Chapter 1 from the book

# HILBERT's TENTH PROBLEM

by Yuri Matiyasevich

Russian original was published by NAUKA Publishers
Moscow, 1993; ISBN 5-02-014356-X

English translation was published by the MIT Press
Cambridge, London, 1993; ISBN 0-262-13295-8

.

With kind permission from the MIT Press, the Foreword to the English translation, written by Martin Davis, English translation of the Preface and Chapters 1 and 5 of the book are put on the WWW site with URL

http://logic.pdmi.ras.ru/~yumat/H10Pbook

and mirrored on

http://www.informatik.uni-stuttgart.de/ifi/ti
/personen/Matiyasevich/H10Pbook

Updated Bibliography is available via URL

http://logic.pdmi.ras.ru/Hilbert10

# 1 Principal Definitions

In this chapter we introduce *Diophantine sets*, the main subject of study in this book, and we establish some of their simplest properties.

## 1.1 Diophantine equations as a decision problem

Let us recall that a *Diophantine equation* is an equation of the form

$$D(x_1, \ldots, x_m) = 0, \tag{1.1.1}$$

where $D$ is a polynomial with integer coefficients. In addition to (1.1.1), Diophantine equations can be written in the more general form

$$D_{\mathrm{L}}(x_1, \ldots, x_m) = D_{\mathrm{R}}(x_1, \ldots, x_m), \tag{1.1.2}$$

where $D_{\mathrm{L}}$ and $D_{\mathrm{R}}$ are again polynomials with integer coefficients. When we speak of "an arbitrary Diophantine equation," we shall have in mind an equation of the form (1.1.1) since an equation of the form (1.1.2) can easily be transformed into an equation of the form (1.1.1) by transposing all the terms to the left-hand side. However, we will often use the notation (1.1.2) for particular equations if this form turns out to be easier to grasp. We shall also take another advantage of the more general form (1.1.2); namely, in this case we can demand that $D_{\mathrm{L}}$ and $D_{\mathrm{R}}$ are polynomials with non-negative coefficients.

Diophantine equations typically have several unknowns, and we must distinguish the *degree of* (1.1.1) *with respect to a given unknown* $x_i$ and the (*total*) *degree of* (1.1.1), i.e., the maximum, over all the monomials constituting the polynomial $D$, of the sum of the degrees of the individual variables in such a monomial.

In specifying a Diophantine equation it is necessary to provide not only a representation of the form (1.1.1) (or equivalently (1.1.2)), but also to indicate the range of the unknowns. Hilbert, in his Tenth Problem, spoke of solutions *in rational integers*. In the present book we shall just use the term "*integers*" because the case of *algebraic integers* will be almost completely ignored. (The cases of other ranges for the unknowns will be considered in Sections 1.3, 7.3, and 7.4.)

Hilbert's Tenth Problem is an example of a *decision problem*. A decision problem consists of countably many *individual problems*, for each of which an answer "YES" or "NO" is to be given. We shall refer to these individual problems as *subproblems* of the corresponding decision problem. Each individual subproblem is specified by a finite amount of information. (In the case of Hilbert's Tenth Problem, this information is the polynomial $D$ from (1.1.1)).

---

The essence of a decision problem lies in the requirement to find a single method that can be used for obtaining the answer to any of the individual subproblems. Since Diophantus's time, number theorists have found solutions for many Diophantine equations and have established the unsolvability of many other equations. However, for many particular classes of equations, and even for certain individual equations, it was necessary to invent a specific method. In the Tenth Problem, Hilbert asked for a *universal* method for deciding the solvability of Diophantine equations.

A decision problem can be solved either directly or indirectly. In the the former case, one provides a procedure for finding the answer to any individual subproblem, while in the latter case one *reduces* the given decision problem to another, the solvability of which has already been shown. We will not give a formal definition of what constitutes such a reduction, because the general theory of reducibility will not be needed, and in each particular case of such a reduction it will be clear from the context what is actually meant.

An unsolvability proof for a decision problem can also be either direct or indirect. In the latter case one also reduces one problem to another, but what is required is a reduction in the reverse direction. Namely, to establish the unsolvability of a decision problem, one has to reduce *to it* another problem the unsolvability of which has already been shown. In the first few chapters of this book, we reduce to Hilbert's Tenth Problem successively more and more complicated problems. This chain of reductions should lead ultimately to a problem for which we can give a direct proof of unsolvability. However, to be able to give such a proof, we need some way of surveying all conceivable methods of solving the problem. The possibility of doing this became available only after the development of the mathematically rigorous general notion of computability. All the necessary definitions are given in Chapter 5, where we establish the algorithmic unsolvability of Hilbert's Tenth Problem.

