DIOPHANTINENESS OF ENUMERABLE SETS

MATHEMATICS

1970

SovietRxiv

Abstract

Full Text

UDC 51.01:518.5+511.5

MATHEMATICS

Yu. V. MATIYASEVICH

DIOPHANTINENESS OF ENUMERABLE SETS

(Presented by Academician I. M. Vinogradov on 5 II 1970)

Hilbert' s 10th problem was formulated in the following way (see ([1])):

Given a Diophantine equation with an arbitrary number of unknowns and integer rational coefficients. Indicate a method by which, in a finite number of operations, one can determine whether this equation is solvable in rational integers.

When this problem was formulated, only a positive solution of the problem could have been in question, since the precise concept of an algorithm had not yet been developed. The emergence of this concept made it possible to prove the algorithmic unsolvability of mass problems.

Such unsolvable problems were found first in mathematical logic, and then in algebra and number theory. In particular, M. Davis, H. Putnam, and J. Robinson ([2]) proved that there is no algorithm allowing one to recognize the existence of integer solutions of the so-called **exponential-Diophantine equations**, i.e., equations that are built from natural numbers and variables by means of addition, multiplication, and exponentiation. Using this result, as well as the work of J. Robinson ([3]), we shall show that Hilbert' s 10th problem is also algorithmically unsolvable.

1. Lowercase Latin letters, except for i and j, are used everywhere below as variables for positive integers; i and j are variables ranging over nonnegative integers.

We shall say that a predicate* $\mathcal{P}(u, v)$ **has exponential growth** if $\mathcal{P}(u, v)$ implies the inequality $v \leq u^u$ and, for every k, there exist u, v such that $\mathcal{P}(u, v)$ and $u^k < v$.

A predicate $\mathcal{S}(x_1, \ldots, x_n)$ is called **Diophantine** if one can indicate a polynomial** M such that $\mathcal{S}(x_1, \ldots, x_n)$ holds if and only if there exist numbers $y_1, \ldots, y_j$ such that

$$M(x_1, \ldots, x_n, y_1, \ldots, y_j) = 0.$$

From the above-mentioned works of M. Davis, H. Putnam, and J. Robinson it follows that if at least one Diophantine predicate has exponential growth, then every enumerable*** predicate is Diophantine.

The predicate "v is the $2u$-th Fibonacci number" has exponential growth. We shall establish its Diophantineness. This will thereby complete the proof of the following assertion:

Every enumerable predicate is Diophantine.

Moreover, for every n one can indicate an $(n+1)$-ary Diophantine predicate $\mathcal{U}_n(x_1, \ldots, x_n, s)$ such that any enumerable n-ary predicate can be obtained from $\mathcal{U}_n$ by fixing the value of s.

Since there exist enumerable but algorithmically unsolvable predicates (see ([4], [5])), the following assertion is valid:

* By predicates we mean properties and relations that are representable by formulas of the formal arithmetical language.

** Without loss of generality, one may assume that the degree of the polynomial M is not greater than 4.

*** A predicate is called **enumerable** if one can indicate an effectively computable sequence of n-tuples of numbers containing all and only those n-tuples on which it is true.

There is no algorithm that makes it possible to determine, for an arbitrary Diophantine equation, whether it has solutions.*

Combining our result with the results of paper ([6]), we also obtain the following consequences:

1) One can specify a polynomial of degree five $Q(y_1, \ldots, y_k, z)$ with integer coefficients such that any enumerable set $\mathcal{M}$ of natural numbers (for example, the set of prime numbers) coincides with the set of natural values of the polynomial $Q(y_1, \ldots, y_k, a_M)$, where a_M is a certain number effectively constructed from the set $\mathcal{M}$.

2) One can specify polynomials $R(y_1, \ldots, y_k, z)$ and $S(y_1, \ldots, y_k, z)$ with integer coefficients such that any enumerable set of integers coincides with the set of integral values of the fraction

$$\frac{S(y_1, \ldots, y_k, a_M)}{R(y_1, \ldots, y_k, a_M)},$$

where a_M is a certain number effectively constructed from the set $\mathcal{M}$.

