On a Diophantine representation of the predicate of provability.

M. Carl and B.Z. Moroz

§1. Introduction.

By a well-known theorem of Matiyasevich [8], [9], a recursively enumerable set is Diophantine (and therefore there is no algorithm deciding whether a given Diophantine equation is soluble in $\mathbb{Z}$). Moreover, given a recursively enumerable set S, one can actually construct a polynomial $P_S(t, \vec{x})$ in $\mathbb{Z}[t, \vec{x}]$ such that

$$S = \{a \mid a \in \mathbb{N},\ \exists\, \vec{b}\ (\vec{b} \in \mathbb{Z}^n\ \&\ P_S(a, \vec{b}) = 0)\}.$$

The set of the theorems of a formalised mathematical theory, say $\mathcal{T}$, being recursively enumerable, is Diophantine (cf. [3, pp. 327-328]); therefore one can construct a polynomial $F_{\mathcal{T}}(t, \vec{x})$ in $Z[t, \vec{x}]$ such that the Diophantine equation

$$F_{\mathcal{T}}(a, \vec{x}) = 0$$

is soluble in $\mathbb{Z}$ if and only if $a = \mathcal{N}(\mathfrak{A})$ for a formula $\mathfrak{A}$ provable in $\mathcal{T}$, where

$$\mathcal{N} \colon \mathfrak{F} \to \mathbb{N}$$

is a suitable numbering of the set $\mathfrak{F}$ of the well-formed formulae of $\mathcal{T}$. Let $\mathcal{P}$ be the predicate calculus with a single binary predicate letter (and no function letters or individual constants). The goal of this work is to write down explicitly a polynomial $F_{\mathcal{P}}(t, \vec{x})$ as above. By Kalmár's theorem [7] (cf. also [12, p. 223]), analysis of provability in any pure predicate calculus can be reduced to studying provability in $\mathcal{P}$. Moreover, the Gödel-Bernays set theory, to be denoted by $\mathfrak{S}$, is finitely axiomatisable in $\mathcal{P}$ [5], [12, Ch.4]; therefore, loosely speaking, one may say that the polynomial $F_{\mathcal{P}}(t, \vec{x})$ encodes the content of pure mathematics (as formalised in $\mathfrak{S}$). On denoting by $\mathfrak{A}$ the conjunction of the proper (non-logical) axioms of $\mathfrak{S}$ and letting

$$b = \mathcal{N}(\mathfrak{A} \supset \mathfrak{B})$$

for some (obviously) false in $\mathfrak{S}$ formula $\mathfrak{B}$, one obtains a Diophantine equation

$$F_{\mathcal{P}}(b, \vec{x}) = 0, \tag{1}$$

whose insolubility is equivalent to the consistency of $\mathfrak{S}$. Thus to prove that equation (1) has no solutions in $\mathbb{Z}$, one has to employ an additional axiom, for instance, the axiom asserting existence of an inaccessible ordinal (cf. [4], where some combinatorial statements have been constructed, whose provability depends on that axiom).

In Section 2, we describe the language of $\mathcal{P}$, define a numbering

$$\mathcal{N}\colon \mathcal{P} \to \mathbb{N},$$

and give a Diophantine description of three groups of axioms of $\mathcal{P}$. After recalling the necessary preliminaries on Diophantine coding and proving a few technical lemmata, we complete our Diophantine description of the axioms and the rules of inference of $\mathcal{P}$. Finally, in Section 6, we shall write down a polynomial $F_{\mathcal{P}}(t, \vec{x})$, encoding the predicate of provability in $\mathcal{P}$.

Notation and conventions. As usual, $\mathbb{R}, \mathbb{Z}$, and $\mathbb{N}$ stand for the field of real numbers, the ring of rational integers, and the monoid of positive rational integers respectively. A finite sequence of symbols is denoted by $\vec{x}$ and $L(\vec{x})$ stands for its length (we write, for instance, $\vec{x} := (y_1, \ldots, y_n)$ and $L(\vec{x}) = n$); let

$$\vec{x} * \vec{y} := (a_1, \ldots, a_n, b_1, \ldots, b_m)$$

stand for the concatenation of the sequences

$$\vec{x} := (a_1, \ldots, a_n) \text{ and } \vec{y} := (b_1, \ldots, b_m).$$

The polynomial

$$p(x_1, x_2) = \frac{(x_1 + x_2 - 2)(x_1 + x_2 - 1)}{2} + x_2$$

defines a bijection

$$p\colon \mathbb{N}^2 \to \mathbb{N},\ p\colon \vec{a} \mapsto p(\vec{a}) \text{ for } \vec{a} \in \mathbb{N}^2;$$

moreover,

$$p(\vec{a}) \geq \max\{a_1, a_2\} \text{ for } \vec{a} \in \mathbb{N}^2$$

(cf. [2, p. 237]). Given an arithmetical formula $\mathfrak{A}$, let

$$(\forall j \leq n)\, \mathfrak{A} := \forall j\ ((j \in \mathbb{N}\ \&\ j \leq n) \ \Rightarrow\ \mathfrak{A}).$$

For $\vec{a} \in \mathbb{R}^n,\ \vec{a} := (a_1, \ldots, a_n)$, let

$$\vec{a}^{\,2} := \sum_{i=1}^{n} a_i^2 \text{ and } |\vec{a}| := \max\{|a_j| \mid 1 \leq j \leq n\}.$$

§2. The predicate calculus $\mathcal{P}$.

The predicate calculus $\mathcal{P}$ is a first order theory. The alphabet of its language consists of the set

$$\mathcal{X} := \{t_i \mid i \in \mathbb{N}\}$$

of individual variables, the binary predicate letter ϵ, the logical connectives: $\{\neg,\ \supset\}$ ("negation" and "implication"), the universal quantifier $\forall$, and the parentheses $\{(,\ )\}$. The set $\mathfrak{F}$ of the formulae of $\mathcal{P}$ is defined inductively. An expression of the form $(x \mathrel{\epsilon} y)$, with $\{x,\ y\} \subset \mathcal{X}$, is a(n elementary) formula; if $\mathfrak{A}$ and $\mathfrak{B}$ are formulae, then $\neg\,\mathfrak{A}$, $(\mathfrak{A} \supset \mathfrak{B})$, and $\forall x\, \mathfrak{A}$ are formulae.

Let us define inductively two functions

$$n\colon \mathfrak{F} \to \mathbb{N},\ m\colon \mathfrak{F} \to \mathbb{N},$$

and let $\mathcal{N}(\mathfrak{A}) := p(n(\mathfrak{A}),\ m(\mathfrak{A}))$.

Definition. Let

$$n(t_i \mathrel{\epsilon} t_j) = p(i,j),\ m(t_i \mathrel{\epsilon} t_j) = 1$$

for $\{i,\ j\} \subseteq \mathbb{N}$. For $\{\mathfrak{A},\ \mathfrak{B}\} \subseteq \mathfrak{F}$ and $i \in \mathbb{N}$, let

$$n(\neg\,\mathfrak{A}) = 3n(\mathfrak{A}) - 2,\ m(\neg\,\mathfrak{A}) = m(\mathfrak{A}) + 1,$$

$$n(\mathfrak{A} \supset \mathfrak{B}) = 3p(n(\mathfrak{A}), n(\mathfrak{B})),\ m(\mathfrak{A} \supset \mathfrak{B}) = p(m(\mathfrak{A}), m(\mathfrak{B})) + 1,$$

and

$$n(\forall t_i\, \mathfrak{A}) = 3p(i, n(\mathfrak{A})) - 1,\ m(\forall t_i\, \mathfrak{A}) = m(\mathfrak{A}) + 1.$$

Proposition 1. *The map $\mathcal{N}\colon \mathfrak{F} \to \mathbb{N}$ is a bijection.*

Proof. It is clear that $m(\mathfrak{F}) = \mathbb{N}$. For $l \in \mathbb{N}$, let

$$\mathfrak{F}_l := \{\mathfrak{A} \mid \mathfrak{A} \in \mathfrak{F},\ m(\mathfrak{A}) = l\}.$$

We shall prove, by induction on l, that the map $n\colon \mathfrak{F}_l \to \mathbb{N}$ is a bijection. It then follows that the maps $(n,m)\colon \mathfrak{F} \to \mathbb{N}^2$ and $\mathcal{N}(= p \circ (n,m))$ are also bijective. Since

$$\mathfrak{F}_1 := \{(t_i \mathrel{\epsilon} t_j) \mid \{i,\ j\} \subseteq \mathbb{N}\},$$

for $l = 1$, the assertion follows from the properties of the map p. Let $l > 1$; we prove that $n(\mathfrak{F}_l) = \mathbb{N}$, the injectivety of n being proved by a similar argument. Let $k \in \mathbb{N}$; we have to find a formula $\mathfrak{A}$ in $\mathfrak{F}$ with $n(\mathfrak{A}) = k$. For

$k=3k_1-2,\ k_1\in\mathbb{N}$, one can find, by the inductive supposition, a (unique) formula $\mathfrak{A}$ with $n(\mathfrak{A})=k_1,\ m(\mathfrak{A})=l-1,\ \mathfrak{A}\in\mathfrak{F}$; then $n(\neg\,\mathfrak{A})=k$. If $k=3k_1-1,\ k_1\in\mathbb{N}$, let $k_1=p(i,j)$ with $\{i,\ j\}\subseteq\mathbb{N}$; by the inductive supposition, there is a (unique) formula $\mathfrak{A}$ in $\mathfrak{F}_{l-1}$ with $n(\mathfrak{A})=j$. Then $m(\forall t_i\ \mathfrak{A})=l$ and $n(\forall t_i\ \mathfrak{A})=k$. Finally, for $k=3k_1,\ k_1\in\mathbb{N}$, let $l=p(i,j)+1$. By the inductive supposition, there are (uniquely determined) formulae $\mathfrak{A}_1$ and $\mathfrak{A}_2$ such that

$$\mathfrak{A}_1\in\mathfrak{F}_i,\ \mathfrak{A}_2\in\mathfrak{F}_j,\ n(\mathfrak{A}_1)=i',\ n(\mathfrak{A}_2)=j',\ p(i',j')=k_1;$$

then $m(\mathfrak{A}\supset\mathfrak{B})=l$ and $n(\mathfrak{A}\supset\mathfrak{B})=k$. Thus $n(\mathfrak{F}_l)=\mathbb{N}$, as claimed.

