A polynomial encoding provability in pure mathematics (outline of an explicit construction)

M. Carl B.Z. Moroz

To professor G.E. Mints on his seventieth birthday

1. Let V be an algebraic variety defined over $\mathbb{Z}$, the ring of rational integers. The study of the structure of the set $V(\mathbb{Z})$ of the integral points of such a variety is one of the major goals in number theory and arithmetic geometry. One may ask, in particular, whether $V(\mathbb{Z})$ is an empty or a finite set. It is an easy and well-known corollary of the celebrated theorem of Matiyasevich [11] that, in a given formal system, neither statement can be proved or disproved for infinitely many varieties V (cf. [11] - [13], [4, pp. 327-328], [5]). For instance, there is a hypersurface V over $\mathbb{Z}$ such that neither the assertion

$$V(\mathbb{Z}) = \emptyset, \tag{1}$$

nor its negation is provable in, say, the Zermelo-Fraenkel set theory (=:ZF).

Given a recursively enumerable subset S of the set $\mathbb{N}$ of the positive rational integers, Matiyasevich's construction allows, in principle, to write down a polynomial $P_S(t, \vec{x})$, $\vec{x} := (x_1, \dots, x_{n(S)})$, with integral rational coefficients such that, for $a \in \mathbb{N}$, the Diophantine equation $P_S(a, \vec{x}) = 0$ is soluble in $\mathbb{Z}^{n(S)}$ if and only if $a \in S$. The set T of the (ZF-)provable mathematical theorems is recursively enumerable. Therefore, given a suitable numbering $\mathcal{N}$ of the set of the well-defined mathematical assertions, one can construct a polynomial $F(t, \vec{x})(:= P_{\mathcal{N}(T)}(t, \vec{x}))$ such that the Diophantine equation $F(a, \vec{x}) = 0$ is soluble if and only if $a \in \mathcal{N}(T)$. In this sense, the arithmetic of the affine hypersurface, defined by the equation

Received by the editors April 2012.
Communicated by A. Weiermann.
2010 *Mathematics Subject Classification* : 11D72, 11G35, 11U05, 03E55.
Key words and phrases : Matiyasevich's theorem, Diophantine coding, Gödel-Bernays set theory.