Hilbert's Tenth Problem

Yuri V. Matiyasevich

with a foreword by Martin Davis

The MIT Press
Cambridge, Massachusetts
London, England

Start of Citation[PU]MIT Press[/PU][DP]1993[/DP]End of Citation

Foreword

While I was still an undergraduate at City College in New York, I read my teacher E. L. Post's plaint that Hilbert's Tenth Problem "begs for an unsolvability proof." This was the beginning of my lifelong obsession with the problem. Although I have had the good fortune to be able to make some contributions towards the "unsolvability proof" for which the problem was begging, my greatest insight turned out to be a thought I had uttered in jest. During the 1960s I often had occasion to lecture on Hilbert's Tenth Problem. At that time it was known that the unsolvability would follow from the existence of a single Diophantine equation that satisfied a condition that had been formulated by Julia Robinson. However, it seemed extraordinarily difficult to produce such an equation, and indeed, the prevailing opinion was that one was unlikely to exist. In my lectures, I would emphasize the important consequences that would follow from either a proof or a disproof of the existence of such an equation. Inevitably during the question period I would be asked for my own opinion as to how matters would turn out, and I had my reply ready: "I think that Julia Robinson's hypothesis is true, and it will be proved by a clever young Russian."

This book was written by that Russian. In 1970, Yuri Matiyasevich presented his beautiful and elegant construction of a Diophantine equation that satisfies Julia Robinson's hypothesis. This showed not only that Hilbert's Tenth Problem is unsolvable, but also that two fundamental concepts arising in different areas of mathematics are equivalent. The notion of *recursively enumerable* or *semidecidable* set of natural numbers from computability theory turns out to be equivalent to the purely number-theoretic notion of *Diophantine* set. Dr. Matiyasevich has taken full advantage of the rich interplay between the methods of elementary number theory and computability theory that this equivalence makes possible to produce a remarkable and appealing book. The reader will find new and simplified proofs of some of the main results, various extensions and applications, and many interesting exercises.

The history of the subject is recounted with meticulous care in the "Commentaries" that follow each chapter of the book. Dr. Matiyasevich has also provided a very personal account of his involvement with Hilbert's Tenth Problem in his article "My Collaboration with Julia Robinson" in the *Mathematical Intelligencer* (Matiyasevich [1992]). In this brief introduction, I would like to offer a few vignettes from my own involvement with the problem. As a graduate student at Princeton University, I had chosen what I knew was an excellent topic for my dissertation: the extension of Kleene's arithmetic hierarchy into the constructive transfinite, what has come to be called the *hyperarithmetic hierarchy*. This was a completely unex-

plored area, was quite fascinating, and was sure to yield results. But, I couldn't stop myself from thinking about Hilbert's Tenth Problem. I thought it unlikely that I would get anywhere on such a difficult problem and tried without success to discipline myself to stay away from it. In the end, my dissertation, written under the supervision of Alonzo Church, had results on both the hyperarithmetic hierarchy and Hilbert's Tenth Problem. In my dissertation, I conjectured the equivalence of the two notions mentioned above (in this book referred to as my "daring hypothesis") and saw how to improve Gödel's use of the Chinese Remainder Theorem as a coding device so as to obtain a representation for recursively enumerable sets that formally speaking seemed close to the desired result. The obstacle that remained in this so-called Davis normal form was a single bounded universal quantifier.

I met Julia Robinson at the 1950 International Congress of Mathematicians in Cambridge, Massachusetts, immediately after completing my doctorate. She had approached Hilbert's Tenth Problem from a direction opposite to mine. Where I had tried to simplify the arithmetic representation of arbitrary recursively enumerable sets, she had been trying to produce Diophantine definitions for various specific sets and especially for the exponential function. She had introduced what was to become her famous "hypothesis" and shown that under that assumption the exponential function is in fact Diophantine. It's been said that I told her that I doubted that her approach would get very far, surely one of the more foolish statements I've made in my life.

During the summer of 1957, there was an intensive five week "Institute for Logic" at Cornell University attended by almost all American logicians. Hilary Putnam and I together with our families were sharing a house in Ithaca, and he and I began collaborating, almost without thinking about it. Hilary proposed the idea of using the Chinese Remainder Theorem coding one more time to code the sequences whose existence was asserted by the bounded universal quantifier in the Davis normal form. My first reaction was skeptical. But, as pointed out in the Commentary to Chapter 3 in this book, the Chinese Remainder Theorem provides a "unique opportunity" because of the fact that polynomials preserve congruences. In fact, we were able to obtain two particular sets with quite simple definitions concerning which we were able to show that their being Diophantine would imply the same for all recursively enumerable sets.

Hilary and I resolved to seek other opportunities to work together, and we were able to obtain support for our research during the three summers of 1958, 1959, and 1960. We had a wonderful time. We talked constantly about everything under the sun. Hilary gave me a quick course in classical European philosophy, and I

gave him one in functional analysis. We talked about Freudian psychology, about the current political situation, about the foundations of quantum mechanics, but mainly we talked mathematics. It was during the summer of 1959 that we did our main work together on Hilbert's Tenth Problem. In a recent letter, Hilary wrote:

> What I remember from that summer is not so much the mathematical details as the sheer *intensity* with which we worked. I have never in my life been so absorbed in a mathematical problem, and I'm sure the same was true of you. Our method, as I remember it, was that one of us would propose an attack and we would both work on it together, writing on the board and arguing with each other, making suggestions, etc., until something came of it or we reached a dead end. I could not let go of the problem even at night; this is the only time when I regularly stayed up to four in the morning ... I think we felt in our bones that the problem would yield to our approach; otherwise I can't explain the sense of mounting excitement.