Notation. For $\mathfrak{A}\in\mathfrak{F}$ and $\{x,\ y\}\subset\mathcal{X}$, let $[\mathfrak{A}]_f$ and $\mathfrak{A}[x|y]$ stand for the set of the free variables of $\mathfrak{A}$ and the formula obtained from $\mathfrak{A}$ on replacing each of the free occurences of the variable x in $\mathfrak{A}$ by y.

Definition. Let $\mathfrak{A}\in\mathfrak{F}$; *the variable y is free for x in* $\mathfrak{A}$, if the variable x does not occur in $\mathfrak{A}$ in the scope of a quantifier $\forall y$.

There are five groups of axioms in $\mathcal{P}$ (cf. [12, pp. 69-70]):

$$\mathcal{A}_1:=\{\mathfrak{A}\supset(\mathfrak{B}\supset\mathfrak{A})\mid\{\mathfrak{A},\ \mathfrak{B}\}\subseteq\mathfrak{F}\};$$

$$\mathcal{A}_2:=\{(\mathfrak{A}\supset(\mathfrak{B}\supset\mathfrak{C}))\supset((\mathfrak{A}\supset\mathfrak{B})\supset(\mathfrak{A}\supset\mathfrak{C}))\mid\{\mathfrak{A},\ \mathfrak{B},\ \mathfrak{C}\}\subseteq\mathfrak{F}\};$$

$$\mathcal{A}_3:=\{(\neg\,\mathfrak{B}\supset\neg\,\mathfrak{A})\supset((\neg\,\mathfrak{B}\supset\mathfrak{A})\supset\mathfrak{B})\mid\{\mathfrak{A},\ \mathfrak{B}\}\subseteq\mathfrak{F}\};$$

$$\mathcal{A}_4:=\{\forall x\ (\mathfrak{A}\supset\mathfrak{B})\supset(\mathfrak{A}\supset\forall x\ \mathfrak{B})\mid\{\mathfrak{A},\ \mathfrak{B}\}\subseteq\mathfrak{F},\ x\in\mathcal{X}\setminus[\mathfrak{A}]_f\};$$

$$\mathcal{A}_5:=\{\forall x\ \mathfrak{A}\supset\mathfrak{A}[x|y]\mid\mathfrak{A}\in\mathfrak{F},\ \{x,\ y\}\subseteq\mathcal{X},$$

$$\text{the variable } y \text{ is free for } x \text{ in } \mathfrak{A}\}.$$

The set $\mathfrak{T}$ of the theorems of $\mathcal{P}$ is defined inductively:

($\mathcal{B}_0$) $\cup_{j=1}^{5}\mathcal{A}_j\subseteq\mathfrak{T}$.

($\mathcal{B}_1$) If $\{\mathfrak{A},\ (\mathfrak{A}\supset\mathfrak{B})\}\subseteq\mathfrak{T}$, then $\mathfrak{B}\in\mathfrak{T}$ ("modus ponens").

($\mathcal{B}_2$) If $\mathfrak{A}\in\mathfrak{T}$, then $\forall x\ \mathfrak{A}\in\mathfrak{T}$ ("generalisation").

In what follows, we shall construct a polynomial $F(t,\vec{x})$ in $Z[t,\vec{x}]$ such that

$$\mathcal{N}(\mathfrak{T})=\{a\mid a\in\mathbb{N},\ \exists\,\vec{b}\ (\vec{b}\in\mathbb{Z}^{L(\vec{x})}\ \&\ F(a,\vec{b})=0)\}.$$

Our first task is to give a Diophantine description of the predicate "$\mathfrak{A}$ is an axiom of $\mathcal{P}$"; in this section, we describe that predicate for the first three groups of the axioms.

Proposition 2. *Let* $g_1(u,\vec{x}) :=$

$(u - p(x_1,x_2))^2 + (x_1 - 3p(x_3, 3p(x_4,x_3)))^2 + (x_2 - p(x_5, p(x_6,x_5)+1) - 1)^2$

with $\vec{x} := (x_1,\ldots,x_6)$. *Then*

$$\mathcal{N}(\mathcal{A}_1) = \{u \mid \exists\,\vec{b}\,(\vec{b} \in \mathbb{N}^6 \;\&\; g_1(u,\vec{b}) = 0)\}.$$

Proof. Let

$$\mathfrak{C} := (\mathfrak{A} \supset (\mathfrak{B} \supset \mathfrak{A})),\ n(\mathfrak{A}) = x_3, n(\mathfrak{B}) = x_4, m(\mathfrak{A}) = x_5, m(\mathfrak{B}) = x_6.$$

Then $n(\mathfrak{B} \supset \mathfrak{A}) = 3p(x_4,x_3)$ and $m(\mathfrak{B} \supset \mathfrak{A}) = p(x_6,x_5)+1$. Since $n(\mathfrak{C}) = 3p(n(\mathfrak{A}), n(\mathfrak{B} \supset \mathfrak{A}))$ and $m(\mathfrak{C}) = p(m(\mathfrak{A}), m(\mathfrak{B} \supset \mathfrak{A})) + 1$, equation $g_1(u,\vec{x}) = 0$ asserts that $\mathcal{N}(\mathfrak{C}) = u$. This proves the proposition.

Proposition 3. *Let* $g_2(u,\vec{x}) :=$

$$(u - p(x_1,x_2))^2 + (x_1 - 3p(q_1(\vec{x}), q_2(\vec{x})))^2 + (x_2 - p(q_3(\vec{x}), q_4(\vec{x})) - 1)^2,$$

where

$$q_1(\vec{x}) := 3p(x_3, 3p(x_4,x_5)), q_4(\vec{x}) := 1 + p(1 + p(x_6,x_7), 1 + p(x_6,x_8))$$

$$q_2(\vec{x}) := 3p(p(x_3,x_4), 3p(x_3,x_5)), q_3(\vec{x}) := 1 + p(x_6, 1 + p(x_7,x_8)),$$

and $\vec{x} := (x_1,\ldots,x_8)$. *Then*

$$\mathcal{N}(\mathcal{A}_2) = \{u \mid \exists\,\vec{b}\,(\vec{b} \in \mathbb{N}^6 \;\&\; g_2(u,\vec{b}) = 0)\}.$$

Proof. Let

$$\mathfrak{D} := ((\mathfrak{A} \supset (\mathfrak{B} \supset \mathfrak{C})) \supset ((\mathfrak{A} \supset \mathfrak{B}) \supset (\mathfrak{A} \supset \mathfrak{C}))),\ n(\mathfrak{D}) = x_1, m(\mathfrak{D}) = x_2;$$

$$n(\mathfrak{A}) = x_3, n(\mathfrak{B}) = x_4, n(\mathfrak{C}) = x_5, m(\mathfrak{A}) = x_6, m(\mathfrak{B}) = x_7, m(\mathfrak{B}) = x_8.$$

An easy calculation shows that, in these notations, $g_2(u,\vec{x}) = 0$ if and only if $\mathcal{N}(\mathfrak{D}) = u$. This proves the proposition.

Proposition 4. *Let* $g_3(u,\vec{x}) :=$

$$(u - p(x_1,x_2))^2 + (x_1 - 3p(q_1(\vec{x}), q_2(\vec{x})))^2 + (x_2 - p(q_3(\vec{x}), q_4(\vec{x})) - 1)^2,$$

where

$$q_1(\vec{x}) := 3p(3x_4 - 2, 3x_3 - 2), q_2(\vec{x}) := 3p(3p(3x_4 - 2, x_3), x_4),$$

$$q_3(\vec{x}) := 1 + p(x_6 + 1, x_5 + 1), q_4(\vec{x}) := 1 + p(1 + p(x_6 + 1, x_5), x_6),$$

and $\vec{x} := (x_1,\ldots,x_6)$. *Then*

$$\mathcal{N}(\mathcal{A}_3) = \{u \mid \exists\,\vec{b}\,(\vec{b} \in \mathbb{N}^6 \;\&\; g_3(u,\vec{b}) = 0)\}.$$

Proof. Let

$$\mathfrak{C} := ((\neg\,\mathfrak{B} \supset \neg\,\mathfrak{A}) \supset ((\neg\,\mathfrak{B} \supset \mathfrak{A}) \supset \mathfrak{B})),\ n(\mathfrak{C}) = x_1, m(\mathfrak{C}) = x_2;$$

$$n(\mathfrak{A}) = x_3, n(\mathfrak{B}) = x_4, m(\mathfrak{A}) = x_5, m(\mathfrak{B}) = x_6.$$

Then equation $g_3(u, \vec{x}) = 0$ is easily seen to assert that $\mathcal{N}(\mathfrak{C}) = u$.

