Hilbert's Tenth Problem and Paradigms of Computation

Yuri Matiyasevich

Steklov Institute of Mathematics
Laboratory of Mathematical Logic
27, Fontanka
St.Petersburg, Russia 191023
yumat@pdmi.ras.ru
http://logic.pdmi.ras.ru/~yumat

Abstract. This is a survey of a century long history of interplay between Hilbert's tenth problem (about solvability of Diophantine equations) and different notions and ideas from the Computability Theory.

1 Statement of the Problem: Intuitive Notion of Algorithm

In the year 1900 the prominent German mathematician David Hilbert delivered to the *Second International Congress of Mathematicians* (held in Paris) his famous lecture titled *Mathematische Probleme* [12]. There he put forth 23 (groups of) problems which were, in his opinion, the most important open problems in mathematics that the pending 20th century would inherit from passing 19th century. Problem number 10 was stated as follows:

> **10. Entscheidung der Lösbarkeit einer diophantischen Gleichung.**
> Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoefficienten sei vorgelegt : *man soll ein Verfahren angeben, nach welchem sich mittels einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.* [1]

A *Diophantine equation* is an equation of the form

$$P(x_1, \ldots, x_m) = 0 \tag{1}$$

[1] **10. Determination of the Solvability of a Diophantine Equation.** Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *Devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

S.B. Cooper, B. Löwe, and L. Torenvliet (Eds.): CiE 2005, LNCS 3526, pp. 310–321, 2005.

where P is a polynomial with integer coefficients. Hilbert raised the question about solving Diophantine equations in *"rational integers"* which were nothing else but numbers $0, \pm 1, \pm 2, \ldots$; without loss of generality in this paper we will deal with solving Diophantine equations in natural numbers so all lower-case Latin letters will range over $0, 1, 2, \ldots$

Since Diophantus's time (3rd century A.D.) number-theorists have found solutions for plenty of Diophantine equations and also have proved the unsolvability of a large number of other equations. However, for different classes of equations, or even for different individual equations, one had to invent different specific methods. In the 10th problem Hilbert asked for a *universal* method for recognizing the solvability of Diophantine equations, i.e., in modern terminology the 10th problem is a *decision problem* (the only one among the 23 problems).

Note that Hilbert did not use the word "algorithm" in his statement of the tenth problem. Instead, he used the rather vague wording "*a process according to which it can be determined by a finite number of operations ...*". Although he could have used the word "algorithm," it would not really have helped much to clarify the statement of the problem because, at that time, there was no rigorous definition of the general notion of an algorithm. What existed was a number of examples of particular mathematical algorithms (such as celebrated Euclid's algorithm for finding the greatest common divisor of two integers), and an intuitive conception of an algorithm in general.

Does it imply that Hilbert's tenth problem was ill-posed? Not at all. The absence of a general definition of an algorithm was not in itself an obstacle to finding a positive solution of Hilbert's tenth problem. If somebody invented the required "*process*", it should be clear that in fact this process does the job, so an intuitive conception of an algorithm would be sufficient for positive solution of the tenth problem which was, most likely, Hilbert's expectation.

2 Davis's Conjecture: Are All Effectively Enumerable Sets Diophantine?

The first investigations aimed at a proof of algorithmic undecidability of Hilbert's tenth problem appeared at the beginning of 1950's. In particular, at that time Martin Davis considered *Diophantine sets* which are sets of natural numbers having *Diophantine representations*, i.e., definitions of the form

$$a \in \mathfrak{M} \Longleftrightarrow \exists x_1 \ldots x_m [P(a, x_1, \ldots, x_m) = 0] \tag{2}$$

where P is again a polynomial with integer coefficients one of the variables of which, a, is now a *parameter*. Davis's aim was to give a characterization of the whole class of Diophantine sets. The computability theory immediately puts a condition which is necessary for a set to be Diophantine: every Diophantine set is, evidently, effectively enumerable. Davis conjectured ([5, 6]) that this necessary condition is also sufficient:

Davis's conjecture. *A set of natural numbers is Diophantine if and only if it is effectively enumerable.*

Effectively enumerable sets can be defined via the notion of an algorithm, but the things can be taken in the reversed order: having given an independent definition of a effectively enumerable set, one can develop the whole theory of computability in terms of effectively enumerable sets instead of algorithms; examples of such an approach can be found in G.S. Tseitin's paper [38] and P. Martin-Löf's book [25]. Thus Davis's conjecture opened a way to base the computability theory on the number-theoretical notion of a Diophantine set.

