY 7. *Every non-empty recursively enumerable set of natural numbers is the range of a function obtained from particular natural numbers and variables (whose domain is the natural numbers) by addition, subtraction, multiplication and exponentiation.*

PROOF. Again let $P(s, x_1, \cdots, x_k, 2^{x_1}, \cdots, 2^{x_k})$ be the function of Corollary 5 (modified so that the sets and variables range over the natural numbers) corresponding to a given non-empty set $\mathcal{S}$. Let $a$ be any element of $\mathcal{S}$. Then the range of the function

$$(s - a)0^{P^2} + a$$

is exactly $\mathcal{S}$. (Here, it is understood that $0^0 = 1$.)

Finally, we obtain a theorem about possible bounds for solutions of a diophantine equation with a finite number of solutions. As far as we know, it is the first general theorem about bounds for solutions of arbitrary diophantine equations. Since our method of proof is quite roundabout, it seems likely that number theorists can come up with a direct proof and perhaps an improvement.

COROLLARY 8. *Consider diophantine equations $P(x, y, u_1, \cdots, u_m) = 0$ such that to every $x$ there are but a finite number of values of $y$ for which $P = 0$ is solvable. If to every such equation $P = 0$ there are $k$ and $n$ so that every solution of $P = 0$ satisfies $y < k(x * n)$, then to every such equation there are $k'$ and $n'$ so that each solution satisfies $y < k'x^{n'}$.*

PROOF. Suppose some relation $\varphi$ satisfying (1) and (2) is diophantine. Then every recursively enumerable relation would be diophantine. In particular, there would be a diophantine equation $P(x, y, u_1, \cdots, u_m) = 0$ which is solvable if and only if $y = x * x$. But for such an equation, there could not be super-power bounds on $y$ in terms of $x$. Hence the hypothesis of the corollary implies that no diophantine relation satisfies (1) and (2). But if $\varphi(u, v)$ is diophantine and $\varphi(u, v)$ implies $v < k(u * n)$, then the relation $\varphi(u, v) \wedge u > 1$ is also diophantine and satisfies (1) for some value of $n$. Hence it must fail to satisfy (2). That is, for some $n'$, $\varphi(u, v) \wedge u > 1$ implies $v < u^{n'}$. Therefore for some $k'$ and $n'$, $\varphi(u, v)$ implies $v < k'u^{n'}$.

## 3. Proof of the main theorem

We show first that the binomial coefficient

$$\binom{\alpha}{k} = \alpha(\alpha - 1) \cdots (\alpha - k + 1)/k!$$

is existentially definable in terms of exponentiation for rational values of $\alpha$ greater than $k$. That is:

LEMMA 1. *The relation given by*

$$x/y = \binom{p/q}{k} \wedge p > qk$$

*is exponential diophantine.*

PROOF. Let $\alpha = p/q$, $\alpha > k$. Then, by Taylor's theorem with Lagrange's form for the remainder

$$\begin{aligned} a^{2k+1}(1 + a^{-2})^{\alpha} &= \sum_{j=0}^{k} \binom{\alpha}{j} a^{2k-2j+1} + \binom{\alpha}{k+1} a^{-1}(1 + \theta a^{-2})^{\alpha-k-1} \\ &= \sum_{j=0}^{k} \binom{\alpha}{j} a^{2k-2j+1} + \theta' \alpha^{k+1} a^{-1} 2^{\alpha-1} \end{aligned}$$

where $\theta$ and $\theta'$ are some real numbers between 0 and 1. Let $\alpha = p/q$ and $S_k(a) = \sum_{j=0}^{k} \binom{\alpha}{j} a^{2k-2j+1}$. We wish to choose $a$ so that

$$S_k(a) = [a^{2k+1}(1 + a^{-2})^{p/q}]$$

and

$$S_{k-1}(a) = [a^{2k-1}(1 + a^{-2})^{p/q}] .$$

Here $[\lambda]$ is the greatest integer in $\lambda$.

