PIMS Distinguished Chair Lectures

YURI MATIYASEVICH

PIMS Distinguished Chair,
University of Calgary, February–March, 2000

On Hilbert's Tenth Problem

Edited by Michael P. Lamoureux

Pacific Institute for the Mathematical Sciences
Distinguished Lecturer Series

supported by the
Natural Sciences and Engineering Research
Council

Number 1

ON HILBERT'S TENTH PROBLEM

by

Yuri Matiyasevich

Edited by
Michael Lamoureux

Published by
The Pacific Institute for the Mathematical
Sciences

Expository Lectures
from the PIMS Distinguished Chair Program
held at the University of Calgary
February–March, 2000.

Research supported in part by the Natural Sciences and
Engineering Research Council of Canada.

Preface

In the year 2000, the Pacific Institute for the Mathematical Sciences (PIMS) began its Distinguished Chair Programme, an initiative through which the six founding PIMS institutions[1] host extended visits of top mathematicians from around the world. These visits are built around collaborations with researchers at the host university, and include a series of lectures presented by the distinguished researchers, on any topic of their choice. They have been recorded on video for Web distribution, and transcribed for publication by the Institute.

PIMS's first Distinguished Chair was Dr. Yuri Matiyasevich, of the Steklov Institute of Mathematics at Saint Petersburg, Russia, who spent the months of February and March, 2000 at the University of Calgary. Dr. Matiyasevich is recognized for his outstanding work in logic, and in particular for his contributions to the resolution of Hilbert's Tenth Problem, involving the solution of Diophantine equations. His visit to Calgary was particularly rewarding, with lectures attracting full audiences of mathematical and computational scientists in both pure and applied areas, and setting a high standard for the ongoing programme.

Thanks are due to a number of individuals whose efforts helped to make this visit a successful one. In particular, we must acknowledge the diligence of Dr. James Jones, who both nominated Dr. Matiyasevich for the position, and acted as principal host during his visit; Dr. Rex Westbrook, who opened his house to the Matiyasevich family during their stay in Canada; and Ms. Marian Miles, who took care of the many details involved in bringing a family from overseas for an extended visit to Canada. We are highly indebited to the Department of Mathematics and Statistics at the University of Calgary, which provided the facilities and other resources necessary to host our distinguished visitor.

As editor, I would also like to extend my personal thanks to Dr. Matiyasevich's wife Nina and daughter Dasha, who did an excellent job in transcribing the five lectures into the notes you see here. As well, thanks are due to Ms. Cathy Beveridge for her technical assistance with the manuscript. Without their efforts, this book would not exist.

Dr. Michael Lamoureux, PIMS Deputy Director

[1] Simon Fraser University, and the universities of Alberta, British Columbia, Calgary, Victoria, and Washington.

Biography

Dr. Matiyasevich is a distinguished logician and mathematician based at the Steklov Institute of Mathematics at St. Petersburg. He is known for his outstanding work in logic, number theory, and theory of algorithms.

At the International Congress of Mathematicians in Paris in 1900 David Hilbert presented a famous list of 23 unsolved problems. It was 70 years later before a solution was found for Hilbert's tenth problem. Matiyasevich, at the young age of 22, achieved international fame for his solution.

Contents

Chapter 1

History of the problem

In this introductory chapter, I shall briefly describe the origin of Hilbert's tenth problem, the history of its solution, and some related problems which still remain open for solution.

1.1 Hilbert's address

Mathematics is a science which, to a great extent, is driven by problems. Throughout history, some of these problems have presented major challenges and teken decades to solve. One such challenge was Hilbert's tenth problem, namely, the question of the solvability of Diophantine equations.

In the year 1900, scientists from around the world gathered together in Paris for the *Second International Congress of Mathematicians*. One of the invited lecturers was the great German mathematician David Hilbert. As it was the last year of the nineteenth century, he decided to survey what were, in his opinion, the most important open problems in mathematics that the pending century would inherit from its predecessor.

Hilbert's famous paper *Mathematische Probleme* [17], which recounts his lecture, lists twenty three specific problems. While most of them are collections of related problems, the tenth problem is so short that it can be reproduced here in its entirety.

> **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]

[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

1.1.1 What are Diophantine equations

A *Diophantine equation* is an equation of the form

$$D(x_1, \ldots, x_m) = 0 \tag{1.1}$$

where D is a polynomial with integer coefficients.

What are rational integers

In his tenth problem, Hilbert raises the question of solving Diophantine equations in *"rational integers"*. This terminology may sound a bit strange and misleading. In fact, Hilbert had in mind nothing more than the familiar integers $0, \pm 1, \pm 2, \ldots$ He used the name *rational integers* because the term *integers* can also be understood in a broader sense of *algebraic integers*. Below, the word *integer* will be used in its "familiar sense" unless otherwise stated explicitly.

Who was Diophantus

Diophantus was a Greek mathematician who lived in the third century A.D. The equations that bear his name are polynomial equations with integer coefficients. Although the ancient Greek mathematicians had solved polynomial equations long before Diophantus, they had always done so in a geometrical way. For example, the solution of the equation

$$x^2 = 2 \tag{1.2}$$

would have been given as the diagonal of the square with unit sides. Diophantus began to solve polynomial equations in terms of rational numbers. For him, the equation (1.2) had no solution.

1.1.2 Why the problem was still open in 1900

Since Diophantus' time, number-theorists have found solutions for many Diophantine equations and also proved the insolvability of a large number of other equations. Why then did Hilbert consider, in 1900, that the algorithmic solution of Diophantine equations was an open problem?

Mathematicians, having investigaed the existing solutions and proofs of insolvability for Diophantine equations, realized that many different, specific methods had been invented for various classes of equations, or even for different individual equations. In the tenth problem Hilbert asked for a *universal* method for recognizing the solvability of Diophantine equations.

---

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.*

1.1.3 Modern understanding of Hilbert's tenth problem

Today we consider Hilbert's tenth problem to be a *decision problem.* This means that the problem consists of an infinite number of subproblems (specified by particular equations) each of which requires an answer "YES" or "NO" ("there is" or "there is not" a solution). An expected solution to the problem should be an algorithm that is both applicable to an arbitrary equation and produces the correct answer.

Why Hilbert did not use the word algorithm

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 his statement because, at that time, there was no rigorous definition of the general notion of an algorithm. What was known were different examples of particular mathematical algorithms, such as Euclid's algorithm for finding the greatest common divisor of two integers. However, 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 was a bonafide "algorithm."

The situation is fundamentally different when there is no possible algorithm, as turned out to be the case with Hilbert's tenth problem. To prove that no possible algorithm exists, or even to state it rigorously, one requires a definition of an algorithm. Such a definition was not developed until much later, in the 1930's, in the work of Kurt Gödel, Alan Turing, Emil Post, Alonso Church, and other logicians, when different tools were introduced to describe computational processes: the λ-calculus, recursive functions, Turing machines, and so on. Alonso Church was the first to understand that each specific, particular definition adequately reflects our intuitive idea about the general notion of algorithms. This assertion is now known as *Church's thesis.*

Church's thesis is the principal tool required to prove that Hilbert's tenth problem is undecidable.

1.1.4 The negative solution of Hilbert's tenth problem

Today we know that Hilbert's tenth problem has no solution. That means that it is undecidable as a decision problem.

Theorem (The undecidability of Hilbert's tenth problem) *There is no algorithm which, for a given arbitrary Diophantine equation, would tell whether the equation has a solution or not.*

A stronger form of the undecidability of Hilbert's tenth problem

The non-existence of an algorithm for Hilbert's tenth problem means that any given algorithm $\mathcal{A}$ (presumed to be the universal equation solver) fails for some particular equation

$$D_{\mathcal{A}}(x_1, \ldots, x_m) = 0. \tag{1.3}$$

That is, for this *counterexample,* either the algorithm never stops, or its output, if any, is wrong.

Theorem (A stronger form of the undecidability of Hilbert's tenth problem) *There is an algorithm which, for a given algorithm $\mathcal{A}$, produces a counterexample to the assumption that $\mathcal{A}$ solves Hilbert's tenth problem.*

Would Hilbert accept this as a "solution"?

The algorithmic undecidability of Hilbert's tenth problem is a *negative solution.* But would Hilbert himself accept this as a "solution" at all? I believe the answer is "YES". To support this point of view, I wish to cite a part of Hilbert's famous lecture *Mathematische Probleme* [17], in which the problems were posed:

> Mitunter kommt es vor, daß wir die Beantwortung unter ungenügenden Voraussetzungen oder in unrichtigem Sinne erstreben und infolgedessen nicht zum Ziele gelangen. Es entsteht dann die Aufgabe, die Unmöglichkeit der Lösung des Problems unter den gegebenen Voraussetzungen und in dem verlangten Sinne nachzuweisen. Solche Unmöglichkeitsbeweise wurden schon von den Alten geführt, indem sie z. B. zeigten, daß die Hypotenuse eines gleichschenkligen rechtwinkligen Dreiecks zur Kathete in einem irrationalen Verhältnisse steht. In der neueren Mathematik spielt die Frage nach der Unmöglichkeit gewisser Lösungen eine hervorragende Rolle, und wir nehmen so gewahr, daß alte schwierige Probleme wie der Beweis des Parallelenaxioms, die Quadratur des Kreises oder die Auflösung der Gleichungen 5. Grades durch Wurzelziehen, wenn auch in anderem als dem ursprünglich gemeinten Sinne, dennoch eine völlig befriedigende und strenge Lösung gefunden haben.
>
> Diese merkwürdige Tatsache neben anderen philosophischen Gründen ist es wohl, welche in uns eine Überzeugung entstehen läßt, die jeder Mathematiker gewiß teilt, die aber bis jetzt wenigstens niemand durch Beweise gestützt hat–ich meine die Überzeugung, daß ein jedes bestimmte mathematische Problem einer strengen Erledigung notwendig fähig sein müsse, sei es, daß es gelingt, die Beantwortung der gestellten Frage zu geben, sei es, daß die Unmöglichkeit seiner Lösung und damit die Notwendigkeit des Mißlingens aller Versuche dargetan wird.[2]

[2] Occasionally it happens that we seek the solution under insufficient hypotheses or in an incorrect sense, and for this reason we do not succeed. The problem then arises: how do we

1.2 Variations of Diophantine equations

The stronger form of the undecidability of Hilbert's tenth problem stated above, indicates that there is a close relationship between algorithms and Diophantine equations. The existence of such a relationship was conjectured in the beginning of the 1950's by the American mathematician Martin Davis. Before I state his conjecture, it is necessary to introduce more terminology. To this goal, consider, initially, a modification of Hilbert's tenth problem.

1.2.1 Natural number solutions

In the tenth problem, Hilbert asked about the existence of solutions in integers. One can also consider the similar problem about solvability in natural numbers. For a given Diophantine equation, *the problem of deciding whether it has a solution in integers* and *the problem of deciding whether it has a solution in natural numbers* are, in general, two quite different problems.

For example, the equation

$$(x+1)^3 + (y+1)^3 = (z+1)^3 \tag{1.4}$$

clearly has infinitely many integer solutions of the form $x = z,\ y = -1$. However, the fact that this equation has no solutions in natural numbers is not trivial at all.

On the other hand, let

$$D(x_1, \ldots, x_m) = 0 \tag{1.5}$$

be an arbitrary Diophantine equation; suppose that we are looking for its solutions in integers $x_1, \ldots, x_m$. Consider another equation

$$D(p_1 - q_1, \ldots, p_m - q_m) = 0. \tag{1.6}$$

It is clear that any solution of equation (1.6) in natural numbers $p_1, \ldots, p_m$, $q_1, \ldots, q_m$ yields the solution

$$\begin{aligned} x_1 &= p_1 - q_1 \\ &\vdots \\ x_m &= p_m - q_m \end{aligned} \tag{1.7}$$

show the impossibility of the solution under the given hypotheses, or in the sense contemplated. Such proofs of impossibility were effected by the ancients, for instance when they showed that the ratio of the hypotenuse to the side of a right isosceles triangle is irrational. In later mathematics, the question as to the impossibility of certain solutions plays a preëminent part, and we perceive in this way that old and difficult problems, such as the proof of the axiom of parallels, the squaring of circle, or the solution of equations of the fifth degree by radicals have finally found fully satisfactory and rigorous solutions, although in another sense than that originally intended.

It is probably this important fact along with other philosophical reasons that gives rise to the conviction (which every mathematician shares, but which no one has as yet supported by a proof) that every definite mathematical problem must necessary be susceptible of an exact settlement, either in the form of an actual answer to the question asked, or by the proof of the impossibility of its solution and therewith the necessary failure of all attempts.

of equation (1.5) in integers $x_1, \ldots, x_m$. Moreover, for any $x_1, \ldots, x_m$ forming a solution of equation (1.5) we can find natural numbers $p_1, \ldots, p_m, q_1, \ldots, q_m$ satisfying (1.7) and, hence, yielding a solution of equation (1.6).

Thus, one says that the problem of solvability of equation (1.5) in integers *reduces* to the problem of solvability of equation (1.6) in natural numbers. Respectively, one also says that the decision problem of recognizing the solvability of Diophantine equations in integers *reduces* to the decision problem of recognizing the solvability of Diophantine equations in natural numbers.

In fact, these two decision problems are *equivalent* in the sense that each of them reduces to the other one, but the reduction in the other direction is less evident. Let

$$D(p_1, \ldots, p_m) = 0 \tag{1.8}$$

be an arbitrary Diophantine equation for which we are looking for natural number solutions. Consider the following equation:

$$D(w_1^2 + x_1^2 + y_1^2 + z_1^2, \ldots, w_m^2 + x_m^2 + y_m^2 + z_m^2) = 0. \tag{1.9}$$

It is clear that any solution of the latter equation in integers yields a solution of the former equation in natural numbers. Conversely, every solution of (1.8) in natural numbers $x_1, \ldots, x_m$ can be obtained from some solution of equation (1.9) in integers $w_1, \ldots, z_m$, because, by Lagrange's theorem, every natural number is the sum of four squares.

Thus, we see that the two problems – that of recognizing whether a Diophantine equation has a solution in integers, and that of recognizing whether it has a solution in natural numbers – are, in general, different problems for a *particular equation*, but they are equivalent when considered as decision problems, i.e., algorithmic problems about the *whole class* of Diophantine equations.

For technical reasons, it is easier to work with variables ranging over natural numbers, and, therefore, most of the time, I shall suppose that our unknowns are natural numbers.

1.2.2 Parametric equations

Besides *individual* Diophantine equations, one can also consider *families* of Diophantine equations. Such a family is defined by a Diophantine equation of the form

$$D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0, \tag{1.10}$$

where D is a polynomial with integer coefficients, the variables of which are split into two groups:

- the *parameters* $a_1, \ldots, a_n$;
- the *unknowns* $x_1, \ldots, x_m$.

We shall suppose that the parameters, as well as the unknowns, can assume positive integer values only.

For some choices of the values of the parameters $a_1, \ldots, a_n$ the equation can have a solution in the unknowns $x_1, \ldots, x_m$; for other choices of the values of the parameters, it can have no solution.

1.2.3 Diophantine sets

Consider the set $\mathfrak{M}$ of all n-tuples $\langle a_1, \ldots, a_n \rangle$ for which the parametric equation (1.10) has a solution, that is

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow \exists x_1 \ldots x_m \{D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0\}. \tag{1.11}$$

Sets having such representations are called *Diophantine sets*. An equivalence of the form (1.11) is called the *Diophantine representation* of the set $\mathfrak{M}$. With an abuse of language, one can say that the equation (1.10) itself is a representation of the set.

Examples

Some easy examples of Diophantine sets are the following:

- *the set of all squares*, represented by the equation

$$a - x^2 = 0; \tag{1.12}$$

- *the set of all composite numbers*, represented by the equation

$$a - (x_1 + 2)(x_2 + 2) = 0; \tag{1.13}$$

- *the set of all positive integers which are not powers of* 2, represented by the equation

$$a - (2x_1 + 3)x_2 = 0. \tag{1.14}$$

Although it is perhaps less evident, *the set of all numbers which are* not *squares* is also Diophantine; this set is represented by the equation

$$(a - z^2 - x - 1)^2 + ((z + 1)^2 - a - y - 1)^2 = 0. \tag{1.15}$$

However, if one asks about the complements of the other two sets above, the answers are not clear at all.

- Is *the set of all prime numbers* Diophantine?

- Is *the set of all powers of 2* Diophantine?

1.3 Davis's conjecture

It is natural to seek a characterization of the whole class of Diophantine sets or, at least, some necessary or sufficient conditions for a set to be Diophantine. One necessary condition arises if one looks at Diophantine sets from the computational point of view. As soon as on is given a parametric Diophantine equation

$$D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0 \tag{1.16}$$

one can effectively list all n-tuples from the Diophantine set $\mathfrak{M}$ represented by this equation. Namely, one needs only to look over, in some order, all $(n+m)$-tuples of possible values of all the variables $a_1, \ldots, a_n$, $x_1, \ldots x_m$ and check every time whether the equality (1.16) holds or not. If it does, one puts the n-tuple $\langle a_1, \ldots, a_n \rangle$ on the list of elements of $\mathfrak{M}$. In this way, every n-tuple from $\mathfrak{M}$ will sooner or later appear on the list, although perhaps many times.

The above described algorithm for listing Diophantine sets has a very special form. Allowing for arbitrary algorithms, we arrive at the following notion studied in computability theory.

Definition *A set $\mathfrak{M}$ of n-tuples of natural numbers is called* listable *or* effectively enumerable, *if there is an algorithm which would print in some order, possibly with repetitions, all the elements of the set $\mathfrak{M}$.*

For example, it is easy to write a program which would, working for an infinitely long time, print all prime numbers or all powers of 2, and thus the corresponding sets are listable.

As discussed above, for a set $\mathfrak{M}$ to be Diophantine, it is *necessary* that $\mathfrak{M}$ is listable. Martin Davis [8] conjectured that this condition is also *sufficient.*

Davis's conjecture *The notions of a Diophantine set and a listable set coincide; i.e., a set is Diophantine if and only if it is listable.*

This conjecture immediately implies the undecidability of Hilbert's tenth problem because there were known examples of listable sets without algorithms for recognizing their elements.

1.3.1 Corollaries of Davis's conjecture

Davis's conjecture was bold and had many striking consequences.

Prime numbers as all positive values of a polynomial

Davis's conjecture, if true, implied the existence of a particular polynomial P such that the equation

$$P(a, x_1, \ldots, x_m) = 0 \tag{1.17}$$

has a solution if and only if a is a prime number. Hilary Putnam [42] noted that such an equation can be rewritten in the following form:

$$a = (x_0 + 1)(1 - P^2(x_0, x_1, \ldots, x_n)) - 1. \tag{1.18}$$

In fact, every solution of equation (1.17) can be extended to a solution of equation (1.18) by putting

$$x_0 = a. \tag{1.19}$$

On the other hand, in any solution of equation (1.18) with non-negative a, the product in the right-hand side should be positive, which is possible only if

$$P(x_0, \ldots, x_n) = 0, \tag{1.20}$$

which implies (1.19) and consequently (1.17).