3 Davis's Conjecture: First Step to the Proof via Arithmetization

Martin Davis's made the first step to proving his conjecture by showing in [6] that every effectively enumerable set $\mathfrak{M}$ has an almost Diophantine representation:

Theorem (Martin Davis). *Every effectively enumerable set $\mathfrak{M}$ has a representation of the form*

$$a \in \mathfrak{M} \Longleftrightarrow \exists z \forall y_{\leq z} \exists x_1 \ldots x_m [P(a, x_1, \ldots, x_m, y, z) = 0] \tag{3}$$

where P is a polynomial with integer coefficients and $\forall y_{\leq z}$ is the bounded universal quantifier "for all y not greater than z".

A representation of this type became known as the *Davis normal form*. To obtain it, Davis started in [6] with a representation of the set $\mathfrak{M}$ by an arbitrary arithmetical formula with any number of bounded universal quantifiers. The existence of such arithmetical formulas for every effectively enumerable set was demonstrated by Kurt Gödel in his classical paper [10]. Thanks to the bound on the universal quantifiers, every such formula defines an effectively enumerable and hence these formulas could be used for foundation of the Computability Theory.

4 Original Proof of Davis: Post's Normal Forms

According to a footnote in Davis' paper [6], the idea of obtaining the representation (3) by combining universal quantifiers from a general arithmetic representation was due to the (anonymous) referee of the paper. The original proof of Davis (outlined in [5] and given with details in [8]) was quite different. Namely, Davis managed to arithmetize *Post normal forms* using only one universal quantifier. These forms are a special case of more general *canonical forms* introduced by Emil L. Post [36] as a possible foundation of computability theory (and the above cited book [25] uses just Post canonical forms).

5 Davis's Conjecture Proved: Effectively Enumerable Sets Are Diophantine

It took two decades before Davis's conjecture became a theorem (for historical details see, for example, [29]; for an extensive bibliography on Hilbert's tenth problem visit [43]). The following weaker result due to Martin Davis, Hilary Putnam, and Julia Robinson [9] was a mile-stone on the way to the proof of Davis's conjecture:

DPR-Theorem. *For every effectively enumerable set $\mathfrak{M}$ there exists a representation of the form*

$$a \in \mathfrak{M} \Longleftrightarrow \exists x_1 \ldots x_m [E(a, x_1, x_2, \ldots, x_m) = 0] \tag{4}$$

where E is an exponential polynomial*, i.e., an expression constructed by combining the variables and particular integers using the traditional rules of addition, multiplication and exponentiation.*

The last step in the proof of Davis's conjecture was done in [26], and nowadays corresponding theorem is often called

DPRM-Theorem. *The notions of a Diophantine set and the notion of an effectively enumerable set coincide.*

Thus a (seemingly narrow) notion from the Number Theory turned out to be equivalent to the very general notion from the Computability Theory.

6 Existential Arithmetization I: Turing Machines

Already the very first proof of the DPRM-theorem given in [26] was constructive in the sense that as soon as a set $\mathfrak{M}$ is presented in any standard form, it is possible to find corresponding Diophantine representation (2). This was done in the following four steps:

1. construction of an arithmetical formula with many bounded universal quantifiers;
2. transformation of this formula into Davis normal form (3);
3. elimination the single bounded universal quantifier at the cost of passing to exponential Diophantine equations, getting an exponential Diophantine representation (4);
4. elimination of the exponentiation.

Now that we know that in fact no universal quantifier is necessary at all, it would be more natural to try to perform the whole arithmetization by using only purely existential formulas. From technical point of view for the success of this approach it is crucial to select an appropriate device for the initial representation of the set $\mathfrak{M}$.

For the first time such a purely existential arithmetization was done in [28] with the set $\mathfrak{M}$ being recognized by a Turing machine; a simplified way of constructing Diophantine representation by arithmetization of Turing machines is presented in [29]; yet another construction based on Turing machines is given in [39].