To give a Diophantine description of the sets of axioms $\mathcal{N}(\mathcal{A}_4)$ and $\mathcal{N}(\mathcal{A}_5)$, we shall make use of the techniques developed in the works relating to the tenth Hilbert problem, cf. [10] and references therein.

§3. On Diophantine coding.

In this section, following [2] (see also [10]), we state a few lemmata about Diophantine coding.

Lemma 1. *Let $f(t, \vec{x}) \in \mathbb{Z}[t, \vec{x}]$ with $L(\vec{x}) = n$ and suppose that*

$$S = \{a \mid a \in \mathbb{N},\ \exists\, \vec{b}\ (\vec{b} \in \mathbb{N}^n\ \&\ f(a, \vec{b}) = 0)\}.$$

Then

$$S = \{a \mid a \in \mathbb{N},\ \exists\, \vec{b}\ (\vec{b} \in \mathbb{Z}^{4n}\ \&\ g(a, \vec{b}) = 0)\},$$

where

$$g(t, \vec{y}) := f(t, \vec{z}),\ \vec{z} := (z_1, \ldots, z_n),\ z_j := \sum_{i=1}^{4} y_{ji}^2,\ 1 \le j \le n.$$

Proof. See, for instance, [10, pp. 4-6].

Lemma 2. *Let $f_3(m, n, k; \vec{x}) :=$*

$$(x_1^2 - (x_2^2 - 1)x_3^2 - 1)^2 + (x_4^2 - (x_2^2 - 1)x_5^2 - 1)^2 + (x_6^2 - (x_7^2 - 1)x_8^2 - 1)^2 +$$
$$(x_5 - x_9 x_3^2)^2 + (x_7 - 1 - x_{10} x_3)^2 + (x_7 - x_2 - x_{11} x_4)^2 + (x_6 - x_1 - x_{12} x_4)^2 +$$
$$(x_8 - k - 4(x_{13} - 1)x_3)^2 + (x_3 - k - x_{14} + 1)^2 + (x_{17} - n - x_{18})^2 + (x_{17} - k - x_{19})^2 +$$
$$((x_1 - x_3(x_2 - n) - m)^2 + (x_{15} - 1)^2 (2x_2 n - n^2 - 1)^2)^2 +$$
$$(m + x_{16} - 2x_2\, n + n^2 + 1)^2 + (x_2^2 - (x_{17}^2 - 1)(x_{17} - 1)^2 x_{20}^2 - 1)^2,$$

where $\vec{x} := (x_1, \ldots, x_{20})$. Then $m = n^k$ if and only if

$$\exists\, \vec{a}\ (\vec{a} \in \mathbb{N}^{20}\ \&\ f_3(m, n, k; \vec{a}) = 0).$$

Proof. See [2, pp. 244-248].

Lemma 3. *Let* $f_4(m, n, k; \vec{x}) :=$

$$f_3(x_1, 2, n; \vec{x}^{(1)}) + f_3(x_5, x_4, n; \vec{x}^{(2)}) + f_3(x_6, x_3, k; \vec{x}^{(3)}) +$$

$$(x_1 + x_2 - x_3)^2 + (x_4 - x_3 - 1)^2 + (x_6 x_7 + x_8 - x_5)^2 +$$

$$(x_5 + x_9 - (x_7 + 1)x_6)^2 + (x_7 - m - (x_{10} - 1)x_3)^2 + (m + x_{11} - x_3)^2,$$

where $\vec{x} = \vec{x}^{(0)} * \cdots * \vec{x}^{(3)}$ *with* $\vec{x}^{(0)} := (x_1, \ldots, x_{11})$, $\vec{x}^{(1)} := (x_{12}, \ldots, x_{31})$, $\vec{x}^{(2)} := (x_{32}, \ldots, x_{51})$, $\vec{x}^{(3)} := (x_{52}, \ldots, x_{71})$. *Then*

$$m = \frac{n!}{(n-k)!k!}$$

if and only if

$$\exists\, \vec{a}\ (\vec{a} \in \mathbb{N}^{71}\ \&\ f_4(m, n, k; \vec{a}) = 0).$$

Proof. See [2, pp. 249-250].

Lemma 4. *Let* $f_2(m, n; \vec{x}) :=$

$$f_3(x_3, x_1, x_2; \vec{x}^{(1)}) + f_3(x_4, x_3, n; \vec{x}^{(2)}) + f_3(x_5, x_4, n; \vec{x}^{(3)}) +$$

$$(x_1 - 2n - 1)^2 + (x_2 - n - 1)^2 + (m x_5 + x_6 - x_4)^2 + (x_4 + x_7 - (m+1)x_5)^2,$$

where $\vec{x} = \vec{x}^{(0)} * \cdots * \vec{x}^{(3)}$ *with* $\vec{x}^{(0)} := (x_1, \ldots, x_7)$, $\vec{x}^{(1)} := (x_8, \ldots, x_{27})$, $\vec{x}^{(2)} := (x_{28}, \ldots, x_{47})$, $\vec{x}^{(3)} := (x_{48}, \ldots, x_{118})$. *Then* $m = n!$ *if and only if*

$$\exists\, \vec{a}\ (\vec{a} \in \mathbb{N}^{118}\ \&\ f_2(m, n; \vec{a}) = 0).$$

Proof. See [2, pp. 251-252].

Lemma 5. *Let* $f_1(m, n, a, b; \vec{x}) :=$

$$(x_1 - a - bm)^2 + (x_3 - bx_2 - 1)^2 + (bx_4 - a - x_3 x_5)^2 + (m + x_8 - x_3)^2 + (x_9 - x_4 - n)^2 +$$

$$(m + x_3 x_{11} - x_6 x_7 x_{10})^2 + f_2(x_7, n; \vec{x}^{(3)}) + f_3(x_6, b, n; \vec{x}^{(2)}) + f_4(x_{10}, x_9, n; \vec{x}^{(4)}),$$

where

$$\vec{x} = \vec{x}^{(0)} * \cdots * \vec{x}^{(4)},\ \vec{x}^{(0)} := (x_1, \ldots, x_{11}),\ \vec{x}^{(1)} := (x_{12}, \ldots, x_{31}),$$

$$\vec{x}^{(2)} := (x_{32}, \ldots, x_{51}),\ \vec{x}^{(3)} := (x_{52}, \ldots, x_{169}),\ \vec{x}^{(4)} := (x_{170}, \ldots, x_{240}).$$

Then

$$m = \prod_{k=1}^{n} (a + bk)$$

if and only if

$$\exists\, \vec{c}\ (\vec{c} \in \mathbb{N}^{240}\ \&\ f_1(m, n, a, b; \vec{c}) = 0).$$

Proof. See [2, p. 252].

Proposition 5. *Let*

$\sigma(u,j,w;\vec{z}) := (u-p(z_1,z_2))^2+(w+z_3(1+jz_2)-z_1)^2+(w+z_4-jz_2-2)^2$

with $\vec{z} := (z_1,\dots,z_4)$*. There is a function*

$$S\colon \mathbb{N}^2 \to \mathbb{N},$$

satisfying the following conditions:
(i) $w = S(j,u)$ *if and only if* $\exists\, \vec{b}\ (\vec{b} \in \mathbb{N}^4\ \&\ \sigma(u,j,w;\vec{b}) = 0)$*;*
(ii) $\forall j, u\ (S(j,u) \le u)$*;*
(iii) *if* $\{a_k \mid 1 \le k \le n\} \subseteq \mathbb{N}$ *for some* n *in* $\mathbb{N}$*, then there is a number* u *in* $\mathbb{N}$ *such that* $a_k = S(k,u)$ *for* $1 \le k \le n$*.*

Proof. See [2, p. 237].

