papers, and the bibliographic material together make *Logical Methods* a very useful source of RET information.

REFERENCES

[C1981a] **CROSSLEY**, J. (ed.), *Reminiscences of logicians, II*. pp. 1–25 in [C1981b].

[C1981b] **CROSSLEY**, J. (ed.), *Aspects of Effective Algebra*. Yarra Glen, Australia, Upside Down A Book Company.

[CN1974] **CROSSLEY**, J. and A. **NERODE**, Combinatorial Functors. Berlin, Springer-Verlag.

[D1966] **DEKKER**, J. C. E., *Les Fonctions Combinatoires et les Isols*. Paris, Gauthier-Villars.

[D1990] **DEKKER**, J. C. E., *Myhill's theory of combinatorial functions*. Modern Logic **1**, 3–21.

[McL1982] **MCLAUGHLIN**, T., *Regressive Sets and the Theory of Isols*. New York, Marcel Dekker.

[N1961] **NERODE**, A., *Extensions to isols*. Annals of Math. **73**, 362–403.

****

Yuri V. Matiyasevich, *Hilbert's Tenth Problem*, The MIT Press, Cambridge, Massachusetts, 1993. English translation of *Desyataya problema Gil'berta*, Nauka Publishers, Moscow, 1993 (Russian).

Reviewed by

VALENTINA HARIZANOV

Department of Mathematics
The George Washington University
Washington, D. C. 20052, USA
email: val@math.gwu.edu

"This conviction of the solvability of every mathematical problem is a powerful incentive to the worker. We hear within us the perpetual call: There is the problem. Seek its solution. You can find it by pure reason, for in mathematics there is no ignorabimus." – David Hilbert, 1900

Hilbert's Tenth Problem is an interesting and beautiful book about Hilbert's tenth problem. In 1900, at the Second International Congress of Mathematicians, assembled in Paris, the eminent German mathematician David Hilbert (1862–1943) presented in his address "Mathematische Probleme" twenty-three unsolved problems, which would challenge the mathematicians of the twentieth century. The tenth problem was the shortest problem and the only *decision problem.* (Actually, in order to "shorten his talk as Minkowski and Hurwitz had urged," Hilbert covered only ten of the twenty-three problems in his famous lecture. The other thirteen, including the tenth, are stated exclusively in the published version (Reid [*1970*, 81–82]).)

Hilbert's Tenth Problem unifies, in a strikingly beautiful way, two different areas of mathematics: number theory and computability theory. Stated simply, Hilbert's tenth problem is this: Is there an algorithm that determines whether any given Diophantine equation has a solution in the integers? A Diophantine equation is an equation of the form

$$D(x_1, ..., x_m) = 0 ,$$

where D is a polynomial in the variables $x_1, ..., x_m$ with integer coefficients. Diophantine equations are named after Diophantus of Alexandria, who wrote *Arithmetica* in thirteen Books around the third century A.D., a milestone in the development of number theory. Only six Books have survived (Heath [*1964*, 2–3]). The treatise *Arithmetica* is a peculiar blend of Greek and Oriental mathematics with systematic use of algebraic symbolism, which initiated the study of equations with positive rational solutions. An algorithm (or decision procedure) is a general and systematic method for solving a problem. The rigorous mathematical theory of algorithms, recursion (or computability) theory, was not established until three and a half decades after Hilbert posed the problem.

Hilbert's Tenth Problem is written by Yuri Matiyasevich, a gifted logician and number theorist and the chairman of the Laboratory of Mathematical Logic at the St. Petersburg branch of the Steklov Institute of Mathematics of the Russian Academy of Sciences. When the book appeared in 1993, its author was twenty-three years older than the "clever young Russian" who found the ingenious solution to Hilbert's tenth problem. On January 4, 1970, the twenty-two-year-old Yuri Matiyasevich added the final link to a proof chain forged over many years by several well-known mathematicians, including Martin Davis, Hilary Putnam, and Julia Robinson. By establishing the existence of the so-called *Julia Robinson predicate*, Yuri Matiyasevich proved that nobody

could devise an algorithm which determines whether a Diophantine equation has a solution in the integers.

In the first half of the book (the first five chapters), Matiyasevich presents a self-contained and quite detailed solution to Hilbert's tenth problem. He has greatly simplified the original solution. The author builds all necessary logical machinery from scratch, and even presents well-known number-theoretic facts (Lagrange's four-squares theorem, the Chinese remainder theorem, Kummer's theorem, and a summation formula for a generalized geometric series) in the Appendix. In order to be accessible to a broader audience, the book does not require any previous knowledge of recursion theory. Chapter 5 presents all necessary notions and facts, and shows how recursion theory, combined with the number-theoretic results of the first four chapters, ultimately resolves the mystery of our intrinsic inability to "*devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers*" (Hilbert, 1900).