7 Existential Arithmetization II: Register Machines

When arithmetizing Turing machine, one has first to introduce a method to represent the content of the tape of the machine by numbers. In this respect another kind of abstract computing devices, *register machines*, turned out to be more suitable as a starting point for constructing Diophantine representations. Register machines were introduced almost simultaneously by several authors: J. Lambek [22], Z. A. Melzak [32], M. L. Minsky [33, 34], and J. C. Shepherdson and H. E. Sturgis [37]. Like Turing machines, register machines have very primitive instructions but, in addition, they deal directly with numbers rather than with words. This led to a "visual proof" of simulation of register machines by Diophantine equations (see [17, 18, 31]).

8 Existential Arithmetization III: Partial Recursive Functions

Another classical tool for the foundations of the Computability Theory are *partial recursive functions*. Existential arithmetization of these functions was done in [30] where Diophantine representations are constructed inductively, alongside construction of a partial recursive function from the initial functions. In order to deal with the primitive recursion and with the operator of minimization it turned out useful to generalize the notion of a partial recursive function: instead of dealing, say, with one-argument function f it was more convenient to work with a function F, defined on arbitrary n-tuples of natural number by

$$F(\langle a_1, \ldots, a_n \rangle) = \langle f(a_1), \ldots, f(a_n) \rangle. \tag{5}$$

9 Universality in Number Theory: Collapse of Diophantine Hierarchy

The DPRM-theorem allows a transfer of a number of ideas from the Computability Theory to the Number Theory. One example of such a transfer is the existence of a *universal Diophantine equation*, i.e., an equation

$$U(a, k, y_1, \ldots, y_M) = 0 \tag{6}$$

with the following property: *for arbitrary Diophantine equation*

$$P(a, x_1, \ldots, x_m) = 0 \tag{7}$$

there exist (effectively calculable) number k_P such that for arbitrary value of the parameter a the equation (7) *has a solution in $x_1, \ldots, x_m$ if and only if equation*

$$U(a, k_P, y_1, \ldots, y_M) = 0 \tag{8}$$

has a solution in $y_1, \ldots, y_M$. This implies that traditional number-theoretical hierarchy of Diophantine equations of degree 1, 2, ... with 1, 2 , ... unknowns collapses at some level. While the existence of (6) immediately follows from DPRM-theorem and the existence of, say, a universal Turing machine, the mere idea of the existence of a such universal object in the theory of Diophantine equations looked quite implausible not only for number-theorists, but for some logicians also (see [21]).

The existence of a universal Diophantine equation is an example of a result which is number-theoretical by its statement, but which was originally proved by tools from Computability Theory; today such an equation (6) can be constructed by purely number-theoretical methods (see [29]).

10 Growth of Solution: Speeding Up Diophantine Equations

Another example of a transfer of ideas from Computability Theory to Number Theory is as follows. M.Davis [7] used the DPRM-theorem in order to get for Diophantine equations an analog of a speed-up theorem of Manuel Blum [3]. Namely, *for every total computable function $\alpha(a, x)$ one can construct two one-parameter Diophantine equations*

$$P_1(a, x_1, \ldots, x_k) = 0, \qquad P_2(a, x_1, \ldots, x_k) = 0 \tag{9}$$

such that

(i) for every value of the parameter a exactly one of these two equations has a solution;

(ii) if Diophantine equations

$$Q_1(a, y_1, \ldots, y_l) = 0, \qquad Q_2(a, y_1, \ldots, y_l) = 0 \tag{10}$$

are solvable for the same values of the parameter a as, respectively, equations (9)*, then one can construct a third pair of Diophantine equations*

$$R_1(a, z_1, \ldots, z_m) = 0, \qquad R_2(a, z_1, \ldots, z_m) = 0 \tag{11}$$

such that

- *these equations are again solvable for the same values of the parameter a as, respectively, equations* (9)*;*
- *for all sufficiently large values of the parameter a for every solution $y_1, \ldots, y_l$ of one of the equations* (10) *there exists a solution $z_1, \ldots, z_m$ of the corresponding equation* (11) *such that*