Proposition 6. *Let* $P(u_1,u_2;\vec{y},\vec{z}) \in \mathbb{Z}[u_1,u_2;\vec{y},\vec{z}]$*, with* $L(\vec{z}) = l$*, and suppose there is a polynomial* $R(u_1,u_2;\vec{y})$ *in* $\mathbb{Z}[u_1,u_2;\vec{y}]$ *such that*

$$|P(n,j;\vec{a},\vec{b})| \le R(n,T;\vec{a})$$

for $\vec{a} \in \mathbb{N}^{L(\vec{y})},\ \{n,\ j\} \subseteq \mathbb{N},\ j \le n,\ \vec{b} \in \mathbb{N}^l,\ |\vec{b}| \le T$ *and*

$$R(c_1,c_2;\vec{a}) > max\{c_1,c_2\}$$

for $\{c_1,c_2\} \subseteq \mathbb{N},\ \vec{a} \in \mathbb{N}^{L(\vec{y})}$*. Write, for brevity,*

$$H_l(\vec{x},\vec{b}) := f_2(b_5,b_4;\vec{x}^{(2)}) + f_1(b_5,n,1,b_6;\vec{x}^{(3)}) + (b_6-b_1b_5-1)^2 +$$

$$(b_2-b_6b_7)^2 + (\vec{x}^{(4)}-\vec{x}^{(1)}-\vec{\beta})^2 + \sum_{i=1}^{l} f_1(b_6x_i^{(5)},b_3,x_i^{(4)},1;\vec{x}^{(5+i)}),$$

where

$$\vec{b} := (b_1,\dots,b_7),\ \vec{\beta} := (\beta_1,\dots,\beta_l)\ \textit{with}\ \beta_i = b_3+1\ \textit{for}\ 1 \le i \le l,$$
$$\vec{x} = \vec{x}^{(1)} * \cdots * \vec{x}^{(5+l)}\ \textit{with}\ \vec{x}^{(j)} := (x_1^{(j)},\dots,x_{L(\vec{x}^{(j)})}^{(j)}),$$
$$L(\vec{x}^{(1)}) = L(\vec{x}^{(4)}) = L(\vec{x}^{(5)}) = l,\ L(\vec{x}^{(2)}) = 118,$$
$$L(\vec{x}^{(3)}) = L(\vec{x}^{(5+i)}) = 240\ \textit{for}\ 1 \le i \le l,$$

and

$$L(\vec{x}) = \sum_{1\le i\le 5+l} L(\vec{x}^{(i)}) = 244l+358.$$

Then

$$(\forall j \leq n)\, \exists\, \vec{c}\, (\vec{c} \in \mathbb{N}^l \;\&\; P(n, j; \vec{a}, \vec{c}) = 0) \iff$$
$$\exists\, \vec{x}, \vec{b}\, (\vec{b} \in \mathbb{N}^7 \;\&\; \vec{x} \in \mathbb{N}^{L(\vec{x})} \;\&\; (P(n, b_1; \vec{a}, \vec{x}^{(1)}) - b_2)^2 +$$
$$(R(n, b_3; \vec{a}) - b_4)^2 + H_l(\vec{x}, \vec{b}) = 0))\ \textit{for}\ \vec{a} \in \mathbb{N}^{L(\vec{y})}.$$

Proof. See [2, pp. 253-256].

§4. A few technical lemmata.

Lemma 6. *The variable t_i does not occur as a free variable in a formula φ if and only if there is a sequence of formulae $\{\varphi_1, \ldots, \varphi_n\}$ such that $\varphi_n = \varphi$ and, for every j in the interval $1 \leq j \leq n$, one of the following conditions holds true:*

(i) $\varphi_j := (t_k \,\epsilon\, t_l)$ *and* $i \notin \{k, l\}$,
(ii) $\varphi_j := \forall t_i\, \psi$ *for some* ψ *in* $\mathfrak{F}$,
(iii) $\varphi_j := (\varphi_k \supset \varphi_l)$ *with* $1 \leq k, l < n$,
(iv) $\varphi_j := \neg\varphi_k$ *with* $1 \leq k < n$,
(v) $\varphi_j := \forall t_\nu\, \varphi_k$ *with* $\nu \in \mathbb{N}$, $1 \leq k < n$.

Proof. Let $m(\varphi) = 1$ and suppose that t_i is not a free variable of φ. Then $\varphi := (t_k \,\epsilon\, t_l)$ with $i \notin \{k, l\}$ and we may take $n = 1$, $\varphi_1 = \varphi$. If $m(\varphi) = 1$ and there is a sequence $\{\varphi_1, \ldots, \varphi_n\}$ as above, then φ_n must satisfy condition (i) (since $m(\varphi_n) = m(\varphi) = 1$) and therefore t_i is not a free variable of φ $(= \varphi_n)$. Let $m(\varphi) = l$, $l > 1$ and suppose the assertion be true for any formula φ' with $m(\varphi') < l$. If φ_n satisfies condition (ii), then t_i is not a free variable of φ $(= \varphi_n)$. If φ_n satisfies one of the conditions $(iii), (iv), (v)$, then t_i is not a free variable of either φ_k or φ_l, by the inductive supposition, and therefore t_i is not a free variable of φ. Suppose that t_i is not a free variable of φ. Since $m(\varphi) > 1$, the formula φ must contain one of the logical connectives $\neg$, $\supset$, $\forall$. If $\varphi \in \{\neg\, \psi,\ \forall t_\nu\, \psi\}$ and $\nu \neq i$, then t_i is not a free variable of ψ, therefore, by the inductive supposition, there is a sequence of formulae $\{\varphi_1, \ldots, \varphi_\mu\}$ with $\varphi_\mu := \psi$ and we may let $n = \mu + 1$, $\varphi_n = \varphi$. If $\varphi := (\psi_1 \supset \psi_2)$, then t_i is not a free variable of either ψ_1, or of ψ_2, and, by the inductive supposition, there are two sequences of formulae $\{\varphi_1, \ldots, \varphi_\mu\}$ and $\{\varphi'_1, \ldots, \varphi'_\nu\}$ with $\varphi_\mu := \psi_1$ and $\varphi_\nu := \psi_2$; in this case, the sequence of formulae $\{\varphi_1, \ldots, \varphi_\mu, \varphi'_1, \ldots, \varphi'_\nu, \varphi\}$ satisfies the conditions of the lemma.

Lemma 7. *Let $\{r_1, r_2\} \subseteq \mathbb{N}$ and $\{\varphi, \psi\} \subseteq \mathfrak{F}$. Then the variable t_{r_2} is free for t_{r_1} in φ and $\psi := \varphi[t_{r_1}|t_{r_2}]$ if and only if there are three sequences*

$$\{\varphi_1, \ldots, \varphi_n\},\ \{\psi_1, \ldots, \psi_n\},\ \{d_1, \ldots, d_n\}$$

such that

$$\{\varphi_j,\ \psi_j\} \subseteq \mathfrak{F}\ \&\ d_j \in \{1,2\}\ \textit{for}\ 1 \le j \le n,\ \varphi_n = \varphi,\ \psi_n = \psi,$$

and, for every j in the interval $1 \le j \le n$, one of the following conditions holds true:

1) $\varphi_j := (t_{r_3}\ \epsilon\ t_{r_4})$ *with* $r_1 \notin \{r_3, r_4\},\ d_j = 2,\ \psi_j := \varphi_j$*;*
2) $\varphi_j := (t_{r_3}\ \epsilon\ t_{r_4})$ *with* $r_1 \in \{r_3, r_4\},\ d_j = 1,\ \psi_j := \varphi_j[t_{r_1}|t_{r_2}]$*;*
3) $\varphi_j := \neg\varphi_k,\ d_j = d_k,\ \psi_j := \neg\psi_k$ *with* $1 \le k < j$*,*
4) $\varphi_j := (\varphi_k \supset \varphi_l),\ \psi_j := (\psi_k \supset \psi_l),\ d_j = (d_k - 1)(d_l - 1) + 1$ *with* $1 \le k, l < j$*;*
5) $\varphi_j := \forall t_{r_3}\ \varphi_k$ *with* $r_3 \notin \{r_1, r_2\},\ \psi_j := \forall t_{r_3}\ \varphi_k,\ d_j = d_k,\ 1 \le k < j$*;*
6) $\varphi_j := \forall t_{r_1}\ \varphi_k$ *with* $1 \le k < j,\ \psi_j := \varphi_j,\ d_j = 2$*;*
7) $\varphi_j := \forall t_{r_2}\ \varphi_k$ *with* $r_1 \ne r_2,\ \psi_j := \varphi_j,\ d_j = d_k = 2,\ 1 \le k < j$*.*

Moreover,

$$d_j = \begin{cases} 1 & \textit{if}\ \ t_{r_1} \in [\varphi_j]_f \\ 2 & \textit{if}\ \ t_{r_1} \notin [\varphi_j]_f \end{cases}$$

for $1 \le j \le n$*.*

Proof. Let $m(\varphi) = 1$, then $\varphi := (t_{r_3}\ \epsilon\ t_{r_4})$ with $\{r_3, r_4\} \subseteq \mathbb{N}$, so that the variable t_{r_2} is free for t_{r_1} in φ. Let $\psi := \varphi[t_{r_1}|t_{r_2}],\ n = 1$, and

$$d_1 = \begin{cases} 1 & \text{if}\ \ r_1 \in \{r_3, r_4\} \\ 2 & \text{if}\ \ r_1 \notin \{r_3, r_4\}; \end{cases}$$

the assertion of the lemma is now obvious. Let now $m(\varphi) = l,\ l > 1$ and suppose the assertion be true for any formula φ' with $m(\varphi') < l$. If $\varphi_j := \forall t_{r_1}\ \varphi'$ with $\varphi' \in \mathfrak{F}$, then $t_{r_1} \notin [\varphi]_f$ and the assertion is obvious; if $\varphi_j := \forall t_{r_2}\ \varphi'$ with $\varphi' \in \mathfrak{F}$, then t_{r_2} is free for t_{r_1} in φ if and only if $t_{r_1} \notin [\varphi']_f$ (and therefore $t_{r_1} \notin [\varphi]_f$) and the assertion is again obvious. Finally, if

$$\varphi \in \{\neg\ \varphi',\ \forall t_{r_3}\ \varphi',\ \varphi' \supset \varphi''\},\ \text{with}\ \{\varphi',\ \varphi''\} \subseteq \mathfrak{F},\ r_3 \notin \{r_1, r_2\},$$

then one can deduce the assertion from the inductive supposition arguing as in the proof of Lemma 6.