## 1.2 Systems of Diophantine equations

Although Hilbert asked for a general method for deciding whether a single Diophantine equation does or does not have a solution, Diophantus had considered systems of equations as well. However, it easy to see that a positive solution of Hilbert's Tenth Problem would also give us a method for deciding whether a system of Diophantine equations does or does not have a solution. In fact, the system consisting of the $k$ equations

$$\begin{aligned} D_1(x_1, \ldots, x_m) &= 0 \\ &\vdots \\ D_k(x_1, \ldots, x_m) &= 0 \end{aligned} \tag{1.2.1}$$

has a solution in integers $x_1, \ldots, x_m$ if and only if the Diophantine equation

$$D_1^2(x_1, \ldots, x_m) + \cdots + D_k^2(x_1, \ldots, x_m) = 0 \tag{1.2.2}$$

has one. Moreover, the set of solutions of (1.2.1) coincides with the set of solutions of (1.2.2). Thus, for systems of Diophantine equations the number of equations is not such an essential characteristic as it is in the cases of linear algebraic or differential equations.

In what follows, we shall also use a transformation in the reverse direction, namely, the transformation of an equation

$$D(x_1, \ldots, x_m) = 0 \tag{1.2.3}$$

into the system of Diophantine equations

$$\begin{aligned} D_1(x_1, \ldots, x_m, y_1, \ldots, y_n) &= 0 \\ &\vdots \\ D_k(x_1, \ldots, x_m, y_1, \ldots, y_n) &= 0 \end{aligned} \tag{1.2.4}$$

that, in general, contains some additional unknowns $y_1, \ldots, y_n$. The operation of passing from (1.2.3) to (1.2.4) need not be inverse to that of passing from (1.2.1) to (1.2.2); i.e., if we compress the system (1.2.4) into a single equation in the manner described above we would not in general obtain the initial equation (1.2.3). The only relation between (1.2.3) and (1.2.4) that is of interest to us is that system (1.2.4) should have a solution if and only if equation (1.2.3) has one. We require neither that every solution of (1.2.3) could be expanded (by choosing values of $y_1, \ldots, y_n$) into a solution of (1.2.4), nor that every solution of (1.2.4) should include a solution of (1.2.3).

One possible reason for transforming an equation (1.2.3) into a system (1.2.4) could be to obtain a system consisting of very simple equations. For example, it is easy to see that any Diophantine equation can be transformed into an equivalent system (in the sense explained above) consisting of equations of the two forms

$$\alpha = \beta + \gamma \tag{1.2.5}$$

and

$$\alpha = \beta\gamma, \tag{1.2.6}$$

where $\alpha$, $\beta$, and $\gamma$ are either particular natural numbers or certain of the unknowns $x_1, \dots, x_m, y_1, \dots, y_n$. We proceed to explain how such a transformation is possible using the equation

$$4x^3y - 2x^2z^3 - 3y^2x + 5z = 0 \tag{1.2.7}$$

as an example. First of all we transpose the negative terms, obtaining the equation

$$4x^3y + 5z = 2x^2z^3 + 3y^2x. \tag{1.2.8}$$

Next we introduce 14 new unknowns and obtain the equivalent system

$$\begin{gathered} p_1 = 4x, \quad p_2 = p_1x, \quad p_3 = p_2x, \quad p_4 = p_3y; \\ q_1 = 5z; \\ r_1 = 2x, \quad r_2 = r_1x, \quad r_3 = r_2z, \quad r_4 = r_3z, \quad r_5 = r_4z; \\ s_1 = 3y, \quad s_2 = s_1y, \quad s_3 = s_2x; \\ t_1 = p_4 + q_1, \quad u_1 = r_5 + s_3, \quad t_1 = 1u_1. \end{gathered} \tag{1.2.9}$$

As an application of this simple transformation technique, let us
consider what would result if we first transform a Diophantine equation into an equivalent system (1.2.1) consisting of equations of the forms (1.2.5) and (1.2.6), and then compress this system into a single equation (1.2.2). Clearly, the initial equation has or hasn't a solution according as the resulting equation (1.2.2) has or hasn't one. However, the latter equation is of degree 4 regardless of the degree of the former. Thus, *to solve Hilbert's Tenth Problem positively, it would be sufficient to find a method for deciding whether a Diophantine equation of degree* 4 *has a solution.*

## 1.3 Solutions in natural numbers

In his Tenth Problem, Hilbert asked about solutions in integers. Sometimes an integer solution is evident. For example, the equation

$$(x+1)^3 + (y+1)^3 = (z+1)^3 \tag{1.3.1}$$

clearly has infinitely many solutions of the form $x = z$, $y = -1$. On the other hand, the fact that equation (1.3.1) has no solutions in non-negative $x$, $y$, and $z$

is not trivial at all. Thus, for a particular Diophantine equation, *the problem of deciding whether it has an integer solution* and *the problem of deciding whether it has a non-negative solution* are in general two separate problems.