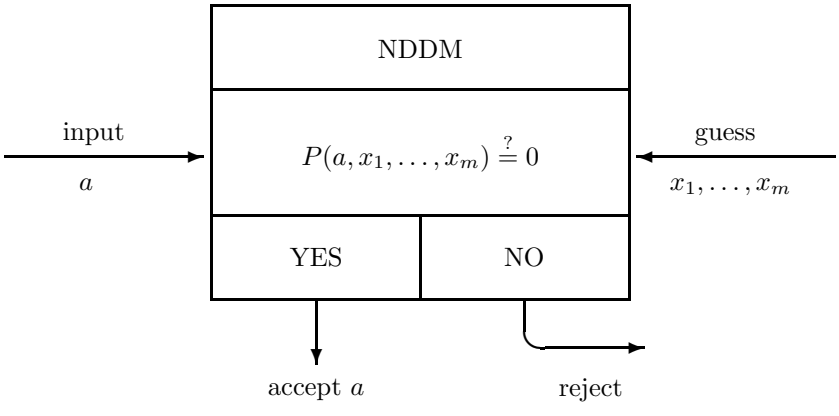
$$y_1 + \cdots + y_l > \alpha(a, z_1 + \cdots + z_m). \tag{12}$$

These formulation of a Diophantine speed-up contains, for the sake of the most generality, the notion of a total computable function; by substituting for α any particular (fast growing) total computable function, one would obtain a purely number-theoretic result which, however, has never been imagined by number-theorist.

11 Diophantine Machines: Capturing Nondeterminism

The DPRM-theorem allows one to treat Diophantine equations as computing devices. This was done in a picturesque form by Leonard Adleman and Kenneth Manders in [2]. Namely, they introduced the notion of *Non-Deterministic Diophantine Machine*, NDDM for short.

A NDDM is specified by a parametric Diophantine equation (7) and works as follows: on input a it guesses the numbers $x_1, \ldots, x_m$ and then checks (7); if the equality holds, then a is accepted.



The DPRM-theorem is exactly the statement that NDDMs are as powerful as, say, Turing machines, i.e., every set acceptable by a Turing machine is accepted by some NDDM, and, of course, *vice versa*.

The idea behind the introduction of a new computing device was as follows: in NDDM we have full separation of guessing and deterministic computation, and the latter is very simple—just the calculation of the value of a polynomial.

12 Unambiguity: Equations with Unique Solution

NDDMs are essentially non-deterministic computing devices. For such devices non-determinism is sometimes fictitious in the sense that at most one path can lead to accepting; if this is so one speaks about *unambiguous computations*. Corresponding property for (exponential) Diophantine representations was called

single-foldness: a representation (2) or (4) is called *single-fold representation* if for given value of the parameter a there exists at most one choice of the unknowns $x_1, \ldots, x_m$.

The existence of single-fold exponential Diophantine representations for every effectively enumerable set was established in [27] and later was improved to the existence single-fold exponential Diophantine representations with only 3 existential variables (see [14, 29]).

The existence of single-fold (or even weaker *finite-fold*) Diophantine representations is a major open problem; the positive answer would shed light on some difficulties met in Number Theory in connection with effectivisation of some results about Diophantine equations (for more details see, for example, [27, 29]).

Single-fold exponential Diophantine representations found applications in the descriptional complexity (see below).

13 Diophantine Complexity: D Versus NP

While the DPRM-theorem implies that NDDMs are as powerful as any other abstract computational device, the intriguing crucial question remains open: *how efficient are the NDDMs?* Adleman and Manders supposed that in fact NDDMs are as efficient as Turing machines.

For the latter there are two natural complexity measures: TIME and SPACE. For NDDMs there is only one natural complexity measure which plays the role of both TIME and SPACE. This measure is SIZE, which is the size (in bits) of the smallest solution of the equation (it is not essential whether we define this solution as the one with the smallest possible value of $\max\{x_1, \ldots, x_m\}$, or of $x_1 + \cdots + x_m$).

Adleman and Manders obtained in [2] the first results comparing the efficiency of NDDMs and Turing machines by estimating the SIZE of a NDDM simulating a Turing machine with TIME in special ranges.

Imposing bounds on the SIZE, we can define a corresponding complexity class. It was shown by A.K. Vinogradov and N.K. Kossovskii [40] that in this way one can define all Grzegorczyk classes starting from $\mathcal{E}^3$. Of course, the lower classes are of greater interest, and, what is typical, they turned out to be more difficult.

