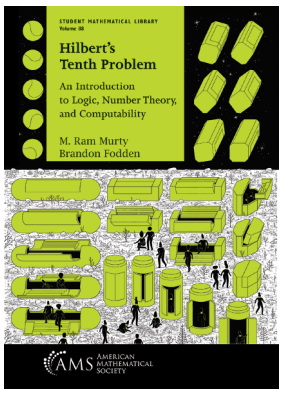
BOOK REVIEW

Hilbert's Tenth Problem

Reviewed by Alexandra Shlapentokh



Hilbert's Tenth Problem
An Introduction to Logic, Number Theory, and Computability
by M. Ram Murty and Brandon Fodden

Before proceeding with this review, we note, in the spirit of disclosure that has become a requirement in many fields, that the reviewer has also written a book on Hilbert's Tenth Problem [Sh2007]. The scope and goals of that book differ substantially from the book reviewed here, but, of course, there is a nonempty intersection.

The book under review was conceived as a textbook for advanced undergraduates and graduate students. Its subtitle is *An Introduction to Logic, Number Theory, and Computability*. Besides basic facts concerning first-order logic, number theory, and recursive functions, the text also covers some set theory, model theory, and a few other topics. At first glance, a course covering so many topics would seem unnecessarily ambitious, especially if it is aiming at undergraduates. However, there is a reason for touching on all of these areas of mathematics. This reason is a proof of the unsolvability of Hilbert's Tenth Problem, described in detail in the book, as well as some extensions of the problem, requiring fairly sophisticated number-theoretic tools.

Hilbert's Tenth Problem was the tenth problem on the list of 23 problems presented by David Hilbert to an International Congress of Mathematicians in 1900. Using a modern rewording, one can phrase the question posed by Hilbert as follows. Is there an algorithm (or a computer program) taking as input coefficients (assumed to be integers) of a polynomial equation in several variables, and outputting a "yes" or "no" answer to the question: "Does this equation have solutions in $\mathbf{Z}$?"? (At the time Hilbert formulated the problem, the modern notion of algorithm did not yet exist. So, the problem was phrased differently; Hilbert's original text is reproduced in the book.) The problem was not completely solved until 1968, when Yuri Matiyasevich [Mat68] showed that exponentiation over integers can be rewritten in a polynomial form. This result, together with the results obtained earlier by Martin Davis, Hilary Putnam, and Julia Robinson [DPR61], completed the proof of the statement that the algorithm requested by Hilbert did not exist. In fact, a lot more was shown. The theorem proved by the four authors showed that any recursively enumerable set is Diophantine.

Recursively enumerable sets (r.e. sets) are the sets that can be listed by a program allowed to run for a possibly infinite amount of time. A Diophantine subset of $\mathbf{Z}$ is defined as follows. A set $A \subset \mathbf{Z}^k$ is called Diophantine if there exists a polynomial

$$p(T_1,\dots,T_k,X_1,\dots,X_m) \in \mathbf{Z}[T_1,\dots,T_k,X_1,\dots,X_m]$$

such that for any k-tuple $(t_1,\dots,t_k) \in \mathbf{Z}^k$, the statement

$$"(t_1,\dots,t_k) \in A"$$

is equivalent to the statement

$$"\text{There exist } x_1,\dots,x_m \in \mathbf{Z} \text{ with } p(t_1,\dots,t_k,x_1,\dots,x_m) = 0."$$

The polynomial $p(T_1,\dots,T_k,X_1,\dots,X_m)$ is called a Diophantine definition of A over $\mathbf{Z}$.

One could say that this is a number-theoretic version of the definition of a Diophantine set. Diophantine sets can also be described as sets existentially definable over $\mathbf{Z}$ in

Alexandra Shlapentokh is a professor of mathematics at East Carolina University. Her email address is shlapentokha@ecu.edu.