Suppose $q^k k! \mid a$ (i.e., $q^k k!$ divides $a$), then both $S_k(a)$ and $S_{k-1}(a)$ are integers, since the denominator of $\binom{p/q}{j}$ divides $q^k k!$ for all $j \leqq k$ and $a$ comes in each term of the sums to at least the first power. Also if $a > 2^{p-1} p^{k+1}$, then the remainders in the expressions obtained by Taylor's theorem (for both $k$ and $k - 1$) are less than 1. Hence if we put $a = 2^p p^{k+1} q^k k!$, then

$$\begin{aligned} u = S_k(a) &\longleftrightarrow u \leqq a^{2k+1}(1 + a^{-2})^{p/q} > u + 1 \\ &\longleftrightarrow a^{2p} u^q \leqq a^{(2k+1)q}(a^2 + 1)^p < a^{2p}(u + 1)^q \end{aligned}$$

and a similar formula holds for $S_{k-1}(a)$. Therefore both $S_k(a)$ and $S_{k-1}(a)$ are existentially definable in terms of exponentiation and factorial for this particular choice of $a$. Since the relation $y = x!$ is exponential diophantine, (see Julia Robinson [8]) $u = S_k(a)$ and $v = S_{k-1}(a)$ are also exponential

diophantine relations of $u$, $v$, $p$, $q$, and $k$. The lemma follows from

$$\binom{p/q}{k} = a^{-1}S_k(a) - aS_{k-1}(a) .$$

LEMMA 2. *The relation* $y = \prod_{k\leq K}(a + bk)$ *is exponential diophantine*[5].

PROOF. $\prod_{k\leq K}(a + bk) = \binom{a/b + K}{K} b^K K!$ .

We next recall the following basic theorem[6].

THEOREM B. *Every recursively enumerable set* $\mathcal{S}$ *can be expressed in the form*

$$x \in \mathcal{S} \longleftrightarrow \bigvee_y \bigwedge_{k\leq y} \bigvee_{z_1\leq y} \cdots \bigvee_{z_m\leq y} P(x, y, k, z_1, \cdots, z_m) = 0$$

*where* $P$ *is a polynomial with integer coefficients.*

From this it follows that we need only show that every relation of the form

$$\bigwedge_{k\leq y} \bigvee_{z_1\leq y} \cdots \bigvee_{z_m\leq y} P(x, y, k, z_1, \cdots, z_m) = 0$$

where $P$ is a polynomial, is exponential diophantine, in order to obtain our main theorem. But this last will follow at once from Lemma 2 and the following lemma:

LEMMA 3. *Let* $F(x, y, k, z_1, \cdots, z_m)$ *be any polynomial with integer coefficients. Let* $G(x, y)$ *be any polynomial*[7] *such that* $G(x, y) \geqq y$ *and*

$$\bigwedge_{k\leq y} \bigwedge_{z_1\leq y} \cdots \bigwedge_{z_m\leq y} | F(x, y, k, z_1, \cdots, z_m) | \leqq G(x, y) .$$

*Then*

$$\begin{aligned} &\bigwedge_{k\leq y} \bigvee_{z_1\leq y} \cdots \bigvee_{z_m\leq y} F(x, y, k, z_1, \cdots, z_m) = 0 \\ (3)\quad &\longleftrightarrow \bigvee_c \bigvee_t \bigvee_{a_1} \cdots \bigvee_{a_m} \{t = G(x, y)! \wedge 1 + ct = \prod_{k\leq y}(1 + kt) \\ &\quad \wedge 1 + ct \mid F(x, y, c, a_1, \cdots, a_m) \wedge \bigwedge_{i\leq m} 1 + ct \mid \prod_{j\leq y}(a_i - j)\} . \end{aligned}$$

PROOF. We shall first assume the right side of the equivalence and show that it implies the left side. Let $k$ be any number not exceeding $y$ and $p_k$ be a prime dividing $1 + kt$. Then put

$$\text{Rem } (a_i, p_k) = z_{ki} \qquad \text{for } i = 1, \cdots, m .$$

[5] That $\binom{a}{k}$ and $\Pi_{k\leq K}(a + bk)$ are exponential diophantine was first proved by Davis and Putnam, extending the methods of Julia Robinson [8]. Note that the lemma remains true if $a$ or $b$ is zero.