On the other hand, let

$$D(x_1, \dots, x_m) = 0 \tag{1.3.2}$$

be an arbitrary Diophantine equation and suppose that we are looking for its non-negative solutions. Let us consider the following system:

$$\begin{aligned} D(x_1, \dots, x_m) &= 0 \\ x_1 &= y_{1,1}^2 + y_{1,2}^2 + y_{1,3}^2 + y_{1,4}^2 \\ &\vdots \\ x_m &= y_{m,1}^2 + y_{m,2}^2 + y_{m,3}^2 + y_{m,4}^2. \end{aligned} \tag{1.3.3}$$

Clearly, any solution of this system in *arbitrary* integers includes a solution of (1.3.2) in *non-negative* integers. The converse is true as well; namely, for any solution of (1.3.2) in non-negative integers $x_1, \dots, x_m$, there are integer values of $y_{1,1}, \dots, y_{m,4}$ giving a solution of (1.3.3), because every non-negative integer can be represented as the sum of the squares of four integers (see the Appendix). As we know from Section 1.2, the system (1.3.3) can be compressed into a single equation

$$E(x_1, \dots, x_m, y_{1,1}, \dots, y_{m,4}) = 0 \tag{1.3.4}$$

solvable in integers if and only if the original equation (1.3.2) is solvable in non-negative integers.

Thus, we have shown that the decision problem of determining the existence or non-existence of non-negative solutions is reducible to the decision problem of determining the existence or non-existence of integer solutions. Hence we have proved that to establish the unsolvability of Hilbert's Tenth Problem in its original form, it is sufficient to establish the unsolvability of its analog for non-negative solutions. For technical reasons, it is easier to work with non-negative solutions, and in the rest of the book lower-case italic Latin letters will denote non-negative integers unless the contrary is clearly stated. Following the tradition in mathematical logic, we will also speak of the non-negative integers as the *natural numbers*; thus in particular, we shall consider 0 to be a natural number.

Our further efforts will be directed towards establishing the unsolvability of the analog of Hilbert's Tenth Problem for natural number solutions. We shall reach this goal in Chapter 5. However, *a priori,* it is conceivable that this analog is solvable whereas the original problem is unsolvable. Let us check that in fact this cannot happen, i.e., that we lose essentially nothing by restricting the range of unknowns to natural numbers.

Let

$$D(\chi_1,\ldots,\chi_m)=0 \tag{1.3.5}$$

be an arbitrary Diophantine equation and suppose that now we are seeking its solutions in integers $\chi_1, \ldots, \chi_m$. Let us consider the equation

$$D(x_1-y_1,\ldots,x_m-y_m)=0. \tag{1.3.6}$$

Clearly, any solution of equation (1.3.6) (which, according to our agreement concerning lower-case Latin letters, consists of natural numbers $x_1, \ldots, x_m, y_1, \ldots, y_m$) generates a solution

$$\begin{aligned} \chi_1 &= x_1-y_1 \\ &\vdots \\ \chi_m &= x_m-y_m \end{aligned} \tag{1.3.7}$$

of equation (1.3.5) in integers $\chi_1, \ldots, \chi_m$. On the other hand, for any solution $\chi_1, \ldots, \chi_m$ of equation (1.3.5) one can find natural numbers $x_1, \ldots, x_m, y_1, \ldots, y_m$ satisfying (1.3.7) and hence giving a solution of equation (1.3.6).

Thus, we have also made a reduction in the opposite direction; i.e., we have shown that the problem of the existence of integer solutions is reducible to the problem of the existence of solutions in natural numbers. The two reductions show that these two problems are equivalent *as decision problems* although, as was discussed at the beginning of this section, for a particular equation the answer may well depend on the range of the unknowns.

## 1.4 Families of Diophantine equations

In addition to systems of Diophantine equations, number theory also studies families of Diophantine equations. By a *family of Diophantine equations*, we understand a relation of the form

$$D(a_1,\ldots,a_n,x_1,\ldots,x_m)=0 \tag{1.4.1}$$

where $D$ is a polynomial with integer coefficients with respect to all the variables $a_1, \dots, a_n, x_1, \dots, x_m$, separated into *parameters* $a_1, \dots, a_n$ and *unknowns* $x_1, \dots, x_m$. Fixing values of the parameters results in the particular Diophantine equations that comprise the family. A family of Diophantine equations is *not* an infinite *system* of equations because the unknowns need not satisfy all the equations simultaneously, as would be the case for a system. Families of Diophantine equations are also called *parametric equations*. For a parametric Diophantine equation, we must distinguish the *degree of the equation with respect to its unknowns* from the *degree of the equation with respect to all of its variables*.