Thus Davis's conjecture implied the existence of a particular polynomial (namely, the right-hand side in (1.18)) such that the set of all its non-negative values was exactly the set of all prime numbers. This corollary was considered, by many researchers, as an informal argument against Davis's conjecture.

Universal Diophantine equation

One can list all of the listable sets:

$$\mathfrak{M}_0, \mathfrak{M}_1, \ldots, \mathfrak{M}_k, \ldots \tag{1.21}$$

Formally, for every n there exists a listable set $\mathfrak{U}_n$ of $(n+1)$-tuples such that

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M}_k \iff \langle a_1, \ldots, a_n, k \rangle \in \mathfrak{U}_n. \tag{1.22}$$

Davis's conjecture implied that the set $\mathfrak{U}_n$, being listable, should have a Diophantine representation:

$$\begin{aligned} &\langle a_1, \ldots, a_n, a_{n+1} \rangle \in \mathfrak{U}_n \iff \\ &\quad \exists y_1 \ldots y_M \{U_n(a_1, \ldots, a_n, a_{n+1}, y_1, \ldots, y_M) = 0\}. \end{aligned} \tag{1.23}$$

Thus a Diophantine representation of an *arbitrary* listable set of n-tuples can be obtained from a *single* polynomial U_n just by fixing the value of one of its variables:

$$\begin{aligned} &\langle a_1, \ldots, a_n \rangle \in \mathfrak{M}_k \iff \\ &\quad \exists y_1 \ldots y_M \{U_n(a_1, \ldots, a_n, k, y_1, \ldots, y_M) = 0\}. \end{aligned} \tag{1.24}$$

In other words, the equation

$$U_n(a_1, \ldots, a_n, k, y_1, \ldots, y_M) = 0 \tag{1.25}$$

is *universal* in the following sense: for every Diophantine equation

$$D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0, \tag{1.26}$$

one can effectively find a particular number k_D, such that, for given values of the parameters $a_1, \ldots, a_n$, equation (1.26) has a solution in $x_1, \ldots, x_m$ if and only if the equation

$$U_n(a_1, \ldots, a_n, k_D, y_1, \ldots, y_M) = 0 \tag{1.27}$$

has a solution in $y_1, \ldots, y_M$.

Note that equation (1.27) has a fixed degree and a fixed number of unknowns, while equation (1.26) can be of an arbitrary high degree and can have an unlimited number of unknowns.

1.3.2 Davis's normal form

Martin Davis's first step to proving his conjecture was to prove in [8] that every listable set $\mathfrak{M}$ has an almost Diophantine representation.

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

$$\begin{aligned}&\langle a_1, \ldots, a_n\rangle \in \mathfrak{M} \Longleftrightarrow \\ &\quad \exists z \forall y \leq z \exists x_1 \ldots x_m \{D(a_1, \ldots, a_n, x_1, \ldots, x_m, y, z) = 0\}.\end{aligned}$$

A representation of this type is said to be in the *Davis normal form*. This form of representation was a quantitative improvement over the classical result of Kurt Gödel [16] who demonstrated the existence of similar arithmetical representations with an arbitrary number of universal quantifiers. All that remained to prove Davis's conjecture was to eliminate the sole universal quantifier. This last step took twenty years.

1.3.3 Exponential Diophantine equation

The universal quantifier was eliminated from the Davis normal form in the celebrated joint paper of Martin Davis, Hilary Putnam and Julia Robinson [12] published in 1961. However, the cost of this elimination was rather high. Namely, Davis, Putnum and Robinson were forced to consider a broader class of equations, the so-called *exponential Diophantine equations*. These are equations of the form

$$E_{\mathrm{L}}(x_1, x_2, \ldots, x_m) \;=\; E_{\mathrm{R}}(x_1, x_2, \ldots, x_m) \tag{1.28}$$

where E_{L} and E_{R} are so-called *exponential polynomials*, i.e., expressions constructed by combining the variables and particular positive integers using the traditional rules of addition, multiplication and exponentiation.

An example of an exponential Diophantine equation is

$$(x+1)^{y+2} + x^3 = y^{(x+1)^x} + y^4. \tag{1.29}$$

Exponential Diophantine representations

Similar to the case of Diophantine equations, one can consider parametric exponential Diophantine equations. In addition, one can introduce the notions of exponential Diophantine sets and exponential Diophantine representations. Davis, Putnam and Robinson proved an analogue of Davis's conjecture for exponential Diophantine equations, namely, that there is an *exponential Diophantine representation* for every listable set.

Theorem (Martin Davis, Julia Robinson, Hilary Putnam [12]) *For every listable set $\mathfrak{M}$ of n-tuples of non-negative integers there is a representation of the form*

$$\begin{aligned}&\langle a_1,\ldots,a_n\rangle \in \mathfrak{M} \Longleftrightarrow\\ &\exists x_1\ldots x_m E_{\mathrm{L}}(a_1,\ldots,a_n,x_1,x_2,\ldots,x_m) =\\ &\qquad\qquad E_{\mathrm{R}}(a_1,\ldots,a_n,x_1,x_2,\ldots,x_m)\end{aligned}$$

where E_{L} and E_{R} are exponential polynomials.

Universal exponential Diophantine equation

This theorem was a great breakthrough because it gives a purely existential representation and, thus, one has immediate corollaries about these equations. In particular, one can construct *a universal exponential Diophantine equation*

$$E_{\mathrm{L}}(a_1,\ldots,a_n,k,x_1,x_2,\ldots,x_m) \;=\; E_{\mathrm{R}}(a_1,\ldots,a_n,k,x_1,x_2,\ldots,x_m) \quad (1.30)$$

and, hence, solving an arbitrary exponential Diophantine equation can be reduced to solving an exponential Diophantine equation with a fixed number of unknowns. In fact, it is known today that this number can be as low as only three unknowns. The original proof of this estimate was given in [32] and was also reproduced in [34, 51].

Although such a reduction in the number of unknowns is purely a number-theoretical statement, it was not discovered nor even suspected by number-theorists. Rather, it was initially proven by logicians using notions from computability theory. Today one can construct [34, 35] a universal exponential Diophantine equation by purely number-theoretical tools.

However, despite the remarkable results of Davis, Putnam and Robinson, even some logicians found the existence of a universal Diophantine equation implausible. In his synopsis for *Mathematical Reviews* [23] of this celebrated paper of Davis, Putnam and Robinson [12], G. Kreisel wrote:

> These results are superficially related to Hilbert's tenth Problem on (ordinary, i.e., non-exponential) Diophantine equations. The proof of the authors' results, though very elegant, does not use recondite facts in the theory of numbers nor in the theory of r.e. sets, and so it is likely that the present result is not closely connected with

Hilbert's tenth Problem. Also it is not altogether plausible that all (ordinary) Diophantine problems are uniformly reducible to those in a fixed number of variables of fixed degree, which would be the case if all r.e. sets were Diophantine.

1.3.4 From exponential to genuine Diophantine equations

In order to prove DAvis's conjecture, in view of the work by Davis, Putnam and Robinson, it was sufficient to show that the set $\mathfrak{A}$ of all triples of the form $\langle a, b, a^b \rangle$ is Diophantine. In fact, suppose that this is so and let

$$\begin{aligned} \langle a, b, c \rangle \in \mathfrak{A} &\Leftrightarrow a^b = c \\ &\Leftrightarrow \exists z_1 \ldots z_m \{A(a, b, c, z_1, \ldots, z_m) = 0\} \end{aligned} \tag{1.31}$$

be the corresponding Diophantine representation. With the aid of such a polynomial A, one can transform an arbitrary exponential Diophantine equation into an equivalent Diophantine equation with extra unknowns.

Consider (1.29) as an example equation. Here there are three exponentiations and one can use three copies of the Diophantine equation from (1.31) to transform equation (1.29) into an equivalent Diophantine equation

$$\begin{aligned} A^2(x+1, x+2, s', z_1', \ldots, z_m') &+ \\ A^2(x+1, x, s'', z_1'', \ldots, z_m'') &+ \\ A^2(y, s'', s''', z_1''', \ldots, z_m''') &+ \\ (s' + x^3 - s''' - y^4)^2 &= 0. \end{aligned} \tag{1.32}$$

In other words, in order to prove that *every* listable set is Diophantine it was sufficient to prove that *one particular* set of triples has a Diophantine representation (1.31).

Robinson predicates

The study of this problem was begun by Julia Robinson much earlier, at the beginning of the 1950's, i.e., at the same time when Davis posed his conjecture.

Robinson failed to find a Diophantine representation for exponentiation. However, in [45], she found a condition sufficient for the existence of such a representation.

Theorem (Julia Robinson) *There is a polynomial* $A(a, b, c, z_1, \ldots, z_m)$ *such that*

$$a^b = c \quad \Leftrightarrow \quad \exists z_1 \ldots z_m \{A(a, b, c, z_1, \ldots, z_m) = 0\}$$

provided that there is a Diophantine equation

$$J(u, v, y_1, \ldots, y_w) = 0 \tag{1.33}$$

such that

- *in every solution of the equation we have* $u < v^v$;
- *for every* k *there is a solution such that* $u > v^k$.

Equation (1.33) defines a relation between u and v which holds if and only if the equation has a solution. Robinson called relations satisfying the above two inequalities *relations of exponential growth.* They also became known as *Robinson predicates.*

Now, in order to prove Davis's conjecture, it remained to find a single relation of exponential growth defined by a Diophantine equation. Surprisingly, among numerous two-parameter equations studied in number theory from the time of Diophantus up to the end of 1960's, no equation was known that defined a relation of exponential growth.

This fact, together with the unbelievable corollaries of Davis's conjecture, produced serious doubts about the existence of a Robinson relation. At some point, Robinson herself lost her belief in it and began to look for a positive solution of Hilbert's tenth problem (see [43]).

The last step

Finally, in a work published in 1970 [28], I was able to construct the required equation defining a relation with exponential growth. It was precisely the relation

$$v = \phi_{2u} \tag{1.34}$$

where ϕ_0, ϕ_1, ... is the well-known sequence of Fibonacci numbers:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots \tag{1.35}$$

This celebrated sequence has been extensively studied since the time of Fibonacci. Nevertheless, I was able to find a new property for this sequence which had been unknown to number-theorists for centuries, namely

$$\phi_n^2 \mid \phi_m \Longrightarrow \phi_n \mid m. \tag{1.36}$$

It is not difficult to prove this property of Fibonacci numbers *after* it has been stated (see Chapter 3).

My construction of a relation of exponential growth turned out to be chronologically the last step in the proof of Davis's conjecture which now is often referred to as the *DPRM-theorem*, denoting Davis-Putnam-Robinson-Matiyasevich.

DPRM-theorem *Every listable set* $\mathfrak{M}$ *of* n*-tuples of non-negative integers has a Diophantine representation, that is*

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow$$
$$\exists x_1 \ldots x_m \{D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0\}$$

for some polynomial with integer coefficients.

Nowadays, detailed and simplified proofs of this theorem can be found in many publications, in particular, in [1, 4, 6, 9, 10, 21, 26, 27, 29, 34, 51]. There is also an Internet website devoted to Hilbert's tenth problem, as listed in [54].

1.4 Some corollaries of the DPRM-theorem

With the proof of Davis's conjecture, one obtains all the corollaries previously believed to be implausible.

The whole proof is constructive in the sense that given any standard representation of a listable set, one can actually find its Diophantine representation.

1.4.1 Polynomial for primes exhibited

The very first example of one of those "implausible" corollaries is a representation of the prime numbers by polynomials. That is, there is a particular polynomial representing the set of prime numbers, as described in [22].

Theorem (J.P. Jones, D. Sato, H. Wada, D. Wiens) *The set of all prime numbers is equal to the set of all positive values of the polynomial*

$$
\begin{aligned}
(k+2)\{\ \ 1\ \ & -[wz+h+j-q]^2 \\
& -[(gk+2g+k+1)(h+j)+h-z]^2 \\
& -[2n+p+q+z-e]^2 \\
& -\left[16(k+1)^3(k+2)(n+1)^2+1-f^2\right]^2 \\
& -\left[e^3(e+2)(a+1)^2+1-o^2\right]^2 \\
& -\left[(a^2-1)y^2+1-x^2\right]^2 \\
& -\left[16r^2y^4(a^2-1)+1-u^2\right]^2 \\
& -[n+l+v-y]^2 \\
& -\left[\left((a+u^2(u^2-a))^2-1\right)(n+4dy)^2+1-(x+cu)^2\right]^2 \\
& -\left[(a^2-1)l^2+1-m^2\right]^2 \\
& -\left[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x\right]^2 \\
& -\left[z+pl(a-p)+t(2ap-p^2-1)-pm\right]^2 \\
& -[ai+k+1-l-i]^2 \\
& -\left[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m\right]^2\ \}\,.
\end{aligned}
$$

assumed for non-negative integer values of twenty six variables $a,\ldots,z$.

Today, one can construct a polynomial that represents the prime numbers using only ten variables (see [31]).

1.4.2 Universal equations

The existence of universal Diophantine equations means that traditional number-theoretical classifications of Diophantine equations as equations in $1, 2, \ldots$ unknowns and as equations of degree $1, 2, \ldots$ collapse. It is easy to reduce the degree to four, while the current best bound for the number of unknowns is nine. Although I obtained this result and its proof myself (see [30]), for various reasons (see [34]) I never published it. A detailed proof was published by J. P. Jones [18].

However, at present, we cannot construct a single universal Diophantine equation of degree four in nine unknowns only. Naturally, there is a trade-off between the degree and the number of unknowns. Presently, (see [18]), the beset bounds obtainable are as follows: *Solving an arbitrary parametric Diophantine equation can be reduced to solving another Diophantine equation (with the same parameters) of degree D in M unknowns where $\langle D, M\rangle$ is any of the following pairs*:

$$\langle 4, 58\rangle,\ \langle 8, 38\rangle,\ \langle 12, 32\rangle,\ \langle 16, 29\rangle, \langle 20, 28\rangle,\ \langle 24, 26\rangle,\ \langle 28, 25\rangle,\ \langle 36, 24\rangle,$$
$$\langle 96, 21\rangle,\ \langle 2668, 19\rangle,\ \langle 2 \times 10^5, 14\rangle, \langle 6.6 \times 10^{43},\ 13\rangle,\ \langle 1.3 \times 10^{44}, 12\rangle,$$
$$\langle 4.6 \times 10^{44}, 11\rangle,\ \langle 8.6 \times 10^{44}, 10\rangle,\ \langle 1.6 \times 10^{45}, 9\rangle.$$

1.5 Hilbert's tenth problem in the broader sense

One can ask the following question: *would Hilbert be satisfied with the statement of the tenth problem if he knew it would be "solved" in the negative sense*? I believe the answer is "NO." Let me explain my point of view.

1.5.1 Solution in rational numbers

One can only guess why Hilbert asked about solutions only in "*integers.*" This, as explained earlier, is equivalent to asking for an algorithm for solving Diophantine equations in non-negative integers. By contrast, Diophantus was looking for solutions in rational numbers. So why did Hilbert not also ask about "*a process*" to determine the existence of a solution in rational numbers?

The answer is more or less evident. Hilbert was an optimist and believed in the existence of an algorithm for solving Diophantine equations in integers. Such an algorithm would allow one to solve equations in rational numbers as well. Namely, solving an equation

$$D(\chi_1, \ldots, \chi_m) = 0 \tag{1.37}$$

in rational $\chi_1, \ldots, \chi_m$ is equivalent to solving the equation

$$D\left(\frac{x_1 - y_1}{z+1}, \ldots, \frac{x_m - y_m}{z+1}\right) = 0$$

in non-negative integers $x_1, \ldots, x_m$, $y_1, \ldots, y_m$, z. The latter equation is equivalent to the Diophantine equation

$$(z+1)^d D\left(\frac{x_1 - y_1}{z+1}, \ldots, \frac{x_m - y_m}{z+1}\right) = 0$$

where d is the degree of D.

There is a less evident reduction of solving Diophantine equations in rational numbers to solving homogenous Diophantine equations in integers. Start by transforming (1.37) into

$$D\left(\frac{x_1}{z}, \ldots, \frac{x_m}{z}\right) = 0 \tag{1.38}$$

and then into

$$z^d D\left(\frac{x_1}{z}, \ldots, \frac{x_m}{z}\right) = 0. \tag{1.39}$$

An additional trick (see, for example, [34, 51]) is required to guarantee that $z \neq 0$.

So while asking *explicitly* about solving Diophantine equations in integers, Hilbert was also asking *implicitly* about solving Diophantine equations in rational numbers. A positive solution of the tenth problem, as it was originally stated, would give immediately a positive solution to the similar problem about solutions in rational numbers.

However, we have obtained a negative solution of the original statement of the tenth problem. What does this imply for solving Diophantine equations in rational numbers? Nothing. Homogenous Diophantine equations form a very special subclass of all Diophantine equations and it is quite possible that for this narrower class, a corresponding algorithm exists.

1.5.2 Two modern understandings of Hilbert's tenth problem

It is likely that, if Hilbert had anticipated the non-existence of the algorithms for solving Diophantine equations in integers, he would have expanded the statement of the tenth problem to include the case of solving equations in rational numbers. Thus, we can understand the tenth problem in two senses.

- *the narrower sense*, i.e., literally as the problem was stated;
- *the broader sense*, including other problems for which the solutions would *easily* follow from a positive solution of the tenth problem, as it was stated.

In the narrow sense, the tenth problem is closed, but in the broader sense it remains open.

Solving equations in rational numbers

Solving equations in rational numbers remains one of the most important open cases of Hilbert's tenth problem, considered in its broader sense. To date, progress in this case has been rather meagre.

Solving equations in Gaussian integers

Besides solving Diophantine equations in integers, one may be interested in solving them in different rings of integers from various algebraic extensions of the field of rational numbers. For example, one may be interested in solving Diophantine equations in *Gaussian integers*, i.e., complex numbers of the form $a + b\mathrm{i}$ where a and b are rational integers and $\mathrm{i} = \sqrt{-1}$. Clearly, the equation

$$D(\chi_1, \ldots, \chi_m) = 0 \tag{1.40}$$

has a solution in Gaussian integers if and only if equation

$$D(x_1 + y_1\mathrm{i}, \ldots, x_m + y_m\mathrm{i}) = 0 \tag{1.41}$$

has a solution in rational integers. Now one can separate the real and the imaginary parts by writing

$$\begin{aligned} &D(x_1 + y_1\mathrm{i}, \ldots, x_m + y_m\mathrm{i}) = \\ &\quad D_{\mathrm{R}}(x_1, \ldots, x_m, y_1, \ldots, y_m) + D_{\mathrm{I}}(x_1, \ldots, x_m, y_1, \ldots, y_m)\mathrm{i} \end{aligned} \tag{1.42}$$

and rewriting (1.41) as a genuine Diophantine equation

$$D_{\mathrm{R}}^2(x_1, \ldots, x_m, y_1, \ldots, y_m) + D_{\mathrm{I}}^2(x_1, \ldots, x_m, y_1, \ldots, y_m) = 0. \tag{1.43}$$

Hence one may consider solving Diophantine equations in Gaussian integers as part of Hilbert's tenth problem in the broader sense.