Communicated by Notices *Book Review Editor Stephan Ramon Garcia.*

DOI: https://dx.doi.org/10.1090/noti2249

the language of rings or as projections of algebraic sets over $\mathbf{Z}$. Thus, one can immediately see that this notion is on the boundary of several disciplines: number theory, algebraic geometry, computability theory, and model theory. The notion of recursively enumerable set belongs to computability theory, and the question of which quantifiers we are allowed to use is related to the first-order logic.

The connection between the fact that Diophantine sets and r.e. sets are the same and the unsolvability of Hilbert's Tenth Problem depends on a classical theorem from recursion theory stating that there are nonrecursive r.e. sets. (The book is using a somewhat out-of-date terminology with respect to certain objects in computability theory. Some time ago, the word "recursive" was replaced by the word "computable" by mathematicians working in the area. However, since the book is using the term "recursive," we will continue to use this term also in our review.)

A set is recursive if there is an algorithm (or a program) to determine whether a given integer belongs to the set. So, let $U \subset \mathbf{Z}$ be an r.e. set that is not recursive. Let $q(t, x_1, \ldots, x_m)$ be a Diophantine definition of U over $\mathbf{Z}$. Now assume we had the algorithm requested by Hilbert. Then, given $t \in \mathbf{Z}$, we could determine whether $q(t, x_1, \ldots, x_m) = 0$ has integer solutions. Therefore, we could determine whether $t \in U$. Since U is not recursive, we have a contradiction.

Keeping the above in mind, it is now clear that any text attempting to present a proof of the unsolvability of Hilbert's Tenth Problem and other problems arising from Hilbert's question has to start with a fairly broad base. This book meets the challenge of presenting all these topics in the first four chapters quite well. It hews to essential things and does not overload the reader.

The discussion of Hilbert's Tenth Problem itself starts in Chapter 5. As is usually the case, the solution is not presented chronologically, in the order in which it was obtained, but in a manner that would make it easier to understand. In Section 1 of the chapter the discussion is started noting that we can replace the search for integer solutions of polynomial equations by the search for natural number solutions via the Lagrange Four Squares Theorem. Next the section provides a few examples of easy-to-understand Diophantine sets, and explains that the book will concentrate on the problem of constructing a Diophantine definition for a given set, as opposed to trying to determine the elements of the set from a given Diophantine definition. The section ends with a discussion of Diophantine functions, i.e., functions with Diophantine graphs. Cantor's pairing function and Goedel's β function are shown to be Diophantine.

Cantor's pairing function $P(x,y): \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ is a bijection defined by the formula

$$P(x,y) = \frac{(x+y)(x+y+1)}{2} + x.$$

If $F^{-1} = P$ and $F(z) = (L(z), R(z))$, then $P(L(z), R(z)) = z$, $L(P(x,y)) = x$, and $R(P(x,y)) = y$. Observe that $P(x,y), L(z), R(z)$ are Diophantine. Indeed,

$$\begin{aligned} z = P(x,y) &\Leftrightarrow 2z = (x+y)(x+y+1) + 2x, \\ x = L(z) &\Leftrightarrow \exists y : 2z = (x+y)(x+y+1) + 2x, \\ y = R(z) &\Leftrightarrow \exists x : 2z = (x+y)(x+y+1) + 2x. \end{aligned}$$

It is also important to note that $L(z) \le z$ and $R(z) \le z$.

The function $\beta(i,u)$ is defined to be the remainder from the division of $L(u)$ by $1 + (1+i)R(u)$. One of the important theorems in the section shows that given an enumeration of all finite sequences of positive integers, for every finite sequence $a_1, \ldots, a_N$, there exists a positive integer u, such that $\beta(u,i) = a_i$. Furthermore, given that $L(z) \le z$ and $R(z) \le z$, one can show that $\beta(u,i) \le u$. This fact is crucial for defining bounded universal quantifiers later. From the definition of $\beta(u,i)$ it is not hard to show that the function is Diophantine.