Notation. Let

$$h_0(\vec{j}; \vec{x}) := (j_2 - j_1 + x_1)^2 + (j_3 - j_1 + x_2)^2\ \text{with}\ \ \vec{j} := (j_1, j_2, j_3),\ \vec{x} := (x_1, x_2).$$

It is clear that

$$\exists\ \vec{x}\ (\vec{x} \in \mathbb{N}^2\ \&\ h_0(\vec{j}, \vec{x}) = 0)\ \Leftrightarrow\ \max\{j_2, j_3\} < j_1.$$

The following lemma is a Diophantine reformulation of Lemma 6.

Lemma 8. *Let* $\mathcal{C}_i := \{\mathfrak{A} \mid \mathfrak{A} \in \mathfrak{F},\ t_i \notin [\mathfrak{A}]_f\}$. *Then*

$$\mathcal{N}(\mathcal{C}_i) = \{v \mid \mathfrak{B}_4(i, v)\},$$

where $\mathfrak{B}_4(i, v) :=$

$$\exists\, w, n\ (\{w, n\} \subseteq \mathbb{N}\ \&\ (\forall j_1 \leq n)\ \exists\, \vec{y}(\vec{y} \in \mathbb{N}^{35}\ \&\ (Q_4(n, j_1; i, v, w; \vec{y}) = 0)))$$

with

$$Q_4(n, j_1; i, v, w; \vec{y}) := \sum_{\nu=1}^{3} \sigma(w, j_\nu, x_\nu; \vec{z}^{(\nu)}) + \sigma(w, n, v; \vec{z}^{(4)}) +$$

$$h_0(\vec{j}; x_4, x_5) + \sum_{\nu=1}^{3} (x_\nu - p(x_{4+2\nu}, x_{5+2\nu}))^2 + \prod_{\nu=1}^{5} q_\nu(i, \vec{x});$$

$$q_1(i, \vec{x}) := (x_7 - 1)^2 + (x_6 - p(x_{12}, x_{13}))^2 + ((x_{12} - i)^2 - x_{14})^2 + ((x_{13} - i)^2 - x_{15})^2,$$

$$q_2(i, \vec{x}) := (x_6 - 3p(i, x_{16}) + 1)^2 + (x_7 - x_{17} - 1)^2,$$

$$q_3(i, \vec{x}) := (x_6 - 3p(x_8, x_{10}))^2 + (x_7 - p(x_9, x_{11}) - 1)^2,$$

$$q_4(i, \vec{x}) := (x_6 - 3x_8 + 2)^2 + (x_7 - x_9 - 1)^2,$$

$$q_5(i, \vec{x}) := (x_6 - 3p(x_{12}, x_8) + 1)^2 + (x_7 - x_9 - 1)^2;$$

$$\vec{j} := (j_1, j_2, j_3),\ \vec{x} := (x_1, \ldots, x_{17}),\ \vec{y} := (j_2, j_3) * \vec{x} * \vec{z},$$

$\vec{z} := \vec{z}^{(1)} * \cdots * \vec{z}^{(4)}$, *and* $\vec{z}^{(\nu)} := (z_1^{(\nu)}, \ldots, z_4^{(\nu)})$ *for* $1 \leq \nu \leq 4$, *so that* $L(\vec{y}) = 35$.

Proof. In view of Proposition 2, the formula

$$\exists\, w, \vec{z}(w \in \mathbb{N}\ \&\ \vec{z} \in \mathbb{N}^{16}\ \&\ (\sum_{\nu=1}^{3} \sigma(w, j_\nu, x_\nu; \vec{z}^{(\nu)}) + \sigma(w, n, v; \vec{z}^{(4)}) = 0))$$

asserts that there is a sequence of natural numbers $\{a_1, \ldots, a_N\}$, satisfying the following conditions:

$$\{a_1, \ldots, a_N\} \subseteq \mathbb{N};\ a_{j_\nu} = x_\nu \text{ for } 1 \leq \nu \leq 3,\ a_n = v,$$

while the formula $\exists\, \vec{x}(h_0(\vec{j}; x_4, x_5) = 0)$ asserts that $\max\{j_2, j_3\} < j_1$. Let $\{\varphi_1, \ldots, \varphi_n\}$ be a sequence of formulae in $\mathfrak{F}$ with $\mathcal{N}(\varphi_\nu) = a_\nu$ for $1 \leq \nu \leq n$. If

$$\sum_{\nu=1}^{3} (x_\nu - p(x_{4+2\nu}, x_{5+2\nu}))^2 = 0,$$

then $n(\varphi_{j_\nu}) = x_{4+2\nu}$ and $m(\varphi_{j_\nu}) = x_{5+2\nu}$ for $1 \le \nu \le 3$. It follows now that $q_1(i,\vec{x}) = 0$ if and only if $m(\varphi_{j_1}) = 1$, $\varphi_{j_1} := (t_{12} \ \epsilon \ t_{13})$ and $i \notin \{12, 13\}$; $q_2(i,\vec{x}) = 0$ if and only if $\varphi_{j_1} := \forall t_i \psi$ for some ψ in $\mathfrak{F}$; $q_3(i,\vec{x}) = 0$ if and only if $\varphi_{j_1} := (\varphi_{j_2} \supset \varphi_{j_3})$ with $1 \le j_2, j_3 < j_1$; $q_4(i,\vec{x}) = 0$ if and only if $\varphi_{j_1} := \neg\varphi_{j_2}$ with $1 \le j_2 < j_1$; $q_5(i,\vec{x}) = 0$ if and only if $\varphi_{j_1} := \forall t_\nu \varphi_{j_2}$ with $\nu \in \mathbb{N}$, $1 \le j_2 < j_1$. Thus, in view of Lemma 6, the formula $\mathfrak{B}_4(i,v)$ asserts that the variable t_i does not occur as a free variable in the formula $\mathcal{N}^{-1}(v)$.

Corollary 1. *Let*

$$\mathfrak{A}_4(u) := \exists\, i, v\ (\{i,v\} \subseteq \mathbb{N}\ \&\ \mathfrak{B}_4(i,v)\ \&\ \exists\, \vec{y}(\vec{y} \in \mathbb{N}^4\ \&\ (h_4(u;i,v;\vec{y}) = 0))),$$

where

$$h_4(u;i,v;\vec{y}) := (u - p(q_7(i,\vec{y}), q_8(\vec{y})))^2 + (v - p(y_3,y_4))^2,$$

$$q_7(i,\vec{y}) := 3p(3p(i, 3p(y_1,y_3)) - 1, 3p(y_1, 3p(i,y_3) - 1)),$$

$$q_8(\vec{y}) := p(p(y_2,y_4) + 2, p(y_2, y_4 + 1)) + 1;\ \vec{y} := (y_1, \ldots, y_4).$$

Then

$$\mathcal{N}(\mathcal{A}_4) = \{u \mid \mathfrak{A}_4(u)\}.$$

Proof. Let

$$\mathfrak{C} := \forall t_i\ (\mathfrak{A} \supset \mathfrak{B}) \supset (\mathfrak{A} \supset \forall t_i\ \mathfrak{B})$$

and let

$$n(\mathfrak{A}) = y_1, m(\mathfrak{A}) = y_2, n(\mathfrak{B}) = y_3, m(\mathfrak{B}) = y_4.$$

An easy calculation shows then that

$$\mathcal{N}(\mathfrak{C}) = p(q_7(i,\vec{y}), q_8(\vec{y})) \text{ and } \mathcal{N}(\mathfrak{B}) = p(y_3,y_4).$$

The assertion follows now from Lemma 8.

The following lemma is a Diophantine reformulation of Lemma 7.