3) One can specify a polynomial of degree five $D(y_1, \ldots, y_k)$ with integer coefficients such that there is no algorithm making it possible to determine, from the number n, whether the equation $D(y_1, \ldots, y_k) = n$ has solutions.

2. Definition 1. $\varphi_0 = 0,\ \varphi_1 = 1,\ \varphi_{n+1} = \varphi_n + \varphi_{n-1}.$ φ_j is called the j-th Fibonacci number.

Lemma 1. $\varphi_{2(n+1)} = 3\varphi_{2n} - \varphi_{2(n-1)}.$

Corollary. $\varphi_{2(n-1)} = 3\varphi_{2n} - \varphi_{2(n+1)}.$

Lemma 2. $\varphi_{2(k+j)} \equiv -\varphi_{2(k+1-j)} \pmod{\varphi_{2k} + \varphi_{2k+2}}$, $0 \le j \le k+1$ (induction on j; the induction step follows from Lemma 1 and its corollary).

Lemma 3. $\varphi_{2(2k+1+j)} \equiv \varphi_{2j} \pmod{\varphi_{2k} + \varphi_{2k+2}}$ (induction on j; the basis follows from Lemmas 2 and 1, and the induction step from Lemma 1).

Lemma 4. $\varphi_{2((2k+1)i+j)} \equiv \varphi_{2j} \pmod{\varphi_{2k}+\varphi_{2k+2}}$ (induction on i; the induction step follows from Lemma 3).

Corollary of Lemmas 4 and 2. Modulo $(\varphi_{2k} + \varphi_{2k+2})$

$$\varphi_{2((2k+1)i+j)} \equiv \begin{cases} \varphi_{2j}, & \text{for } 0 \le j \le k, \\ \varphi_{2k} + \varphi_{2k+2} - \varphi_{2(2k+1-j)}, & \text{for } k+1 \le j \le 2k. \end{cases}$$

Definition 2. For every $m \ge 2,\ \psi_{m,0} = 0,\ \psi_{m,1} = 1,\ \psi_{m,n+1} = m\psi_{m,n} - \psi_{m,n-1}.$

Lemma 5. If $m \ge 2,\ d \mid (m-3)$, then $\psi_{m,j} \equiv \varphi_{2j} \pmod{d}$ (induction on j; the induction step follows from Lemma 1).

Lemma 6. If the numbers k, m, n, v are such that $m \ge 2,\ v < \varphi_{2k+1},\ (\varphi_{2k} + \varphi_{2k+2}) \mid (m-3),\ \psi_{m,n} \equiv v \pmod{\varphi_{2k} + \varphi_{2k+2}}$, then there exist numbers i, j such that $v = \varphi_{2j},\ n = (2k+1)i + j$ (by Lemma 5 and the corollary of Lemmas 4 and 2).

Lemma 7. If $m \ge 2,\ l \mid (m-2)$, then $\psi_{m,j} \equiv j \pmod{l}$ (induction on j).

Lemma 8. $\varphi_{i+1}^2 - \varphi_i\varphi_{i+1} - \varphi_i^2 = (-1)^i$ (induction on i).

Lemma 9. If the numbers j, k are such that $(k^2 - jk - j^2)^2 = 1$, then there exists a number i such that $j = \varphi_i,\ k = \varphi_{i+1}$ (reverse induction on $j+k$: if $j > 0$, then $j \le k$; put $j_1 = k - j,\ k_1 = j$, then $(k_1^2 - j_1k_1 - j_1^2)^2 = 1,\ j_1 + k_1 < j + k$).

Lemma 10. For every $m \ge 2$,

$$\psi_{m,i+1}^2 - m\psi_{m,i}\psi_{m,i+1} + \psi_{m,i}^2 = 1$$

(induction on i).

