

# Basic Diophantine Relations<sup>1</sup>

Marcin Acewicz  
Institute of Informatics  
University of Białystok  
Poland

Karol Pałk   
Institute of Informatics  
University of Białystok  
Poland

**Summary.** The main purpose of formalization is to prove that two equations  $y_a(z) = y$ ,  $y = x^z$  are Diophantine. These equations are explored in the proof of Matiyasevich’s negative solution of Hilbert’s tenth problem.

In our previous work [6], we showed that from the diophantine standpoint these equations can be obtained from lists of several basic Diophantine relations as linear equations, finite products, congruences and inequalities. In this formalization, we express these relations in terms of Diophantine set introduced in [7]. We prove that these relations are Diophantine and then we prove several second-order theorems that provide the ability to combine Diophantine relation using conjunctions and alternatives as well as to substitute the right-hand side of a given Diophantine equality as an argument in a given Diophantine relation. Finally, we investigate the possibilities of our approach to prove that the two equations, being the main purpose of this formalization, are Diophantine.

The formalization by means of Mizar system [3], [2] follows Z. Adamowicz, P. Zbierski [1] as well as M. Davis [4].

MSC: 11D45 03B35 68T99

Keywords: Hilbert’s 10th problem; Diophantine relations

MML identifier: HILB10.3, version: 8.1.08 5.52.1328

## 1. PRELIMINARIES

From now on  $n, m, k$  denote natural numbers,  $p, q$  denote  $n$ -element finite 0-sequences of  $\mathbb{N}$ ,  $i_1, i_2, i_3, i_4, i_5, i_6$  denote elements of  $n$ , and  $a, b, c, d, e$  denote integers.

---

<sup>1</sup>This work has been financed by the resources of the Polish National Science Centre granted by decision no. DEC-2015/19/D/ST6/01473.

Let  $X$  be a set,  $p$  be a  $\mathbb{Z}$ -valued series of  $X$ ,  $\mathbb{R}_F$ , and  $a$  be an integer element of  $\mathbb{R}_F$ . Observe that  $a \cdot p$  is  $\mathbb{Z}$ -valued.

Now we state the propositions:

- (1) Let us consider a non empty ordinal number  $O$ , an element  $i$  of  $O$ , an add-associative, right zeroed, right complementable, well unital, distributive, non trivial double loop structure  $L$ , and a function  $x$  from  $O$  into  $L$ . Then  $\text{eval}(1.1(i, L), x) = x(i)$ .
- (2)  $i_1$  is an element of  $n + k$ .
- (3) If  $k < m$ , then  $n + k \in n + m$ .
- (4) Let us consider an  $(n + k)$ -element finite 0-sequence  $p$ . If  $n \neq 0$  and  $k \neq 0$ , then  $(p \upharpoonright n)(i_1) = p(i_1)$ .

## 2. BASIC DIOPHANTINE RELATIONS

Now we state the propositions:

- (5) Let us consider a diophantine subset  $A$  of the  $n$ -xtuples of  $\mathbb{N}$ , and  $k$ . Suppose  $k \leq n$ . Then  $\{p \upharpoonright k : p \in A\}$  is a diophantine subset of the  $k$ -xtuples of  $\mathbb{N}$ .

PROOF: Consider  $k_1$  being a natural number,  $Q$  being a  $\mathbb{Z}$ -valued polynomial of  $n + k_1, \mathbb{R}_F$  such that for every object  $s$ ,  $s \in A$  iff there exists an  $n$ -element finite 0-sequence  $x$  of  $\mathbb{N}$  and there exists a  $k_1$ -element finite 0-sequence  $y$  of  $\mathbb{N}$  such that  $s = x$  and  $\text{eval}(Q, {}^@ (x \hat{\ } y)) = 0$ .

Set  $D = \{p \upharpoonright k, \text{ where } p \text{ is an } n\text{-element finite 0-sequence of } \mathbb{N} : p \in A\}$ .  $D \subseteq$  the  $k$ -xtuples of  $\mathbb{N}$ . Reconsider  $k_2 = n - k$  as a natural number. Reconsider  $P = Q$  as a  $\mathbb{Z}$ -valued polynomial of  $k + (k_2 + k_1), \mathbb{R}_F$ . For every object  $s$ ,  $s \in D$  iff there exists a  $k$ -element finite 0-sequence  $x$  of  $\mathbb{N}$  and there exists a  $(k_2 + k_1)$ -element finite 0-sequence  $y$  of  $\mathbb{N}$  such that  $s = x$  and  $\text{eval}(P, {}^@ (x \hat{\ } y)) = 0$  by [5, (13)], [8, (54),(17),(27)].  $\square$

- (6) Let us consider integers  $a, b, c, i_1$ , and  $i_2$ . Then  $\{p : a \cdot p(i_1) = b \cdot p(i_2) + c\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$ . The theorem is a consequence of (1).
- (7)  $\{p : a \cdot p(i_1) > b \cdot p(i_2) + c\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$ . The theorem is a consequence of (2) and (1).