Section 2 is devoted to the equation that has become inseparable from Hilbert's Tenth Problem and its extensions, even though it was not present in the original proof. We are talking about the Pell equation, $x^2 - dy^2 = 1$, of course. The authors of the book note that an Indian mathematician Brahmagupta discovered this equation long before it came to the attention of Western mathematicians. Thus, they refer to it as Brahmagupta-Pell. For reasons of brevity and habit, we will continue to refer to the Pell equation. If $x, y, d \in \mathbf{Z}$, and d is not a square of an integer, then, using a bit of algebraic number theory, one can easily see that the $\mathbf{Q}$-norm of the element

$$(x - \sqrt{dy}) \in \mathbf{Q}(\sqrt{d})$$

is in fact $x^2 - dy^2$, and the Pell equation tells us that this element is a unit. If $d > 0$, then the unit group is a group of rank 1, with -1 and 1 being the only torsion elements. Therefore, when $d > 0$, solutions to the Pell equation form a cyclic group modulo the subgroup $\{-1, 1\}$. If we assume additionally that $d = a^2 - 1$ with $a \in \mathbf{Z}$, then we can identify a generator of the group as $a - \sqrt{d}$, and all solutions of the equation will arise from powers of this generator. The book proves this using strictly elementary methods.

The interest in the Pell equation in connection with Hilbert's Tenth Problem stems from the fact that solutions to this polynomial equation grow exponentially and therefore can be used to define exponential function in terms of polynomial equations. A Diophantine definition of the exponential function obtained via the Pell equation is discussed in Section 3 of the chapter.

The fact that exponentiation over integers is definable via polynomial equations was discovered by Yuri Matiyasevich. Instead of the Pell equation he used Fibonacci numbers, but his method was essentially the same. Shortly after Matiyasevich announced his solution, Martin Davis, Gregory

Chudnovsky, and Nikolai Kosovskii independently of each other realized that one can use the Pell equation in place of the Fibonacci numbers.

In Section 5.4 more examples of Diophantine functions are described. In particular, there is a proof that the binomial coefficients have a Diophantine definition. This proof depends on the fact that exponentiation is Diophantine.

In Section 5.5 the fact that the exponential function and the binomial coefficients are Diophantine is used to define bounded universal quantifiers. While the use of the universal quantifier itself is forbidden in this world of existential definitions, for natural numbers $y,x_1,\ldots,x_n$ and a polynomial $P(y,k,x_1,\ldots,x_n,y_1,\ldots,y_m)$, one can define the statement

$$\forall k_{\leq y}\exists y_1,\ldots,y_m\, P(y,k,x_1,\ldots,x_n,y_1,\ldots,y_m)=0,$$

using polynomial equations.

In Section 5.6, the book returns to the discussion of recursive functions initiated in Chapter 4. In that chapter recursive functions are defined as functions one can construct from some basic functions (constant functions, successor function, projections, etc.) using ring arithmetic operations, composition, primitive recursion, and bounded minimization. Note that earlier, we talked about recursive sets as sets with an algorithm to determine whether a given integer is an element of the set. Following this line of thought, it would be natural to define a recursive function as a function with a recursive graph. Is there a conflict between the two definitions? Not according to Church's Thesis, stating that any function with an algorithm to compute its value on a given input is in fact recursive. Therefore, we can also say that a set is r.e. if and only if it is the range of some recursive function.

Using the identification of algorithmically computable (sometimes called effectively computable) functions with recursive functions, the book completes the proof of the assertion that all r.e. sets are Diophantine. It is pretty easy to see that any Diophantine set is r.e. Let $p(T_1,\ldots,T_k,X_1,\ldots,X_m)$ be a Diophantine definition of a set $A\subset N^k$. Using any effective enumeration of $k+m$-tuples of natural numbers, start substituting these tuples into $p(T_1,\ldots,T_k,X_1,\ldots,X_m)$. Each time the result is 0, record the k-tuple $T_1,\ldots,T_m$ as being in A.

