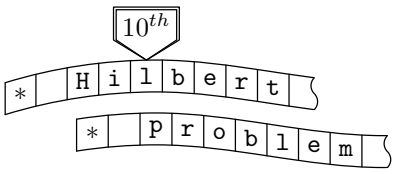


1

10^{th} Hilbert Problem

Yu. V. Matiyasevich, Ya. Abramov, A. Ya. Belov-Kanel, I. A. Ivanov-Pogodaev, A. S. Malistov

Equations both parts of which are polynomial functions with integer coefficients, and the solutions are to be expressed in integer numbers are quite common in mathemetics.

In 1900 David Hilbert [1900] delivered his famous lecture entitled "Mathematische Probleme" before the Second International Congress of Mathematicians. This paper contains 23 problems, or, more precisely, 23 groups of related problems, that the nineteenth century left for the twentieth century to solve. Problem number ten is about Diophantine equations:

> **10. Determination of the solvability of a Diophantine equation**
>
> *Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

Today we read the words "devise a process" to mean "find an algorithm." When Hilbert's Problems were posed, there was no mathematically rigorous general notion of algorithm available. The lack of such a notion was not in itself an obstacle to a positive solution of Hilbert's Tenth Problem, because for any particular algorithm it was always clear that it actually gave the desired general method for solving the corresponding problem.

During the 1930's, Kurt Godel, Alonzo Church, Alan Turing, and other logicians provided a rigorous formulation of the notion of computability; this made it possible to establish algorithmic unsolvability, i.e., the impossibility of the existence of an algorithm with certain properties. Soon afterwards the first examples of algorithmically unsolvable problems were found, first in mathematical logic itself and then in other branches of mathematics.

Computability theory produced all the necessary tools for tackling the unsolvability of Hilbert's Tenth Problem. The first in a series of papers in this direction appeared at the beginning of the 1950's. The continuing effort culminated in a "negative solution" of Hilbert's Tenth Problem in 1970 by Yury Matiyasevich.

We will follow that proof.

A. Diophantine Sets

We will seek only nonnegative integer solutions of the equations in this problem.

Consider an equality $D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$, where D is a polynomial with integer coefficients with respect to all the variables a_1, $\ldots$, a_n, x_1, $\ldots$, x_m. Suppose that the variables are separated into *parameters* $a_1, \ldots a_n$ and *unknowns* $x_1, \ldots x_m$.Fixing values of the parameters results in the particular Diophantine equations that comprise the family. (Note: we consider *integer* parameters and coefficients and seek *nonnegative integer* solutions).

For example, consider $D(a_1, a_2, x) = a_1x^2+a_2x$. The equations (for example) $x^2 = 0$, $2x^2+6x = 0$, $3x^2 - 17x = 0$ are in the family. In the first case we choose $a_1 = 1$, $a_2 = 0$. In the second case we do $a_1 = 2$, $a_2 = 6$, in the third case we do $a_1 = 3$, $a_2 = -17$.

The family of Diophantine equations $D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ deines a set M consisting of the n-tuples $(a_1, \ldots, a_n)$ of values of the parameters $a_1, \ldots, a_n$ for which there are values of the unknowns $x_1, \ldots x_m$ satisfying the equality $D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$. The number n is called

the dimension of the set M and equivalence $D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ is called a Diophantine representation of M. Sets having Diophantine representations are also called Diophantine.

The set of even numbers is Diophantine: the equation $2x = a$ has an integer solution if and only if a is even. Also, consider the set of pairs (a, b) such that a is odd and b is even and $b > 2$. To prove that this set is Diophantine we should consider the representation $2(2x + 1) = a^2(b^3 - 14)$.

♦ **A1.** *Prove that the following number sets are Diophantine:*
a) the set of even positive numbers;
b) the set of odd numbers;
c) the set of squares;
d) the set of cubes.

♦ **A2.** *Prove that any system of Diophantine equations are equivalent to some unique Diophantine equation. (i.e. the sets of solutions are the same.)*

♦ **A3.** *Prove that the union and intersection of two Diophantine sets of the same dimension is also Diophantine.*

♦ **A4.** *Suppose that the n-tuples set $\mathfrak{M}$ are Diophantine. Consider the m-tuples set $(a_1, \ldots, a_m)$ such that there exist $a_{m+1}, \ldots, a_n$ with $(a_1, \ldots, a_n) \in \mathfrak{M}$. Prove that this m-tuples set $(a_1, \ldots, a_m)$ is Diophantine.*

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 $(a_1 - a_2)^2 = x + 1$, one can say that the relation $\neq$ is Diophantine. More formally, we say that a property P of natural numbers is a Diophantine property if the set of numbers having this property is Diophantine. Correspondingly, an equivalence of the form $P(a) \Leftrightarrow \exists x_1 \ldots x_m[D(a, x_1, \ldots, x_m) = 0]$ is called a Diophantine representation of property P.