Our "approach" was still to apply the Chinese Remainder Theorem to Davis normal form. But this time, we were combining this attack with Julia Robinson's methods, attempting to see if by permitting exponentiation in our Diophantine definitions we could eliminate the troublesome bounded universal quantifier. The problem in using the Chinese Remainder Theorem was the need for suitable moduli, relatively prime in pairs. Gödel's method was to obtain such moduli in an arithmetic progression, and hence definable in Diophantine terms. We found ourselves with the need to find exponential Diophantine definitions for sums of the reciprocals of the terms of a finite arithmetic progression as well as of the product of such terms. To deal with the second problem, we used binomial coefficients with rational numerators, for which we could find exponential Diophantine definitions extending Julia Robinson's methods, but requiring the binomial theorem with rational exponents, an infinite power series expansion. For the first, we used a rather elaborate (and as it turned out, quite unnecessary) bit of elementary analysis, involving the Taylor expansion of the Gamma function. Even with all that, we still couldn't get the full result we wanted. We needed to be able to assert that if one of our moduli was a divisor of a product that it had to necessarily divide one of the factors. And this seemed to require that the moduli be not only relatively prime in pairs, but actual prime numbers. In the end, we were forced to assume the hypothesis (still unproved to this date) that there are arbitrarily long arithmetic progressions

of prime numbers, in order to prove that every recursively enumerable set has an exponential Diophantine definition.

We sent our results to Julia Robinson, and she responded shortly thereafter saying:

> I am very pleased, surprised, and impressed with your results on Hilbert's Tenth Problem. Quite frankly, I did not think your methods could be pushed further ...
>
> I believe I have succeeded in eliminating the need for [the assumption about primes in arithmetic progression] by extending and modifying your proof. I have this written out for my own satisfaction but it is not yet in shape for anyone else.

The letter also showed quite neatly how to dispense with the messy analysis involving the Gamma function that Hilary and I had used. Soon afterwards, we received the details of Julia's proof, and it was our turn to be "very pleased, surprised, and impressed." She had avoided our hypothesis about primes in arithmetic progression in an elaborate and very clever argument by making using of the prime number theorem for arithmetic progressions to obtain enough primes to permit the proof to go through. She graciously accepted our proposal that our work (which had already been submitted for publication) be withdrawn in favor of a joint publication. Soon afterwards, she succeeded in a drastic simplification of the proof: where Hilary and I were trying to use the Gödel coding to obtain a logical equivalence, her elegant argument made use of the fact that the primes were only needed for the implication in one direction, and that in that direction one could make do with a prime divisor of each modulus. (Later Yuri Matiyasevich showed that in fact any sufficiently large coprime moduli could be used so that our efforts in connection with prime factors were really unnecessary; see Exercise 2 in Chapter 6.)

With the result that every recursively enumerable set has an exponential Diophantine definition combined with Julia Robinson's earlier work on Diophantine definitions of the exponential function, it was now clear that my "daring hypothesis" of the equivalence of the two notions, recursively enumerable set and Diophantine set, was entirely equivalent to the much weaker hypothesis (now called JR) that Julia Robinson had proposed ten years earlier that one single Diophantine equation could be found whose solutions satisfied a simple condition. During the summer of 1960, Hilary and I were in Boulder, Colorado participating in a special institute intended to teach mathematicians something about physics. Hilary and I continued

to argue about quantum mechanics and explored the possibility of finding a third degree equation to satisfy Julia Robinson's condition. It turned out once again that we needed information that the number theorists were unable to provide, this time about the units in pure cubic extensions of the rational numbers.

During the following years, I continued trying to prove Julia Robinson's hypothesis. I was particularly interested in trying to use what was known about quadratic number fields. It was this work that led me to the equation $9(x^2 + 7y^2)^2 - 7(u^2 + 7v^2)^2$, in which there is still some interest. (See the Commentary to Chapter 2.) At this time, Julia had become rather pessimistic about JR and, for a brief period, she actually worked towards a positive solution of Hilbert's Tenth Problem. A letter from her dated April 1968 responding to my report on the above equation said:

> I have enjoyed studying it, but my faith in JR still hasn't been restored. However, for the first time. I can see how it might be proved. Indeed, maybe your equation works, but it seems to need an infinite amount of good luck!

Early in 1970, a telephone call from my old friend Jack Schwartz informed me that the "clever young Russian" I had predicted had actually appeared. Julia Robinson sent me a copy of John McCarthy's notes on a talk that Grigoriĭ Tseitin had given in Novosibirsk on the proof by the twenty-two-year-old Yuri Matiyasevich of the Julia Robinson hypothesis. Although the notes were brief, everything important was there, and I was able to have the great pleasure of reconstructing the proof. But I was not satisfied until I had produced my own variant of Dr. Matiyasevich's proof and presented it (on March 10) at a seminar at Rockefeller University at Hao Wang's invitation.

I met Yuri a few months later at the International Congress of Mathematicians in Nice, where he was an invited speaker. I was finally able to tell him that I had been predicting his appearance for some time.

Martin Davis