The converse, saying that every r.e. set is Diophantine is much more difficult. This is the statement that requires most of the work done so far. In this section, the book first shows that every recursive function is Diophantine. Here $\beta(u,i)$ plays an important role in the proof of the assertion that primitive recursion applied to a Diophantine function results in a Diophantine function. To show that bounded minimization applied to a Diophantine function results in a Diophantine function, we use the fact that the bounded universal quantifier is Diophantine, and thus use the fact that exponentiation is Diophantine.

Section 5.7 completes the proof of unsolvability of Hilbert's Tenth Problem using the argument we described at the beginning of this review.

Chapter 6 describes improvements of the original result and some of its consequences. Here is a partial list:

1. If $A=\mathbf{N}\cup\aleph_0$ and $k\in A$, $k\neq 0$, then there is no algorithm to determine whether an arbitrary equation has exactly k solutions [Dav72].
2. Any Diophantine set has a definition with a polynomial of degree at most 4. It is known that not all Diophantine sets can be described by a polynomial of degree 2 [Sie72], but it is an open question whether it can be done with polynomials of degree 3.
3. There exists a natural number m such that every Diophantine set of natural numbers can be described with a polynomial with at most $m+1$ variables. It is known that $m\leq 9$ [Jo78], [Jo82].
4. There exists a polynomial such that the positive part of its range consists of precisely the positive prime numbers [JSWW76].

Among the more surprising facts concerning Diophantine definitions, described in detail in Chapter 6 devoted to applications of Hilbert's Tenth Problem, are the following:

1. There exists a Diophantine equation such that it has no solutions if and only if Goldbach's conjecture is true.
2. There exists a Diophantine equation such that it has no solutions if and only if the Riemann hypothesis is true [DMR76].
3. There exists a Diophantine equation such that it has no solutions if and only if ZFC set theory is consistent.
4. There exists a Diophantine equation such that it has no solutions if and only if Peano arithmetic is consistent.

These connections between Diophantine definability and some of the most interesting questions in mathematics tell us that the existential language of rings, i.e., the existential language of polynomial equations, has an enormous expressive power, and so, in some sense, it is not a surprise that we cannot algorithmically determine whether an arbitrary statement of this language is true.

The last chapter of the book is devoted to extensions of Hilbert's Tenth Problem. In principle, one can pose Hilbert's question for any recursively presentable ring R, i.e., a ring where we have an algorithmic way of listing all the elements and executing the ring operations. Arguably, the two most important unresolved questions in the subject are Hilbert's Tenth Problem for $R=\mathbf{Q}$ and R being the ring of integers of an arbitrary number field. The book does not discuss the question related to $\mathbf{Q}$, but does have a discussion concerning Hilbert's Tenth Problem over rings of integers.

The discussion of necessity becomes rather technical, but the authors of the book again manage to reduce the technical details to a minimum. It seems that their intent is to explain definitions and present relevant facts, rather than to develop a complete picture of some small parts of

the subjects involved, as was done in Chapters 1–4. The main goal of the chapter is to explain the statement of a theorem proved by Ram Murty and Hector Pasten [MP2018] connecting Hilbert's Tenth Problem for rings of integers of number fields to several well-known number-theoretic conjectures.

Section 7.1 provides the necessary background from algebraic number theory, including the definition of algebraic numbers, Dedekind zeta function, unit groups, field discriminants, the generalized ideal class group, L-series $L(s,\chi)$, valuations, the adele ring A_K of a field K, $GL_n(A_K)$, the group of ideles, and grossencharacters. A student who has never seen these notions before is unlikely to derive much benefit from this section. However, for someone who has seen at least a part of this material, possibly having forgotten some details, this section would be a very nice refresher.

This comment applies to Sections 7.2 and 7.3 also. Section 7.2 contains a discussion of the zeta function and L-functions. A sequence of definitions and facts continues through Section 7.3, where elliptic curves and their L-functions are introduced. Within the three pages of the section, the reader is introduced to, among other things, elliptic curves, their conductors, and their L-series, the Taniyama-Shimura conjecture, the Mordell-Weil Theorem, the Birch and Swinnerton-Dyer conjecture, the parity conjecture, and the Shafarevich-Tate group.