Similarly, a relation 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

$$R(a_1, \ldots, a_n) \Leftrightarrow \exists x_1 \ldots x_m[D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0]$$

is called a Diophantine representation of relation R.

At last, function $a = F(b_1, \ldots b_k)$ is called a Diophantine function if the set of all $k + 1$-tuples $[a, b_1, \ldots, b_k]$ for which the equality $a = F(b_1, \ldots b_k)$ holds is Diophantine.

♦ **A5.** *Prove that the following relations are Diophantine: a) "greater" relation $(a > b)$;*

b) "divisibility" relation (a divide b).

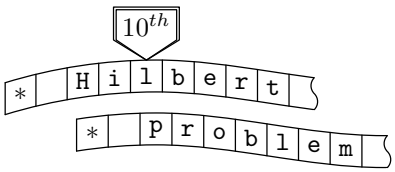
c) Consider the set of triples (a, b, c) such that a is a remainder of division b with c. (**notation: $\mathbf{a = b}$ (mod c)**) Prove that this set is Diophantine.

d) Consider the set of triples (a, b, c) such that $a = \min\{b \pmod c, (c - b) \pmod c\}$ (**notation: $\mathbf{a = b}$ (amod c)**) (This is the distance to the nearest integer number dividing by c.)

e) Prove that the set of triples (a, b, c) such that $a = \left[\frac{b}{c}\right]$ is Diophantine.

♦ **A6.** *Prove that the "relative primality" relation and GCD and LCM functions are Diophantine.*

♦ **A7.** *Prove that the following sets are Diophantine:*
a) the set of all integer numbers which are not squares;
b) the set of pairs (a, b) such that a is not power of b.



3

Pell equation

Definition. Equation $x^2 - dy^2 = 1, d \in \mathbb{N}$ is called *Pell Equation.*

♦ **A8.** *Pell Equation.*

a) Solution (x, y) is called *nontrivial*, if $y \neq 0$. Let d be a square. Prove that Pell equation has no nontrivial solution.

b) Let (u_1, v_1) and (u_2, v_2) be the solutions of the Pell equation $x^2 - dy^2 = 1$. So if $u_3 + \sqrt{d}v_3 = (u_1 + \sqrt{d}v_1) \cdot (u_2 + \sqrt{d}v_2)$ then (u_3, v_3) is solution too. In particular, if (x, y) is a solution then (x_n, y_n) is solution with $x_n + \sqrt{d}y_n = (x + \sqrt{d}y)^n$.

c) The solution is called *minimal* if it is nontrivial and $|x+y|$ is minimum. Prove that any solution is a minimal one in some degree.

It is known that for any d which is not a square some solution does exist. It is a hard problem so we do not include it into this list. You can find a proof e.g. in Bugayenko "Pell Equation"

♦ **A9.** *Special case of Pell equation.* a) $d = k^2 - 1 \Rightarrow (k, 1)$ *is a minimal solution.*

b) $d = k^2 - 1$, (x_1, y_1) is a minimal solution, $(x_n, y_n) = (x_1, y_1)^n$. Prove that $y_n \equiv n mod(k-1)$.

c) Another case of Pell equation. Find the solutions of $x^2 - (\frac{b^2}{4} - 1)y^2 = 1$.

Consider the following sequence: $\alpha_0(b) = 0$, $\alpha_1(b) = 1$, $\alpha_{n+2}(b) = b\alpha_{n+1}(b) - \alpha_n(b)$, $b \geqslant 2$.

♦ **A10.** *Prove that* $x^2 - bxy + y^2 = 1, x, y \geqslant 0$, *if and only if*

$$\begin{cases} x = \alpha_{m+1}(b) \\ y = \alpha_m(b) \end{cases} \quad or \quad \begin{cases} x = \alpha_m(b) \\ y = \alpha_{m+1}(b) \end{cases}$$

for some integer m.

♦ **A11.** *Prove that* $\alpha_n(2) = n$;

♦ **A12.** *Prove that* $\alpha_{k+l}(b) = \alpha_k(b) \cdot \alpha_{\ell+1}(b) - \alpha_{k-1}(b) \cdot \alpha_\ell(b)$.

♦ **A13.** *Prove that* $\alpha_n(b) \equiv \alpha_{n+4m}(b) \pmod{v}$, *where* $v = \alpha_{m+1}(b) - \alpha_{m-1}(b)$;

♦ **A14.** *Suppose that* $b_1 \equiv b_2 \pmod{q}$. *Prove that* $\alpha_n(b_1) \equiv \alpha_n(b_2) \pmod{q}$.