Lemma 11. If the numbers j, k, m are such that $m \ge 2,\ j \le k,\ k^2 - mjk + j^2 = 1$, then there exists a number i such that $j = \psi_{m,i},\ k = \psi_{m,i+1}$ (analogously to Lemma 9).

---

* Here it is immaterial whether we are interested in integer, positive-integer, or nonnegative-integer solutions, since, as is known, these three mass problems are equivalent to one another (see ([4], [5])).

Lemma 12. $\text{g. c. d.}(\varphi_i, \varphi_j) = \varphi_{\text{g.c.d.}(i,j)}$ (proved in (7)).

Corollary. $\varphi_n \mid \varphi_{jn}$.

Lemma 13. If p and q are prime numbers, $p \mid \varphi_n$, $q \neq p$, then $p\varphi_n \nmid \varphi_{qn}$.

If p is a prime number, $p \neq 2$, $p \mid \varphi_n$, then $p\varphi_n \mid \varphi_{pn}$, but $p^2\varphi_n \nmid \varphi_{pn}$.

If $2 \mid \varphi_n$, $4 \nmid \varphi_n$, then $4\varphi_n \mid \varphi_{2n}$, but $8\varphi_n \nmid \varphi_{2n}$.

If $4 \mid \varphi_n$, then $2\varphi_n \mid \varphi_{2n}$, but $4\varphi_n \nmid \varphi_{2n}$.

The lemma is proved in (7).

Lemma 14. If p is a prime number, $p \mid \varphi_n$, $p \nmid r$, then $p\varphi_n \nmid \varphi_{rn}$ (induction on the number of prime factors of the number r; the induction step follows from Lemma 12 and Lemma 13).

Lemma 15. If p is a prime number, $p \neq 2$, $p \mid \varphi_n$, then $p^i\varphi_n \mid \varphi_{p^in}$, but $p^{i+1}\varphi_n \nmid \varphi_{p^in}$ (induction on i; the induction step follows from Lemma 12 and Lemma 13).

Lemma 16. If $4 \mid \varphi_n$, then $2^i\varphi_n \mid \varphi_{2^in}$, but $2^{i+1}\varphi_n \nmid \varphi_{2^in}$ (analogously to Lemma 15).

Lemma 17. $\varphi_s^2 \mid \varphi_{rs}$ if and only if $\varphi_s \mid r$ (follows from Lemmas 13-16).

Corollary of Lemmas 12 and 17. If $\varphi_s^2 \mid \varphi_t$, then $\varphi_s \mid t$.

Lemma 18. $2\varphi_{2n} < \varphi_{2(n+1)} \leq 3\varphi_{2n}$ (follows from Lemma 1).

Lemma 19. $n \leq 2^{n-1} \leq \varphi_{2n} < 3^n$ (induction on n; the induction step is by Lemma 18).

3. Theorem. In order that v be the $2u$-th Fibonacci number, it is necessary and sufficient that there exist numbers g, h, l, m, x, y, z such that:

$$u \leq v < l, \tag{1}$$

$$l^2 - lz - z^2 = 1, \tag{2}$$

$$g^2 - gh - h^2 = 1, \tag{3}$$

$$l^2 \mid g, \tag{4}$$

$$l \mid m-2, \tag{5}$$

$$(2h+g) \mid (m-3), \tag{6}$$

$$x^2 - mxy + y^2 = 1, \tag{7}$$

$$l \mid (x-u), \tag{8}$$

$$(2h+g) \mid (x-v). \tag{9}$$

Sufficiency. Let the numbers $u, v, g, h, l, m, x, y, z$ satisfy conditions (1)–(9). According to Lemma 9, from (2) it follows that there exists a number s such that

$$l = \varphi_s. \tag{10}$$

According to Lemmas 9 and 8, from (3) it follows that there exists a number k such that