The main result, due to Matiyasevich (Sections 5.4 and 5.5), which implies the unsolvability of Hilbert's tenth problem, is that the class of *Diophantine sets* (to be defined below) of natural numbers coincides with the class of *recursively enumerable* sets of natural numbers. Recursively enumerable sets are sets whose elements can be listed, not necessarily in any predictable order, by some algorithm. (In his book, Matiyasevich chooses to call recursively enumerable sets *semidecidable*. This is unfortunate, because it may be confused with the term *semirecursive*, introduced in 1966 by Carl Jockusch (*Reducibilities in recursive function theory*, Ph.D. Dissertation, MIT).)

In the first few sections of Chapter 1, Matiyasevich shows how increasingly complicated problems can be reduced to Hilbert's tenth problem. If Hilbert's tenth problem were algorithmically solvable, then these problems would also be algorithmically solvable. The author first shows how a system of Diophantine equations can be easily reduced to a single Diophantine equation. He then shows that since, by Lagrange's four-squares theorem of 1772 (i.e., that every natural number can be expressed as the sum of the squares of four integers), the algorithmic solvability of a Diophantine equation in the integers is equivalent to the algorithmic solvability of a Diophantine equation in the natural numbers. The author also demonstrates Thoralf Skolem's result of 1934 that, in the case of Hilbert's tenth problem, it is sufficient to consider only Diophantine equations of total degree four.

Chapter 1 introduces the main concept of a Diophantine set. Let ω be the set of all natural numbers (including zero). A set $A \subseteq \omega$ is

Diophantine if there is a polynomial $D(y, x_1, ..., x_m)$ in the variables y, $x_1, ..., x_m$ with integer coefficients such that, for every $a \in \omega$, A contains a if and only if there are $b_1, ..., b_m \in \omega$ such that

$$y = a,\ x_1 = b_1, ...,\ x_m = b_m$$

is a solution of the Diophantine equation

$$D(y, x_1, ..., x_m) = 0\,.$$

The formula

$$(\exists x_1 \in \omega) ... (\exists x_m \in \omega)\ [D(y, x_1, ..., x_m) = 0]$$

is called a *Diophantine representation* of A. In a similar fashion, Diophantine relations on ω of any length are defined. A function is Diophantine if its graph is a Diophantine relation. In 1953, Martin Davis established the obvious facts that both the union and the intersection of two Diophantine sets are Diophantine, and the not-so-obvious fact that the complement of a Diophantine set does not have to be Diophantine. Chapter 1 shows that several important sets and relations on ω, such as the inequality relation, the ordering relation, the divisibility relation, the set of numbers which are not powers of two, the set of all composite numbers, the set of all even numbers, and the set of all odd numbers, are Diophantine.

One of the key events in the history of Hilbert's tenth problem was the resolution of the question: Is the binary exponential function f on the natural numbers ($f(0, 0) =$ def 1, and $f(b, c) = b^c$ otherwise) Diophantine? In 1948, Alfred Tarski conjectured that the set of all powers of two is not Diophantine. After failing to prove Tarski's conjecture, Julia Robinson started to work on refuting it. She established, first in 1952 and later in 1969, several sufficient conditions for the exponential function to be Diophantine. One of these conditions was the existence of a relation of exponential growth, now also called a Julia Robinson predicate, which is Diophantine. A binary relation J on ω is a Julia Robinson predicate if the following two conditions are satisfied:

$$(\forall u)(\forall v)\ [J(u, v) \Rightarrow v < u^u]\,;$$
$$(\forall k \in \omega)(\exists u)(\exists v)\ [J(u, v) \wedge v > u^k]\,.$$

Matiyasevich [*1970*] proved the existence of a Diophantine Julia Robinson predicate. His relation M is

$$M(u, v) \Leftrightarrow_{\text{def}} v = \varphi_{2u} ,$$

where φ_0 , φ_1, φ_2, ... are Fibonacci numbers. That is, $\varphi_0 = 0$, $\varphi_1 = 1$, and $\varphi_{n+2} = \varphi_n + \varphi_{n+1}$.