For different values of the parameters, one can obtain equations that do have solutions as well as equations that do not. The parametric Diophantine equation (1.4.1) defines a set $\mathfrak{M}$ consisting of the $n$-tuples of values of the parameters $a_1, \dots, a_n$ for which there are values of the unknowns $x_1, \dots, x_m$ satisfying (1.4.1):

$$\langle a_1, \dots, a_n \rangle \in \mathfrak{M} \iff \exists x_1 \dots x_m \left[ D(a_1, \dots, a_n, x_1, \dots, x_m) = 0 \right]. \tag{1.4.2}$$

The number $n$ is called the *dimension* of the set $\mathfrak{M}$, and equivalence (1.4.2) is called a *Diophantine representation* of $\mathfrak{M}$; taking some liberty, one can speak of (1.4.1) as well as (1.4.2) as a Diophantine representation. Sets having Diophantine representations are also called *Diophantine*. Clearly, every Diophantine set has infinitely many Diophantine representations.

Diophantine sets are the main object of study of this book. In number theory an equation is usually the primary object and one looks for a description of the corresponding set in some other terms. We shall mainly deal with problems of the opposite kind: *A set of $n$-tuples of natural numbers is given. Is this set Diophantine? If it is, find a Diophantine representation for it.*

Sometimes it evident that a set is Diophantine, for example, the set of all even numbers. For other sets it need not be so evident, and in some cases it can be technically difficult to prove that a set is in fact Diophantine. As an example, we can mention the set of all prime numbers, which will be shown to be Diophantine in Section 3.4.

In addition to determining whether some particular sets are Diophantine, one might seek an alternative characterization of the class of Diophantine sets. Such a characterization in terms of the notions of computability theory will be given in Chapter 5, and this will permit us to obtain the negative solution of Hilbert's Tenth Problem.

---

In this chapter we shall establish some of the simplest properties of Diophantine sets and exhibit several examples of Diophantine sets important for the rest of the book.

It is easy to see that *the union of two Diophantine sets of the same dimension is also Diophantine*. In fact, if

$$D_1(a_1, \dots, a_n, x_1, \dots, x_{m_1}) = 0 \tag{1.4.3}$$

and

$$D_2(a_1, \dots, a_n, x_1, \dots, x_{m_2}) = 0 \tag{1.4.4}$$

are Diophantine representations of two sets, then the equation

$$D_1(a_1, \dots, a_n, x_1, \dots, x_{m_1}) \cdot D_2(a_1, \dots, a_n, x_1, \dots, x_{m_2}) = 0 \tag{1.4.5}$$

is a Diophantine representation of their union.

*The intersection of two Diophantine sets of the same dimension is Diophantine as well*; namely, it is defined by the equation

$$D_1^2(a_1, \dots, a_n, x_1, \dots, x_{m_1}) + D_2^2(a_1, \dots, a_n, y_1, \dots, y_{m_2}) = 0. \tag{1.4.6}$$

Note that we not only used the technique of Section 1.2 for combining the two equations (1.4.3) and (1.4.4) into a single equation, but we also first changed the unknowns in equation (1.4.4).

The complement of a Diophantine set of $n$-tuples of natural numbers (with respect to the set of all $n$-tuples of natural numbers) need not be Diophantine, but this fact is not trivial and will be proved only in Section 4.6.

In the definition of a Diophantine representation (1.4.2), no restrictions were imposed on the type of the corresponding equation (1.4.1). We know from Section 1.2 that we could require (1.4.1) to be an equation of degree 4. In what follows, we shall take advantage of another possibility for specializing the equation in a Diophantine representation of a set of natural numbers (i.e., in the case $n = 1$). Namely, it is easy to see that the equation

$$D(a, x_1, \dots, x_m) = 0 \tag{1.4.7}$$

has a solution in unknowns $x_1, \dots, x_m$ if and only if the equation

$$(x_0 + 1)(1 - D^2(x_0, \dots, x_m)) - 1 = a \tag{1.4.8}$$

has a solution in unknowns $x_0, \dots, x_m$. In fact, any solution of equation (1.4.7) can be expanded to a solution of (1.4.8) by putting $x_0 = a$; on the other hand, in any solution of equation (1.4.8) the factor $1 - D^2(x_0, \ldots, x_m)$ must be positive, which is possible only if $D(x_0, \ldots, x_m) = 0$. But then (1.4.8) implies that $x_0 = a$ and hence that the equality (1.4.7) also holds.

