



Enumerable Sets are Diophantine. by Ju. V. Matijasevič; A. Doohovskoy

Review by: Julia Robinson

The Journal of Symbolic Logic, Vol. 37, No. 3 (Sep., 1972), pp. 605-606

Published by: [Association for Symbolic Logic](#)

Stable URL: <http://www.jstor.org/stable/2272763>

Accessed: 10/06/2014 21:02

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at

<http://www.jstor.org/page/info/about/policies/terms.jsp>

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.



Association for Symbolic Logic is collaborating with JSTOR to digitize, preserve and extend access to *The Journal of Symbolic Logic*.

<http://www.jstor.org>

A. O. Slisenko, *Seminars in Mathematics*, V. A. Steklov Mathematical Institute, Leningrad, vol. 8, Consultants Bureau, New York-London 1970, pp. 68–74.

The two reductions of Hilbert's tenth problem given in this paper are of the following form: A class of predicates Q_1, Q_2, Q_3, \dots is given, and it is shown that for any recursively enumerable set \mathfrak{A} there is a representation of \mathfrak{A} , for some Q_i , of the form $a \in \mathfrak{A} \Leftrightarrow \exists y_1 y_2 \dots y_m x_1 x_2 \dots x_n [P(a, y_1, \dots, y_m, x_1, \dots, x_n) = 0 \ \& \ Q_i(y_1, \dots, y_m)]$ where P is a polynomial with integer coefficients; it follows that if all predicates Q_i in the class are Diophantine, then every recursively enumerable set is Diophantine and Hilbert's tenth problem is unsolvable.

To define the first class of predicates $M_2, M_3, \dots, M_s, \dots$, first let $M'_s(w)$ be true iff w is a word on the alphabet $\{0, 1\}$ of the form $10^s \beta_1 0^s \beta_2 0^s \dots \beta_n 0^s$ where each β_i is 0 or 1 and then associate each word $z_k z_{k-1} \dots z_1$ on the alphabet $\{0, 1\}$ with the number $\sum_i z_i \phi_i$ (ϕ_i is the i th Fibonacci number); $M_s(y)$ is then defined to be true iff $M'_s(w)$ where w is the word associated with y by this rule.

The second class contains predicates of the form $K(p, q, s)$ defined on natural numbers which represent real numbers α in the sense that if $K(p, q, s)$ is true then $|p/q - \alpha| < 1/s$, and for all n there exist p, q , and $s > n$ such that $K(p, q, s)$. The real numbers α represented by the predicates considered are of the form $\alpha_i = \sum_{j=0}^{\infty} a_j ((\frac{1}{2} + \frac{1}{2}\sqrt{5})^{i+j})^{-j}$ where $i \geq 2$, each $a_j = 0$ or 1, and the series a_0, a_1, a_2, \dots is universal in the sense that for any other finite series b_0, b_1, \dots, b_k of 0's and 1's, there is some n such that $a_{i+n} = b_i, 0 \leq i \leq k$.

ANN S. FEREBEE

Ů. V. MATIÁSEVIČ. *Arifmetičeskíe představení stěpéněj. Isslédovániá po konstruktivnoj matematiké i matematičeskój logiké, II*, edited by A. O. Slisenko, Zapiski Naučnyh Séminarov Léningradskogo Otdéleníá Ordéna Lénina Matématičeskogo Instituta im. V. A. Stéklóva AN SSSR, vol. 8, Izdatél'stvo "Nauka," Leningrad 1968, pp. 159–165.

YU. V. MATIYASEVICH. *Arithmetic representations of powers*. English translation of the preceding. *Studies in constructive mathematics and mathematical logic, Part II*, edited by A. O. Slisenko, *Seminars in Mathematics*, V. A. Steklov Mathematical Institute, Leningrad, vol. 8, Consultants Bureau, New York-London 1970, pp. 75–78.

Davis, Putnam, and J. Robinson (XXXV 151) showed that every recursively enumerable set can be represented by a Diophantine predicate if the predicate $q \text{ Pow } p$ (q is a power of p) is Diophantine. The author does not show that it is Diophantine, but he does find an explicit arithmetical representation of the closely related predicate $q \text{ Pow } 2n + 1$ of the form $\forall k \exists t s x y [M(k, t, s, x, y, n, q) = 0] \equiv \forall k \leq q \exists t s x y [M(k, t, s, x, y, n, q) = 0]$. This form is simpler than the representation which would be obtained by R. M. Robinson's methods (XXIV 170) and it makes use of properties of the continued fraction approximation to an irrational square root.

ANN S. FEREBEE

Ů. V. MATIÁSEVIČ. *Diofantovost' péréčislímyh množéstv. Doklady Akadémii Nauk SSSR*, vol. 191 (1970), pp. 279–282.

JU. V. MATIJASEVIČ. *Enumerable sets are diophantine*. English translation of the preceding by A. Doohovskoy. *Soviet mathematics*, vol. 11 no. 2 (1970), pp. 354–357. See *Errata*, *ibid.*, vol. 11 no. 6 (for 1970, pub. 1971), p. vi.