This problem was shown to be undecidable by J. Denef [13]. Denef found a reduction in the opposite direction, i.e., he showed how solving a Diophantine equation

$$D(x_1, \ldots, x_m) = 0 \tag{1.44}$$

in rational integers can be reduced to solving another Diophantine equation

$$G(\chi_1, \ldots, \chi_w) = 0 \tag{1.45}$$

in Gaussian integers. As a result of this reduction, the undecidability of Hilbert's tenth problem in the narrower sense implies the undecidability of its counterpart in Gaussian integers.

Cases of other rings of algebraic integers

Similar reductions were found by different researchers (for references see survey [41]) for rings of integers from some other algebraic extensions of the field of rational numbers. While these progress for the tenth problem in the broader sense, the reductions were done only for certain specific extensions. The general case of arbitrary extensions still remains an important open case of the tenth problem in the broader sense.

1.5.3 Connections with other famous problems

Considered in a broader sense, Hilbert's tenth problem deals with solutions that would *easily* follow from a positive solution of the problem, as it was originally stated. Thus, the scope of the tenth problem in the broader sense depends on one's understanding of the word "*easily*." Certainly, solving Diophantine equations in rational numbers or in Gaussian integers would follow easily. Yet, there are many other problems whose reductions to the tenth problem are not difficult, but simply less evident. Some examples of these problems are presented below.

Fermat's Last Theorem

Hilbert did not *explicitly* include Fermat's Last Theorem in his *Problemen*. Formally, this theorem considers the insolvability of an infinite series of Diophantine equations

$$x^n + y^n = z^n \tag{1.46}$$

with $n \geq 3$, $x \geq 1$, $y \geq 1$, and, thus, it is not a case of the tenth problem (for which Hilbert considered solving a single Diophantine equation rather than an infinite series of them).

Fermat's equation is a Diophantine equation in x, y, z for a fixed value of n, but is an exponential Diophantine equation if viewed as an equation in four unknowns n, x, y, z. Knowing how to transform an arbitrary exponential Diophantine equation into a genuine Diophantine equation with extra unknowns, one is able (as was actually done in [47, 5]) to construct a particular polynomial F with integer coefficients such that equation

$$F(n, x, y, z, u_1, \ldots, u_m) = 0 \tag{1.47}$$

has a solution in u_1, $\ldots$,u_m if and only if n, x, y and z form a solution to (1.46). Hence, Fermat's Last Theorem is equivalent to the statement that the particular, genuine, Diophantine equation

$$F(w + 3, x + 1, y + 1, z, u_1, \ldots, u_m) = 0 \tag{1.48}$$

has no solution in non-negative unknowns. A positive solution of the tenth problem in its original formulation would provide a tool to prove or disprove Fermat's Last Theorem. So, while it was not included *explicitly* among Hilbert's problems, Fermat's Last Theorem is *implicitly* present as a very particular case of the tenth problem.

Goldbach's Conjecture

Hilbert included *Goldbach's Conjecture* in his eighth problem. The conjecture, which is still open, states that *every even integer greater than 2 is the sum of two prime numbers.*

Consider the set $\mathfrak{G}$ of even numbers which are greater than 2, but which still are not the sum of two primes. For any particular number a, one can easily

check whether it is a counterexample to Goldbach's conjecture or not. Thus, this set $\mathfrak{G}$ of counterexamples is listable and, hence, Diophantine. Consequently, one can find a particular Diophantine equation

$$G(a, x_1, \ldots, x_m) = 0 \tag{1.49}$$

that has a solution if and only if a spoils the conjecture. In other words, Goldbach's conjecture is equivalent to the statement that the set $\mathfrak{G}$ is empty, and, hence, to the statement that Diophantine equation

$$G(x_0, x_1, \ldots, x_m) = 0 \tag{1.50}$$

has no solution at all.

Thus, the positive solution of the tenth problem in its original form would allow one to know whether Goldbach's conjecture is true or not.

The Riemann Hypothesis

Besides Goldbach's conjecture, Hilbert included in his eighth problem another outstanding conjecture, the famous *Riemann Hypothesis*. In its original formulation, it is a statement about the complex zeros of Riemann's *zeta function* which is the analytical continuation of the series

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}. \tag{1.51}$$

that converges for $\Re(z) > 1$.

Nevertheless, we can also construct a particular Diophantine equation

$$R(x_1, \ldots, x_m) = 0 \tag{1.52}$$

that has no solution if and only if the Riemann hypothesis is true. Such a reduction requires either the use of the theory of functions of a complex variable or the use of the fact that the Riemann Hypothesis can be reformulated as a statement about the distribution of prime numbers (for details see [11, 34]).

Thus, once again, an outstanding mathematical problem is seen as a specific case of Hilbert's tenth problem in its original formulation.

The Four Color Conjecture

In mathematical logic there is a powerful tool, *arithmetization*, which allows one to reduce to numbers many problems which are not about numbers at all.

As my last example, I shall consider yet another famous challenge to mathematicians, the Four Color Conjecture, which was established as a theorem in 1976 by the work of K. Appel and W. Haken [3]. This is a problem about coloring planar maps, but again we can construct a particular Diophantine equation

$$C(x_1, \ldots, x_m) = 0 \tag{1.53}$$

that has no solution if and only if the Four Color Conjecture is true. Again, a problem which was not included by Hilbert in his *Problemen* appears in an implicit form in the tenth problem.

What use could be made of such reductions

I have described the reductions of four famous problems to Diophantine equation:

- Fermat's Last Theorem,
- Goldbach's Conjecture,
- Riemann Hypothesis,
- Four Color Conjecture.

Two of these four problems have now been solved; two others remain open. The reductions of these problems may be considered striking, amazing, and amusing, but could they also be deemed to be useful? Hilbert's tenth problem is undecidable so a universal method to solve all these problems does not exist. We can hardly hope to solve any of these problems by looking at their corresponding, particular Diophantine equations because they are rather complicated.

However, we can reverse the order of our problem solving strategy. The tenth problem is undecidable, therefore, we need to invent more and more *ad hoc* methods to solve more and more Diophantine equations. This way, we can view the proof of Fermat's Last Theorem and that of the Four Color Theorem as deep tools for treating particular Diophantine equations and we can try to extend these techniques to other equations.

The reduction of famous problems to Diophantine equations can also be considered as a psychological "explanation" of the insolvability of Hilbert's tenth problem: one could hardly expect that so many difficult problems, from such diverse areas of mathematics, could be tackled by some universal "*process.*"

Chapter 2

Number-theoretical prerequisites

In this chapter, I introduce more terminology and some useful tools for constructing exponential Diophantine representations, as well as particular examples of such representations which are important for the proof in Chapter Four.

2.1 Exponential Diophantine equations

Consider *exponential Diophantine equations*. They are equations of the form

$$E_{\mathrm{L}}(x_1, \ldots, x_m) \;=\; E_{\mathrm{R}}(x_1, \ldots, x_m) \tag{2.1}$$

where E_{L} and E_{R} are so-called *exponential polynomials*, i.e., expressions constructed by combining the variables and particular non-negative integers using the traditional rules of addition, multiplication and exponentiation. We assume the unknowns $x_1, \ldots, x_m$ are *natural numbers*, i.e., the numbers $0, 1, 2, \ldots$.

It is necessary to define the value of 0^0. This can be done in different ways—compare three numbers

$$\lim_{\epsilon \to 0+} 0^{\epsilon} = 0, \qquad \lim_{\epsilon \to 0+} \epsilon^{0} = 1, \qquad \lim_{\epsilon \to 0+} \epsilon^{\epsilon} = 1. \tag{2.2}$$

For the purpose of the proof, it is convenient to define $0^0 = 1$.

2.1.1 Why subtraction is not allowed in exponential Diophantine equations

The expression

$$(x - y)^{2^{x-y}} \tag{2.3}$$

looks like a well-formed formula. However, there is no reasonable way to assign a numerical value to it, for example, if $x = 1$, $y = 3$. This is the reason

why subtraction is not allowed in exponential Diophantine equations. Without subtraction, one remains safely within the set of natural numbers.

2.1.2 Systems of exponential Diophantine equations

Although Hilbert asked about solving individual equations, one is often interested in solving a system of equations. It is easy to see, however, that treating systems of exponential Diophantine equations is not more difficult than working with a single equation. In fact, the system

$$E_{\mathrm{L}}(x_1, \ldots, x_m) = E_{\mathrm{R}}(x_1, \ldots, x_m) \tag{2.4}$$

$$F_{\mathrm{L}}(x_1, \ldots, x_m) = F_{\mathrm{R}}(x_1, \ldots, x_m) \tag{2.5}$$

of two exponential Diophantine equations can be combined into the equivalent single equation

$$\begin{aligned} (E_{\mathrm{L}}(x_1, \ldots, x_m) - E_{\mathrm{R}}(x_1, \ldots, x_m))^2 &+ \\ (F_{\mathrm{L}}(x_1, \ldots, x_m) - F_{\mathrm{R}}(x_1, \ldots, x_m))^2 &= 0. \end{aligned} \tag{2.6}$$

One can then eliminate subtraction by squaring and transposing negative terms to the right-hand side:

$$\begin{aligned} E_{\mathrm{L}}^2(x_1, \ldots, x_m) + E_{\mathrm{R}}^2(x_1, \ldots, x_m) + F_{\mathrm{L}}^2(x_1, \ldots, x_m) + F_{\mathrm{R}}^2(x_1, \ldots, x_m) = \\ 2E_{\mathrm{L}}(x_1, \ldots, x_m)E_{\mathrm{R}}(x_1, \ldots, x_m) + 2F_{\mathrm{L}}(x_1, \ldots, x_m)F_{\mathrm{R}}(x_1, \ldots, x_m). \end{aligned} \tag{2.7}$$

2.1.3 Families of exponential Diophantine equations

Besides *individual* Diophantine equations, one may also consider *families* of exponential Diophantine equations. Such a family is defined by an equation of the form

$$E_{\mathrm{L}}(a_1, \ldots, a_n, x_1, \ldots, x_m) = E_{\mathrm{R}}(a_1, \ldots, a_n, x_1, \ldots, x_m) \tag{2.8}$$

where $E_{\mathrm{L}}, E_{\mathrm{R}}$ are exponential polynomials, the variables of which are split into two groups:

- the *parameters* $a_1, \ldots, a_n$;
- the *unknowns* $x_1, \ldots, x_m$.

For the purposes of this discussion, the parameters are restricted to non-negative integer values only, as are the unknowns.

For some choices of the values of the parameters $a_1, \ldots, a_n$, the equation will have a solution in the unknowns $x_1, \ldots, x_m$; for other choices of the values of the parameters, it will have no solution.

2.2 Exponential Diophantine sets

We can consider the set $\mathfrak{M}$ of all n-tuples $\langle a_1, \ldots, a_n \rangle$ for which the parametric equation (2.8) has a solution, that is

$$\begin{aligned} &\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow \\ &\quad \exists x_1 \ldots x_m \{ E_{\mathrm{L}}(a_1, \ldots, a_n, x_1, \ldots, x_m) = \\ &\qquad E_{\mathrm{R}}(a_1, \ldots, a_n, x_1, \ldots, x_m) \}. \end{aligned} \tag{2.9}$$

Sets having such representations are said to be *exponential Diophantine*. An equivalence of the form (2.9) is called an *exponential Diophantine representation* of the set $\mathfrak{M}$. With an abuse of the language, one can say that the equation (2.8) is itself a representation of the set.

The number n will be called the *dimension* of the set $\mathfrak{M}$.

2.2.1 Generalized exponential Diophantine representations

Naturally, one can consider systems of parametric equations and for a system consisting, say, of two equations

$$E_{\mathrm{L}}(a_1, \ldots, a_n, x_1, \ldots, x_m) = E_{\mathrm{R}}(a_1, \ldots, a_n, x_1, \ldots, x_m) \tag{2.10}$$

$$F_{\mathrm{L}}(a_1, \ldots, a_n, x_1, \ldots, x_m) = F_{\mathrm{R}}(a_1, \ldots, a_n, x_1, \ldots, x_m) \tag{2.11}$$

one can consider the set $\mathfrak{M}$ of all n-tuples of the parameters for which this system has a solution in $x_1, \ldots, x_m$. Of course, since this set $\mathfrak{M}$ is an exponential Diophantine set, its exponential Diophantine representation can b given by the parametric analogue of (2.7). However, when E_L, E_R, F_L and F_R are replaced by concrete polynomials, it is not easy to recognize that this analogue of (2.7) is equivalent to the system of two equations (2.10) and (2.11). It is more natural to write

$$\begin{aligned} &\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow \\ &\quad \exists x_1 \ldots x_m \{ E_{\mathrm{L}}(a_1, \ldots, a_n, x_1, \ldots, x_m) = E_{\mathrm{R}}(a_1, \ldots, a_n, x_1, \ldots, x_m) \& \\ &\qquad F_{\mathrm{L}}(a_1, \ldots, a_n, x_1, \ldots, x_m) = F_{\mathrm{R}}(a_1, \ldots, a_n, x_1, \ldots, x_m) \}. \end{aligned} \tag{2.12}$$

Such equivalences will be called generalized exponential Diophantine representations. However, there is no formal definition of a generalized exponential Diophantine representation. Intuitively, they will be formulas which can be easily transformed into genuine exponential Diophantine representations. Thus, as soon as some new technique for constructing exponential Diophantine representations is introduced, the notion of a generalized exponential Diophantine representation would enlarge respectively.

Disjunction instead of conjunction

By replacing, in (2.12), the sign of conjunction & by the sign of disjunction $\vee$, one obtains another generalized exponential Diophantine representation:

$$\begin{aligned}\langle a_1,\dots,a_n\rangle \in \mathfrak{M} \Longleftrightarrow \\ \exists x_1\dots x_m\{E_{\mathrm{L}}(a_1,\dots,a_n,x_1,\dots,x_m) = E_{\mathrm{R}}(a_1,\dots,a_n,x_1,\dots,x_m) \vee \\ F_{\mathrm{L}}(a_1,\dots,a_n,x_1,\dots,x_m) = F_{\mathrm{R}}(a_1,\dots,a_n,x_1,\dots,x_m)\}. \qquad (2.13)\end{aligned}$$

In contrast to conjunction having a system of equations as its counterpart, there are no other tools in traditional mathematics for expressing the disjunction of a set of equations.

To justify calling (2.13) a generalized exponential Diophantine representation one can consider, naturally, the equation

$$\begin{aligned}(E_{\mathrm{L}}(a_1,\dots,a_n,x_1,\dots,x_m) - E_{\mathrm{R}}(a_1,\dots,a_n,x_1,\dots,x_m)) \times \\ (F_{\mathrm{L}}(a_1,\dots,a_n,x_1,\dots,x_m) - F_{\mathrm{R}}(a_1,\dots,a_n,x_1,\dots,x_m)) = 0. \qquad (2.14)\end{aligned}$$

Here again, one needs to expand the brackets and transpose negative terms; such simple equivalent algebraic transformations will not be mentioned explicitly below.

Inequality instead of equality

It is also possible put a negation in front of an exponential Diophantine equation:

$$\neg\{E_{\mathrm{L}}(a_1,\dots,a_n,x_1,\dots,x_m) = E_{\mathrm{R}}(a_1,\dots,a_n,x_1,\dots,x_m)\} \qquad (2.15)$$

or, equivalently,

$$E_{\mathrm{L}}(a_1,\dots,a_n,x_1,\dots,x_m) \neq E_{\mathrm{R}}(a_1,\dots,a_n,x_1,\dots,x_m). \qquad (2.16)$$

In this case, in order to obtain a genuine exponential Diophantine representation, one needs to introduce a new unknown; formula (2.16) is equivalent to

$$\exists y\{(E_{\mathrm{L}}(a_1,\dots,a_n,x_1,\dots,x_m) - E_{\mathrm{R}}(a_1,\dots,a_n,x_1,\dots,x_m))^2 = y+1\}. \qquad (2.17)$$

Now one can consider as a generalized exponential Diophantine representation any formula constructed from exponential Diophantine polynomials with the aid of equality and inequality relations and any combination of conjunctions and disjunctions.

2.2.2 Operations on exponential Diophantine sets

It is easy to see that the union of two exponential Diophantine sets of equal dimension is also an exponential Diophantineset. In fact, let these sets be represented by equations (2.10) and (2.11) respectively (without loss of generality, one can assume that the number of unknowns is the same in both representations). The union is then represented by equation (2.14).

Intersection of exponential Diophantine sets

The intersection of two exponential Diophantine sets of equal dimension is again an exponential Diophantine set. However, simply taking the parametric counterpart of (2.6) results in the equation

$$\begin{aligned}(E_{\mathrm{L}}(a_1,\ldots,a_n,x_1,\ldots,x_m)-E_{\mathrm{R}}(a_1,\ldots,a_n,x_1,\ldots,x_m))^2 \quad +\\ (F_{\mathrm{L}}(a_1,\ldots,a_n,x_1,\ldots,x_m)-F_{\mathrm{R}}(a_1,\ldots,a_n,x_1,\ldots,x_m))^2=0\end{aligned} \tag{2.18}$$

which does not represent the intersection of the sets represented by (2.10) and (2.11). In fact, even if some n-tuple $\langle a_1,\ldots,a_n\rangle$ belongs to both sets, the corresponding values of $x_1,\ldots,x_m$ need not be the same in (2.10) and (2.11).

To obtain an exponential Diophantine representation of the intersection, one needs to be more careful and *rename* the unknowns in one of the equations:

$$\begin{aligned}(E_{\mathrm{L}}(a_1,\ldots,a_n,x_1,\ldots,x_m)-E_{\mathrm{R}}(a_1,\ldots,a_n,x_1,\ldots,x_m))^2 +\\ (F_{\mathrm{L}}(a_1,\ldots,a_n,y_1,\ldots,y_m)-F_{\mathrm{R}}(a_1,\ldots,a_n,y_1,\ldots,y_m))^2=0.\end{aligned} \tag{2.19}$$

The complement of an exponential Diophantine set

The complement of an exponential Diophantine set need not be an exponential Diophantine set itself. This fact is non-trivial. The existence of a Diophantine set with a non-Diophantine complement was proved by Davis [8] who used corresponding logical tools to achieve this proof. His argument can be easily extended to show that this complement is not an exponential Diophantine set either.

2.3 More logical terminology

The whole of mathematics can be presented using sets as the basic foundation. However, it is more convenient to use also *properties*, *relations* and *functions*.