Thus, *a set of natural numbers is Diophantine if and only if it is the set of all natural number values assumed by some polynomial with integer coefficients for natural number values of its variables.*

## 1.5 Logical terminology

The entire contents of this book could be presented in terms of Diophantine sets, their unions and intersections, and the relation of set membership. However, it is often more convenient to use, instead of the language of sets, an essentially equivalent language of properties and relations. For example, instead of saying that the set of even numbers is Diophantine, one can say that the property *is an even number* is Diophantine. Similarly, instead of considering the set with the representation

$$(a_1 - a_2)^2 = x + 1, \tag{1.5.1}$$

one can say that the relation $\neq$ is Diophantine.

More formally, we say that a property $\mathcal{P}$ of natural numbers is a *Diophantine property* if the set of numbers having this property is Diophantine. Correspondingly, an equivalence of the form

$$\mathcal{P}(a) \iff \exists x_1 \ldots x_m [D(a, x_1, \ldots, x_m) = 0] \tag{1.5.2}$$

is called a *Diophantine representation of property* $\mathcal{P}$. Similarly, a relation $\mathcal{R}$ among $n$ natural numbers is called a *Diophantine relation* if the set of all $n$-tuples for which the relation holds is Diophantine. Correspondingly, an equivalence of the form

$$\mathcal{R}(a_1, \ldots, a_n) \iff \exists x_1 \ldots x_m [D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0] \tag{1.5.3}$$

is called a *Diophantine representation of relation* $\mathcal{R}$.

Instead of unions of sets, in this terminology one speaks of the logical connective "OR" (disjunction). In other words, if $\mathcal{R}_1$ and $\mathcal{R}_2$ are Diophantine relations (or properties) then the relation (or property) $\mathcal{R}$ such that for all $a_1, \ldots, a_n$

$$\mathcal{R}(a_1, \ldots, a_n) \iff \mathcal{R}_1(a_1, \ldots, a_n) \vee \mathcal{R}_2(a_1, \ldots, a_n) \tag{1.5.4}$$

is also Diophantine. To prove this formally, we should really begin with given Diophantine representations (1.4.3) and (1.4.4) of the relations $\mathcal{R}_1$ and $\mathcal{R}_2$, respectively, and construct from them a Diophantine representation (1.4.5) of the relation $\mathcal{R}$. However, we shall usually omit this step and confine ourselves to representations of the form (1.5.4). We can consider (1.5.4) to be a generalized Diophantine representation of the relation $\mathcal{R}$ provided that we have already shown that the relations $\mathcal{R}_1$ and $\mathcal{R}_2$ are Diophantine.

Similarly, intersection of sets has as its logical counterpart the connective "AND" (conjunction). So, an equivalence of the form

$$\mathcal{R}(a_1, \ldots, a_n) \iff \mathcal{R}_1(a_1, \ldots, a_n) \,\&\, \mathcal{R}_2(a_1, \ldots, a_n) \tag{1.5.5}$$

can be considered to be a generalized Diophantine representation of the relation $\mathcal{R}$ provided, of course, that we have shown that the relations $\mathcal{R}_1$ and $\mathcal{R}_2$ are Diophantine.

Clearly, we can go even further in this direction and regard any formula constructed from parametric Diophantine equations by using, in whatever order, disjunction, conjunction, and existential quantification as constituting a generalized Diophantine representation. Examples of such formulas will be given in the next section. When required, each generalized Diophantine representation can be transformed into the appropriate corresponding canonical form, (1.4.2), (1.5.2), or (1.5.3).

In simplifying proofs that certain sets are Diophantine, the following notion will often be helpful: A function is called a *Diophantine function* if its graph is a Diophantine set. Correspondingly, a *Diophantine representation of a function $F$* is an equivalence of the form

$$a = F(b_1, \ldots, b_n) \iff \exists x_1 \ldots x_m \, [D(a, b_1, \ldots, b_n, x_1, \ldots, x_m) = 0] \tag{1.5.6}$$

where $D$ is a polynomial with integer coefficients.