$$h = \varphi_{2k}, \quad g = \varphi_{2k+1}. \tag{11}$$

Hence

$$2h + g = \varphi_{2k} + \varphi_{2k+2}. \tag{12}$$

According to the corollary of Lemmas 12 and 17, from (10)–(11), (4) it follows that

$$l \mid (2k+1). \tag{13}$$

From (1), (4), (11), (5) it follows that

$$2 \leq l < \varphi_{2k+1}, \quad m \geq 2. \tag{14}$$

According to Lemma 11, from (14), (7) it follows that there exists a number n such that

$$x = \psi_{m,n}. \tag{15}$$

According to Lemma 6, from (14), (1), (12), (6), (9) it follows that there exist numbers i, j such that

$$v = \varphi_{2j}, \quad n = (2k+1)i + j. \tag{16}$$

According to Lemma 7, from (14), (5), (15) it follows that $x \equiv n (\mathrm{mod}\, l)$. Hence, from (8), (16), (13) it follows that

$$u \equiv j (\mathrm{mod}\, l). \tag{17}$$

According to Lemma 19, from (16) it follows that $j \leqslant v$. Hence, from (1), (17) it follows that $u = j$, and, according to (16), $v = \varphi_{2u}$. Sufficiency is established.

Necessity. Let $v = \varphi_{2u}$. According to Lemma 19, the first inequality in (1) is satisfied. Put $l = \varphi_{6s+1}$, $z = \varphi_{6s}$, where s is so large that the second inequality in (1) is also satisfied. According to Lemma 8, condition (2) is satisfied. Put $g = \varphi_{l(6s+1)}$, $h = \varphi_{l(6s+1)-1}$. According to Lemma 17, condition (4) is satisfied. According to Lemma 12, l is odd, since $2 = \varphi_3$. Therefore, according to Lemma 8, condition (3) is also satisfied. According to Lemma 12, $\gcd(h, g) = 1$, and since l is odd and divides g, we have $\gcd(2h + g, l) = 1$. Therefore, according to the Chinese remainder theorem, we can choose a number m so that conditions (5)–(6) are satisfied. Put $x = \psi_m$, u, $y = \psi_{m,u+1}$. According to Lemma 10, condition (7) is satisfied; according to Lemma 7, condition (8) is satisfied; according to Lemma 5, condition (9) is satisfied. Necessity is proved.

Conditions (1)–(9) can easily be replaced by a single Diophantine predicate (see ([4], [5])). Thus the predicate "v is the $2u$-th Fibonacci number" is Diophantine. It follows from Lemma 19 that it has exponential growth.

4. Some constructions of the present work were inspired by the methods of J. Robinson from the article ([8]).

Leningrad Branch of the V. A. Steklov Mathematical Institute of the Academy of Sciences of the USSR

Received 5 II 1970

REFERENCES

[1] D. Hilbert, *Gesammelte Abhandlungen*, **3**, Berlin, 1935.
[2] M. Davis, H. Putnam, J. Robinson, *Ann. Math.*, **74**, 3, 425 (1961); Russian transl.: *Sborn. per. Matematika*, **8**, 5, 69 (1964).
[3] J. Robinson, *Trans. Amer. Math. Soc.*, **72**, 3, 437 (1952); Russian transl.: *Sborn. per. Matematika*, **8**, 5, 3 (1964).
[4] A. I. Mal' tsev, *Algorithms and Recursive Functions*, Moscow, 1965.
[5] M. Davis, *Computability and Unsolvability*, N. Y., 1958.
[6] H. Putnam, *J. Symb. Logic*, **25**, 3, 220 (1960); Russian transl.: *Sborn. per.*

Matematika, **8**, 5, 55 (1964).
[7] N. N. Vorob' ev, *Fibonacci Numbers*, Moscow, 1969.
[8] J. Robinson, *Proc. Am. Math. Soc.*, **22**, 2, 534 (1969).

Note: Figure translations are in progress. See original paper for figures.