Lemma 9. *Let*

$$\mathcal{C}(\vec{r}) :=$$

$$\{\vec{v} \mid v_1 = \mathcal{N}(\varphi), v_2 = \mathcal{N}(\psi), \varphi \in \mathfrak{F},\ \psi := \varphi[t_{r_1}|t_{r_2}],\ t_{r_2} \textit{ is free for } t_{r_1} \textit{ in } \varphi\},$$

where $\vec{r} := (r_1, r_2)$ *and* $\vec{v} := (v_1, v_2)$. *Then*

$$\mathcal{C}(\vec{r}) = \{\vec{v} \mid \vec{v} \in \mathbb{N}^2\ \&\ \mathfrak{B}_5(\vec{v}, \vec{r})\},$$

where $\mathfrak{B}_5(\vec{v},\vec{r}) := \exists\, \vec{w}, n\ (\vec{w} \in \mathbb{N}^3\ \&\ n \in \mathbb{N}\ \&$

$$(\forall j_1 \le n)\ \exists\, \vec{y}(\vec{y} \in \mathbb{N}^{72}\ \&\ (Q_5(n, j_1; \vec{v}, \vec{r}, \vec{w}; \vec{y}) = 0))$$

with

$$Q_5(n, j_1; \vec{v}, \vec{r}, \vec{w}; \vec{y}) := \sum_{1 \le i,\nu \le 3} \sigma(w_i, j_\nu, x_{3(i-1)+\nu}, \vec{z}_i^{(\nu)}) + \sum_{i \in \{1,2\}} \sigma(w_i, n, v_i, \vec{z}_i^{(4)}) +$$

$$h_0(\vec{j}; x_{13}, x_{14}) + \sum_{i=1}^{6} (x_i - p(x_{i1}, x_{i2}))^2 + \sum_{i=7}^{9} (x_i - 1)^2 (x_i - 2)^2 + \prod_{i=1}^{7} q_i(\vec{r}, \vec{x}),$$

where

$$q_1(\vec{r}, \vec{x}) :=$$

$$(x_{12}-1)^2+(x_7-2)^2+(x_4-x_1)^2+(x_{11}-p(r_3, r_4))^2+((r_3-r_1)^2(r_4-r_1)^2-x_{10})^2,$$

$$q_2(\vec{r}, \vec{x}) := q_2'(\vec{r}, \vec{x}) q_2''(\vec{r}, \vec{x})$$

with

$$q_2'(\vec{r}, \vec{x}) := (x_{12}-1)^2+(x_7-1)^2+(x_{42}-1)^2+(x_{11}-p(r_1, r_4))^2+(x_{41}-p(r_2, r_4))^2$$

and

$$q_2''(\vec{r}, \vec{x}) := (x_{12}-1)^2+(x_7-1)^2+(x_{42}-1)^2+(x_{11}-p(r_3, r_1))^2+(x_{41}-p(r_3, r_2))^2,$$

$$q_3(\vec{r}, \vec{x}) := (x_{11} - 3x_{21} + 2)^2 + (x_{12} - x_{22} - 1)^2 + (x_7 - x_8)^2 +$$
$$(x_{41} - 3x_{51} + 2)^2 + (x_{42} - x_{52} - 1)^2,$$

$$q_4(\vec{r}, \vec{x}) := (x_7 - (x_8 - 1)(x_9 - 1) - 1)^2 + (x_{11} - 3p(x_{21}, x_{31}))^2 +$$
$$(x_{12} - p(x_{22}, x_{32}) - 1)^2 + (x_{41} - 3p(x_{51}, x_{61}))^2 + (x_{42} - 3p(x_{52}, x_{62}) - 1)^2,$$

$$q_5(\vec{r}, \vec{x}) := (x_{11} - 3p(r_3, x_{21}) + 1)^2 + (x_{12} - x_{22} - 1)^2 + (x_7 - x_8)^2 +$$
$$(x_{41} - 3p(r_3, x_{51}) + 1)^2 + (x_{42} - x_{52} - 1)^2 + ((r_3 - r_1)^2 (r_3 - r_2)^2 - x_{10})^2,$$

$$q_6(\vec{r}, \vec{x}) := (x_{11} - 3p(r_1, x_{21}) + 1)^2 + (x_{12} - x_{22} - 1)^2 + (x_7 - 2)^2 + (x_4 - x_1)^2,$$

$$q_7(\vec{r}, \vec{x}) := (x_{11} - 3p(r_2, x_{21}) + 1)^2 + (x_{12} - x_{22} - 1)^2 + (x_7 - 2)^2 +$$
$$(x_8 - 2)^2 + (x_4 - x_1)^2 + ((r_2 - r_1)^2 - x_{10})^2;$$

$$\vec{w} := (w_1, w_2, w_3),\ \vec{j} := (j_1, j_2, j_3),\ \vec{z}^{(\nu)} := \vec{z}_1^{(\nu)} * \vec{z}_2^{(\nu)} * \vec{z}_3^{(\nu)} \textit{ for } 1 \le \nu \le 3,$$

$$\vec{z}^{(4)} := \vec{z}_1^{(4)} * \vec{z}_2^{(4)},\ \textit{with } L(\vec{z}_i^{(\nu)}) = 4 \textit{ for } 1 \le i \le 3, 1 \le \nu \le 4,\ \vec{z} := \vec{z}^{(1)} * \cdots * \vec{z}^{(4)};$$

$$\vec{x} := (r_3, r_4) * (x_1, \ldots, x_{14}) * (x_{21}, x_{22}, \ldots, x_{61}, x_{62}),\ \vec{y} := (j_2, j_3) * \vec{x} * \vec{z},$$

so that $L(\vec{y}) = 72$.

Proof. In view of Proposition 2, the formula

$$\exists\, \vec{w}, \vec{z}\ (\vec{w} \in \mathbb{N}^3\ \&\ \vec{z} \in \mathbb{N}^{44}\ \&$$
$$(\sum_{1\le i,\nu\le 3} \sigma(w_i, j_\nu, x_{3(i-1)+\nu}, \vec{z}_i^{(\nu)}) + \sum_{i\in\{1,2\}} \sigma(w_i, n, v_i, \vec{z}_i^{(4)}) = 0))$$

asserts that there are three sequences

$$\{\varphi_1, \ldots, \varphi_n\},\ \{\psi_1, \ldots, \psi_n\},\ \{d_1, \ldots, d_n\}$$

such that

$$\mathcal{N}(\varphi_{j_\nu}) = x_\nu,\ \mathcal{N}(\psi_{j_\nu}) = x_{\nu+3},\ d_{j_\nu} = x_{\nu+6} \text{ for } 1 \le \nu \le 3,$$
$$\mathcal{N}(\varphi_n) = v_1,\ \mathcal{N}(\psi_n) = v_2$$

and the formula

$$\exists\, x_{13}, x_{14}(\{x_{13}, x_{14}\} \subseteq \mathbb{N}\ \&\ (h_0(\vec{j}; x_{13}, x_{14}) = 0))$$

asserts that $\max\{j_2, j_3\} < j_1$. Under the assumption

$$\sum_{i=1}^{6}(x_i - p(x_{i1}, x_{i2}))^2 = 0,$$

the formula

$$\exists\, \vec{x}(\vec{x} \in \mathbb{N}^{34}\ \&\ q_i(\vec{r}, \vec{x}) = 0)$$

is equivalent to the condition $i)$, $1 \le i \le 7$, in Lemma 7. On the other hand, equation

$$\sum_{i=7}^{9}(x_i - 1)^2(x_i - 2)^2 = 0$$

asserts that $d_j \in \{1, 2\}$, for every j in the interval $1 \le j \le n$. Lemma 9 follows now from Lemma 7.

Corollary 2. *Let*

$$\mathfrak{A}_5(u) := \exists\, \vec{v}, \vec{r}\ (\{\vec{v}, \vec{r}\} \subseteq \mathbb{N}^2\ \&\ \mathfrak{B}_5(\vec{v}, \vec{r})\ \&\ \exists\, \vec{s}(\vec{s} \in \mathbb{N}^4\ \&\ (h_5(u; \vec{v}, \vec{r}, \vec{s}) = 0))),$$

where

$$h_5(u; \vec{v}, \vec{r}, \vec{s}) := (u - p(q_9(\vec{r}, \vec{s}), q_{10}(\vec{s})))^2 + (v_1 - p(s_{11}, s_{12}))^2 + (v_2 - p(s_{21}, s_{22}))^2,$$
$$q_9(\vec{r}, \vec{s}) := 3p(3p(r_1, s_{11}) - 1, s_{21}),\ q_{10}(\vec{s}) := p(s_{12} + 1, s_{22}),$$

and $\vec{s} := (s_{11}, s_{12}, s_{21}, s_{22})$. *Then*

$$\mathcal{N}(\mathcal{A}_5) = \{u \mid \mathfrak{A}_5(u)\}.$$

Proof. Let $\mathfrak{C} := (\forall t_{r_1}\ \mathfrak{D} \supset \mathfrak{D}[t_{r_1}|t_{r_2}])$ and let

$$\mathcal{N}(\mathfrak{D}) = v_1 = p(s_{11}, s_{12}),\ \mathcal{N}(\mathfrak{D}[t_{r_1}|t_{r_2}]) = v_2 = p(s_{21}, s_{22}).$$

An easy calculation shows then that $\mathcal{N}(\mathfrak{C}) = p(q_9(\vec{r}, \vec{s}), q_{10}(\vec{s}))$. The assertion follows now from Lemma 9.

§5. Elimination of universal quantifiers.

It follows from Proposition 6 that formulae $\mathfrak{A}_4(u)$ and $\mathfrak{A}_5(u)$ define Diophantine predicates. In this section, we shall explicitly write down polynomials $g_4(u, \vec{x})$ and $g_5(u, \vec{x})$ such that

$$\{u \mid \mathfrak{A}_\nu(u)\} = \{u \mid \exists\, \vec{b}\ (\vec{b} \in \mathbb{N}^{L(\vec{x})}\ \&\ g_\nu(u, \vec{b}) = 0)\}$$

for $\nu = 4, 5$.

Lemma 10. *Let*

$$R_4(z_1, z_2; i, v, w) := 8w^2 + 4v^2 + 100z_1^4 + 10^{10}(i^{16} + z_2^{28}).$$

Then

$$Q_4(n, j_1; i, v, w; \vec{y}) \le R_4(n, T; i, v, w) \text{ for } j_1 \le n,\ |\vec{y}| \le T,$$

$\vec{y} \in \mathbb{N}^{35},\ \{i, v, w, n, j_1\} \subseteq \mathbb{N}$.