Now, along with Diophantine equations we can also treat equations of the form

$$P(\mathfrak{t}_1, \ldots, \mathfrak{t}_k) = 0 \tag{1.5.7}$$

where $P$ is a polynomial with integer coefficients and $\mathfrak{t}_1, \ldots, \mathfrak{t}_k$ are *Diophantine terms*, i.e., expressions constructed in the usual manner from particular natural numbers, variables, the symbols "+", "−", "·", and symbols for Diophantine functions. As when passing from (1.2.7) to (1.2.9), equation (1.5.7) can be transformed (at the expense of introducing new unknowns) into an equivalent system consisting of equations of the forms (1.2.5) and (1.2.6) and of the form

$$\alpha = F(\beta_1, \ldots, \beta_n) \tag{1.5.8}$$

where $F$ is a Diophantine function and $\alpha$ and $\beta_1, \ldots, \beta_n$ are variables or particular natural numbers. Furthermore, we can replace each equation of the form (1.5.8) by a copy of equation (1.5.6) with $a$ replaced by $\alpha$ and $b_1, \ldots, b_n$ replaced by $\beta_1, \ldots, \beta_n$ and also $x_1, \ldots, x_m$ replaced by some new variables that have not yet been used. The resulting system can then be compressed into a single equation equivalent to (1.5.7).

Also, we can permit the use of arbitrary Diophantine terms as arguments of Diophantine relations in generalized Diophantine representations. In fact, if $\mathcal{R}$ is a Diophantine relation, then the assertion

$$\mathcal{R}(\mathfrak{t}_1, \ldots, \mathfrak{t}_n) \tag{1.5.9}$$

is equivalent to the assertion

$$\exists t_1 \ldots t_n \, [\mathcal{R}(t_1, \ldots, t_n) \,\&\, t_1 = \mathfrak{t}_1 \,\&\, \ldots \,\&\, t_n = \mathfrak{t}_n]. \tag{1.5.10}$$

The first conjunctive term in (1.5.10) can be replaced by a copy of the equation from (1.5.3), and the remaining conjunctive terms can be dealt with as with (1.5.7) above.

A Diophantine function need not be defined for all possible values of its arguments. However, in adjoining equation (1.5.8), we impose the condition that $F$ is defined for $\beta_1, \ldots, \beta_n$. That is why, for example, the formula

$$F(a_1, \ldots, a_n) = 0 \vee F(a_1, \ldots, a_n) \neq 0 \tag{1.5.11}$$

is not a generalized Diophantine representation for the relation that is identically true unless $F$ is defined everywhere.

Note that the term "generalized Diophantine representation" should not be regarded as designating a well-defined mathematical concept; this is because such a representation reflects not only objective qualities of sets, properties, relations, or functions, but also the particular order in which we consider them. For example, we could first give for the property *is an even number* the Diophantine representation

$$\text{Even}(a) \iff \exists x \, [2x = a] \tag{1.5.12}$$

and then consider for the property *is an odd number* the generalized Diophantine representation

$$\text{Odd}(a) \iff \text{Even}(a + 1) \tag{1.5.13}$$

or, vice versa, we could first give for Odd the genuine Diophantine representation

$$\text{Odd}(a) \iff \exists x \, [2x + 1 = a] \tag{1.5.14}$$

and then consider the generalized Diophantine representation

$$\mathrm{Even}(a) \iff \mathrm{Odd}(a+1). \tag{1.5.15}$$

However, we cannot *simultaneously* consider both (1.5.13) and (1.5.15) as generalized Diophantine representations.

## 1.6 Some simple examples of Diophantine sets, properties, relations, and functions

Representation (1.5.1) proves that the relation $\neq$ is Diophantine. Similar proofs can be given for the inequalities $\leq$ and $<$:

$$a \leq b \iff \exists x\,[a + x = b], \tag{1.6.1}$$

$$a < b \iff \exists x\,[a + x + 1 = b]. \tag{1.6.2}$$

The relation of divisibility is also Diophantine:

$$a \mid b \iff \exists x\,[ax = b]. \tag{1.6.3}$$

This enables us to give the following generalized Diophantine representation for the function *remainder on dividing* $b$ *by* $c$, written $\mathrm{rem}(b, c)$:

$$a = \mathrm{rem}(b, c) \iff a < c \;\&\; c \mid b - a. \tag{1.6.4}$$

In Section 2.2 we shall need the function $\mathrm{arem}(b, c)$ whose value is the least absolute value $|\chi|$ among all numbers $\chi$ congruent to $b$ with respect to the modulus $c$:

$$\mathrm{arem}(b, c) \equiv \pm b \pmod{c} \;\&\; 0 \leq \mathrm{arem}(b, c) \leq c/2. \tag{1.6.5}$$

This function is also Diophantine:

$$a = \mathrm{arem}(b, c) \iff 2a \leq c \;\&\; [c \mid (b - a) \vee c \mid (b + a)]\,. \tag{1.6.6}$$

We shall also need the fact that the relation of non-divisibility is Diophantine:

$$a \nmid b \iff \mathrm{rem}(b, a) > 0. \tag{1.6.7}$$

Note that the relation $\nmid$ introduced in this way is not the negation of the relation of divisibility $\mid$ because according to (1.6.3) and (1.6.7) both relations are false when $a = 0$ and $b > 0$. This feature could easily be avoided, but in fact we shall use the relation $\nmid$ only in cases when it is certain that the first argument is not zero.