[6] Cf., Davis [2], pp. 113-114. R. M. Robinson [9] gave a new proof of this result in which he showed that we can actually take $m = 4$. However, we shall not make use of this fact here.

[7] If $n > 0$ is the degree of $F$, then we can, for example, take $G(x, y) = cx^n y^n$ where $c$ is the sum of the absolute values of the coefficients of $F$.

It will be sufficient to show that

$$F(x, y, k, z_{k1}, \cdots, z_{km}) = 0$$

and

$$0 < z_{ki} \leqq y \qquad \text{for all } i \leqq m .$$

Since $p_k \mid \prod_{j \leqq y}(a_i - j)$ we have $p_k \mid a_i - j$ for some $j$ with $1 \leqq j \leqq y$. Thus $1 \leqq z_{ki} = \text{Rem } (a_i, p_k) \leqq y$. Furthermore $(p_k, t) = 1$ and $t = G(x, y)!$, so $p_k > G(x, y) \geqq y$. Hence, since $1 \leqq z_{ki} \leqq y$,

$$| F(x, y, k, z_{k1}, \cdots, z_{km}) | \leqq G(x, y) < p_k .$$

From the equation which determines $c$, we have $1 + ct \equiv 0 \pmod{1 + kt}$. Hence $c \equiv k \pmod{1 + kt}$ and finally, $c \equiv k \pmod{p_k}$. Therefore

$$\begin{aligned} F(x, y, k, z_{k1}, \cdots, z_{km}) &\equiv F(x, y, c, a_1, \cdots, a_m) && \pmod{p_k} \\ &\equiv 0 && \pmod{p_k} . \end{aligned}$$

Hence $F(x, y, k, z_{k1}, \cdots, z_{km}) = 0$ which was to be proved.

On the other hand, suppose the left side of the equivalence holds. That is, for every $k \leqq y$, there are $z_{k1}, \cdots, z_{km} \leqq y$ such that

$$F(x, y, k, z_{k1}, \cdots, z_{km}) = 0 .$$

We need to show that the right side can be satisfied. Let $t$ and $c$ be determined by the two equations on the right side. Then for every $k, j \leqq y$ and $k \neq j$, $(1 + kt, 1 + jt) = 1$. We see this by noticing that if a prime $p$ divides both $1 + kt$ and $1 + jt$, then $p$ divides $(k - j)t$. But any prime dividing $k - j$ also divides $t$ since $t = G(x, y)!$ and $G(x, y) \geqq y$. Hence $p \mid t$ but then it cannot divide $1 + kt$. So $1 + kt$ and $1 + jt$ are relatively prime. Hence by the Chinese Remainder Theorem, there are $a_1, \cdots, a_m$ so that

$$a_i \equiv z_{ki} \pmod{1 + kt} \qquad \text{for } k \leqq y \text{ and } i \leqq m . \tag{4}$$

We will show that these $a_1, \cdots, a_m$ satisfy the right side of the equivalence. As before $c \equiv k \pmod{1 + kt}$, so that

$$\begin{aligned} F(x, y, c, a_1, \cdots, a_m) &\equiv F(x, y, k, z_{k1}, \cdots, z_{km}) && \pmod{1 + kt} \\ &\equiv 0 && \pmod{1 + kt} \end{aligned}$$

for $k \leqq y$. Since all the moduli are relatively prime, it follows that

$$\prod_{k \leqq y}(1 + kt) \mid F(x, y, c, a_i, \cdots, a_m) .$$

But from (4) we have

$$1 + kt \mid a_i - z_{ki} \qquad \text{where } z_{ki} \leqq y .$$

Hence

$$1 + kt \mid \prod_{j \leqq y}(a_i - j) \qquad \text{for every } k \leqq y .$$

But since these divisors are relatively prime, we obtain

$$\prod_{k \leqq y}(1 + kt) \mid \prod_{j \leqq y}(a_i - j) \qquad \text{for every } i \leqq m .$$

Hence the right side of the equivalence holds and the lemma follows.

