Hilbert's Tenth Question

KRIT BOONSIRISETH

June 24, 2019

Hilbert's tenth question asked if there is a general algorithm, which given a polynomial Diophantine equation, decides whether the equation has a solution with all unknowns taking integer values.

Matiyasevich's theorem states that any *recursively enumerable set* (sets S for which there is a Turing machine that halts iff the input is in S) is a *Diophantine set* (sets S for which there is a Diophantine equation that is solvable iff certain parameters are in S). This problem set is based on this idea: it is very easy to construct or *program* all sorts of sets in the medium of polynomials.

Further reading: Smith, Peter, "The MDRP Theorem," `https://www.logicmatters.net/resources/pdfs/MRDP.pdf`, 2011.

1. Show that there is a real polynomial $P \in \mathbb{R}[x, y]$ such that the image of P is the *open* interval $(0, \infty)$.

2. Show that for some n, there is a polynomial $P \in \mathbb{Z}[x_1, \ldots, x_n]$ such that $P(\mathbb{Z}^n) = \mathbb{Z}_{\geqslant 0}$. This basically makes Diophantine sets with respect to $\mathbb{Z}_{\geqslant 0}$ also ones with respect to $\mathbb{Z}$.

3. Show that for some n, there is a polynomial $P \in \mathbb{Z}[x_1, \ldots, x_n]$ such that $P(\mathbb{Z}^n) = \mathbb{Z} \setminus \{0\}$

4. Show that in fact $n = 2$ suffices.

5. Show that the set of non-square positive integers is Diophantine, that is, there is an integer n and a polynomial $P \in \mathbb{Z}[x, y_1, \ldots, y_n]$ such that for each integer $t \geqslant 0$, $P(x, y_1, \ldots, y_n) = 0$ has a solution $(y_1, \ldots, y_n) \in \mathbb{Z}^n_{\geqslant 0}$ iff t is not a perfect square.

6. (harazi; `https://artofproblemsolving.com/community/c6h28496`) Is there a polynomial f with possibly many variables such that the set of positive values that the polynomial takes when its variables are restricted to integer values is exactly the set of numbers of the form
$$\left(\frac{(1+\sqrt{2})^n + (1-\sqrt{2})^n}{2}\right)^2$$

7. Show that the set $\mathbb{Z}_{>0} - \{2^n\}$ is Diophantine.

† 8. (ELMO 2019) Carl chooses a *functional expression*[1] E which is a finite nonempty string formed from a set $x_1, x_2, \dots$ of variables and applications of a function f, together with addition, subtraction, multiplication (but not division), and fixed real constants. He then considers the equation $E = 0$, and lets S denote the set of functions $f\colon \mathbb{R} \to \mathbb{R}$ such that the equation holds for any choices of real numbers $x_1, x_2, \dots$. (For example, if Carl chooses the functional equation

$$f(2f(x_1) + x_2) - 2f(x_1) - x_2 = 0,$$

then S consists of one function, the identity function.)

(a) Let X denote the set of functions with domain $\mathbb{R}$ and image exactly $\mathbb{Z}$. Show that Carl can choose his functional equation such that S is nonempty but $S \subseteq X$.

(b) Can Carl choose his functional equation such that $|S| = 1$ and $S \subseteq X$?

†† 9. (USA TSTST 2015) A *Nim-style game* is defined as follows. Two positive integers k and n are specified, along with a finite set S of k-tuples of integers (not necessarily positive). At the start of the game, the k-tuple $(n, 0, 0, \dots, 0)$ is written on the blackboard.

A legal move consists of erasing the tuple $(a_1, a_2, \dots, a_k)$ which is written on the blackboard and replacing it with $(a_1+b_1, a_2+b_2, \dots, a_k+b_k)$, where $(b_1, b_2, \dots, b_k)$ is an element of the set S. Two players take turns making legal moves, and the first to write a negative integer loses. In the event that neither player is ever forced to write a negative integer, the game is a draw.

Prove that there is a choice of k and S with the following property: the first player has a winning strategy if n is a power of 2, and otherwise the second player has a winning strategy.

†† 10. The above, but the first player wins iff n is prime.[2]

[1] These can be defined formally in the following way: the set of functional expressions is the minimal one (by inclusion) such that (i) any fixed real constant is a functional expression, (ii) for any positive integer i, the variable x_i is a functional expression, and (iii) if V and W are functional expressions, then so are $f(V)$, $V + W$, $V - W$, and $V \cdot W$.

[2] As a *primer*, here's a polynomial which only attains prime values in $\mathbb{Z}_{>0}$: $(k+2)(1 - [wz+h+j-q]^2 - [(gk+2g+k+1)(h+j)+h-z]^2 - [16(k+1)^3(k+2)(n+1)^2+1-f^2]^2 - [2n+p+q+z-e]^2 - [e^3(e+2)(a+1)^2+1-o^2]^2 - [(a^2-1)y^2+1-x^2]^2 - [16r^2y^4(a^2-1)+1-u^2]^2 - [n+\ell+v-y]^2 - [(a^2-1)\ell^2+1-m^2]^2 - [ai+k+1-\ell-i]^2 - [((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2 - [p+\ell(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2 - [q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2 - [z+p\ell(a-p)+t(2ap-p^2-1)-pm]^2)$