Proof. Under the conditions

$$j_1 \le n,\ |\vec{y}| \le T,\ \vec{y} \in \mathbb{N}^{35},\ \{i, v, w, n, j_1\} \subseteq \mathbb{N},$$

it follows that

$$h_0(\vec{j}; x_4, x_5) \le 16T^2 + 4n^2,\ \sum_{\nu=1}^{3}(x_\nu - p(x_{4+2\nu}, x_{5+2\nu}))^2 \le 50T^4,$$

$\sigma(w, j_\nu, x_\nu, \vec{z}^{(\nu)}) \le 2w^2 + 60T^6$ for $\nu = 2, 3,\ \sigma(w, j_1, x_1, \vec{z}^{(1)}) \le 2w^2 + 72T^4n^2$, and $\sigma(w, n, v, \vec{z}^{(4)}) \le 2w^2 + 4v^2 + 70T^4n^2$. Moreover, under the same conditions, we have

$$q_1(i, \vec{x}) \le 16i^4 + 60T^4,\ q_2(i, \vec{x}) \le 4i^4 + 270T^4,\ q_3(i, \vec{x}) \le 125T^4,$$

$q_4(i, \vec{x}) \le 45T^2$, and $q_5(i, \vec{x}) \le 130T^4$. The assertion of the lemma follows from these estimates and the definition of the polynomial $Q_4(n, j_1; i, v, w; \vec{y})$ in Lemma 8.

Lemma 11. *Let*

$R_5(z_1,z_2;\vec{v},\vec{r},\vec{w}) := 8\vec{w}^2+4\vec{v}^2+2\cdot 10^4 z_1^4+3\cdot 10^{26} z_2^{64}+5\cdot 10^{17} r_1^{64}+5\cdot 10^{17} r_2^{64})$.

Then

$$Q_5(n,j_1;\vec{v},\vec{r},\vec{w};\vec{y}) \le R_5(n,T;\vec{v},\vec{r},\vec{w}) \textit{ for } j_1 \le n,\ |\vec{y}| \le T,$$

$$\vec{y} \in \mathbb{N}^{72}, \{n,j_1\} \subseteq \mathbb{N}, \{\vec{v},\vec{r}\} \subseteq \mathbb{N}^2, \vec{w} \in \mathbb{N}^3.$$

Proof. Under the conditions

$$j_1 \le n, |\vec{y}| \le T, \vec{y} \in \mathbb{N}^{72}, \{n,j_1\} \subseteq \mathbb{N}, \{\vec{v},\vec{r}\} \subseteq \mathbb{N}^2, \vec{w} \in \mathbb{N}^3,$$

it follows that $h_0(\vec{j};x_{13},x_{14}) \le 16T^2+4n^2$,

$$\sum_{i=1}^{6}(x_i-p(x_{i1},x_{i2}))^2+\sum_{i=7}^{9}(x_i-1)^2(x_i-2)^2 \le 100T^4,$$

$$\sum_{1\le i\le 3}\sigma(w_i,j_\nu,x_{3(i-1)+\nu},\vec{z}_i^{(\nu)}) \le 2\vec{w}^2+180T^6 \text{ for } \nu=2,3,$$

$$\sum_{1\le i\le 3}\sigma(w_i,j_1,x_{3i-2},\vec{z}_i^{(1)}) \le 2\vec{w}^2+108T^8+108n^4,$$

and

$$\sum_{i\in\{1,2\}}\sigma(w_i,n,v_i,\vec{z}_i^{(4)}) \le 2\vec{w}^2+4\vec{v}^2+70T^8+70n^4.$$

Moreover, under the same conditions, we have $q_1(\vec{r},\vec{x}) \le 200T^8+200r_1^8$,

$$q_2'(\vec{r},\vec{x}) \le 40T^4+2r_1^4+2r_2^4,\ q_2''(\vec{r},\vec{x}) \le 20T^4+8r_1^4+8r_2^4,$$

$$q_3(\vec{r},\vec{x}) \le 100T^2,\ q_4(\vec{r},\vec{x}) \le 250T^4,\ q_5(\vec{r},\vec{x}) \le 500T^8+50r_1^8+50r_2^8,$$

$$q_6(\vec{r},\vec{x}) \le 150T^4+20r_1^4,\ q_7(\vec{r},\vec{x}) \le 150T^4+4r_1^4+4r_2^4.$$

The assertion of the lemma follows from these estimates and the definition of the polynomial $Q_5(n,j_1;\vec{v},\vec{r},\vec{w};\vec{y})$ in Lemma 9.

Notation. Let

$$P_4(n,j_1;i,v,w;\vec{y}) := 2^8 Q_4(n,j_1;i,v,w;\vec{y}),$$

$$R_4'(z_1,z_2;i,v,w) := 2^8 R_4(z_1,z_2;i,v,w),$$

$$P_5(n,j_1;\vec{v},\vec{r},\vec{w};\vec{y}) := 2^{14} Q_5(n,j_1;\vec{v},\vec{r},\vec{w};\vec{y}),$$

$$R'_5(z_1, z_2; \vec{v}, \vec{r}, \vec{w}) := 2^{14} R_5(z_1, z_2; \vec{v}, \vec{r}, \vec{w}).$$

Since $2p(x, y) \in Z[x, y]$, it follows that

$$P_4(n, j_1; i, v, w; \vec{y}) \in Z[n, j_1; i, v, w; \vec{y}]$$

and

$$P_5(n, j_1; \vec{v}, \vec{r}, \vec{w}; \vec{y}) \in Z[n, j_1; \vec{v}, \vec{r}, \vec{w}; \vec{y}].$$

Therefore one concludes as follows.

Proposition 7. *Let* $g_4(u, \vec{z}^{(1)}) :=$

$$h_4(u; i, v, \vec{y}) + H_{35}(\vec{x}, \vec{b}) + (P_4(n, b_1; i, v, w; \vec{x}^{(1)}) - b_2)^2 + (R'_4(n, b_3; i, v, w) - b_4)^2,$$

where $\vec{z}^{(1)} = \vec{x} * \vec{b} * \vec{y} * (i, v, w, n)$, $L(\vec{z}^{(1)}) = 8913$*; then*

$$\mathcal{N}(\mathcal{A}_4) = \{u \mid \exists\, \vec{b}\ (\vec{b} \in \mathbb{N}^{9013}\ \&\ g_4(u, \vec{b}) = 0)\}.$$

Let $g_5(u, \vec{z}^{(2)}) :=$

$$h_5(u; \vec{v}, \vec{r}, \vec{s}) + H_{72}(\vec{x}, \vec{b}) + (P_5(n, b_1; \vec{v}, \vec{r}, \vec{w}; \vec{x}^{(1)}) - b_2)^2 + (R'_5(n, b_3; \vec{v}, \vec{r}, \vec{w}) - b_4)^2,$$

where $\vec{z}^{(2)} = \vec{x} * \vec{b} * \vec{v} * \vec{r} * \vec{s} * \vec{w} * (n)$, $L(\vec{z}^{(2)}) = 17945$*; then*

$$\mathcal{N}(\mathcal{A}_5) = \{u \mid \exists\, \vec{b}\ (\vec{b} \in \mathbb{N}^{17945}\ \&\ g_5(u, \vec{b}) = 0)\}.$$

Proof. In view of the estimates obtained in Lemmata 10 and 11, the assertion follows from Corollary 1, Corollary 2, and Proposition 6.

§6. The main theorem.

Proposition 8. *Let*

$$G_1(\vec{u}; \vec{x}) := (u_1 - p(x_1, x_2))^2 + (u_2 - p(x_3, x_4))^2 +$$

$$(u_3 - p(x_5, x_6))^2 + (x_5 - 3p(x_3, x_1))^2 + (x_6 - p(x_4, x_2) - 1)^2,$$

where $\vec{u} := (u_1, u_2, u_3)$, $\vec{x} := (x_1, \ldots, x_6)$. *A formula* $\mathfrak{A}_1$ *follows from formulae* $\mathfrak{A}_2$ *and* $\mathfrak{A}_3$ *by the rule* $(\mathcal{B}_1)$ *if and only if*

$$\exists\, \vec{b}\ (\vec{b} \in \mathbb{N}^6\ \&\ G_1(\vec{u}; \vec{b}) = 0)$$

with $u_i := \mathcal{N}(\mathcal{A}_i)$ *for* $1 \le i \le 3$. *Let*

$$G_2(\vec{u}; r, \vec{x}) := (u_1 - p(x_3, x_2 + 1))^2 + (u_2 - p(x_1, x_2))^2 + (x_3 - 3p(r, x_1) - 1)^2,$$

where $\vec{u} := (u_1, u_2)$, $\vec{x} := (x_1, x_2, x_3)$. *A formula* $\mathfrak{A}_1$ *follows from a formula* $\mathfrak{A}_2$ *by the rule* $(\mathcal{B}_2)$ *if and only if*

$$\exists\, \vec{b}, r\ (\vec{b} \in \mathbb{N}^3\ \&\ r \in \mathbb{N}\ \&\ G_2(\vec{u}; r, \vec{b}) = 0)$$

with $u_i := \mathcal{N}(\mathfrak{A}_i)$ *for* $i = 1, 2$.