2.3.1 Exponential Diophantine properties

A property of natural numbers is said to be *exponential Diophantine* if the set of all numbers having this property is itself exponential Diophantine.

For example, the property "to be an odd number", denoted Odd(a), is exponential Diophantine because the set of all odd numbers is so:

$$a\in\{w : w \text{ is odd}\}\iff\exists x\{a=2x+1\}. \tag{2.20}$$

Instead of (2.20) one can write down an *exponential Diophantine representation* of the property Odd:

$$\mathrm{Odd}(a)\iff\exists x\{a=2x+1\}. \tag{2.21}$$

Once one has established that some property is Diophantine, it can be used in generalized exponential Diophantine representations.

2.3.2 Exponential Diophantine relations

Similar to properties, a relation among n natural numbers is called *exponential Diophantine* if the set of all n-tuples of natural numbers satisfying this relation is itself exponential Diophantine. For example, the relation "less" has an exponential Diophantine representation:

$$a < b \iff \exists x\{a + x + 1 = b\}. \tag{2.22}$$

Consequently, from now on, the sign $<$ (as well as $\leq$) can be used in generalized exponential Diophantine representations.

Other useful relations are that of divisibility and congruence having, respectively, the representations

$$a \mid b \iff \exists x\{ax = b\}, \tag{2.23}$$

$$a \equiv b \pmod{c} \iff \exists x\{(a-b)^2 = c^2 x\}. \tag{2.24}$$

2.3.3 Exponential Diophantine functions

Finally, a map from n-tuples of natural numbers into natural numbers is called an *exponential Diophantine function* if its graph is an exponential Diophantine set.

It is easy to see that the composition of exponential Diophantine functions is again an exponential Diophantine function. In fact, suppose that one has two exponential Diophantine functions (to simplify notation, consider both functions to have one argument only)

$$a = A(b) \iff \exists x_1 \ldots x_m\{E_L(a, b, x_1, \ldots, x_m) = E_R(a, b, x_1, \ldots, x_m)\}, \tag{2.25}$$

$$b = B(c) \iff \exists x_1 \ldots x_m\{F_L(b, c, x_1, \ldots, x_m) = F_R(b, c, x_1, \ldots, x_m)\}. \tag{2.26}$$

Then the composite function $a = A(B(c))$ is represented by the system

$$\begin{aligned} E_L(a, z, x_1, \ldots, x_m) &= E_R(a, z, x_1, \ldots, x_m), \\ F_L(z, c, y_1, \ldots, y_m) &= F_R(z, c, y_1, \ldots, y_m) \end{aligned} \tag{2.27}$$

(notice that the unknowns have been renamed!) which can be combined into a single exponential Diophantine equation with parameters a and c, and unknowns $x_1, \ldots, x_m, y_1, \ldots, y_m, z$.

2.4 Positional notation

The interplay between number theory and computability theory will be based on *positional notation*. For any positive *base* b, every natural number a has a unique representation of the form

$$a = \sum_{k=0}^{\infty} a_k b^k \tag{2.28}$$

with $0 \le a_k < b$ for $k = 0, 1, \ldots$ (of course, all but finitely many of the numbers $a_0, a_1, \ldots$ are zero). Thus one can look at every number as a string of *digits* $\ldots a_2 a_1 a_0$.

Let $\mathrm{Digit}(a, b, k)$ denote the k-th digit of number a in base-b notation, i.e., number a_k from (2.28). Observe that Digit is an exponential Diophantine function. In fact,

$$d = \mathrm{Digit}(a, b, k) \Longleftrightarrow \exists xy\{a = xb^{k+1} + db^k + y \;\&\; d < b \;\&\; y < b^k\}. \quad (2.29)$$

If the left-hand side is true, one can obtain values of x and y (justifying the right-hand side) by cutting base-b notation of a:

$$\underbrace{\ldots a_{k+1}}_{x}\, d\, \underbrace{a_{k-1} \ldots a_0}_{y}. \quad (2.30)$$

Similarly, if some numbers x and y satisfy the equality and two inequalities in the right-hand side of (2.29), then base-b notation of a can be obtained by gluing together base-b notations of x and y (the latter being padded by leading zeros to length k, if required) with digit d between them.

2.5 Binomial coefficients

Binomial coefficients play important roles in the investigation of Hilbert's tenth problem. First, one must ensure that there is an exponential Diophantine representation for them.

2.5.1 Binomial coefficients are Diophantine

Binomial coefficients form the well-known Pascal triangle

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
. & . & . & . & . & . & . & . & . & . & . & . & .
\end{array} \quad (2.31)$$

The traditional definition of binomial coefficients is based on the formal expansion

$$(u + 1)^a = C_{a,a}u^a + C_{a,a-1}u^{a-1} + \ldots + C_{a,0}. \quad (2.32)$$

The numbers $C_{a,b}$ are defined in a unique way by considering (2.32) as an *identity*, i.e., as an equality valid for all values of u. This definition is unsuitable because one cannot use universal quantifiers in exponential Diophantine representations. Luckily, it is sufficient to treat (2.32) as an *equation* having a solution with a large enough value of u. In fact, (2.32) shows that $C_{a,a}, \ldots, C_{a,0}$

are nothing else but the digits of the number $(u+1)^a$ in base-u notation provided that u is large enough, i.e., greater than each of these numbers. Here are examples with $u = 10$ (compare with (2.31)):

$$\begin{array}{rcr} 11^0 & = & 1 \\ 11^1 & = & 11 \\ 11^2 & = & 121 \\ 11^3 & = & 1331 \\ 11^4 & = & 14641 \\ 11^5 & = & 161051 \end{array} \tag{2.33}$$

The above observation immediately gives a generalized exponential Diophantine representation for binomial coefficients:

$$c = \binom{a}{b} \Longleftrightarrow \exists u\{u = 2^a + 1 \ \&\ c = \mathrm{Digit}((u+1)^b, u, b)\}. \tag{2.34}$$

Observe that the value $u = 2^a + 1$ is indeed sufficiently large because the sum of all the binomial coefficients in (2.32), i.e., its value for $u = 1$, is only 2^a.

Note that according to (2.34), $\binom{a}{b} = 0$ as soon as $a < b$.

2.5.2 Kummer's theorem

Being a positive natural number, the binomial coefficient $\binom{a+b}{b}$ can be represented in a unique way as the product of prime numbers:

$$\binom{a+b}{b} = 2^{\alpha_2(a,b)} 3^{\alpha_3(a,b)} 5^{\alpha_5(a,b)} \ldots \tag{2.35}$$

The nineteenth century German mathematician Ernst Kummer [24] found a surprising way to calculate $\alpha_p(a,b)$: *write a and b in base-p notation and add them; the number of carries from digit to digit performed during this addition is exactly $\alpha_p(a,b)$.*

Kummer's result was rediscovered by several researchers, including ones from twentieth century. To prove it, note that the identity

$$\left(\begin{array}{c} a+b \\ a \end{array} \right) = \frac{(a+b)!}{a!\,b!} \tag{2.36}$$

implies that

$$\alpha_p(a,b) = \beta_p(a+b) - \beta_p(a) - \beta_p(b), \tag{2.37}$$

where $\beta_p(k)$ stands for the exponent of p in the prime factorization of $k!$. It is not difficult to see that

$$\beta_p(k) = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \ldots, \tag{2.38}$$

because among the numbers $1, \ldots, k$, there are exactly $\lfloor \frac{k}{p} \rfloor$ numbers divisible by p, exactly $\lfloor \frac{k}{p^2} \rfloor$ numbers divisible by p^2, and so on. Thus,

$$\alpha_p(a,b) = \sum_{l \geq 1} \left(\left\lfloor \frac{a+b}{p^l} \right\rfloor - \left\lfloor \frac{a}{p^l} \right\rfloor - \left\lfloor \frac{b}{p^l} \right\rfloor \right). \tag{2.39}$$

Now it suffices to note that in this sum, the l-th summand is equal to either 1 or 0, depending on whether or not there is a carry from the $(l-1)$-th digit.

2.6 Digit-by-digit comparison of natural numbers

Kummer's theorem turned out to be a bridge between number theory and computer science: it connects divisibility properties of numbers with properties of their positional notations. For the purpose of this discussion, the most important format will be binary notation.

2.6.1 Binary orthogonality

Consider two natural numbers, a and b, written in base-2 notation:

$$a = \sum_{k=0}^{\infty} a_k 2^k, \qquad b = \sum_{k=0}^{\infty} b_k 2^k \tag{2.40}$$

where a_k and b_k are either 0 or 1. The numbers a and b are said to be *orthogonal*, written $a \perp b$, if $a_k b_k = 0$ for every k.

Kummer's theorem immediately gives a generalized exponential Diophantine representation of the relation of orthogonality:

$$a \perp b \Longleftrightarrow \mathrm{Odd}\left(\binom{a+b}{b} \right). \tag{2.41}$$

In fact, both the left-hand side and the right-hand side of this equivalence are true if and only if no carry occurs during the addition of $a+b$ in binary notation.

2.6.2 Binary masking

A number c with binary notation

$$c = \sum_{k=0}^{\infty} c_k 2^k \tag{2.42}$$

is said to *mask* number b with binary notation (2.40) if $b_k \leq c_k$ for every k. The masking relation will be denoted as $\preceq$.

Again, Kummer's theorem allows one to give a generalized exponential Diophantine representation of the masking relation:

$$b \prec c \Longleftrightarrow \mathrm{Odd}\left(\binom{c}{b}\right). \tag{2.43}$$

To see why (2.43) is true, note that both sides are false whenever $b > c$. Otherwise, put $a = c - b$. According to (2.41), the right-hand side of (2.43) means that $a \perp b$ so no carry occurs during the calculation of $c = a + b$ and hence b is masked by c.

2.6.3 Digit-by-digit multiplication

A number c with binary notation (2.42) is said to be the result of the *digit-by-digit multiplication* of numbers a and b with binary notations (2.40) if $c_k = a_k b_k$ for every k. The digit-by-digit product of numbers a and b will be denoted by $a \wedge b$.

It is easy to see that if $c = a \wedge b$ then

$$c \preceq a, \tag{2.44}$$

$$c \preceq b, \tag{2.45}$$

$$a - c \perp b - c. \tag{2.46}$$

These three conditions are not only necessary, but also sufficient for a number c to be the digit-by-digit product of a and b. In fact, (2.44) and (2.45) imply that $c_k \leq a_k b_k$ for every k. Suppose that there is k such that $c_k < a_k b_k$ and let k_0 be the smallest such k. Then numbers $a - c$ and $b - c$ are not orthogonal because their k_0-th digits are both "1".

Thus, one has a generalized exponential Diophantine representation of digit-by-digit multiplication:

$$c = a \wedge b \Longleftrightarrow c \preceq a \;\&\; c \preceq b \;\&\; a - c \perp b - c. \tag{2.47}$$

Chapter 3

Exponentiation is Diophantine

In this chapter, I will show that exponentiation is a Diophantine function; i.e., it has a Diophantine representation

$$p = q^r \iff \exists x_1 \ldots x_m \{P(p, q, r, x_1, \ldots, x_m) = 0\} \tag{3.1}$$

for a suitable choice of polynomial P. As indicated in Chapter One, equivalence (3.1) allows the transformation of exponential Diophantine representations of sets, properties, relations and functions into corresponding genuine Diophantine representations.

3.1 Special second-order recurrent sequences

In the proof, the second-order recurrence sequences

$$\alpha_b(0) = 0, \qquad \alpha_b(1) = 1, \qquad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n), \tag{3.2}$$

where $b \geq 2$, play an essential rule.

It is easy to prove by induction that every such sequence is monotonically increasing, namely

$$0 = \alpha_b(0) < \alpha_b(1) < \ldots < \alpha_b(n) < \alpha_b(n+1) < \ldots \tag{3.3}$$

and hence

$$n \leq \alpha(n). \tag{3.4}$$

Moreover, for $b = 2$ the sequence is linear, namely,

$$\alpha_2(n) = n, \tag{3.5}$$

while for $b > 2$ it grows exponentially, namely,

$$(b-1)^n \leq \alpha_b(n+1) \leq b^n. \tag{3.6}$$

3.2 First-order relation

All the required properties of numbers $\alpha_b(n)$ can be proved by induction. However, many of them can be made more "visual" by using matrices and other traditional algebraic tools. To this end, the second-order relation (3.2) can be rewritten as a first-order relation among the matrices

$$A_b(n) = \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix}, \tag{3.7}$$

taking $\alpha_b(-1) = -1$. Namely,

$$A_b(0) = E, \qquad A_b(n+1) = A_b(n)B_b, \tag{3.8}$$

where

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad B_b = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}. \tag{3.9}$$

This implies that

$$A_b(n) = B_b^n. \tag{3.10}$$

3.3 Characteristic equation

Definitions (3.9) together with (3.10) imply that

$$\det(A_b(n)) = 1, \tag{3.11}$$

i.e.,

$$\begin{aligned} \alpha_b^2(n) - \alpha_b(n+1)\alpha_b(n-1) &= \\ \alpha_b^2(n+1) - b\alpha_b(n+1)\alpha_b(n) + \alpha_b^2(n) &= \qquad (3.12) \\ \alpha_b^2(n-1) - b\alpha_b(n-1)\alpha_b(n) + \alpha_b^2(n) &= 1. \qquad (3.13) \end{aligned}$$

Let us show that the converse is also true: *if*

$$x^2 - bxy + y^2 = 1, \tag{3.14}$$

then either

$$x = \alpha_b(m+1), \qquad y = \alpha_b(m) \tag{3.15}$$

or

$$x = \alpha_b(m), \qquad y = \alpha_b(m+1) \tag{3.16}$$

for some m. To distinguish between the two alternatives (3.15) and (3.16), it is sufficient to compare x and y by size, namely, to show that *equation (3.14) together with the inequality*

$$y < x \tag{3.17}$$

implies the existence of some m *for which (3.15) holds.*

This proof will proceed by induction on y.
If $y = 0$, then clearly $x = 1$; i.e., (3.15) holds with $m = 0$.
If $y > 0$, then (3.14) and (3.17) imply that

$$by - x = \frac{y^2 - 1}{x} \geq 0, \tag{3.18}$$

$$by - x = \frac{y^2 - 1}{x} < \frac{y^2}{x} < y. \tag{3.19}$$

Let $x_1 = y$ and $y_1 = by - x$. Then

$$\begin{aligned} x_1^2 - bx_1y_1 + y_1^2 &= y^2 - by(by - x) + (by - x)^2 \\ &= x^2 - bxy + y^2 \\ &= 1. \end{aligned} \tag{3.20}$$

By (3.19), $y_1 < x_1$, and by the induction hypothesis,

$$x_1 = \alpha_b(m_1 + 1), \qquad y_1 = \alpha_b(m_1) \tag{3.21}$$

for some m_1. Hence, for $m = m_1 + 1$,

$$x = bx_1 - y_1 = \alpha_b(m + 1), \qquad y = x_1 = \alpha_b(m). \tag{3.22}$$

3.4 Divisibility properties

Let us show that for positive k

$$\alpha_b(k) \mid \alpha_b(m) \Longleftrightarrow k \mid m. \tag{3.23}$$

Recall that $\alpha_b(k)$ and $\alpha_b(m)$ are elements of the matrices $A_b(k)$ and $A_b(m)$ defined by (3.7) and satisfying (3.10). Let

$$m = n + kl, \qquad 0 \leq n < k. \tag{3.24}$$

We have:

$$\begin{aligned} A_b(m) &= B_b^m \\ &= B_b^{n+kl} \\ &= B_b^n (B_b^k)^l \\ &= A_b(n) A_b^l(k) \\ &= \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \begin{pmatrix} \alpha_b(k+1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^l. \end{aligned}$$

Passing to a congruence modulo $\alpha_b(k)$, we obtain

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \equiv$$

$$\begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \begin{pmatrix} \alpha_b(k+1) & 0 \\ 0 & -\alpha_b(k-1) \end{pmatrix}^l \pmod{\alpha_b(k)},$$

and, hence,

$$\alpha_b(m) \equiv \alpha_b(n)\alpha_b^l(k+1) \pmod{\alpha_b(k)}. \tag{3.25}$$

Now, if $k \mid m$, then $n = 0$, $\alpha_b(n) = 0$ and (3.25) implies the left-hand side of (3.23). Conversely, if the left-hand side of (3.23) is true, then (3.25) implies that

$$\alpha_b(k) \mid \alpha_b(n)\alpha_b^l(k+1). \tag{3.26}$$

But by (3.12), $\alpha_b(k)$ and $\alpha_b(k+1)$ are coprime, hence

$$\alpha_b(k) \mid \alpha_b(n). \tag{3.27}$$

Now it follows from (3.24) and (3.3) that $\alpha_b(n) < \alpha_b(k)$, so (3.27) is possible only if $n = 0$, i.e., if $m = kl$; hence, the left-hand side of (3.23) is true.

3.5 Divisibility properties (continued)

Let us show that for positive k

$$\alpha_b^2(k) \mid \alpha_b(m) \iff k\alpha_b(k) \mid m. \tag{3.28}$$

¿From the previous section we know that both sides of (3.28) are false unless $m = kl$ for some l. In the latter case we have:

$$\begin{aligned} A_b(m) &= B_b^{kl} \\ &= A_b^l(k) \\ &= [\alpha_b(k)B_b - \alpha_b(k-1)E]^l \\ &= \sum_{i=0}^{l}(-1)^{l-i}\left(\begin{array}{c} l \\ i \end{array}\right)\alpha_b^i(k)\alpha_b^{l-i}(k-1)B_b^i. \end{aligned} \tag{3.29}$$

Passing from the equality to a congruence modulo $\alpha_b^2(k)$, we can omit all the summands except the first two:

$$\begin{aligned} A_b(m) &= \left(\begin{array}{cc} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{array}\right) \\ &\equiv (-1)^l\alpha_b^l(k-1)E + (-1)^{l-1}l\alpha_b(k)\alpha_b^{l-1}(k-1)B_b \pmod{\alpha_b^2(k)}, \end{aligned}$$

whence

$$\alpha_b(m) \equiv (-1)^{l-1}l\alpha_b(k)\alpha_b^{l-1}(k-1) \pmod{\alpha_b^2(k)}. \tag{3.30}$$

Now if the right-hand side in (3.28) is true, then $\alpha_b(k) \mid l$, which, together with (3.30), implies the left-hand side in (3.28). Conversely, if the left-hand side of (3.28) is true, then (3.30) implies that

$$\alpha_b(k) \mid l\alpha_b^{l-1}(k-1). \tag{3.31}$$

But by (3.13), $\alpha_b(k)$ and $\alpha_b(k-1)$ are coprime; hence,

$$\alpha_b(k) \mid l \tag{3.32}$$

and the right-hand side of (3.28) is true.