In his book, Matiyasevich does not follow the historical path in establishing that the exponential function is Diophantine. Rather, he proves this theorem directly. Although the proof, which is rather technical, requires almost all of Chapter 2, it is simpler than the original proof. The historical line of reasoning which established that the exponential function is Diophantine is outlined in the Exercises of Chapter 2.

Chapter 3 establishes that certain important relations and functions associated with various codings of finite sequences of natural numbers (Cantor coding, Gödel coding, which uses Chinese remainder theorem, and positional or b-adic coding) are Diophantine. A corollary of these results together with the fact that exponentiation is Diophantine is that the factorial function and the binomial-coefficient function are Diophantine. Hence, the set of all prime numbers is Diophantine.

Chapter 4 is devoted to a purely number-theoretic construction of universal Diophantine equations. Let $n \in \omega$. A universal Diophantine equation corresponding to n has, in addition to n element parameters, some other, so-called code parameters which code all n-ary Diophantine relations. Universal Diophantine equations allow the construction of Diophantine sets with non-Diophantine complements. Historically, the first construction of a universal Diophantine equation was based on the idea of "universal objects" in recursion theory.

While the first four chapters present results and techniques that are exclusively of a number-theoretic nature, Chapter 5 presents the foundations of recursion theory and its interplay with number theory. Matiyasevich chooses the most natural formalization of the intuitive concept of an algorithm: a Turing machine. In 1936, by devising a conceptual machine that carried out algorithms, Alan Turing captured the essence of this notion and provided the necessary tools for negative solutions to decision questions — in other words, for results on the inherent limitation on the ability of algorithms to solve problems. Such problems are called undecidable, noncomputable or nonrecursive. In Section 5.5, Matiyasevich gives a new, direct proof that all recursively enumerable sets are Diophantine. His Diophantine simulation of Turing machines is presented in the book for the first time. Chapter 5 culminates with the

proof that Hilbert's tenth problem is undecidable. The undecidability follows from the facts (F1–F3). (The first one is easily established, as shown in Section 5.6. We have already discussed the other two.)

F1. Decidable sets are exactly those recursively enumerable sets whose complements are also recursively enumerable.

F2. Being a recursively enumerable set is equivalent to being a Diophantine set.

F3. Diophantine sets are not closed under complementation.

It should be mentioned that, historically, a modified version of Hilbert's tenth problem, which uses exponential Diophantine, rather than Diophantine, equations was first solved. An exponential Diophantine equation is an equation of the form

$$E_1(x_1, ..., x_m) = E_2(x_1, ..., x_m),$$

where E_1 and E_2 are algebraic expressions obtained from natural numbers and variables $x_1, ..., x_m$ using addition, multiplication and exponentiation. The definitions of exponential Diophantine relations and functions, and their exponential Diophantine representations, are analogous to the corresponding notions for ordinary Diophantine equations. Davis, Putnam and Robinson [*1961*] obtained the undecidability result for the exponential Diophantine equations. Their crucial theorem was that every recursively enumerable set has an exponential Diophantine representation. Thus, in order to establish Davis' daring hypothesis of 1953 that *every recursively enumerable set has a Diophantine representation*, it was enough to show that the exponential function is Diophantine. That would establish the unsolvability of Hilbert's tenth problem.

In both the first and the second part of the book, Matiyasevich shows that some famous problems which at first glance have little to do with Diophantine equations can be formulated as questions about whether particular Diophantine equations have solutions. One of these problems is Fermat's Last Theorem, which is the statement that the exponential Diophantine equation

$$(p + 1)^{s+3} + (q + 1)^{s+3} - (r + 1)^{s+3} = 0$$

has no solution in the natural numbers for variables p, q, r and s. (Interestingly, Hilbert's list of problems did not include Fermat's Last Theorem.) Using the key result that exponentiation is Diophantine, Matiyasevich shows, in Chapter 2, that there is a Diophantine equation

$$F(p, q, r, s, x_1, ..., x_m) = 0$$

which has a solution in $x_1, ..., x_m$ if and only if p, q, r, s satisfy the above exponential Diophantine equation.

In the second part of the book, Matiyasevich covers various topics related to Hilbert's tenth problem. In the first three sections of Chapter 6, he proves (three times, each time differently) that the set of all Diophantine relations is closed under bounded universal quantification. The first proof gives a constructive method and can be based on Church's thesis from recursion theory, which states that every intuitively decidable problem can be shown to be formally decidable. The second proof uses Gödel's type of coding and follows, with minor simplifications, the original work of Davis, Putnam and Robinson [*1961*]. This method was an essential step in solving Hilbert's tenth problem because it provided a powerful tool for establishing that certain sets are Diophantine. In Chapter 5, Matiyasevich constructs Diophantine representations of recursively enumerable sets without any use of bounded universal quantification. His approach (Matiyasevich [*1976*]) is possible because of the direct simulation of Turing computation by Diophantine equations. The third proof described in Chapter 6 eliminates bounded universal quantifiers by introducing summations with variable upper limit. This method is new, and is presented for the first time in the book.