Adleman and Manders [1] also introduced the class **D** consisting of all sets $\mathfrak{M}$ having representations of the form

$$a \in \mathfrak{M} \iff \exists x_1 \ldots x_m \big[P(a, x_1, \ldots, x_m) = 0 \,\&\, |x_1| + \cdots + |x_m| \le |a|^k\big]$$

where $|a|$ denotes, as usual, the (binary) length of a. It is easy to see that $\mathbf{D} \subseteq \mathbf{NP}$ and the class **D** is known (see [24]) to contain **NP**-complete problems but otherwise the class **D** is little understood. Adleman and Manders asked whether in fact $\mathbf{D} = \mathbf{NP}$. Recently Chris Pollett [35] showed that this is so provided that $\mathbf{D} \subseteq$ **co-NLOGTIME**, and indicated a number of other ways to tackle $\mathbf{D} = \mathbf{NP}$ question.

An arithmetical definitions of the class **NP** via bounded analog of Davis normal form (3) were given by Bernhard R. Hodgson and Clement F. Kent [19, 13] and by Stasis Yukna [41, 42].

Helger Lipmaa [23] introduced **PD**, the "deterministic part" of the class **D**, and used Diophantine equations for secure information exchange protocols.

14 Random Diophantine Equations: Complexity on Average

The class **NP** contains thousands of equivalent problems which are supposed to be difficult (unless $\mathbf{P} = \mathbf{NP}$). However, only few problems from **NP** were proved to be of the maximal difficulty *on average*. Ramarathanam Venkatesan and Sivaramakrishnan Rajagopalan considered the *Randomized Diophantine Problem* and proved that it is average-case complete; unfortunately, their proof is conditional, and their assumption (on existence of a Diophantine equation with a special property) is equivalent to $\mathbf{D} = \mathbf{NP}$.

15 Parallel Computations: Calculation of a Polynomial on a Petri Net

Petri nets and *systems of vector addition* were introduced as tools for describing parallel computations. Michael Rabin used the undecidability of (exponential) Diophantine equation to prove that some relations between systems of vector addition (and hence also between Petri nets, because the latter easily simulate systems of vector addition) are not recognizable (see paper of Michel Hack [11] where a stronger result was obtained, or [29–Section 10.2]). The crucial point was a definition (introduced by Rabin) of a calculation of the values of (exponential) polynomials by systems of vector addition.

16 A Step Above Hilbert's Tenth Problem: Computational Chaos in Number Theory

Diophantine equations are undecidable. However, every Diophantine set is effectively enumerable and hence its *descriptive complexity* is the least possible: for every polynomial P the initial segment of the set $\mathfrak{M}$ from (2), i.e., the intersection of the set $\mathfrak{M}$ with the set

$$\{a \mid a \le N\}, \tag{13}$$

can be coded by $O(\log(N))$ bits only. However, we can reach the maximal descriptive complexity by considering questions which are only slightly more complicated than those from Hilbert's tenth problem. Gregory Chaitin [4] constructed a one-parameter exponential Diophantine equation such that the set

$$\{a \mid \exists^{\infty} x_1 \ldots x_m [E(a, x_1, x_2, \ldots, x_m) = 0]\} \tag{14}$$

requires N bits (up to an additive constant) for *prefix-free coding* of its intersection with the set (13); here $\exists^{\infty}$ means the existence of infinitely many solutions of the equation. Informally, one can say that the set (14) is completely chaotic.

More recently Toby Ord and Tien D. Kieu [20] constructed another exponential Diophantine equation which for every value of a has only finitely many solutions but the parity of the number of solutions again has completely chaotic behavior in the sense of the descriptive complexity. I was able to generalize this result in the following way: instead of asking about the parity of the number of solutions one can ask whether the number of solutions belongs to any fixed decidable infinite set with infinite complement.

All these results were obtained for exponential Diophantine equations because they are based on the existence of single-fold exponential Diophantine representations; the existence of similar chaos among genuine Diophantine equations is a major open question.