♦ **A15.** *Prove that* $2m$ *is the value of the number* k *such that for fixed* n *the following statement holds:* $\alpha_n(w) \pmod{v} = \alpha_{n+k}(w) \pmod{v}$, *where* $w \equiv b \pmod{v}$, $v = \alpha_{m+1}(b) - \alpha_{m-1}(b)$.

♦ **A16.** *Suppose that* $w \equiv b \pmod{v}$, $w \equiv 2 \pmod{u}$, *where* $v > 2\alpha_k(b)$, $u > 2k$. *Prove that the first* k *elements of the sequence*

$$\big(\alpha_0(b), 0\big), \ldots, \big(\alpha_n(b), n\big), \ldots$$

are coincide with the first k *elements of the sequence*

$$\Big(\alpha_0(w) \pmod{v}, \alpha_0(w) \pmod{u}\Big), \ldots, \Big(\alpha_n(w) \pmod{v}, \alpha_n(w) \pmod{u}\Big), \ldots$$

♦ **A17.** *Suppose that* $(\alpha_k(b))^2$ *divides* $\alpha_m(b)$. *Prove that* $\alpha_k(b)$ *divides* m.

♦ **A18.** *Prove that* $2\alpha_k(b) < u \Rightarrow 2k < u$.

♦ **A19.** *Prove that the set* $\{(a,\ b,\ c) \mid\ a = \alpha_c(b),\ b > 3\}$ *is Diophantine.*

♦ **A20.** *Prove that* $(k-1)^n \leqslant \alpha_{n+1}(k) \leqslant k^n$;

♦ **A21.** *Prove that* $(1+s)^n \geqslant 1 + ns \quad s \in \mathbb{R}$, $s > -1$, n — *nonnegative integer.*

♦ **A22.** *Prove that* $b^c = \lim_{n\to\infty} \frac{\alpha_{c+1}(bn+4)}{\alpha_{c+1}(n)}$.

♦ **A23.** *Prove that the set* $\big\{(a, b, c) \;\big|\; a = b^c\big\}$ *is Diophantine.*

B. Coding

Consider the following regulation of the natural numbers pairs:

$$\langle 0,0\rangle, \langle 0,1\rangle, \langle 1,0\rangle, \langle 0,2\rangle, \langle 1,1\rangle, \langle 2,0\rangle, \langle 0,3\rangle \dots$$

Note that the number of the pair $\langle a,b\rangle$ in this sequence can be represented in the polynomial form: $\mathbf{Cantor}(a,b) = ((a+b)^2+3a+b)/2$. The functions $\mathbf{ElemA}(c)$ and $\mathbf{ElemB}(c)$ which are represent the first and the second elements of the pair are also Diophantine:

$$a = \mathbf{ElemA}(c) \iff \exists y\colon [(a+y)^2+3a+y = 2c];$$

$$b = \mathbf{ElemB}(c) \iff \exists x\colon [(x+b)^2+3x+b = 2c]$$

This numeration can be easily generalized for triples, fours, etc. For example, we can assign:
$\mathbf{Cantor}_1(a_1) = a_1$, $\mathbf{Cantor}_{n+1}(a_1,\dots a_{n+1}) = \mathbf{Cantor}_n(a_1,\dots a_{n-1}, \mathbf{Cantor}(a_n, a_{n+1}))$

Further, the number $\mathbf{Cantor}_n(a_1,\dots a_n)$ is called *cantor number* of the tuple $\langle a_1,\dots a_n\rangle$. Let c be the cantor number of the n-tuple. Suppose that $\mathbf{Elem}_{n,m}(c)$ is the value of m-component of that n-tuple with number c. The function $\mathbf{Elem}_{n,m}(c)$ is Diophantine:

$$a = \mathbf{Elem}_{n,m}(c) \iff \exists x_1 \dots x_{m-1}x_{m+1}\dots x_n\colon [2^{2^n}\,\mathbf{Cantor}_n(x_1,\dots x_{m-1}, a, x_{m+1}\dots x_n) = 2^{2^n}c]$$

($\mathrm{Cantor_n}$ is not a polinomial with integer coefficients so we add 2^{2^n} factor.)

We should note that this numeration has one serious defect: if n and m are fixed then function $\mathbf{Elem}_{n,m}(c)$ is Diophantine. However, it is hard to prove that three arguments function $\mathbf{Elem}_{n,m}(c)$ is Diophantine. To deal with tuples with non fixed lenght we should use some different methods.