3.6 Congruence properties

It follows by induction from the definition (3.2) that

$$b_1 \equiv b_2 \pmod{q} \implies \alpha_{b_1}(n) \equiv \alpha_{b_2}(n) \pmod{q}. \tag{3.33}$$

Hence, according to (3.5)

$$\alpha_b(n) \equiv \alpha_2(n) = n \pmod{b-2}. \tag{3.34}$$

Let us check that if

$$n = 2lm \pm j, \tag{3.35}$$

then

$$\alpha_b(n) \equiv \pm\alpha_b(j) \pmod{v} \tag{3.36}$$

where

$$v = \alpha_b(m+1) - \alpha_b(m-1) \tag{3.37}$$

and the choice of "+" or "−" for the sign in (3.36) need not coincide with the choice of the sign in (3.35).

Using the matrix representation once again, we have:

$$\begin{aligned}
A_b(n) &= B_b^n \\
&= B_b^{2lm\pm j} \\
&= \left[[B_b^m]^2\right]^l B_b^{\pm j} \\
&= \left[[A_b^2(m)]\right]^l [A_b(j)]^{\pm 1}, \\
A_b(m) &= \begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \\
&\equiv -\begin{pmatrix} -\alpha_b(m-1) & \alpha_b(m) \\ -\alpha_b(m) & \alpha_b(m+1) \end{pmatrix} \pmod{v}.
\end{aligned}$$

The latter matrix is nothing else but $A_b^{-1}(m)$; hence,

$$A_b^2(m) \equiv -E \pmod{v}, \tag{3.38}$$

$$A_b(n) \equiv \pm[A_b(j)]^{\pm 1} \pmod{v}. \tag{3.39}$$

In this last formula, all four combinations of the signs "+" and "−" are possible. Passing from the matrix congruence (3.39) to element-wise congruence, we get (3.36)

3.7 Diophantine definition of sequence α

We are now ready to show that the relation between the three numbers, a, b, and c, expressed by the formula

$$3 < b \;\&\; a = \alpha_b(c), \tag{3.40}$$

is Diophantine. Namely, we are to check that (3.40) holds if and only if the following system of conditions can be satisfied:

$$3 < b, \tag{3.41}$$
$$u^2 - but + t^2 = 1, \tag{3.42}$$
$$s^2 - bsr + r^2 = 1, \tag{3.43}$$
$$r < s, \tag{3.44}$$
$$u^2 \mid s, \tag{3.45}$$
$$v = bs - 2r, \tag{3.46}$$
$$w \equiv b \pmod{v}, \tag{3.47}$$
$$w \equiv 2 \pmod{u}, \tag{3.48}$$
$$2 < w, \tag{3.49}$$
$$x^2 - wxy + y^2 = 1, \tag{3.50}$$
$$2a < u, \tag{3.51}$$
$$2a < v, \tag{3.52}$$
$$a \equiv x \pmod{v}, \tag{3.53}$$
$$2c < u, \tag{3.54}$$
$$c \equiv x \pmod{u}. \tag{3.55}$$

Representations (2.22), (2.23) and (2.24) for relations "$<$", "$\mid$" and "$\equiv$" are in fact Diophantine so the system (3.41)–(3.55) can be regarded as a (generalized) Diophantine representation of relation (3.40).

3.7.1 The sufficiency

It was shown in Section 3.3 that (3.41) and (3.42) imply that for some k,

$$u = \alpha_b(k). \tag{3.56}$$

Likewise, (3.41), (3.43), and (3.44) imply that for some positive m,

$$s = \alpha_b(m), \qquad r = \alpha_b(m-1) \tag{3.57}$$

and (3.49) and (3.50) imply that for some n,

$$x = \alpha_w(n). \tag{3.58}$$

Let $n = 2lm + j$ or $n = 2lm - j$ with some j such that

$$j \leq m. \tag{3.59}$$

By (3.28), it follows from (3.45), (3.56), and (3.57) that

$$u \mid m. \tag{3.60}$$

By (3.2), it follows from (3.46) and (3.57) that

$$v = \alpha_b(m+1) - \alpha_b(m-1). \tag{3.61}$$

¿From (3.53), (3.58), (3.47) (3.33) and (3.36) we have that

$$a \equiv x \equiv \alpha_b(w) \equiv \alpha_b(n) \equiv \pm\alpha_b(j) \pmod{v}. \tag{3.62}$$

¿From (3.59), (3.3), (3.41), (3.2) and (3.61) we have that

$$2\alpha_b(j) \leq 2\alpha_b(m) \leq (b-2)\alpha_b(m) < b\alpha_b(m) - 2\alpha_b(m-1) = v, \tag{3.63}$$

which together with (3.52) makes (3.62) possible only if

$$a = \alpha_b(j). \tag{3.64}$$

¿From (3.55), (3.34) and (3.48) we have that

$$c \equiv x \equiv \alpha_w(n) \equiv n \pmod{u}. \tag{3.65}$$

¿From (3.4), (3.64) and (3.52) we have that

$$2j \leq 2\alpha_b(j) = 2a < u, \tag{3.66}$$

which together with (3.54) makes (3.65) possible only if

$$c = j. \tag{3.67}$$

Finally, (3.64) and (3.67) imply the second conjunctive term in (3.40) while the first term trivially follows from (3.41).

3.7.2 The necessity

Now we are going to prove that if the numbers a, b, and c satisfy (3.40), then there are numbers s, r, u, t, v, w satisfying (3.42)–(3.55). The above considerations indicate how these numbers are to be chosen.

Condition (3.41) is evidently fulfilled.

We choose u according to (3.56), selecting some positive number k so that the inequalities (3.51) and (3.54) hold and u is odd (we are able to do this thanks to (3.4) and the fact, implied by (3.13), that at least one of any two consecutive terms of the sequence $\alpha_b(n)$ is odd). Let

$$t = \alpha_b(k+1), \tag{3.68}$$

then by (3.13), equation (3.42) holds.

We choose r and s as in (3.57), with

$$m = uk, \tag{3.69}$$

then by (3.13) and (3.3), equation (3.43) and inequality (3.44) both hold. By (3.28), condition (3.45) is also valid.

We can find v satisfying (3.46) and (3.51) because, according to (3.57), (3.2), (3.40), (3.3), (3.4) and (3.51)

$$\begin{aligned} bs - 2r &= \alpha_b(m+1) - \alpha_b(m-1) && (3.70)\\ &= b\alpha_b(m) - 2\alpha_b(m-1) && (3.71)\\ &\geq 4\alpha_b(m) - 2\alpha_b(m-1) && (3.72)\\ &> 2\alpha_b(m) && (3.73)\\ &\geq 2m && (3.74)\\ &\geq 2u && (3.75)\\ &> 2a. && (3.76) \end{aligned}$$

We now verify that u and v are coprime. Suppose that $d \mid u$ and $d \mid v$; then by (3.45), $d \mid s$ and by (3.46), $d \mid 2r$. However, by our choice of u, d is odd; hence, $d \mid r$ and by (3.43) $d \mid 1$. Thus, by the Chinese Remainder Theorem, we can find w satisfying (3.47), (3.48), and (3.49).

Finally, let

$$x = \alpha_w(c), \qquad y = \alpha_w(c+1), \tag{3.77}$$

then by (3.3) equation (3.50) holds.

According to (3.33), it follows from the choice of x, (3.77), and (3.47) that

$$x = \alpha_w(c) \equiv \alpha_b(c) = a \pmod{v} \tag{3.78}$$

so (3.53) is true.

By (3.8) it follows from (3.77) that

$$x \equiv c \pmod{w-2}, \tag{3.79}$$

which, together with (3.48), implies (3.55).

3.8 Exponentiation is Diophantine

Having found a Diophantine representation for the sequence α, we are ready to construct a generalized Diophantine representation for exponentiation.

An eigenvalue λ of the matrix B_b satisfies the equation

$$\lambda^2 - b\lambda - 1 = 0. \tag{3.80}$$

We will select a modulus m such that

$$\lambda \equiv q \pmod{m}. \tag{3.81}$$

According to (3.80), we should have

$$q^2 - bq + 1 \equiv 0 \pmod{m} \tag{3.82}$$

so we simply choose

$$m = bq - q^2 - 1. \tag{3.83}$$

Now we can easily find (modulo m) the corresponding eigenvector:

$$B_b \begin{pmatrix} q \\ 1 \end{pmatrix} = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q \\ 1 \end{pmatrix} \equiv q \begin{pmatrix} q \\ 1 \end{pmatrix} \pmod{m}. \tag{3.84}$$

Consequently, we obtain

$$\begin{aligned} \begin{pmatrix} \alpha_b(r+1) & -\alpha_b(r) \\ \alpha_b(r) & -\alpha_b(r-1) \end{pmatrix} \begin{pmatrix} q \\ 1 \end{pmatrix} &= A_b(r) \begin{pmatrix} q \\ 1 \end{pmatrix} \\ &= B_b^r \begin{pmatrix} q \\ 1 \end{pmatrix} \\ &\equiv q^r \begin{pmatrix} q \\ 1 \end{pmatrix} \pmod{m} \end{aligned} \tag{3.85}$$

and hence

$$q\alpha_b(r) - \alpha_b(r-1) \equiv q^r \pmod{m}. \tag{3.86}$$

As soon as

$$q^r < m, \tag{3.87}$$

we can write

$$p = q^r \iff p < m \;\&\; q\alpha_b(r) - \alpha_b(r-1) \equiv p \pmod{m}. \tag{3.88}$$

We can easily guarantee (3.87) by selecting, according to (3.6),

$$b = \alpha_{q+4}(r+1) + q^2 + 2 \tag{3.89}$$

provided that $q > 0$. The exceptional case $q = 0$ can be easily treated separately and finally we get the following generalized Diophantine representation:

$$\begin{aligned} p = q^r \iff\; & (q = 0 \;\&\; r = 0 \;\&\; p = 1) \vee \\ & (q = 0 \;\&\; 0 < r \;\&\; p = 0) \vee \\ & (\exists b, m \quad \{b = \alpha_{q+4}(r+1) + q^2 + 2 \;\& \\ & \qquad m = bq - q^2 - 1 \;\& \\ & \qquad p < m \;\& \\ & \qquad p \equiv q\alpha_b(r) - (b\alpha_b(r) - \alpha_b(r+1)) \pmod{m}\}). \end{aligned}$$

Chapter 4

Simulation of register machines by equations

In this chapter, I will show that the work of an abstract computer can be simulated by equations— exponential Diophantine equations as described in Chapter Two or genuine Diophantine equations as described in Chapters Two and Three.

4.1 Another definition of listable sets

Listable, or effectively enumerable sets can be defined via abstract computing devices in several formally different yet equivalent ways. In Chapter One, they were defined as sets whose elements can be printed by some abstract computer having no input data but working indefinitely long. In this chapter, it will be more convenient to define listable sets as sets *recognized* or *accepted* by some abstract computer. Such a computer, having received some n-tuple $\langle a_1, \ldots, a_n \rangle$ as input, would stop after finitely many steps when the n-tuple belongs to the considered listable set $\mathfrak{M}$, and never stop otherwise.

Clearly, the new definition of listable sets is at least as broad as the previous one: if one had a computer (without input) printing all elements of the set, it could transformed into a computer (with input) which, instead of printing elements of the set, would compare them with the input value and stop as soon as the equality happened[1].

[1] In fact, the definition of a listable set as the set accepted by some computer is equivalent to the definition as a set whose elements are printed by some computer, but the converse transformation is technically more involved. Suppose there is a computer that accepts some listable set $\mathfrak{M}$, i.e., it stops if and only if the input value belongs to the set. One can imagine infinitely many copies of this computer working on all possible inputs in parallel. As soon as one of these computers stops, a supervisor computer prints the input value of the computer that halted.

This is not a correct description of a computer printing all values of the set because one assumes that infinitely many computers work in parallel. Instead of this, a supervisor computer

To simplify notation, we shall deal with sets of natural numbers; the generalization to sets of higher dimensions is straightforward.

4.2 Register machines

To be able to work with recognizable sets we need to select the "construction" of computers used. For a theoretical treatment, it is better to deal with as primitive computers as possible. A classical example here are the Turing machines. Their operation was simulated by exponential Diophantine equations in [30], with an improved version in [34]. Here, we will simulate so-called *register machines*, which were used for constructing exponential Diophantine representations for the first time in a joint work with J. P. Jones [19] and then in [20, 21] and [33]. Construction presented here is a further simplification.

Register machines are more suitable than Turing machines for simulation by exponential Diophantine equations because they work with numbers. Namely, a register machine has a finite number of *registers* R1, ..., Rn each of which is capable of containing an arbitrarily large natural number. The machine performs a *program* consisting of finitely many *instructions* labeled by S1, ..., Sm. When the machine is to perform an instruction labeled Sk, one also says that the machine is in the *state* Sk.

Instructions can be of three types

I. Sk: Rl + +;Si

II. Sk: Rl − −; Si;Sj

III. Sk: STOP

An instruction of type I means that when in state Sk, the machine is to increase register Rl by 1 and pass to state Si.

An instruction of type II means that when in state Sk, the machine is to decrease register Rl by 1 and pass to state Si; however, if register Rl already contains 0, its value does not change and the machine goes to state Sj rather then to state Si.

An instruction of type III stops calculations; without loss of generality, one assumes that the machine can stop only in state Sm.

Register machines were introduced almost simultaneously by several authors: [25], [36], [37, 38] and [49]. In spite of their very primitive instructions, register machines are in principle as powerful as all other standard abstract computing devices, including Turing machines.

---

should generate copies of accepting computers one by one and launch them with different initial values. So at each moment of time, one would have only finitely many copies of the accepting computer. Generation and concurrent running of several copies of the same computer can be performed by a single program

4.3 The protocol

The operation of a register machine is a dynamic process while solutions of an equation are static. In order to pass from the former to the latter, one uses a *protocol* to describe the operation of the machine. A protocol is a rectangular table similar to those used in spreadsheets. There will be m rows corresponding to the states of the machine, and n rows corresponding to the registers. The columns will correspond to the (discrete) time. For reasons that will become clear later, we will number the columns from right to left.

	q	...	$t+1$	t	...	0	
S1	$s_{1,q}$	...	$s_{1,t+1}$	$s_{1,t}$	...	$s_{1,0}$	s_1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
Sk	$s_{k,q}$	...	$s_{k,t+1}$	$s_{k,t}$	...	$s_{k,0}$	s_k
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
Sm	$s_{m,q}$	...	$s_{m,t+1}$	$s_{m,t}$	...	$s_{m,0}$	s_m
R1	$r_{1,q}$	...	$r_{1,t+1}$	$r_{1,t}$	...	$r_{1,0}$	r_1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
Rl	$r_{l,q}$	...	$r_{l,t+1}$	$r_{l,t}$	...	$r_{l,0}$	r_l
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
Rn	$r_{n,q}$	...	$r_{n,t+1}$	$r_{n,t}$	...	$r_{n,0}$	r_n
Z1	$z_{1,q}$	...	$z_{1,t+1}$	$z_{1,t}$	...	$z_{1,0}$	z_1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
Zl	$z_{l,q}$	...	$z_{l,t+1}$	$z_{l,t}$	...	$z_{l,0}$	z_l
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
Zn	$z_{n,q}$	...	$z_{n,t+1}$	$z_{n,t}$	...	$z_{n,0}$	z_n
	2^c-1	...	2^c-1	2^c-1	...	2^c-1	d
	1	...	1	1	...	1	e
	2^c	...	2^c	2^c	...	2^c	f

The values in the rows corresponding to the states will indicate the current state of the machine: $s_{k,t}=1$ or $s_{k,t}=0$ depending on whether or not on step t the machine is in state Sk. Consequently, the numbers in the rows corresponding to the registers will contain their current values.

4.3.1 Zero indicators

The rows introduced above are sufficient for describing the operation of a register machine. However, in order to simplify its simulation by equation, we introduce n auxiliary rows Z1,...,Zn.

The values in the new cells will indicate whether the values in corresponding R-rows are zeros or not:

$$z_{l,t}=\begin{cases}0, & \text{if } r_{l,t}=0\\ 1, & \text{otherwise.}\end{cases} \tag{4.1}$$

4.3.2 The initial values

Without loss of generality, assume that the machine always starts in state S1 so

$$s_{1,0} = 1, \tag{4.2}$$

$$s_{2,0} = \ldots = s_{m,0} = 0. \tag{4.3}$$

Similarly, assume that the only input data a is placed in register R1, all other registers being empty:

$$r_{1,0} = a, \tag{4.4}$$

$$r_{2,0} = \ldots = r_{n,0} = 0. \tag{4.5}$$

4.3.3 One-step relations

As soon as the values in the t-th column are known, one can fill in the $(t+1)$-st column (unless $s_{m,t} = 1$, in which case the machine stopped).

Register relations

It is easy to see that

$$r_{l,t+1} = r_{l,t} + \sum\nolimits^{+} s_{k,t} - \sum\nolimits^{-} z_{l,t} s_{k,t} \tag{4.6}$$

where Σ^+ summation is over all instructions of the form

$$\mathrm{S}k: \ \mathrm{R}l{+}{+}; \mathrm{S}i$$

and Σ^- summation is over all instructions of the form

$$\mathrm{S}k: \ \mathrm{R}l{-}{-}; \mathrm{S}i; \mathrm{S}j.$$

State relations

Similar to (4.6),

$$s_{d,t+1} = \sum\nolimits^{0} s_{k,t} + \sum\nolimits^{+} z_{l,t} s_{k,t} + \sum\nolimits^{-} (1 - z_{l,t}) s_{k,t} \tag{4.7}$$

where Σ^0 summation is over all instructions of the form

$$\mathrm{S}k: \ \mathrm{R}l{+}{+}; \mathrm{S}d,$$

Σ^+ summation is over all instructions of the form

$$\mathrm{S}k: \ \mathrm{R}l{-}{-}; \mathrm{S}d; \mathrm{S}j,$$

and Σ^- summation is over all instructions of the form

$$\mathrm{S}k: \ \mathrm{R}l{-}{-}; \mathrm{S}i; \mathrm{S}d.$$

4.3.4 Final values

If the input value a belongs to the listable set recognized by this computer, then the computer must halt after some number, say q, of steps so

$$s_{m,q} = 1, \tag{4.8}$$

$$s_{1,q} = \ldots = s_{m-1,q} = 0. \tag{4.9}$$

Without loss of generality, assume that the machine is programmed in such a way that before halting it empties all its registers so

$$r_{1,q} = \ldots = r_{n,q} = 0. \tag{4.10}$$

4.4 Positional coding of the protocol

On input a, if the machine stops after q steps, then one can find numbers $s_{k,t}$, $r_{k,t}$ and $z_{k,t}$ satisfying conditions (4.1)–(4.10). The converse is also true: if for some q, one finds numbers $s_{k,t}$, $r_{k,t}$ and $z_{k,t}$ satisfying conditions (4.1)–(4.8), then the machine stops after q steps. All conditions (4.1)–(4.8) are either Diophantine or can be easily expressed in such a way. The "only" difficulty is that the number of variables and the number of conditions are indeterminate; they depend not only on the program of the machine, but also on the number of steps, q, before the machine stopped.