In order to complete the proof of our theorem, we need only check that the relations appearing on the right side of the equivalence in Lemma 3 are exponential diophantine.

We have already seen that the relations $u = v!$ and $u = \prod_{k \leqq y}(1 + kt)$ are exponential diophantine. The relation $u \mid v$ is of course equivalent to $\mathsf{V}_w uw = v$. Finally,

$$1 + ct \mid \prod_{j \leqq y}(a_i - j) \longleftrightarrow a_i \leqq y \vee \mathsf{V}_u\{a_i > y \wedge (1 + ct)u = \prod_{j \leqq y}(a_i - y - 1 + j)\} .$$

Hence the relations appearing on the right side of (3) are exponential diophantine. Thus, every relation of the form

$$\mathsf{A}_{k \leqq y}\, \mathsf{V}_{z_1 \leqq y} \cdots \mathsf{V}_{z_m \leqq y} F(x, y, k, z_1, \cdots, z_m) = 0 ,$$

where $F$ is a polynomial with integer coefficients, is exponential diophantine. Finally, by Theorem B, every recursively enumerable set is exponential diophantine.

The fact that every recursively enumerable relation $\rho(x_1, \cdots, x_n)$ is exponential diophantine follows from the result for sets. For, let the set $\mathcal{R}$ be defined by the equivalence:

$$r \in \mathcal{R} \longleftrightarrow \mathsf{V}_{x_1, \cdots, x_n}(r = 2^{x_1}3^{x_2} \cdots p_n^{x_n} \wedge \rho(x_1, \cdots, x_n))$$

where $p_n$ is the $n^{\text{th}}$ prime. If $\rho$ is a recursively enumerable relation, then $\mathcal{R}$ is a recursively enumerable set. Hence $\mathcal{R}$ is exponential diophantine. But

$$\rho(x_1, \cdots, x_n) \longleftrightarrow 2^{x_1}3^{x_2} \cdots p_n^{x_n} \in \mathcal{R} .$$

Hence $\rho$ is also exponential diophantine.

NEW YORK UNIVERSITY
PRINCETON UNIVERSITY
UNIVERSITY OF CALIFORNIA, BERKELEY

BIBLIOGRAPHY

1. MARTIN DAVIS, *Arithmetical problems and recursively enumerable predicates*, J. Symb. Logic, 18 (1953), 33-41.
2. ———, Computability and Unsolvability, McGraw-Hill, 1958.
3. ——— and HILARY PUTNAM, *Reduction of Hilbert's tenth problem*, J. Symb. Logic, 23 (1958), 183-187.

4. DAVID HILBERT, *Mathematische Probleme. Vortrag, gehalten auf dem internationalen Mathematiker-Kongress zu Paris 1900.* Nachr. K. Ges. Wiss. Göttingen, Math.-Phys. Kl. 1900, 253-297. Reprinted, Arch. Math. Phys., 3s, 1 (1901), 44-63, 213-237. English translation, Bull. Amer. Math. Soc., 8 (1901-1902), 437-479.
5. S. C. KLEENE, Introduction to Metamathematics, D. Van Nostrand Co., Inc., 1952.
6. E. L. POST, *Recursively enumerable sets of positive integers and their decision problems,* Bull. Amer. Math. Soc., 50 (1944), 284-316.
7. HILARY PUTNAM, *An unsolvable problem in number theory,* to appear in the J. Symb. Logic.
8. JULIA ROBINSON, *Existential definability in arithmetic,* Trans. Amer. Math. Soc., 72 (1952), 437-449.
9. R. M. ROBINSON, *Arithmetical representation of recursively enumerable sets,* J. Symb. Logic, 21 (1956), 162-186.