Positional Code

Suppose that $\langle a_1,\dots,a_n\rangle$ is a sequence of integer numbers (n-tuple). Let us choose $b > a_i$ for all i. Suppose that

$$a = a_n b^{n-1} + a_{n-1}b^{n-2} + \dots + a_1 b^0.$$

In other words, $a_1,\dots,a_n$ are the digits in the positional notation of a with base b. So, using the triple (a,b,n) we can restore the n-tuple $\langle a_1,\dots,a_n\rangle$. The triple (a,b,n) is called *positional code* of the n-tuple $\langle a_1,\dots,a_n\rangle$. $(0,b,0)$ is the positional code of the empty tuple. Note that there are some triples which are not codes of any tuple. But, we can easily prove that the relation "to be positionsal code" is Diophantine:

$$\mathbf{Code}(a,b,c) \iff \begin{cases} b \geqslant 2, \\ a < b^c. \end{cases}$$

♦ **B1.** *Prove that the set of qudruples (a,b,k,c), such that the pair (a,b) encode the sequence and c equals to the k-th member of this sequence.*

♦ **B2.** *a) Encode the sequence $c_i = \binom{n}{i}$ and show that the set of triples (c,m,n), such that $c = \binom{m}{n}$, is diophantine.*

b) Prove that $m! = \lim\limits_{n\to\infty} \dfrac{n^m}{\binom{n}{m}}$ and that the set of numbers, that are factorials, is diophantine.

♦ **B3.** *Prove that the set of prime numbers is diophantine.*

♦ **B4.** *Prove that equation $D(a, x_1, \ldots, x_m) = 0$ has a solution in variables of $x_1, \ldots, x_m$ if and only if then equation*

$$a = (x_0 + 1)(1 - D(x_0, x_1, \ldots, x_m)^2) - 1$$

has a solution in variables of $x_0, x_1, \ldots, x_m$.

♦ **B5.** *Prove that there exists such a polynomial with integer coefficients, such that the set of its positive values is the set of prime numbers.*

Further we will get the skill to unite two sequence into one, to compare their corresponding elements, to check if two triples encode the same sequence, — and all this by solving the corresponding diophantine equation.

♦ **B6.** (***Kummer theorem***) *a) Prove that the number k, such that $n!$ divides on p^k, but doesn't divide on p^{k+1}, equals*

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$$

b) Prove that the number l, such that $\binom{m+n}{n}$ divides on p^l, but doesn't divide on p^{l+1}, is equal to the number of carries over the next columns in p-positional sistem of countering, if we add together numbers m and n

♦ **B7.** *Consider the set of triples (a_1, a_2, p), where p is prime and pairs (a_1, p) and (a_2, p) encode the sequences such that for any k the k-th element of the first sequence not greater than the k-th element of the second sequence. Prove that this set is diophantine.*
Prompt. *What will you get, if you add together a_1 and $a_2 - a_1$?*

♦ **B8.** *Consider the set of quadruples (a, p, n, e), where p is prime and triple (a, p, n) encode the sequence, such that each element of this sequence not greater than e. Prove that this set is diophantine.*

♦ **B9.** *Let (a_1, b_1, n) and (a_2, b_2, n) encode the same sequence and $b_1 < b_2$. Prove that $a_1 \equiv a_2 \pmod{b_2 - b_1}$.*

♦ **B10.** *Let, in the proposes of the previous problem, $b_1^n < b_2 - b_1$. Prove that a_1 is defined uniquely by the numbers $a_2,\ b_1,\ b_2,\ n$.*

♦ **B11.** *Prove that the set of quadruples (a_1, b_1, a_2, b_2), such that (a_1, b_1) and (a_2, b_2) encode the same sequence, is diophantine.*

♦ **B12.** *Consider the set of quadruples (a_1, b_1, a_2, b_2), such that pairs (a_1, b_1) and (a_2, b_2) encode the sequences and for any k the k-th member of the first sequence not greater than the k-th member of the second sequence. Prove that this set is diophantine.*

♦ **B13.** *Consider the set of quadruples (a, b, n, e), where triple (a, b, n) encode the sequence, such that each element of this sequence not greater than e. Prove that this set is diophantine.*

♦ **B14.** *Consider the set of octoples $(A, B, a_1, b_1, n_1, a_2, b_2, n_2)$, such that the pair (A, B) encode the sequence, that can be constructed from the sequence, encodable by the triple (a_1, b_1, n_1), by continuing it by the sequence, encodable by the triple (a_2, b_2, n_2). Prove that this set is diophantine.*

♦ **B15.** *Show how to encode the sequences $p_1 + q_1,\ p_1 + q_2, \ldots,\ p_1 + q_m,\ p_2 + q_1,\ p_2 + q_2, \ldots,\ p_2 + + q_m, \ldots,\ p_n + q_m$ and $p_1 \cdot q_1,\ p_1 \cdot q_2, \ldots,\ p_1 \cdot q_m,\ p_2 \cdot q_1,\ p_2 \cdot q_2, \ldots,\ p_2 \cdot q_m, \ldots,\ p_n \cdot q_m$ by using the codes of $p_1, \ldots, p_n$ and $q_1, \ldots, q_m$.*