Later in Chapter 6, Matiyasevich uses the elimination of bounded universal quantifiers to show how each of two other famous problems, Goldbach's conjecture and Riemann's hypothesis, can be restated as a problem about a particular Diophantine equation having no solution. Goldbach's conjecture claims that every even number greater than two is the sum of two prime numbers. Riemann's hypothesis is the statement that the nontrivial zeroes of Riemann's zeta function all have the real part equal to 1/2. Riemann's zeta function ζ is defined by

$$\zeta(z) = 1 + 2^{-z} + 3^{-z} + ...$$

for $\mathrm{Re}(z) > 1$ and extended, using analytic continuation, to all $z \neq 1$. Both of these problems were included as parts of Hilbert's eighth prob-

lem and are still unsolved. On the other hand, Matiyasevich does not see an obvious way to similarly restate the twin-prime conjecture, which was also included in Hilbert's eighth problem. One of the exercises in Chapter 6 provides another example of a famous problem, the four-color theorem, which can be formulated as a statement that a particular Diophantine equation does not have a solution.

At the end of Chapter 6, Matiyasevich uses the elimination of bounded universal quantifiers to easily construct another universal Diophantine equation. He then constructs a Diophantine set whose complement is not just non-Diophantine but also does not contain any infinite recursively enumerable (equivalently, infinite Diophantine) set. Such sets are called *simple* and were first constructed in recursion theory by Emil Post.

Because Diophantine equations are simple mathematical objects, Hilbert's tenth problem has often been used to establish undecidability of other problems in number theory, algebra, model theory, proof theory, theoretical computer science, linear programming, and analysis. Chapter 7 presents several undecidability results in number theory (including the undecidability of the Gaussian integer counterpart of Hilbert's tenth problem), and Chapter 9 presents several undecidability results in analysis. Although Hilbert was concerned with integer solutions of Diophantine equations, Diophantus himself considered rational solutions. In Chapter 7, Matiyasevich presents the proof that the still unresolved problem of algorithmically determining the existence of a rational solution for a Diophantine equation is equivalent to the problem of algorithmically determining the existence of a nontrivial integer solution for a homogeneous Diophantine equation.

Chapter 8 deals with quantitative aspects of Diophantine relations and their Diophantine representations. From the very beginning, these aspects have been of interest to researchers trying to prove the algorithmic unsolvability of Hilbert's tenth problem. Several measures of complexity are introduced for a Diophantine relation A. For example, the order of A is the least possible degree of a corresponding Diophantine equation, and the rank of A is the least possible number of existential quantifiers in a corresponding Diophantine representation of A. Matiyasevich demonstrates that every Diophantine set has an exponential Diophantine representation with at most three existential quantifiers.

The final, tenth chapter of the book consists of two sections. The first section presents Diophantine games, invented by James P. Jones [*1974*]. A Diophantine game is given by a Diophantine equation with an even number of variables

$$D(x_1, ..., x_m;\ y_1, ..., y_m) = 0 .$$

The game is played according to the following rules:

On moves 1, ..., $2k$–1, ... (for $2k - 1 \leq m$), player I chooses a value for $x_1, ..., x_k, ...$;

On moves 2, ..., 2_k, ... (for $2k \leq m$), player II chooses a value for y_1, ..., $y_k, ...$.

The game ends after $2m$ moves. Player II wins if the chosen values satisfy the Diophantine equation; player I wins otherwise. Clearly, player II has a winning strategy if and only if the following holds:

$$(\forall x_1)(\exists y_1) ... (\forall x_m)(\exists y_m) [D(x_1, ..., x_m;\ y_1, ..., y_m) = 0] .$$

Matiyasevich shows that there is a Diophantine game in which the second player has a winning strategy, but there is no algorithm which determines a reply of the second player to every move of the first player. In the final section he discusses another game, a generalized form of chess that uses only knights but on a multidimensional chessboard. Based on the undecidability of Hilbert's tenth problem, Matiyasevich proves that the problem of determining whether two knights have equal "chess power," and hence the problem of determining whether one knight is "at least as strong as" another one, are undecidable. The author uses this intuitive description in terms of knights and their moves to visualize so-called systems of vector addition and Petri nets invented in the theory of parallel computation.