To overcome this difficulty, we can combine the content of all the cells in a given row into a single number. To this end, we select a number b which should be greater then every $s_{k,t}$, $r_{l,t}$ and $z_{l,t}$. This b will serve as the base for the positional number system, and $s_{k,t}, r_{l,t}$ and $z_{l,t}$ will be digits of the corresponding numbers s_k, r_l and z_l. Formally, define

$$s_k = \sum_{t=0}^{q} s_{k,t} b^t, \tag{4.11}$$

$$r_l = \sum_{t=0}^{q} r_{l,t} b^t, \tag{4.12}$$

$$z_l = \sum_{t=0}^{q} z_{l,t} b^t. \tag{4.13}$$

For technical reasons, we select b to be a positive power of 2:

$$b = 2^{c+1}. \tag{4.14}$$

Definitions (4.11)–(4.14) mean that the binary notation of s_k, r_l and z_l can be obtained as follows—write numbers $s_{k,t}$, $r_{l,t}$ and $z_{l,t}$ in binary notation padded by leading zeros to the length $c+1$, "remove" cell boundaries and, thus, obtain the binary notation for s_k, r_l or z_l. (That was the reason for numbering steps in the protocol from right to left).

Our goal is to rewrite conditions (4.1)–(4.8) in terms of numbers $s_1, \ldots, s_m$, $r_1, \ldots, r_n$ and $z_1, \ldots, z_n$.

4.4.1 Zero indicator relations

To be able to rewrite definition (4.1) in terms of $r_1, \ldots, r_n$ and $z_1, \ldots, z_n$, we will select b even larger than is necessary for the unique decomposition of $s_1, \ldots, s_m$, $r_1, \ldots, r_n$, $z_1, \ldots, z_n$ into the cell contents. Namely, we will suppose that already $b/2 = 2^c$ is larger then every element of the protocol. In other words, the biggest allowed value of cell contents will be $2^c - 1$.

The binary notation of this number, $2^c - 1$, consists of a single block of '1's of length c. This implies that the inequality

$$x \leq 2^c - 1$$

is equivalent to the masking condition

$$x \preceq 2^c - 1.$$

Consequently, we can write

$$r_l \preceq d, \qquad l = 1, \ldots, n, \tag{4.15}$$

where

$$d = \sum_{t=0}^{q} (2^c - 1) b^t \tag{4.16}$$

is the number all b-base digits of which are equal to $2^c - 1$.

Numbers $z_{l,t}$ are either 0 or 1, so the z_l satisfy conditions

$$z_l \preceq e, \qquad l = 1, \ldots, n \tag{4.17}$$

analogous to (4.15) with e defined by

$$e = \sum_{t=0}^{q} b^t. \tag{4.18}$$

Now one can easily express condition (4.1). Consider number

$$r_{l,t} + 2^c - 1.$$

If $r_{l,t} = 0$, then the binary notation of this number, padded to the length $c + 1$, is

$$\mathtt{01\ldots1}.$$

On the other hand, if $r_{l,t} > 0$, then its binary notation looks like

$$\mathtt{1{*}\ldots{*}}$$

where the asterisks replace unknown binary digits. In other words, the leading $(c + 1)$-th digit of $r_{l,t} + 2^c - 1$ is always equal to $z_{l,t}$ and hence

$$2^c z_{l,t} = (r_{l,t} + 2^c - 1) \wedge 2^c. \tag{4.19}$$

Consequently, definition (4.1) can be rewritten as

$$2^c z_l = (r_l + d) \wedge f \tag{4.20}$$

where

$$f = \sum_{t=0}^{q} 2^c b^t. \tag{4.21}$$

4.4.2 Multiple-step relations

Register relations

One can replace ordinary multiplication in (4.6) by digit-by-digit multiplication $z_{l,t} \wedge s_{k,t}$. Multiplying both parts by b^{t+1} and summing up for t from 0 to $q-1$, one obtains an analogue of (4.6):

$$r_l = br_l + b\sum\nolimits^{+} s_k - b\sum\nolimits^{-} (z_l \wedge s_k) \tag{4.22}$$

for $l = 2, \ldots, n$; according to (4.4), for $l = 1$, it should be slightly different, namely,

$$r_1 = a + br_1 + b\sum\nolimits^{+} s_k - b\sum\nolimits^{-} (z_l \wedge s_k). \tag{4.23}$$

State relations

Similar to (4.22), for $d = 2, \ldots, m$ condition (4.7) can be rewritten as

$$s_d = b\sum\nolimits^{0} s_k + b\sum\nolimits^{+} (z_l \wedge s_k) + b\sum\nolimits^{-} ((e - z_l) \wedge s_k) \tag{4.24}$$

while for $d = 1$, one needs to increase the right-hand side by 1 according to (4.2):

$$s_1 = 1 + b\sum\nolimits^{0} s_k + b\sum\nolimits^{+} (z_l \wedge s_k) + b\sum\nolimits^{-} ((e - z_l) \wedge s_k). \tag{4.25}$$

4.4.3 The initial values

The initial values in equation (4.3) are implied by (4.24) because the right-hand side is divisible by b; similarly, initial values in equation (4.5) are implied by (4.22).

Of course, (4.25) implies the initial values (4.2). To be sure that (4.23) implies the initial value in equation (4.4), we impose the condition

$$a < 2^c. \tag{4.26}$$

4.4.4 The final values

The halting condition (4.8) can be written as

$$s_m = b^q. \tag{4.27}$$

It is not necessary to consider the final conditions (4.9) and (4.10).

4.5 From the codes to cell contents

We have seen that on input a, if the machine stops after q steps, then one can find numbers b, c, d, e, f, $r_1, \ldots, r_n$, $s_1, \ldots, s_m$, $z_1, \ldots, z_m$ satisfying conditions (4.14)–(4.27). The converse is also true: if some numbers a, b, c, d, e, f, q, $r_1, \ldots, r_n$, $s_1, \ldots, s_m$, $z_1, \ldots, z_m$ satisfy conditions (4.14)–(4.27), then on input a the machine stops after q steps.

To prove this, we first define numbers $r_{l,t}$, $s_{k,t}$, $z_{l,t}$ by splitting the binary notations of r_l, s_k and z_l respectively into blocks of length $c+1$. Formally, set

$$r_{l,t} = \mathrm{Digit}(r_l, b, t), \tag{4.28}$$

$$s_{k,t} = \mathrm{Digit}(s_k, b, t), \tag{4.29}$$

$$z_{l,t} = \mathrm{Digit}(z_l, b, t) \tag{4.30}$$

We need to check only that conditions (4.14)–(4.27) imply conditions (4.1)–(4.8). This is evident in the case of conditions (4.1)–(4.5) and (4.8).

For conditions (4.6) and (4.7), it is very important that during summations there is no carry "across the boundary of a cell" in the protocol.

It can be shown by induction that for every t, among the numbers $s_{1,t}$, ..., $s_{m,t}$ one and only one is equal to 1, others being equal to 0. This is so for $t = 0$ thanks to (4.24) and (4.25). If this is so for some t, then the same holds for $t+1$. This is so because in the right-hand side of (4.7), all summands but 1 should be equal to 0, the remaining summand being equal to 1; hence, no carry at all occurs in summations (4.24)–(4.25) and relation (4.7) holds.

Similarly, in (4.6), besides the first summand, there can be at most one other summand different from 0. By (4.15), the first summand is at most $2^c - 1$, and the other non-zero summand can be equal only to 1. This implies that no carry "across the boundary of a cell" ever occurs and, hence, relation (4.6) also holds.

4.6 All listable sets are Diophantine

Now, we can easily obtain a Diophantine representation for the listable set $\mathfrak{M}$ accepted by our register machine.

In fact, in (4.16), (4.18) and (4.21), we simply sum up geometrical progressions so these conditions can be rewritten as

$$(b-1)d = (2^c - 1)(b^{q+1} - 1), \tag{4.31}$$

$$(b-1)e = b^{q+1} - 1, \tag{4.32}$$

$$(b-1)f = 2^c(b^{q+1} - 1). \tag{4.33}$$

It was shown in Chapter Two that the relations of masking and digit-by-digit multiplication are exponential Diophantine so conditions (4.15), (4.17), (4.19)–(4.25) can be rewritten as generalized exponential Diophantine equations. Condition (4.26) is also generalized exponential Diophantine.

Conditions (4.14) and (4.27) are exponential Diophantine equations by themselves. Now it remains to apply equivalence (3.1) for transforming exponential Diophantine equations into genuine Diophantine equations.

Chapter 5

Undecidable problems for continuous variables

The undecidability of Hilbert's tenth problem turned out to be a powerful tool for establishing the undecidability of many other decision problems. In spite of the fact that Hilbert's tenth problem deals with integer-valued variables, it has many ramifications for problems dealing with continuous variables. In this chapter, Greek letters will be used for real variables and functions while lower case Latin letters will be used either for integers or for natural numbers depending on the context.

The presentation in this chapter is based on [2, 7, 14, 44, 53]. More undecidability results for continuous variables based on the undecidability of Hilbert's tenth problem can be found in [15, 39, 40, 48, 50].

5.1 Tarski's theorem

It is natural to begin with the direct counterpart of Hilbert's tenth problem for real unknowns: i.e., by considering equations of the form

$$P(\chi_1, \ldots, \chi_m) = 0, \tag{5.1}$$

where P is a polynomial with integer coefficients and $\chi_1, \ldots, \chi_m$ are real unknowns. In contrast to the case of Diophantine equations, it is possible to determine whether (5.1) has a real solution or not. For $m = 1$, this can be done by the well-known *Sturm method*; a far-reaching generalization of this method found by Alfred Tarski [52] enables one to work with any number of unknowns.

5.2 Main alternatives

Tarski's theorem implies that, in order to establish the undecidability of solving equations in real unknowns, one must allow the use of something else besides

addition, subtraction, and multiplication. Hence, one can obtain many different undecidability results depending on the choice of allowed additional tools.

The proofs will always go by reduction to Hilbert's tenth problem, either for integer or for natural number solutions. The undecidability of this decision problem means the following: for every polynomial $D(x_1, \ldots, x_m)$, one and only one of the following alternatives holds:

- either
$$\exists x_1 \ldots x_m \{D(x_1, \ldots, x_m) = 0\} \tag{5.2}$$
- or
$$\forall x_1 \ldots x_m \{D(x_1, \ldots, x_m) \neq 0\} \tag{5.3}$$

but there is no algorithm to determine which of them is true and which is not. Reduction to Hilbert's tenth problem will consist of finding a way to effectively construct corresponding alternatives for the case of continuous variables.

5.3 Equations in many real unknowns

A very simple way to achieve an undecidability result is to allow the use of the trigonometric sine function. Namely, one can consider the following system of equations in real unknowns $\chi_1, \ldots, \chi_m$:

$$\begin{aligned} D(\chi_1, \ldots, \chi_m) &= 0, \\ \sin(\pi\chi_1) &= 0, \\ &\vdots \\ \sin(\pi\chi_m) &= 0 \end{aligned} \tag{5.4}$$

where, as usual, $\pi = 3.14159....$ Clearly, this system either has solutions in real $\chi_1, \ldots, \chi_m$ when alternative (5.2) holds, and does not have solutions in real $\chi_1, \ldots, \chi_m$ when the second alternative (5.3) holds.

Of course, one can combine all equations (5.4) into a single equation:

$$\begin{aligned} &D^2(\chi_1, \ldots, \chi_m) + \\ &\quad \sin^2(\pi\chi_1) + \ldots + \sin^2(\pi\chi_m) = 0. \end{aligned} \tag{5.5}$$

In this way one obtains the following undecidability result.

Undecidable Problem 1 *Let $\mathcal{F}_0$ denote the class of functions in several variables that can be defined by expressions constructed from real variables, the integers and the number π, combined through the traditional rules for addition, subtraction, multiplication, and composition with the sine function in arbitrary order. There is no algorithm for deciding for an arbitrary given function $\Phi(\chi_1, \ldots, \chi_m)$ from the class $\mathcal{F}_0$ whether the equation*

$$\Phi(\chi_1, \ldots, \chi_m) = 0 \tag{5.6}$$

has a real solution.

5.3.1 A slight improvement

The above result can be improved slightly by the elimination of the number π from the definition of the class of functions. Namely, one can introduce a new unknown, say, ψ, and impose the following conditions on it:

$$\sin(\psi) = 0, \qquad 2 \leq \psi \leq 4. \tag{5.7}$$

Clearly, the number π is the only value of ψ satisfying (5.7) so by replacing π by ψ in (5.5) and combining the resulting equation with (5.7) at the cost of the introduction of yet another new unknown for rewriting the inequalities from (5.7) as equalities, one obtains:

$$\begin{aligned} &D^2(\chi_1, \ldots, \chi_m) + \\ &\quad \sin^2(\psi\chi_1) + \ldots + \sin^2(\psi\chi_m) + \\ &\qquad \sin^2(\psi) + (1 - (\psi - 3)^2 - z^2)^2 = 0. \end{aligned} \tag{5.8}$$

Consequently, one gets the following improvement of the previous result:

Undecidable Problem 2 *Let $\mathcal{F}_1$ denote the class of functions in several variables that can be defined by expressions constructed from real variables and the integers, combined through the traditional rules for addition, subtraction, multiplication, and composition with the sine function in arbitrary order. There is no algorithm for deciding for an arbitrary given function Φ from the class $\mathcal{F}_1$ whether the equation*

$$\Phi(\chi_1, \ldots, \chi_k) = 0 \tag{5.9}$$

has a real solution.

5.4 Inequalities in many real unknowns

For the original alternatives (5.2)–(5.3), there are now corresponding alternatives for equation (5.9):

- either
$$\exists \chi_1 \ldots \chi_m \{\Phi(\chi_1, \ldots, \chi_m) = 0\} \tag{5.10}$$
- or
$$\forall \chi_1 \ldots \chi_m \{\Phi(\chi_1, \ldots, \chi_m) \neq 0\} \tag{5.11}$$

with $\Phi(\chi_1, \ldots, \chi_m)$ being the left-hand side of (5.5). This construction makes these alternatives unstable: arbitrary small perturbations of the function Φ may switch the situation from the first alternative to the second one. To achieve "stable" alternatives, note that, in fact, in the case of integer variables one can replace the second alternative (5.3) by a stronger condition. Namely, for every polynomial D one and only one of the following statements is true:

- either
$$\exists x_1 \ldots x_m \{D^2(x_1, \ldots, x_m) = 0\}, \tag{5.12}$$

- or

$$\forall x_1 \ldots x_m \{D^2(x_1, \ldots, x_m) \geq 1\}. \tag{5.13}$$

One can obtain a similar improvement of alternative (5.11) by multiplying the left-hand side of (5.5) by a suitable polynomial.

In fact, let ϵ be the distance from some point $\langle \chi_1, \ldots, \chi_m \rangle$ in $\mathbb{R}^m$ to the nearest point $\langle x_1, \ldots, x_m \rangle$ with integer coordinates. The difference $D^2(\chi_1, \ldots, \chi_m) - D^2(x_1, \ldots, x_m)$ can be easily bounded as

$$|D^2(\chi_1, \ldots, \chi_m) - D^2(x_1, \ldots, x_m)| < B(\chi_1, \ldots, \chi_m)\epsilon \tag{5.14}$$

where B is a suitable polynomial constructed with the use of polynomial D and its partial derivatives. So if (5.11) holds and ϵ is so small that

$$\epsilon < \frac{1}{2B(\chi_1, \ldots, \chi_m)}, \tag{5.15}$$

then

$$D^2(\chi_1, \ldots, \chi_m) > 0.5. \tag{5.16}$$

On the other hand, if ϵ is not small, that is if (5.15) is not true, then the other summands in the left-hand side of (5.5) contribute a significant amount:

$$\begin{aligned} \sin^2(\pi\chi_1) + \ldots + \sin^2(\pi\chi_m) &> \frac{\epsilon^2}{4m} \\ &> \frac{1}{16mB^2(\chi_1, \ldots, \chi_m)}. \end{aligned} \tag{5.17}$$

Thus, with

$$\Phi(\chi_1, \ldots, \chi_m) = 32mB^2(\chi_1, \ldots, \chi_m)(D^2(\chi_1, \ldots, \chi_m) + \tag{5.18}$$

$$\sin^2(\pi\chi_1) + \ldots + \sin^2(\pi\chi_m))), \tag{5.19}$$

the following alternatives correspond to alternatives (5.2)–(5.3):

- either

$$\exists \chi_1 \ldots \chi_m \{\Phi(\chi_1, \ldots, \chi_m) = 0\} \tag{5.20}$$

- or

$$\forall \chi_1 \ldots \chi_m \{\Phi(\chi_1, \ldots, \chi_m) > 1\}. \tag{5.21}$$

Consequently, one obtains the following undecidability result for the class $\mathcal{F}_0$ defined above:

Undecidable Problem 3 *There is no algorithm for deciding for an arbitrary given function $\Phi(\chi_1, \ldots, \chi_m)$ from the class $\mathcal{F}_0$ whether the inequality*

$$\Phi(\chi_1, \ldots, \chi_m) < 1 \tag{5.22}$$

has a real solution.

I leave as an easy exercise an improvement to the case of functions from the class $\mathcal{F}_1$.

5.5 Equations and inequalities in one real unknown

To obtain the undecidability of Diophantine equations, it ws necessary to consider equations with sufficiently many unknowns. Surprisingly, the introduction of the sine function not only allows one to use unknowns for real numbers, but also to reduce the number of such unknowns to one.

Consider the following map from $\mathbb{R}$ to $\mathbb{R}^m$:

$$\chi \mapsto \langle \chi \sin(\chi), \chi \sin(\chi^3), \ldots, \chi \sin(\chi^{2m-1}) \rangle. \tag{5.23}$$

It is easy to check that the range of this map is everywhere dense in $\mathbb{R}^m$. Thus by defining

$$\Psi(\chi) = \Phi(\chi \sin(\chi), \chi \sin(\chi^3), \ldots, \chi \sin(\chi^{2m-1}), \tag{5.24}$$

one can restate alternatives (5.20)–(5.21) as follows:

- either

$$\forall \epsilon > 0 \exists \chi \{\Psi(\chi) < \epsilon\} \tag{5.25}$$

- or

$$\forall \chi \{\Psi(\chi) \geq 1\}. \tag{5.26}$$

One obtains the following quantitative improvements of Undecidable Problems 1 and 3, respectively:

Undecidable Problem 4 *There is no algorithm for deciding for an arbitrary given function $\Psi(\chi)$ from the class $\mathcal{F}_0$ whether the inequality*

$$\Psi(\chi) < 1 \tag{5.27}$$

has a real solution.

Undecidable Problem 5 *There is no algorithm for deciding for an arbitrary given function $\Phi(\chi)$ from the class $\mathcal{F}_0$ whether the equation*

$$\Phi(\chi) = 0 \tag{5.28}$$

has a real solution.