By the time we reach Section 7.4, we have seen all the definitions and facts necessary for a discussion of Hilbert's Tenth Problem over rings of integers of number fields. The section provides a quick tour of the existing results and concentrates on the connection between elliptic curves and Hilbert's Tenth Problem over rings of integers. It leads the reader from a result of Bjorn Poonen [Po2002] through results of Gunther Cornelissen, Thanases Pheidas, and Karim Zahidi [CPZ2006], Alexandra Shlapentokh [Sh2006], and Barry Mazur and Karl Rubin [MR2010] to the theorem of Hector Pasten and Ram Murty described above.

As mentioned at the beginning, this book was conceived as a textbook. All sections come with exercise sets. Chapters 1–6 are accessible to any student, requiring a minimal level of mathematical maturity. If one is to include Chapter 7 in a syllabus, then we recommend that it is designated as "extra credit." Altogether it is a very nice introduction to the subject, illuminating its connection to very recent results and unsolved problems in number theory.

References

[CPZ2006] Gunther Cornelissen, Thanases Pheidas, and Karim Zahidi, *Division-ample sets and the Diophantine problem for rings of integers*, J. Théor. Nombres Bordeaux **17** (2005), no. 3, 727–735. MR2212121 (2006m:11042)

[JSWW76] James Jones, Daihachiro Sato, Hideo Wada, and Douglas Wiens, *Diophantine representation of the set of prime numbers*, Amer. Math. Monthly **83** (1976), no. 6, 449–464. MR0414514 (54 #2615)

[Jo78] James Jones, *Three universal representations of recursively enumerable sets*, J. Symbolic Logic **43** (1978), no. 2, 335–351. MR0498049 (58 #16226)

[Jo82] James Jones, *Universal Diophantine equation*, J. Symbolic Logic **47** (1982), no. 3, 549–571. MR0666816 (84e:10070)

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) **74** (1961), 425–436. MR0133227

[DMR76] Martin Davis, Yuri Matijasevič, and Julia Robinson, *Hilbert's tenth problem, Diophantine equations: positive aspects of a negative solution*, Mathematical developments arising from Hilbert problems (Northern Illinois Univ., De Kalb, Ill., 1974), Proc. Sympos. Pure Math., vol. XXVIII, Amer. Math. Soc., Providence, RI, 1976, 323–378. MR0432534 (55 #5522)

[Dav72] Martin Davis, *On the number of solutions of Diophantine equations*, Proc. Amer. Math. Soc. **35** (1972), 552–554. MR0304347 (46 #3482)

[Mat68] Ju Matijasevič [Yuri Matiyasevich], *Arithmetic representations of powers*, Zap. Nauch. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **8** (1968), 159–165. MR0238698 (39 #62)

[Po2002] Bjorn Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, 33–42. MR2041072 (2004m:11206)

[MR2010] Barry Mazur and Karl Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575. MR2660452 (2012a:11069)

[MP2018] M. Ram Murty and Hector Pasten, *Elliptic curves, L-functions, and Hilbert's tenth problem*, J. Number Theory **182** (2018), 1–18. MR3703929

[Sh2006] Alexandra Shlapentokh, *Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers*, Trans. Amer. Math. Soc. **360** (2008), no. 7, 3541–3555. MR2386235 (2010e:11116)

[Sh2007] Alexandra Shlapentokh, *Hilbert's tenth problem. Diophantine classes and extensions to global fields*, New Mathematical Monographs, vol. 7, Cambridge University Press, Cambridge, 2007, xiv+320 pp., ISBN: 978-0-521-83360-8; 0-521-83360-4. MR2297245 (2009e:11235)

[Sie72] Carl Ludwig Siegel, *Zur Theorie der quadratischen Formen*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II, 1972, 21–46. MR0311578 (47 #140)

Alexandra Shlapentokh

Credits

Front cover image by Jesse Jacobs.
Author photo is courtesy of Alexandra Shlapentokh.