Proof. The assertion follows from the definition of the inference rules $(\mathcal{B}_1)$ and $(\mathcal{B}_2)$ since the formula

$$\exists\, \vec{b}\ (\vec{b} \in \mathbb{N}^6\ \&\ G_1(\vec{u}; \vec{b}) = 0)$$

asserts that $\mathfrak{A}_3 := \mathfrak{A}_2 \supset \mathfrak{A}_1$ and the formula

$$\exists\, \vec{b}, r\ (\vec{b} \in \mathbb{N}^3\ \&\ r \in \mathbb{N}\ \&\ G_2(\vec{u}; r, \vec{b}) = 0)$$

asserts that $\mathfrak{A}_2 := \forall t_r\, \mathfrak{A}_1$.

The following lemma is a Diophantine reformulation of the definition of the set $\mathfrak{T}$ of the theorems of $\mathcal{P}$.

Lemma 12. *Let*

$$Q(n, j_1; v, u; \vec{w}) := \sum_{i=1}^{3} \sigma(u, j_\nu, x_i; \vec{z}^{(i)}) + \sigma(u, n, v; \vec{z}^{(4)}) +$$

$$h_0(\vec{j}; x_4, x_5) + G_1(x_1, x_2, x_3; \vec{y}^{(6)}) G_2(x_1, x_2; \vec{y}^{(7)}) \prod_{i=1}^{5} g_i(x_1, \vec{y}^{(i)}),$$

where

$$\vec{j} := (j_1, j_2, j_3),\ \vec{x} := (x_1, \ldots, x_5),\ \vec{w} := (j_2, j_3) * \vec{x} * \vec{z} * \vec{y},\ \vec{z} := \vec{z}^{(1)} * \cdots * \vec{z}^{(4)},$$

$$\vec{y}^{(5)} = \vec{y} := (y_1, \ldots, y_{17945}),\ \vec{y}^{(6)} = \vec{y}^{(3)} = \vec{y}^{(1)} := (y_1, \ldots, y_6),$$
$$\vec{y}^{(2)} := (y_1, \ldots, y_8),\ \vec{y}^{(4)} := (y_1, \ldots, y_{9013}),\ \vec{y}^{(7)} := (y_1, \ldots, y_4),$$

$L(\vec{z}^{(i)}) = 4$ *for* $1 \le i \le 4$, *so that* $L(\vec{w}) = 17968$. *Then*

$$\mathcal{N}(\mathfrak{T}) = \{v \mid \exists\, u, n\ (\{u, n\} \subseteq \mathbb{N}\ \&\ \mathfrak{A}(v; u, n))\},$$

where

$$\mathfrak{A}(v; u, n) := (\forall j_1 \le n)\ \exists\, \vec{w}(Q(n, j_1; v, u; \vec{w}) = 0).$$

Proof. The formula $\exists\, u, n\ (\{u, n\} \subseteq \mathbb{N}\ \&\ \mathfrak{A}(v; u, n))$ can be easily seen to assert that $v \in \mathcal{N}(\mathfrak{T})$.

Lemma 13. *Let*

$$R(z_1, z_2; v, u) := 8u^2 + 4v^2 + 10^4 z_1^4 + 10^{133} z_2^{232}.$$

Then

$$Q(n, j_1; v, u; \vec{w}) \leq R(n, T; v, u) \text{ for } j_1 \leq n,\ |\vec{w}| \leq T, \vec{w} \in \mathbb{N}^l, l := 17968,$$

with $\{v, u, n, j_1\} \subseteq \mathbb{N}$.

Proof. Under the conditions

$$j_1 \leq n,\ |\vec{w}| \leq T,\ \vec{w} \in \mathbb{N}^l,\ \{v, u, n, j_1\} \subseteq \mathbb{N},$$

it follows that

$$\sum_{i=1}^{3} \sigma(u, j_\nu, x_i; \vec{z}^{(i)}) + \sigma(u, n, v; \vec{z}^{(4)}) + h_0(\vec{j}; x_4, x_5) \leq 8u^2 + 4v^2 + 10^4 n^4 + 10^4 T^8$$

and

$$G_1(x_1, x_2, x_3; \vec{y}^{(6)}) G_2(x_1, x_2; \vec{y}^{(7)}) g_1(x_1, \vec{y}^{(1)}) g_2(x_1, \vec{y}^{(2)}) g_3(x_1, \vec{y}^{(3)}) \leq 2 \cdot 10^{42} T^{48}.$$

Moreover, one can show that

$$g_4(x_1, \vec{y}^{(4)}) \leq 10^{27} T^{56} \text{ and } g_5(x_1, \vec{y}^{(5)}) \leq 10^{63} T^{128}.$$

The assertion of the lemma follows from these estimates and the definition of the polynomial $Q(n, j_1; v, u; \vec{w})$.

Notation. Let

$P(n, j_1; v, u; \vec{w}) := 2^{82} Q(n, j_1; v, u; \vec{w})$ and $R'(z_1, z_2; v, u) := 2^{82} R(z_1, z_2; v, u)$.

Theorem 1. *In notations of Proposition 6, let*

$$F(v, \vec{z}) := (P(n, b_1; v, u; \vec{x}^{(1)}) - b_2)^2 + (R'(n, b_3; v, u) - b_4)^2 + H_l(\vec{x}, \vec{b})$$

with $l := 17968$ *and* $\vec{z} := (u, n) * \vec{x}$, *so that* $L(\vec{z}) = 244l + 360 = 4384552$. *Then*

$$\mathcal{N}(\mathfrak{T}) = \{a \mid a \in \mathbb{N},\ \exists\, \vec{b}\ (\vec{b} \in \mathbb{Z}^{L(\vec{z})}\ \&\ F(a, \vec{b}) = 0)\}.$$

Proof. As in Section 5, one can show that $P(n, j_1; v, u; \vec{w}) \in Z[n, j_1; v, u; \vec{w}]$. Therefore, in view of Lemma 13, the assertion follows from Proposition 6 and Lemma 12.

§7. Concluding remarks.

In accordance with Lemma 1, let $f(v, \vec{t}) := F(v, \vec{z})$, where $\vec{z} := (z_1, \dots, z_n)$, $z_j := \sum_{i=1}^{4} t_{ji}^2$ for $1 \le j \le n$, $\vec{t} := (t_{11}, \dots, t_{14}, \dots, t_{n1}, \dots, t_{n4}), n := 4384308$. Then

$$\mathcal{N}(\mathfrak{T}) = \{a \mid a \in \mathbb{N},\ \exists\, \vec{b}\ (\vec{b} \in \mathbb{Z}^{4n}\ \&\ f(a, \vec{b}) = 0)\}. \tag{2}$$

The universal polynomial $f(v, \vec{t})$, constructed in this paper, is rather complicated, compared to the "combinatorially" universal polynomials of Yu.V. Matiyasevich and J.P. Jones, [6], [10, p. 70]; a somewhat more simple universal polynomial will be found in the forthcoming work [1]. It is an interesting unsolved problem to construct substantially more simple polynomials, satisfying condition (2).

Acknowledgement. We are indebted to Professor Yu.V. Matiyasevich for a private communication [11], relating to this work.

References

[1] M. Carl, Diplomarbeit, Universität Bonn, in preparation.

[2] M. Davis, Hilbert's tenth problem is unsolvable, The American Mathematical Monthly, 80 (1973), 233 - 269.

[3] M. Davis, Yu. Matijasevič, and Ju. Robinson, Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution, *Proceedings of Symposia in Pure Maths,* 28 (1976), 323-378.

[4] H.M. Friedman, Finite functions and the necessary use of large cardinals, *Annals of Mathematics,* 148 (1998), 803-893.

[5] K. Gödel, The consistency of the axiom of choice and of the generalised continuum hypothesis with the axioms of set theory, Princeton University Press, 1940.

[6] J.P. Jones, Universal Diophantine equation, *Journal of Symbolic Logic,* 47 (1982), 549-571.

[7] L. Kalmár, Zurückführung des Entscheidungsproblems auf den Fall von Formeln mit einer einzigen binären Funktionsvariablen, Compositio Mathematica, 4 (1936), 137 - 144.

[8] Yu.V. Matiyasevich, Enumerable sets are Diophantine, *Doklady AN SSSR,* 191:2 (1970), 279-282 (translated in: *Soviet Math. Doklady,* 11 (1970), 354-358).

[9] Yu.V. Matiyasevich, Diophantine representation of enumerable predicates, *Izvestiya AN SSSR. Seriya Matematicheskaya,* 35:1 (1971), 3-30 (translated in: *Mathematics of the USSR. Izvestiya,* 15(1) (1971), 1-28).

[10] Yu.V. Matiyasevich, *Hilbert's Tenth Problem,* The MIT Press, 1993.

[11] Yu.V. Matiyasevich, An e-mail letter to the second author, March 2005.

[12] E. Mendelson, *Introduction to Mathematical Logic,* Chapman & Hall/CRM, 2001.

M. Carl: Mathematisches Institut der Universität Bonn, Beringstrasse 1, D-53115 Bonn, GERMANY
E-mail address: goedel23@gmx.de

B.Z. Moroz: Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, GERMANY
E-mail address: moroz@mpim-bonn.mpg.de