Each chapter of the book ends with a number of related exercises, a few related unsolved problems, and a very interesting and informative *Commentary* which explains development of the subject presented in the chapter. The book ends with hints on the exercises. Since this book requires no specialized knowledge, but only "mathematical maturity," it is suitable for a broad audience of mathematicians, including advanced undergraduate and graduate students with little knowledge of recursion theory. The whole book or only its first part can be used in a topics course on mathematical logic. The first part of the book can serve as an interesting and nontypical introduction to computability theory, with intuitively computable functions rigorously formalized as Diophantine functions.

The book was originally published in Russian. Its English translation appeared the same year, and with a more extensive bibliography than the original book. The first translated version was prepared by the author

himself while he was still "rewriting the Russian original for the $(n+1)$–st time." All of this effort resulted in a very readable book, both in Russian and in English. The translation was further polished by David Jones of MIT Press and by Martin Davis, "neither of whom knows any Russian." However, the translation remains faithful to the original version. Martin Davis, a well-known recursion theorist and a pioneer of the subject of this book, gave its translated version a very touching historical and personal foreword, which includes his prophecy about the rise of a "clever young Russian" who will complete the solution of the famous old problem.

While the first part of the book presents a simplified proof of Hilbert's tenth problem, with several new and unpublished results, the second part of the book presents related topics and applications which have been scattered throughout various papers. This book is exceptional in the sense that all its parts are interesting and important—not only its text, but also its exercises, its commentaries, its appendix, and its foreword in the English translation. While the proofs in the chapters follow a logical order and tend to simplify the material as much as possible, the exercises often provide the history and the development of ideas and proofs. I highly recommend the book to everyone who loves number theory or logic.

Acknowledgment. I thank Georgia Martin for proofreading.

References

Martin **Davis**. 1953. *Arithmetical problems and recursively enumerable predicates*, Journal of Symbolic Logic **18**, 33–41.

—1973. Hilbert's tenth problem is unsolvable, American Mathematical Monthly **80**, 233–269.

Martin **Davis**, Hilary **Putnam** and Julia **Robinson**. 1961. "The decision problem for the exponential Diophantine equations, Annals of Mathematics **74**, 425–436.

Sir Thomas L. **Heath**. 1964. *Diophantus of Alexandria, A Study in the History of Greek Algebra*, New York, Dover Publications.

David **Hilbert**. 1902. *Mathematical problems. Lecture delivered before the International Congress of Mathematicians at Paris in 1900*, Bulletin of the American Mathematical Society **8**: 437–479 (translated by Mary W. Newson).

James P. **Jones**. 1974. *Recursive undecidability — an exposition*, The American Mathematical Monthly **81**, 724–738.

James P. **JONES** and Yuri V. **MATIYASEVICH**. 1991. *Proof of recursive unsolvability of Hilbert's tenth problem*, The American Mathematical Monthly **98**, 689–709.

Yuri V. **MATIYASEVICH**. 1970. *Diofantovost' perechislimykh mnozhestv*, Doklady Akademii Nauk SSSR **191**, 279–282 (Russian). Translated as Enumerable sets are Diophantine, Soviet Mathematics Doklady **11** (1970), 354–358.

— 1973. *On recursive unsolvability of Hilbert's tenth problem*, P. Suppes, L. Henkin, A. Joja and Gr. Moisil (editors), *Logic, Methodology and Philosophy of Science IV, Proceedings of the Fourth International Congress for Logic, Methodology and Philosophy of Science, Bucharest, 1971*, (Amsterdam, North-Holland), 89–110.

— 1976. *Novoe dokazatel'stvo teoremy ob eksponentsial'no diofantovom predstavlenii perechislimykh predikatov*, Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova Akad. Nauk SSSR **60**, 75–92 (Russian). Translated as *A new proof of the theorem on exponential Diophantine representation of enumerable sets*, Journal of Soviet Mathematics **14** (1981), 1475–1486.

Constance **REID**. 1970. *Hilbert*, Berlin, Springer-Verlag.

Julia **ROBINSON**. 1952. *Existential definability in arithmetic*, Transactions of the American Mathematical Society **72**, 437–449.

— 1969. *Unsolvable Diophantine problems*, Proceedings of the American Mathematical Society 22, 534–538.

Alan M. **TURING**. 1936. *On computable numbers, with an application to the Entscheidungsproblem*, Proceedings of the London Mathematical Society *42*, 230–265.