Hilbert's tenth problem as proposed in 1900 was to give a method for telling by means of a finite number of operations whether an arbitrary polynomial equation with integer coefficients has a solution in integers. It does not matter whether we ask for natural number solutions or integer solutions since it is known that the decision problems are equivalent. Here it is shown that no such method exists. In fact, a much stronger theorem is obtained. Let a relation R on the natural numbers be called *Diophantine* if there is some polynomial P with integer coefficients such that

$$R(x_1, \dots, x_n) \leftrightarrow (\exists y_1, \dots, y_k) [P(x_1, \dots, x_n, y_1, \dots, y_k) = 0].$$

The author shows that *every recursively enumerable relation is Diophantine*.

From this sweeping theorem, it is immediate that Hilbert's problem is unsolvable. Let S be a non-recursive recursively enumerable set. Choose a polynomial P such that $n \in S$ iff $P(n, y_1, \dots, y_k) = 0$ has a solution for y_1, \dots, y_k in natural numbers. Then a decision method for the

solvability of $P(n, y_1, \dots, y_k) = 0$ for $n = 0, 1, 2, \dots$ would be a means of computing S , but this is impossible because S is not recursive.

Another corollary mentioned by the author is the following: One can specify a fifth-degree polynomial $Q(y_1, \dots, y_k, z)$ with integer coefficients such that every recursively enumerable set M of natural numbers coincides with the set of non-negative values of the polynomial $Q(y_1, \dots, y_k, a_M)$ where a_M is a certain number effectively constructed for the set M .

The proof is based on two earlier results: (1) The exponential function is Diophantine if there is any Diophantine relation of exponential growth (Julia Robinson 1952, XX 182); and (2) every recursively enumerable relation is exponential Diophantine (Davis, Putnam, and Robinson 1961, XXXV 151). Exponential Diophantine relations are defined similarly to Diophantine relations by widening the class of equations by allowing exponentiation as well as $+$ and \cdot in building up terms.

The author proves that the relation given by $v = \phi_{2u}$ is Diophantine where ϕ_k is the k th Fibonacci number. The Fibonacci sequence is determined by $\phi_0 = 0$, $\phi_1 = 1$, and $\phi_{n+2} = \phi_{n+1} + \phi_n$. It is easily seen that $2^{n-1} < \phi_{2n} < 3^n$ so $v = \phi_{2u}$ is a relation of exponential growth. The ingenious proof, which is given in its entirety in this short paper, is a fine work of elementary number theory. The necessary lemmas can be proved by mathematical induction. (A simpler proof of Lemma 17 is given in the English translation.)

Prior to this paper, the existence of such a Diophantine relation was widely disbelieved. Thus, its discovery is a crucial step in our understanding of Diophantine equations.

JULIA ROBINSON

YU. V. MATIJASEVIČ. *Diophantine representation of recursively enumerable predicates. Proceedings of the Second Scandinavian Logic Symposium*, edited by J. E. Fenstad, Studies in logic and the foundations of mathematics, vol. 63, North-Holland Publishing Company, Amsterdam and London 1971, pp. 171–177.

This is a second version of the paper reviewed above. It outlines somewhat more fully the results of Davis, Putnam, and Robinson upon which the main theorem depends, while omitting some of the details of the proof which are included in the earlier paper. ANN S. FEREBEE

PAUL TURÁN. *On the work of Alan Baker. Actes du Congrès International des Mathématiciens 1970*, Gauthier-Villars, Paris 1971, Vol. 1, pp. 3–5.

ALAN BAKER. *Effective methods in the theory of numbers*. Ibid., pp. 19–26.

Baker reports and summarizes positive solutions of Hilbert's tenth problem in some special cases of quite surprising generality—based, as he explains, on a surprising connection between the seventh and tenth problems of Hilbert. For details and sources we refer to the paper itself (see especially §4) and to the author's *Effective methods in Diophantine problems (1969 Number Theory Institute)*, Proceedings of symposia in pure mathematics, vol. 20, American Mathematical Society, Providence, Rhode Island, 1971, pp. 195–205). Turán, in connection with the award of a Fields medal to Baker, reports more descriptively on the same material.

The relationship to the negative solution of the tenth problem by Matijasevič (see the two preceding reviews) is mentioned by Turán. The reviewer would like to see a confrontation between the two approaches, narrowing the gap between solvable and unsolvable cases by obtaining unsolvability proofs in special cases, as well as positive solutions. ALONZO CHURCH

YU. V. MATIJASEVIČ. *Diophantine representation of recursively enumerable predicates*. Ibid., pp. 235–238.

An n -ary relation among natural numbers ($n \geq 1$) is called Diophantine if there is a polynomial P with integer coefficients such that the relation is equivalent to $(\exists y_1)(\exists y_2) \dots (\exists y_k) \cdot P(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_k) = 0$. This paper summarizes work of Martin Davis, Julia Robinson, and Hilary Putnam concerning the connection between Diophantine relations and recursively enumerable relations, culminating in the result of the author (see reviews above) which fills the final gap by showing that *there exists a (binary) Diophantine relation of exponential order of growth*. There follows: *Every recursively enumerable relation is Diophantine*. A corollary of this “Main Theorem” is the unsolvability of Hilbert's tenth problem. By a result of Putnam (reviewed above, XXXVII 601(2)) another corollary is that every recursively enumer-