References

1. L. Adleman, K. Manders. Computational complexity of decision procedures for polynomials. In: *16th Annual Symposium on Foundations of Computer Science*, pages 169–177, 1975.
2. L. Adleman, K. Manders. Diophantine complexity. In: *17th Annual Symposium on Foundations of Computer Science*, pages 81–88, Houston, Texas, 25-26 October 1976. IEEE.
3. M. Blum. A machine-independent theory of the complexity of recursive functions. *Journal of the ACM*, 14(2):322–336, 1967.
4. G. Chaitin. *Algorithmic Information Theory.* Cambridge, England: Cambridge University Press (1987).
5. M. Davis, Arithmetical problems and recursively enumerable predicates (abstract). *Journal of Symbolic Logic*, 15(1):77–78, 1950.
6. M. Davis. Arithmetical problems and recursively enumerable predicates. *J. Symbolic Logic*, 18(1):33–41, 1953.
7. M. Davis. Speed-up theorems and Diophantine equations. In Randall Rustin, editor, *Courant Computer Science Symposium 7: Computational Complexity*, pages 87–95, 1973. Algorithmics Press, New York.
8. M. Davis. *Computability and Unsolvability.* Dover Publications, New York, 1982.
9. M. Davis, H. Putnam and J. Robinson, The decision problem for exponential Diophantine equations, *Ann. Math.* (2), 74, 425-436, 1961 (Reprinted in *The collected works of Julia Robinson*, S. Feferman, Ed., *Collected Works*, 6, 1996, xliv+338pp. American Mathematical Society, Providence, RI. ISBN: 0-8218-0575-4).
10. K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme. I. *Monatsh. Math. und Phys.*, 38(1):173–198, 1931.
11. M. Hack. The equality problem for vector addition systems is undecidable. *Theoretical Computer Science*, 2(1), 77–95, 1976.

12. D. Hilbert, Mathematische Probleme. Vortrag, gehalten auf dem internationalen Mathematiker Kongress zu Paris 1900, *Nachr. K. Ges. Wiss., Göttingen, Math.-Phys.Kl.* (1900), 253-297. See also David Hilbert, *Gesammelte Abhandlungen*, Berlin : Springer, vol. 3 (1935), 310 (Reprinted: New York : Chelsea (1965)). English translation: *Bull. Amer. Math. Soc.*, 8 (1901-1902), 437-479. Reprinted in : *Mathematical Developments arising from Hilbert problems*, Proceedings of symposia in pure mathematics, vol.28, American Mathematical Society, Browder Ed., 1976, pp.1-34.
13. B. R. Hodgson and C. F. Kent. A normal form for arithmetical representation of NP-sets. *Journal of Computer and System Sciences*, 27(3):378–388, 1983.
14. J. P. Jones and Ju. V. Matijasevič. Exponential Diophantine representation of recursively enumerable sets. In J. Stern, editor, *Proceedings of the Herbrand Symposium: Logic Colloquium '81*, volume 107 of *Studies in Logic and the Foundations of Mathematics*, pages 159–177, Amsterdam. North Holland, 1982.
15. J. P. Jones and Ju. V. Matijasevič. A new representation for the symmetric binomial coefficient and its applications. *Les Annales des Sciences Mathématiques du Québec*, 6(1):81–97, 1982.
16. J. P. Jones and Yu. V. Matijasevich. Direct translation of register machines into exponential Diophantine equations. In L. Priese, editor, *Report on the 1st GTI-workshop*, number 13, pages 117–130, Reihe Theoretische Informatik, Universität-Gesamthochschule Paderborn, 1983.
17. J. P. Jones and Y. V. Matijasevič. Register machine proof of the theorem on exponential Diophantine representation of enumerable sets. *J. Symbolic Logic*, 49(3):818–829, 1984.
18. J. P. Jones, Y. V. Matijasevič. Proof of recursive unsolvability of Hilbert's tenth problem. *Amer. Math. Monthly* 98(8):689–709, 1991.
19. C. F. Kent and B. R. Hodgsont. An arithmetical characterization of NP. *Theoretical Computer Science*, 21(3), 255–267, 1982.
20. T. Ord and T. D. Kieu. On the existence of a new family of Diophantine equations for Ω. Fundam. Inform. 56, No.3, 273-284 (2003).
21. G. Kreisel, "Davis, Martin; Putnam, Hilary; Robinson, Julia. The decision problem for exponential Diophantine equations." *Mathematical Reviews*, 24#A3061:573, 1962.
22. J. Lambek. How to program an infinite abacus. *Canad. Math. Bull.*, 4:295–302, 1961.
23. H. Lipmaa. On Diophantine Complexity and Statistical Zero-Knowledge Arguments. Lecture Notes in Computer Science, v. 2894, 2003, 398–415.
24. K. L. Manders and L. Adleman. NP-complete decision problems for binary quadratics. *J. Comput. System Sci.*, 16(2):168–184, 1978.
25. P. Martin-Löf. *Notes on Constructive Mathematics*. Almqvist & Wikseil, Stockholm, 1970.
26. Yu. V. Matiyasevich. Diofantovost' perechislimykh mnozhestv. *Dokl. AN SSSR*, 191(2):278–282, 1970. Translated in: *Soviet Math. Doklady*, 11(2):354-358, 1970.
27. Yu. V. Matiyasevich. Sushchestvovanie neèffektiviziruemykh otsenok v teorii èksponentsial'no diofantovykh uravneniĭ. *Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR (LOMI)*, 40:77–93, 1974. (Translated in: *Journal of Soviet Mathematics*, 8(3):299–311, 1977.)