(To prove the latter result, it suffices to define $\Phi(\chi) = 2\Psi(\chi) - 1$.)

5.6 Identities in one real variable

One can extend the class of admissible functions by allowing the use of the absolute value function. With this function, the alternatives (5.25)–(5.26) can be restated in the following way:

- either
$$\exists\chi\{1 - \Psi(\chi) + |1 - \Psi(\chi)| \neq 0\} \tag{5.29}$$
- or
$$\forall\chi\{1 - \Psi(\chi) + |1 - \Psi(\chi)| = 0\}. \tag{5.30}$$

Consequently, one obtains:

Undecidable Problem 6 *Let $\mathcal{F}_2$ denote the class of functions in one real variable that can be defined by expressions constructed from the variable, the integers and the number π, combined through the traditional rules for addition, subtraction, and multiplication, and composition with the functions* sin *and* abs *(absolute value) in arbitrary order. There is no algorithm for deciding for an arbitrary given function $\Phi(\chi)$ from the class $\mathcal{F}_2$ whether the equality*

$$\Phi(\chi) = 0 \tag{5.31}$$

holds identically for all values of χ.

5.7 Convergence of definite integrals

This section addresses the undecidability of a decision problem relating to integration rather than one about solving equations.

Alternatives (5.25)–(5.26) can be rewritten in yet another incarnation as follows:

- either
$$\int_{-\infty}^{+\infty} \frac{d\chi}{(\chi^2+1)(2\Psi(\chi)-1)^2} = \infty \tag{5.32}$$
- or
$$\int_{-\infty}^{+\infty} \frac{d\chi}{(\chi^2+1)(2\Psi(\chi)-1)^2} < \infty. \tag{5.33}$$

By extending the class of admissible functions by division, one obtains:

Undecidable Problem 7 *Let $\mathcal{F}_3$ denote the class of functions of one real variable that can be defined by expressions constructed from the variable, the integers and the number π, combined through the traditional rules for addition, subtraction, multiplication, division, and composition with the* sin *function in arbitrary order. Then there is no method for deciding for an arbitrary function Φ in the class $\mathcal{F}_3$ whether the integral*

$$\int_{-\infty}^{+\infty} \Phi(\eta)\, d\eta \tag{5.34}$$

converges or not.

5.8 The existence of an antiderivative

One now deals with indefinite integrals rather than definite integrals as in the previous section. Modern computer algebra systems are capable of finding symbolic antiderivatives for a wide class of functions. For this purpose a number of sophisticated algorithms have been developed. Typically, such an algorithm is defined for dealing with two classes of functions, say class $\mathcal{F}_4$ and class $\mathcal{F}_5$. For every function from the former class, the algorithm either produces the corresponding antiderivative belonging to the latter class, or indicates that no function from the latter class is the required antiderivative.

In order to have an undecidability result, one should select these classes in such a way that there should be at least one function in $\mathcal{F}_4$ with no antiderivative in $\mathcal{F}_5$, because otherwise the answer would be trivially always positive. In fact, for the proof, we need a somewhat stronger property than this: namely, assume that the *class $\mathcal{F}_4$ contains a function Υ that is defined for all values of its argument, while the class $\mathcal{F}_5$ does not contain any function Ω such that* $\Upsilon(\chi) = \Omega'(\chi)$ *for* $\chi \in (\alpha, \beta)$. for any non-empty open interval (α, β). As a possible example, consider $\Upsilon(\chi) = 2^{x^2}$ because the antiderivative of this function is not representable as the composition of elementary functions on any interval.

Assume that *the class $\mathcal{F}_4$ contains the class $\mathcal{F}_2$ and is closed under multiplication.* Thus, this class should contain the function

$$\Delta(\eta) = 1 + |4\eta - 4| - |4\eta - 3| \tag{5.35}$$

which is step-wise linear:

$$\Delta(\chi) = \begin{cases} 1, & \text{if } \chi \leq .5, \\ 2(1-\chi), & \text{if } .5 \leq \chi \leq 1, \\ 0, & \text{if } 1 \leq \chi, \end{cases} \tag{5.36}$$

Under the above assumptions, the class $\mathcal{F}_4$ also contains function

$$\Lambda(\chi) = \Delta\left(\Psi(\chi)\right) \Upsilon(\chi) \tag{5.37}$$

where Ψ is defined by (5.24). Now, if (5.26) is true, then $\Lambda(\chi) = 0$ for every χ and, hence, any constant is an antiderivative of Λ. On the other hand, if (5.25) is true, then $\Lambda(\chi) = \Upsilon(\chi)$ in some non-empty interval where of $\Psi(\chi) < .5$, and, hence, Λ has no antiderivative from the class $\mathcal{F}_5$. Thus one gets:

Undecidable Problem 8 *With all the above stated assumptions about the classes $\mathcal{F}_4$ and $\mathcal{F}_5$, there is no method for determining for an arbitrary function in $\mathcal{F}_4$ whether it has an antiderivative in $\mathcal{F}_5$.*

5.9 Solvability of systems of ordinary differential equations

This section again deals with equations, and indeed polynomial equations, but now they will be ordinary differential equations, or more precisely, systems of

such equations. Consequently, the unknowns will be real differentiable functions of one independent variable τ rather than real numbers. To make matters definite, assume that τ ranges over the interval $[0, 1]$.

To simulate real unknowns, constant functions will be used: i.e., functions satisfying the differential equation of the form

$$\Upsilon'(\tau) = 0. \tag{5.38}$$

It is easy to check that in every solution of the system

$$\Pi'(\tau) = 0, \qquad \Xi''(\tau) + \Pi^2(\tau)\Xi(\tau) = 0 \tag{5.39}$$

with boundary conditions

$$3 \leq \Pi(0) \leq 4, \tag{5.40}$$

$$\Xi(0) = 0, \qquad \Xi(1) = 0, \qquad \Xi'(0) = 1, \tag{5.41}$$

the solution $\Pi(\tau)$ is equal (identically) to the number π. Similarly, in every solution of the system

$$\Upsilon'(\tau) = 0, \qquad \Psi''(\tau) + \Pi^2(\tau)\Upsilon^2(\tau)\Psi(\tau) = 0 \tag{5.42}$$

with boundary conditions

$$\Psi(0) = \Psi(1) = 0, \qquad \Psi'(0) = \Pi(0)\Upsilon(0), \tag{5.43}$$

the solution $\Upsilon(\tau)$ is identically equal to some integer y.

Thus, a Diophantine equation

$$D(y_1, \ldots, y_m) = 0 \tag{5.44}$$

has a solution in integers $y_1, \ldots, y_m$ if and only if the system of differential equations

$$\Pi'(\tau) = 0, \tag{5.45}$$

$$\Xi''(\tau) + \Pi^2(\tau)\Xi(\tau) = 0, \tag{5.46}$$

$$\Upsilon_1'(\tau) = 0, \tag{5.47}$$

$$\Psi_1''(\tau) + \Pi^2(\tau)\Upsilon_1^2(\tau)\Psi_1(\tau) = 0, \tag{5.48}$$

$$\vdots \tag{5.49}$$

$$\Upsilon_m'(\tau) = 0, \tag{5.50}$$

$$\Psi_m''(\tau) + \Pi^2(\tau)\Upsilon_m^2(\tau)\Psi_m(\tau) = 0, \tag{5.51}$$

$$D\big(\Upsilon_1(\tau), \ldots, \Upsilon_m(\tau)\big) = 0 \tag{5.52}$$

has a solution on $[0, 1]$ satisfying the boundary conditions

$$3 \leq \Pi(0) \leq 4, \tag{5.53}$$

$$\Xi(0) = \Xi(1) = 0, \qquad \Xi'(0) = 1, \tag{5.54}$$

$$\begin{array}{ll} \Psi_1(0) = \Psi_1(1) = 0, & \Psi_1'(0) = \Pi(0)\Upsilon_1(0), \\ \vdots & \vdots \\ \Psi_m(0) = \Psi_m(1) = 0, & \Psi_m'(0) = \Pi(0)\Upsilon_m(0). \end{array} \tag{5.55}$$

Introducing new unknown functions, one can easily replace these boundary conditions by additional equations. Inequalities (5.53) can be rewritten as

$$3 + \Delta_1^2(0) = \Pi(0), \qquad \Pi(0) + \Delta_2^2(0) = 4 \tag{5.56}$$

A condition of the form

$$\Delta(\alpha) = \beta \tag{5.57}$$

with constants α and β can be replaced by the equation

$$\Delta(\tau) - \beta = (\tau - \alpha)\Omega(\tau). \tag{5.58}$$

An equation containing Δ'' can be replaced by a system of two first-order equations in Δ' and an additional function.

Thus, one obtains the following undecidability result:

Undecidable Problem 9 *There is no algorithm for determining for an arbitrary system of differential equations of the form*

$$\begin{aligned} P_1\big(\tau, \Xi_1(\tau), \ldots, \Xi_k(\tau), \Xi_1'(\tau)\big) &= 0 \\ &\vdots \\ P_k\big(\tau, \Xi_1(\tau), \ldots, \Xi_k(\tau), \Xi_k'(\tau)\big) &= 0, \end{aligned} \tag{5.59}$$

where P_1, ..., P_k are polynomials with integer coefficients, whether the system has a solution on the interval $[0, 1]$.

In Undecidable Problems 4 and 5, the number of unknowns was reduced to one. Similarly, a quantitative improvement is possible for Undecidable Problem 9, namely, it is sufficient to consider a single (high order) differential equation with one unknown function. This is left here as a (not so easy) exercise; the answer can be found in [15].

5.10 Uniqueness of solutions of ordinary differential equations

Thanks to the boundary conditions (5.55), in order to obtain the undecidability result in Problem 9, it is sufficient to consider system (5.59), for which functions identically equal to 0 do not form a solution. One can add this solution by putting

$$Q_l(\tau, \chi_1, \ldots, \chi_k, \eta) = (\chi_1^2 + \ldots + \chi_k^2)P_l(\tau, \chi_1, \ldots, \chi_k, \eta), \quad 1 \le l \le k. \tag{5.60}$$

Thus one gets:

Undecidable Problem 10 *There is no algorithm for determining for an arbitrary system of differential equations of the form*

$$\begin{aligned} Q_1\big(\tau, \Xi_1(\tau), \ldots, \Xi_k(\tau), \Xi_1'(\tau)\big) &= 0 \\ &\vdots \\ Q_k\big(\tau, \Xi_1(\tau), \ldots, \Xi_k(\tau), \Xi_k'(\tau)\big) &= 0, \end{aligned} \tag{5.61}$$

where $Q_1, \ldots, Q_k$ are polynomials with integer coefficients, whether the system has unique solution on the interval $[0,1]$.

5.11 Formal power series solutions of ordinary differential equations

All the above reductions to Hilbert's tenth problem were based on the explicit or implicit use of the sine function in order to imitate the discrete structure of integers by continuous objects. The remaining examples will be based on a different idea; namely, looking for solutions of differential equations in formal power series.

Consider the system

$$\Psi'(\tau) = 0, \tag{5.62}$$

$$\tau\Phi'(\tau) = \Psi(\tau)\Phi(\tau) \tag{5.63}$$

with unknowns

$$\Psi(\tau) = \sum_{k=0}^{\infty} \psi_k \tau^k, \tag{5.64}$$

$$\Phi(\tau) = \sum_{k=0}^{\infty} \phi_k \tau^k. \tag{5.65}$$

Clearly, this system has solutions of two kinds:

- a degenerate solution

$$\psi_0 = \psi_1 = \ldots = 0, \qquad \phi_1 = \phi_2 = \ldots = 0, \tag{5.66}$$

- a non-degenerate solution

$$\phi_0 = y, \qquad \phi_1 = \phi_2 = \ldots = 0, \tag{5.67}$$

$$\psi_0 = \ldots = \psi_{y-1} = 0, \quad \psi_y = y, \quad \psi_{y+1} = \ldots = 0. \tag{5.68}$$

In the non-degenerate case, y must be a natural number and this fact can be used to reduce the question of solvability of Diophantine equation (5.44) in natural numbers to the question of the existence of a formal power solution for a system of differential equations

$$\begin{aligned} \Psi_1'(\tau) &= 0, \\ \tau\Phi_1'(\tau) &= \Psi_1(\tau)\Phi_1(\tau), \\ &\vdots \\ \Psi_m'(\tau) &= 0, \\ \tau\Phi_m'(\tau) &= \Psi_m(\tau)\Phi_1(\tau), \\ D(\Psi_1(\tau), \ldots, \Psi_m(\tau)) &= 0 \end{aligned} \tag{5.69}$$

with the additional condition

$$\Phi_1(\tau)\dots\Phi_m(\tau) \not\equiv 0. \tag{5.70}$$

Consequently, one obtains the following result:

Undecidable Problem 11 *There is no algorithm for deciding for an arbitrary system of differential equations of the form*

$$\begin{aligned} P_1\big(\tau,\Xi_1(\tau),\dots,\Xi_k(\tau),\Xi_1'(\tau)\big) &= 0,\\ &\vdots\\ P_k\big(\tau,\Xi_1(\tau),\dots,\Xi_k(\tau),\Xi_k'(\tau)\big) &= 0, \end{aligned} \tag{5.71}$$

where the P's are polynomials with integer coefficients whether the system has a solution in formal power series satisfying the additional condition

$$\Xi_1(\tau) \not\equiv 0. \tag{5.72}$$

5.12 Convergent power series solutions of ordinary differential equations

The undecidable problem stated above has a definite aesthetic shortcoming; namely, the forced addition of an inequality. To eliminate this shortcoming, one can replace equations (5.62)–(5.63) by equations

$$\Psi'(\tau) = 0, \tag{5.73}$$

$$\tau^2\Phi'(\tau) - ((\Psi(\tau)-1)\tau+1)\Phi(\tau)+1 = 0. \tag{5.74}$$

All formal power solutions of this system are of the form

$$\phi_0 = y, \qquad \phi_1 = \phi_2 = \dots = 0, \tag{5.75}$$

$$\psi_0 = 1,\dots,\psi_n = (1-\phi_0)(2-\phi_0)\dots(n-\phi_0),\dots. \tag{5.76}$$

Such a solution is convergent if and only if y is a positive integer. One obtains:

Undecidable Problem 12 *There is no algorithm for deciding for an arbitrary system of differential equations of the form*

$$\begin{aligned} P_1\big(\tau,\Xi_1(\tau),\dots,\Xi_k(\tau),\Xi_1'(\tau)\big) &= 0,\\ &\vdots\\ P_k\big(\tau,\Xi_1(\tau),\dots,\Xi_k(\tau),\Xi_k'(\tau)\big) &= 0, \end{aligned} \tag{5.77}$$

where the P's are polynomials with integer coefficients, whether the system has a convergent formal power series solution.

5.13 Power series solutions of partial differential equations

Instead of dealing with several formal power series in one variable, one can consider formal power series

$$\Psi(\tau_1,\ldots,\tau_m)=\sum_{y_1,\ldots,y_m}\psi_{y_1,\ldots,y_m}\tau_1^{y_1}\ldots\tau_m^{y_m} \tag{5.78}$$

in m independent variables $\tau_1,\ldots,\tau_m$. The differential operator $\tau_k\frac{\partial}{\partial\tau_k}$ acts on monomial $\tau_k^{y_k}$ as a multiplication by y_k:

$$\tau_k\frac{\partial}{\partial\tau_k}\tau_k^{y_k}=y_k\tau_k^{y_k}. \tag{5.79}$$

Consequently, the operator

$$D\left(\tau_1\frac{\partial}{\partial\tau_1},\ldots,\tau_m\frac{\partial}{\partial\tau_m}\right) \tag{5.80}$$

acts as element-wise multiplication by $D(y_1,\ldots,y_m)$:

$$D\left(\tau_1\frac{\partial}{\partial\tau_1},\ldots,\tau_m\frac{\partial}{\partial\tau_m}\right)\Psi(\tau_1,\ldots,\tau_m)= \sum_{y_1,\ldots,y_m}D(y_1,\ldots,y_m)\psi_{y_1,\ldots,y_m}\tau_1^{y_1}\ldots\tau_m^{y_m}. \tag{5.81}$$

Thus, as soon as Diophantine equation (5.44) has a solution in natural numbers, some coefficients in (5.81) *must* be equal to zero. If there is no solution to (5.44), the coefficients can be set as arbitrary numbers by the choice of suitable ψ's. For example, by putting

$$\psi_{y_1,\ldots,y_m}=\frac{1}{D(y_1,\ldots,y_m)} \tag{5.82}$$

one can make all the coefficients equal to 1 and, consequently, (5.81) becomes equal to

$$\sum_{y_1,\ldots,y_m}\tau_1^{y_1}\ldots\tau_m^{y_m}=\frac{1}{1-\tau_1}\cdot\ldots\cdot\frac{1}{1-\tau_m}. \tag{5.83}$$

In other words, the partial differential equation

$$(1-\tau_1)\ldots(1-\tau_m)\,D\left(\tau_1\tfrac{\partial}{\partial\tau_1},\ldots,\tau_m\tfrac{\partial}{\partial\tau_m}\right)\Psi(\tau_1,\ldots,\tau_m)=1 \tag{5.84}$$

has a formal power series solution if and only if Diophantine equation (5.44) has *no* solutions in natural numbers. Consequently, one gets:

Undecidable Problem 13 *There is no algorithm for deciding for an arbitrary polynomial P with integer coefficients whether the partial differential equation*

$$P\left(\tau_1,\ldots,\tau_m,\tfrac{\partial}{\partial\tau_1},\ldots,\tfrac{\partial}{\partial\tau_m}\right)\Psi(\tau_1,\ldots,\tau_m)=1 \tag{5.85}$$

has a formal power series solution.

5.14 Equations with non-computable solutions

Thus far, the results obtained have dealt with the non-existence of algorithms for decision problems: i.e., problems which require a binary answer "YES" or "NO". The last example to be considered here pertains to the non-existence of algorithms for computing rational coefficients forming a formal power series solution of a system of linear partial differential equations. Note that while such a power series expansion always exists, the consideration here is the question of computing the coefficients.