Having proved that rem is Diophantine, we can give a generalized Diophantine representation for the function *integer part of* $b/c$, written $b \operatorname{div} c$, namely,

$$a = b \operatorname{div} c \iff ac + \operatorname{rem}(b, c) = b \tag{1.6.8}$$

and a generalized Diophantine representation of congruence with respect to a positive modulus:

$$a \equiv b \pmod{c} \iff \operatorname{rem}(a, c) = \operatorname{rem}(b, c). \tag{1.6.9}$$

It is known that $\gcd(b, c)$, *the greatest common divisor of the positive integers* $b$ *and* $c$, can be represented in the form $bx - cy$, and clearly, every number of this form is divisible by $\gcd(b, c)$. Thus, we have the following generalized Diophantine representation for gcd:

$$a = \gcd(b, c) \iff bc > 0 \,\&\, a \mid b \,\&\, a \mid c \,\&\, \exists xy\,[a = bx - cy]. \tag{1.6.10}$$

In turn, gcd being Diophantine allows us to show that the function $\operatorname{lcm}(b, c)$, *the least common multiple of the positive integers* $b$ *and* $c$, is also:

$$a = \operatorname{lcm}(b, c) \iff bc = a \gcd(b, c). \tag{1.6.11}$$

## Exercises

1. In Section 1.3 we established the equivalence of two decision problems about solvability of Diophantine equations in integers and in natural numbers. Show that they are also equivalent to the analogous problem concerning solvability in positive integers.

2. Passing from equation (1.3.2) to system (1.3.3) results in a five-fold increase in the number of unknowns. We can eliminate the unknowns $x_1, \ldots, x_m$ using their explicit expression in terms of $y_{1,1}, \ldots, y_{m,4}$, which results in only a four-fold increase in the number of unknowns. Find another method resulting in an even smaller increase in the number of unknowns.

3. Passing from equation (1.3.5) to equation (1.3.6) doubles the number of unknowns. Show that the problem of the solvability of (1.3.5) in integers can be reduced to the problem of the solvability in natural numbers of some Diophantine equation with $m$ unknowns.

4. Equation (1.4.7) is equivalent to equation (1.4.8) only under our convention that the parameter $a$ and the unknowns are natural numbers. Show that a set of natural numbers is Diophantine if and only if it is the set of all natural numbers assumed by some polynomial with integer coefficients for arbitrary *integral* values of the variables.

5. It is easy to see that every finite set is Diophantine but that no finite set containing more than one element can be the set of *all* values assumed by some polynomial with integer coefficients for natural number (or arbitrary integer) values of the variables. For a less trivial example, show that no set that contains at least two elements and consists only of prime numbers can be represented in this form either, even if one considers the numbers $-2, -3, -5, \ldots$ to be prime. (It will be shown in Section 3.4 that the set of all prime numbers is Diophantine).

6. According to the previous exercise, there must be, among the values assumed by the polynomial from the left-hand side of (1.4.8), some negative integers in addition to the elements of the set defined by equation (1.4.7). Show that for every Diophantine set $\mathfrak{M}$ of natural numbers there is a polynomial with integer coefficients whose range (i.e., the set of *all* values that it assumes) is the union of the set $\mathfrak{M}$ and the set of all negative integers (the variables can be either natural numbers or arbitrary integers).

7. Show that for every Diophantine set $\mathfrak{M}$ of natural numbers there are polynomials $P$ and $Q$ with integer coefficients such that the set $\mathfrak{M}$ is exactly the set of *all integer* values assumed by the fraction

$$\frac{P(x_0, \ldots, x_m)}{Q(x_0, \ldots, x_m)}$$

for natural number values of the variables.

8. The special form of Diophantine representations of one-dimensional sets from Section 1.4 has different generalizations for the multidimensional case. Show that

(a) every $n$-dimensional Diophantine set $\mathfrak{M}$ has a representation of the form

$$D(x_1, \ldots, x_m) = A(a_1, \ldots, a_n)$$

where $A$ and $D$ are polynomials with integer coefficients;
(b) for every such set $\mathfrak{M}$ there are also polynomials $D_1, \ldots, D_n$ with integer

coefficients such that $\langle a_1, \dots, a_n \rangle \in \mathfrak{M}$ if and only if the system

$$D_1(x_1, \dots, x_m) = a_1$$
$$\vdots$$
$$D_n(x_1, \dots, x_m) = a_n$$

has a solution.