28. Yu. Matiyasevich. Novoe dokazatel'stvo teoremy ob èksponentsial'no diofantovom predstavlenii perechislimykh predikatov. *Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR (LOMI)*, 60:75–92, 1976. (Translated in: *Journal of Soviet Mathematics*, 14(5):1475–1486, 1980.)
29. Yu. Matiyasevich. *Desyataya Problema Gilberta.* Moscow, Fizmatlit, 1993. English translation: Hilbert's tenth problem. MIT Press, 1993. French translation: Le dixième problème de Hilbert, Masson, 1995. URL: `http://logic.pdmi.ras.ru/~yumat/H10Pbook`, mirrored at `http://www.informatik.uni-stuttgart.de/ifi/ti/personen/Matiyasevich/H10Pbook`.
30. Yu. Matiysevich. A direct method for simulating partial recursive functions by Diophantine equations. Annals Pure Appl. Logic, 67, 325–348, 1994.
31. Yu. Matiyasevich, *Hilbert's tenth problem: what was done and what is to be done.* Contemporary mathematics, 270, pp. 1–47, 2000.
32. Z. A. Melzak. An informal arithmetical approach to computability and computation. *Canad. Math. Bull.*, 4:279–294, 1961.
33. M. L. Minsky. Recursive unsolvability of Post's problem of "tag" and other topics in the theory of Turing machines. *Ann. of Math. (2)*, 74:437–455, 1961.
34. M. L. Minsky. *Computation: Finite and Infinite Machines.* Prentice Hall, Englewood Cliffs; New York, 1967.
35. C. Pollett. On the Bounded Version of Hilbert's Tenth Problem. Arch. Math. Logic, vol. 42. No. 5. 2003. pp. 469–488.
36. E. L. Post. Formal reductions of the general combinatorial decision problem. Amer. J. Math., v. 65 (1943), 197-215. Reprinted in "The collected works of E. L. Post", M. Davis, editor. Birkhäuser, Boston, 1994.
37. J. C. Shepherdson and H. E. Sturgis. Computability of recursive functions, *J. ACM* 10(2):217–255, 1963.
38. G.S.Tseitin. Odin sposob izlozheniya teorii algorifmov i perechislimykh mnozhestv. Trudy Matematicheskogo instituta im. V. A. Steklova 72 (1964) 69–99. English translation in "Proceedings of the Steklov Institute of Mathematics".
39. P. van Emde Boas. Dominos are forever. In L. Priese, editor, *Report on the 1st GTI-workshop*, number 13, pages 75–95, Reihe Theoretische Informatik, Universität-Gesamthochschule Paderborn, 1983.
40. A. K. Vinogradov and N. K. Kosovskiĭ. Ierarkhiya diofantovykh predstavleniĭ primitivno rekursivnykh predikatov. *Vychislitel'naya tekhnika i voprosy kibernetiki*, no. 12, 99–107. Lenigradskiĭ Gosudarstvennyĭ Universitet, Leningrad 1975.
41. S.Yukna. Arifmeticheskie predstavleniya klassov mashinnoĭ slozhnosti. *Matematicheskaya logika i eë primeneniya*, no. 2:92–107. Institut Matematiki i Kibernetiki Akademii Nauk Litovskoĭ SSR, Vil'nyus, 1982.
42. S.Yukna. Ob arifmetizatsii vychisleniĭ. *Matematicheskaya logika i eë primeneniya*, no. 3:117–125. Institut Matematiki i Kibernetiki Akademii Nauk Litovskoĭ SSR, Vil'nyus, 1983.
43. `http://logic.pdmi.ras.ru/Hilbert10`.