Now the mere undecidability of Hilbert's tenth problem will not be sufficient for the proof and it will be necessary to invoke the full power of the DPRM-theorem (stated in Chapter One and proved in Chapters Two through Four) which asserts that every listable set $\mathfrak{M}$ has a Diophantine representation:

$$a \in \mathfrak{M} \Longleftrightarrow \exists x_2 \ldots x_m \{D(a, x_2, \ldots, x_m) = 0\}. \tag{5.86}$$

Consider the following system of partial differential equations:

$$(1-\tau_2)\ldots(1-\tau_m)\, D\left(\tau_1 \tfrac{\partial}{\partial \tau_1}, \tau_2 \tfrac{\partial}{\partial \tau_2}, \ldots, \tau_m \tfrac{\partial}{\partial \tau_m}\right) \Psi(\tau_1, \tau_2, \ldots, \tau_m) = \Xi(\tau_1, \tau_2, \ldots, \tau_m), \tag{5.87}$$

$$\tfrac{\partial}{\partial \tau_2}\Xi(\tau_1, \tau_2, \ldots, \tau_m) = \cdots = \tfrac{\partial}{\partial \tau_m}\Xi(\tau_1, \tau_2, \ldots, \tau_m) = 0. \tag{5.88}$$

According to (5.88), function Ξ depends only on τ_1; that is

$$\Xi(\tau_1, \tau_2, \ldots, \tau_m) = \sum_{k=0}^{\infty} \xi_k \tau_1^k. \tag{5.89}$$

Multiplying the left-hand side and the right-hand side in (5.87) by the left-hand side and the right-hand side, respectively, in the identity

$$\tfrac{1}{1-\tau_2} \cdots \tfrac{1}{1-\tau_m} = \textstyle\sum_{y_2, \ldots, y_m} \tau_2^{y_1} \ldots \tau_m^{y_m} \tag{5.90}$$

and using (5.81) one sees that

$$D(y_1, \ldots, y_m)\psi_{y_1, \ldots, y_m} = \xi_{y_1} \tag{5.91}$$

and, hence,

$$a \in \mathfrak{M} \Longrightarrow \xi_a = 0. \tag{5.92}$$

In fact, this is the only restriction on Ξ; that is, putting

$$\psi_{y_1, \ldots, y_m} = \begin{cases} 0, & \text{if } y_1 \in \mathfrak{M} \\ \frac{\xi_{y_1}}{D(y_1, \ldots, y_m)}, & \text{otherwise} \end{cases} \tag{5.93}$$

one obtains a solution of (5.87)–(5.88). Thus, this system always has a solution, and in this solution, all coefficients are rational numbers.

The mere existence of a listable set with the undecidable problem of membership will no longer be sufficient. A stronger result about the existence of some listable sets $\mathfrak{M}_0$ and $\mathfrak{M}_1$ of natural numbers which are *effectively inseparable* is required. This property means the following:

- the sets $\mathfrak{M}_0$ and $\mathfrak{M}_1$ do not intersect: that is

$$\mathfrak{M}_0 \cap \mathfrak{M}_1 = \emptyset, \tag{5.94}$$

but their complements $\overline{\mathfrak{M}_0}$ and $\overline{\mathfrak{M}_1}$ do intersect:

$$\overline{\mathfrak{M}_0} \cap \overline{\mathfrak{M}_1} \neq \emptyset; \tag{5.95}$$

- the latter property, (5.95), is inherited by all listable extensions $\mathfrak{M}_0^*$ and $\mathfrak{M}_1^*$ of sets $\mathfrak{M}_0$ and $\mathfrak{M}_1$ which meet the former condition, (5.94). That is, if $\mathfrak{M}_0^*$ and $\mathfrak{M}_1^*$ are any listable sets such that

$$\mathfrak{M}_0 \subseteq \mathfrak{M}_0^*, \qquad \mathfrak{M}_1 \subseteq \mathfrak{M}_1^* \tag{5.96}$$

and

$$\mathfrak{M}_0^* \cap \mathfrak{M}_1^* = \emptyset \tag{5.97}$$

then

$$\overline{\mathfrak{M}_0^*} \cap \overline{\mathfrak{M}_1^*} \neq \emptyset. \tag{5.98}$$

Proofs of the existence of such effectively inseparable listable sets can nowadays be found in many standard textbooks.

Let

$$a \in \mathfrak{M}_0 \Longleftrightarrow \exists x_2 \ldots x_m \{D_0(a, x_2, \ldots, x_m) = 0\} \tag{5.99}$$

and

$$a \in \mathfrak{M}_1 \Longleftrightarrow \exists x_2 \ldots x_m \{D_1(a, x_2, \ldots, x_m) = 0\} \tag{5.100}$$

be Diophantine representations for sets $\mathfrak{M}_0$ and $\mathfrak{M}_1$, respectively. Consider the following system of partial differential equations, which consists of two copies of equations (5.87)–(5.88) and one additional equation:

$$(1-\tau_2)\ldots(1-\tau_m)\, D_0\left(\tau_1\tfrac{\partial}{\partial\tau_1}, \tau_2\tfrac{\partial}{\partial\tau_2}, \ldots, \tau_m\tfrac{\partial}{\partial\tau_m}\right)\Psi(\tau_1,\tau_2,\ldots,\tau_m) = \Xi_0(\tau_1,\tau_2,\ldots,\tau_m), \tag{5.101}$$

$$\tfrac{\partial}{\partial\tau_2}\Xi_0(\tau_1,\tau_2,\ldots,\tau_m) = \cdots = \tfrac{\partial}{\partial\tau_m}\Xi_0(\tau_1,\tau_2,\ldots,\tau_m) = 0, \tag{5.102}$$

$$(1-\tau_2)\ldots(1-\tau_m)\, D_1\left(\tau_1\tfrac{\partial}{\partial\tau_1}, \tau_2\tfrac{\partial}{\partial\tau_2}, \ldots, \tau_m\tfrac{\partial}{\partial\tau_m}\right)\Psi_1(\tau_1,\tau_2,\ldots,\tau_m) = \Xi_1(\tau_1,\tau_2,\ldots,\tau_m), \tag{5.103}$$

$$\tfrac{\partial}{\partial\tau_2}\Xi_1(\tau_1,\tau_2,\ldots,\tau_m) = \cdots = \tfrac{\partial}{\partial\tau_m}\Xi_1(\tau_1,\tau_2,\ldots,\tau_m) = 0, \tag{5.104}$$

$$(1-\tau_1)\big(\Xi_0(\tau_1,\tau_2,\ldots,\tau_m) - \Xi_1(\tau_1,\tau_2,\ldots,\tau_m)\big) = 1. \tag{5.105}$$

The additional equation (5.105) is equivalent to

$$\xi_{0,a} + \xi_{1,a} = 1, \qquad a = 0, 1, \ldots \tag{5.106}$$

where

$$\Xi_0(\tau_1, \tau_2, \ldots, \tau_m) = \sum_{k=0}^{\infty} \xi_{0,k} \tau^k, \tag{5.107}$$

$$\Xi_1(\tau_1, \tau_2, \ldots, \tau_m) = \sum_{k=0}^{\infty} \xi_{1,k} \tau^k. \tag{5.108}$$

This condition is easily satisfied thanks to (5.94), which implies that the restriction caused by the analogue of (5.92) forces at most one of the numbers, $\xi_{0,a}$ or $\xi_{1,a}$, to be equal to 0 and, hence, we have full freedom in the choice of the other number.

Now suppose that there is an algorithm which calculates some rational numbers $\xi_{0,0}, \xi_{0,1}, \ldots$ such that the formal power series Ξ_0 defined by (5.107), together with some formal power series Ξ_1, Ψ_0 and Ψ_1, satisfy equations (5.101)–(5.105). One defines

$$\mathfrak{M}_0^* = \{a \mid \xi_{0,a} = 0\}, \tag{5.109}$$

$$\mathfrak{M}_1^* = \{a \mid \xi_{0,a} \neq 0\}. \tag{5.110}$$

Clearly both sets $\mathfrak{M}_0^*$ and $\mathfrak{M}_1^*$ are listable.

it is necessary to check that the conditions in (5.96) are satisfied. If $a \in \mathfrak{M}_0$, then by an analogue of (5.92), $\xi_{0,a} = 0$ and, hence, $a \in \mathfrak{M}_0^*$ as required. On the other hand, if $a \in \mathfrak{M}_1$, then by an analogue of (5.92), $\xi_{1,a} = 0$, which by (5.106) implies that $\xi_{0,a} = 1$ and, hence, $a \in \mathfrak{M}_1^*$ as required.

The sets $\mathfrak{M}_0^*$ and $\mathfrak{M}_1^*$ are evidently complements of one another, hence, both intersections (5.97) and (5.98) are empty, which contradicts the choice of $\mathfrak{M}_0$ and $\mathfrak{M}_1$ as effectively inseparable sets. This contradiction implies that numbers $\xi_{0,0}, \xi_{0,1}, \ldots$ cannot be calculated by an algorithm.

Bibliography

[1] Z. Adamowicz and P. Zbierski, *Logic of Mathematics*, John Wiley & Sons, New York, 1997.

[2] A. Adler, *Some recursively unsolvable problems in analysis*, Proceedings of the American Mathematical Society, **22**(2), pp. 523–526, 1969.

[3] K. Appel and W. Haken, *Every planar map is four colorable. Part I: Discharging*, Illinois Journal of Mathematics, **21**(3), pp. 429–490, 1977.

[4] J.-P. Azra, *Relations Diophantiennes et la solution négative du 10e problème de Hilbert*, Lecture Notes in Mathematics, **244**, pp. 11–28, Springer-Verlag, 1971.

[5] C. Baxa, *A note on Diophantine representations*, American Mathematical Monthly, **100**(2), pp. 138–143, 1993.

[6] E. Börger, *Computability, Complexity, Logic*, North-Holland, Amsterdam, 1989.

[7] B. F. Caviness, *On canonical forms and simplification*, Journal of the ACM, **17**(2), pp. 385–396, 1970.

[8] M. Davis, *Arithmetical problems and recursively enumerable predicates*, Journal of Symbolic Logic, **18**(1), pp. 33–41, 1953.

[9] M. Davis, *Hilbert's tenth problem is unsolvable*, American Mathematical Monthly, **80**(3), pp. 233–269, 1973.

[10] M. Davis, *Computability and Unsolvability*, Dover Publications, New York, 1982.

[11] M. Davis, Y. Matiyasevich and J. Robinson, *Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution*, Proceedings of Symposia in Pure Mathematics, **28**, pp. 323–378, 1976 (Reprinted in [46]).

[12] M. Davis, H. Putnam and J ,Robinson, *The decision problem for exponential Diophantine equations*, Annals of Mathematics (2), **74**, pp. 425–436, 1961 (Reprinted in [46]).

[13] J. Denef, *Hilbert's Tenth Problem for quadratic rings*, Proceedings of the American Mathematical Society, **48**(1), pp. 214–220, 1975.

[14] J. Denef and L. Lipshitz, *Power series solutions of algebraic differential equations*, Mathematische Annalen, **267**(2), pp. 213–238, 1984.

[15] J. Denef and L. Lipshitz, *Decision problems for differential equations*, Journal of Symbolic Logic, **54**(3), pp. 941–950, 1989.

[16] K. Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme: I*, Monatsh. Math. und Phys., **38**(1), pp. 173–198, 1931.

[17] D. Hilbert, *Mathematische Probleme. Vortrag, gehalten auf dem internationalen Mathematiker Kongress zu Paris 1900*, Nachr. K. Ges. Wiss., Göttingen, Math.-Phys.Kl., (1900), pp. 253–297. See also Arch. Math. Phys., (1901) pp. 44–63 and pp. 213–237. See also David Hilbert, *Gesammelte Abhandlungen*, Berlin : Springer, vol. 3 (1935), 310 (Reprinted: New York: Chelsea (1965)). French translation with corrections and additions: Compte rendu du Deuxième Congrès International des Mathématiciens tenu à Paris du 6 au 12 août 1900, Gauthier-Villars, 1902, pp. 58–114 (réédition : Editions Gabay, Paris 1992). English translation : *Bull. Amer. Math. Soc.* (1901–1902) pp. 437–479. Reprinted in : *Mathematical Developments arising from Hilbert problems*, Proceedings of Symposia in Pure Mathematics, **28**, American Mathematical Society, Browder Ed., 1976, pp. 1–34.

[18] J. P. Jones. *Universal Diophantine equation*, Journal of Symbolic Logic, **47**, pp. 549–571, 1982.

[19] J. P. Jones and Yu. V. Matiyasevich. *Direct translation of register machines into exponential Diophantine equations*, in L. Priese, editor, Report on the first GTI-workshop, no. 13, pp. 117–130, Reihe Theoretische Informatik, Universität-Gesamthochschule Paderborn, 1983.

[20] J. P. Jones and Y. V. Matijasevič, *Register machine proof of the theorem on exponential Diophantine representation of enumerable sets*, Journal of Symbolic Logic, **49**(3), pp. 818–829, 1984.

[21] J. P. Jones, Y. V. Matijasevič, *Proof of recursive unsolvability of Hilbert's tenth problem*, American Mathematical Monthly, **98**(8), pp. 689–709, 1991.

[22] J. P. Jones, D. Sato, H. Wada, and D. Wiens, *Diophantine representation of the set of prime numbers*, The American Mathematical Monthly, **83**(6), pp. 449–464, 1976.

[23] G. Kreisel, *Davis, Martin; Putnam, Hilary; Robinson, Julia. The decision problem for exponential Diophantine equations*, Mathematical Reviews **24**, #A3061:573, 1962.

[24] E. E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, Journal für die Reine und Angewandte Mathematik, **44**, pp. 93–146, 1852.

[25] J. Lambek, *How to program an infinite abacus*, Canadian Mathematical Bulletin, **4**, pp. 295–302, 1961.

[26] Yu. I. Manin *A Course in Mathematical Logic*, Springer, New York; Heidelberg; Berlin, 1977.

[27] M. Margenstern, *Le théorèm de Matiyassévitch et résultats connexes*, in C. Berline, K. McAloon, and J.-P. Ressayre, editors, Model Theory and Arithmetic, Lecture Notes in Mathematics **890**, pp. 198–241. Springer-Verlag, 1981.

[28] Yu. V. Matiyasevich, *Diofantovost' perechislimykh mnozhestv*, Dokl. AN SSSR, **191**(2), pp. 278–282, 1970. Translated in: Soviet Math. Doklady, **11**(2), pp. 354–358, 1970.

[29] Yu. Matiyasevich, *Diofantovy mnozhestva*, Uspekhi Mat. Nauk, **27**:5(167), pp. 185–222, 1972. Translated in: Russian Mathematical Surveys, **27**(5), pp. 124–164, 1972.

[30] 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**, pp. 75–92, 1976. (Translated as Yu. V. Matiyasevich, *A new proof of the theorem on exponential Diophantine representation of enumerable sets*, Journal of Soviet Mathematics, **14(5)**, pp. 1475–1486, 1980.)

[31] Yu. Matiyasevich, *Prostye chisla perechislyayutsya polinomom ot 10 peremennykh*, Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR, **68**, pp. 62–82, 1977. (Translated as Yu. V. Matijasevič, *Primes are nonnegative values of a polynomial in 10 variables*, Journal of Soviet Mathematics, **15**(1), pp. 33–44, 1981.)

[32] Yu. V. Matiyasevich, *Algorifmicheskaya nerazreshimost' eksponentsial'no diofantovykh uravneniĭ s tremya neizvestnymi.* Issledovaniya po teorii algorifmov i matematicheskoĭ logike, A. A. Markov and V. I. Homich, Editors, Akademiya Nauk SSSR, Moscow **3**, pp. 69–78,1979. Translated in: *Selecta Mathematica Sovietica*, **3**(3), pp. 223–232, 1983/84.

[33] Yu. V. Matiyasevich, *Ob issledovaniyakh po nekotorym algorifmicheskim problemam algebry i teorii chisel*, Trudy Matematicheskogo Instituta im. V. A. Steklova AN SSSR, **168**, pp. 218–235, 1984. (Translated as Yu. V. Matiyasevich, *On investigations on some algorithmic problems in algebra and number theory*, Proceedings of Steklov Institute of Mathematics, **168**(3), pp. 227–252, 1986.)

[34] 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. Online at `http://logic.pdmi.ras.ru/~yumat/H10Pbook`, mirrored at `www.informatik.uni-stuttgart.de/ifi/ti/personen/Matiyasevich/H10Pbook`.

[35] You. Matiiassevitch, *Les equations-bricoleurs*, Revue de Mathematiques Speciales, **5:**, pp. 305–309, 1994.

[36] Z. A. Melzak, *An informal arithmetical approach to computability and computation*, Canadian Mathematical Bulletin, **4**, pp. 279–294, 1961.

[37] M. L. Minsky, *Recursive unsolvability of Post's problem of "tag" and other topics in the theory of Turing machines*, Annals of Mathematics (2), **74**, pp. 437–455, 1961.

[38] M. L. Minsky, *Computation: Finite and Infinite Machines*, Prentice Hall, Englewood Cliffs; New York, 1967.

[39] P. Pappas, *A Diophantine problem for Laurent polynomial rings*, Proceedings of the American Mathematical Society, **93**(4), pp. 713–718, 1985.

[40] Yu. G. Penzin, *Nerazreshimye teorii kol'tsa nepreryvnykh funktsiĭ*, Algoritmicheskie voprosy algebraicheskikh sistem, pp. 142–147, Irkutsk, 1978.

[41] Th. Pheidas, *Extensions of Hilbert's tenth problem*, Journal of Symbolic Logic, **59**(2), pp. 372–397, 1994.

[42] H. Putnam *An unsolvable problem in number theory*, Journal of Symbolic Logic, **25**(3), pp. 220–232, 1960.

[43] C. Reid, *The autobiography of Julia Robinson*, in More Mathematical People, pp. 262–280, Academic Press, 1990; augmented version in: C. Reid, *JULIA. A life in mathematics*, The Mathematical Association of America, 1996.

[44] D. Richardson, *Some undecidable problems involving elementary functions of a real variable*, Journal of Symbolic Logic, **33**(4), pp. 514–520, 1968.

[45] J. Robinson, *Existential definability in arithmetic*, Transactions of the American Mathematical Society, **72**, pp. 437-449, 1952 (Reprinted in [46]).

[46] J. Robinson, *The collected works of Julia Robinson*, edited by S. Feferman, introduction by C. Reid. Collected Works 6, 1996, xliv+338pp. American Mathematical Society, Providence, RI.

[47] K. Ruohonen, *Hilbertin kymmenes probleema*, (Finnish), Arkhimedes, no. 1–2, pp. 71–100, 1972.

[48] B. Scarpellini, *Zwei unentscheidbare Probleme der Analysis.* Zeitschrift für Mathematische Logik und Grundlagen der Mathematik, **9**(4), pp. 265–289, 1963.

[49] J. C. Shepherdson and H. E. Sturgis, *Computability of recursive functions*, Journal of the ACM, **10**(2), pp. 217–255, 1963.

[50] M. F. Singer, *The model theory of ordered differential fields*, Journal of Symbolic Logic, **43**(1), pp. 82–91, 1978.

[51] C. Smoryński, *Logical number theory* I*: An Introduction*, Berlin, Springer-Verlag, 1991.

[52] A. Tarski, *A Decision Method for Elementary Algebra and Geometry*, University of California Press, Berkeley and Los Angeles, 1951.

[53] P. S. Wang, *The undecidability of the existence of zeros of real elementary functions*, Journal of the ACM, **21**(4), pp. 586–589, 1974.

[54] URL: `http://logic.pdmi.ras.ru/Hilbert10`.