9. Show that every Diophantine function has a representation of the form

$$a = F(b_1, \dots, b_n) \iff \exists x_0 \dots x_m\, [a = E(b_1, \dots, b_n, x_0, \dots, x_m)]$$

where $E$ is a polynomial with integer coefficients.

10. Show that the following sets are Diophantine:

(a) the set of all composite numbers;
(b) the set of all numbers that are not powers of 2;
(c) the set of all numbers that are not perfect squares.

11. For a less trivial example, show that the relation *$a$ is not a power of $b$* is Diophantine.

12. Show that for every positive algebraic number $\chi$ the two-place relation *$p/q$ is a convergent of the continued fraction for $\chi$* is Diophantine.

13. Let a *trigonometric Diophantine equation* be an equation of the form

$$R\left(x_1, \dots, x_m, T_1\left(\frac{P_1(x_1, \dots, x_m)}{Q_1(x_1, \dots, x_m)}\pi\right), \dots, T_l\left(\frac{P_l(x_1, \dots, x_m)}{Q_l(x_1, \dots, x_m)}\pi\right)\right) = 0$$

where $P_1, \dots, P_l, Q_1, \dots, Q_l, R$ are polynomials with integer coefficients and $T_1, \dots, T_l$ are trigonometric functions. Show that the problem of testing for the existence of a solution of a trigonometric Diophantine equation is reducible to Hilbert's Tenth Problem.

14. Show that if $R(x_1, \dots, x_m)$ is a polynomial of degree $k$ with *real* coefficients that assumes only integral values when $x_1, \dots, x_m$ are natural numbers, then

$$R(x_1, \dots, x_m) = P\left(\binom{x_1}{1}, \dots, \binom{x_1}{k}, \dots, \binom{x_m}{1}, \dots, \binom{x_m}{k}\right)$$

for some polynomial $P$ with integer coefficients.

15. As was mentioned in Section 1.4, in the *general* case the complement of a Diophantine set need not be Diophantine. For the *special* case of a Diophantine set defined by an equation with one unknown, show that its complement is Diophantine.

## Unsolved problems

1. Can every Diophantine set be defined by an equation of degree 3 with respect to all its variables? With respect to all unknowns?

2. Is Hilbert's Tenth Problem reducible to its restriction to equations of degree 3?

3. Is the restriction of Hilbert's Tenth Problem to equations of degree 3 undecidable?

## Commentary

All of Diophantus's extant writings are available in English (Heath [1910]) and Russian (Diophantus [1974]) translations with commentaries.

Hilbert's Tenth Problem is the only decision problem among the twenty-three problems that Hilbert listed.

Number theorists did not show much interest in the inverse problem of finding for a set, property, or relation a Diophantine representation or proving the impossibility of such a representation. Problems of that kind are more typical for investigations in mathematical logic. From "The Autobiography of Julia Robinson" (see Reid [1986]), we know that in 1948 Alfred Tarski posed the problem of proving that the set of all powers of 2 is not Diophantine. For Julia Robinson [1952], this problem was the starting point for a systematic investigation to determine whether various particular sets are Diophantine. In this same period, Martin Davis [1953] analyzed the class of Diophantine sets as a whole. In particular, he showed that this class is closed under union and intersection but not under complementation. Also, he established the equivalence of Hilbert's Tenth Problem to its counterpart for solutions in natural numbers. Another paper from that period of pioneering investigations on Hilbert's Tenth Problem is Myhill [1953].

The special forms of Diophantine representations of one-dimensional sets from Section 1.4 and Exercises 1.4, 1.6, and 1.7 were proposed by Hilary Putnam [1960].

The general Diophantine equation was reduced to one of degree 4 by Skolem [1934]. Reduction of a general Diophantine equation to a system of Diophantine equations of degree 2 having a special form was considered by Britton [1979].

The problem of the algorithmic unsolvability of equations of degree 3 was stated in Davis, Matiyasevich, and Robinson [1976]. The three unsolved problems stated above are, of course, closely related to one another. Namely, a positive answer to the first implies a positive answer to the second, which in turn implies a positive answer to the third. However, the three problems are not equivalent; *a priori*, the answer to the first problem could turn out to be negative while the answer to the third was positive. For the counterparts of these three problems for the case of equations of degree 2, negative answers follow from Siegel [1972].