The scheme *UnionDiophantine* deals with a natural number  $n$  and a unary predicate  $\mathcal{P}, \mathcal{Q}$  and states that

- (Sch. 1)  $\{p, \text{ where } p \text{ is an } n\text{-element finite 0-sequence of } \mathbb{N} : \mathcal{P}[p] \text{ or } \mathcal{Q}[p]\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$

provided

- $\{p, \text{ where } p \text{ is an } n\text{-element finite 0-sequence of } \mathbb{N} : \mathcal{P}[p]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$  and
- $\{p, \text{ where } p \text{ is an } n\text{-element finite 0-sequence of } \mathbb{N} : \mathcal{Q}[p]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .

The scheme *Eq* deals with a natural number  $n$  and a unary predicate  $\mathcal{P}, \mathcal{Q}$  and states that

(Sch. 2)  $\{p, \text{ where } p \text{ is an } n\text{-element finite 0-sequence of } \mathbb{N} : \mathcal{P}[p]\} = \{q, \text{ where } q \text{ is an } n\text{-element finite 0-sequence of } \mathbb{N} : \mathcal{Q}[q]\}$

provided

- for every  $n$ -element finite 0-sequence  $p$  of  $\mathbb{N}$ ,  $\mathcal{P}[p]$  iff  $\mathcal{Q}[p]$ .

Now we state the propositions:

(8)  $\{p : a \cdot p(i_1) \geq b \cdot p(i_2) + c\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .

PROOF: Define  $\mathcal{P}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv a \cdot \$_1(i_1) > b \cdot \$_1(i_2) + c$ . Define  $\mathcal{Q}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv a \cdot \$_1(i_1) = b \cdot \$_1(i_2) + c$ . Define  $\mathcal{R}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv \mathcal{P}[\$_1]$  or  $\mathcal{Q}[\$_1]$ . Define  $\mathcal{S}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv a \cdot \$_1(i_1) \geq b \cdot \$_1(i_2) + c$ .  $\{p : \mathcal{P}[p]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .  $\{p : \mathcal{Q}[p]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .  $\{p : \mathcal{P}[p]$  or  $\mathcal{Q}[p]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .  $\{p : \mathcal{R}[p]\} = \{q : \mathcal{S}[q]\}$ .  $\square$

(9)  $\{p : a \cdot p(i_1) = b \cdot p(i_2) \cdot p(i_3)\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ . The theorem is a consequence of (1).

(10)  $\{p : \text{there exists a natural number } z \text{ such that } a \cdot p(i_1) = b \cdot p(i_2) + z \cdot c \cdot p(i_3)\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ . The theorem is a consequence of (2) and (1).

The scheme *IntersectionDiophantine* deals with a natural number  $n$  and a unary predicate  $\mathcal{P}, \mathcal{Q}$  and states that

(Sch. 3)  $\{p, \text{ where } p \text{ is an } n\text{-element finite 0-sequence of } \mathbb{N} : \mathcal{P}[p] \text{ and } \mathcal{Q}[p]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$

provided

- $\{p, \text{ where } p \text{ is an } n\text{-element finite 0-sequence of } \mathbb{N} : \mathcal{P}[p]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$  and
- $\{p, \text{ where } p \text{ is an } n\text{-element finite 0-sequence of } \mathbb{N} : \mathcal{Q}[p]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .

The scheme *Substitution* deals with a 6-ary predicate  $\mathcal{P}$  and a ternary functor  $\mathcal{F}$  yielding a natural object and states that

(Sch. 4) For every  $i_1, i_2, i_3, i_4$ , and  $i_5$ ,  $\{p : \mathcal{P}[p(i_1), p(i_2), \mathcal{F}(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5))]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$

provided

- for every  $i_1, i_2, i_3, i_4, i_5$ , and  $i_6$ ,  $\{p : \mathcal{P}[p(i_1), p(i_2), p(i_3), p(i_4), p(i_5), p(i_6))]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$  and
- for every  $i_1, i_2, i_3$ , and  $i_4$ ,  $\{p : \mathcal{F}(p(i_1), p(i_2), p(i_3)) = p(i_4)\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .

The scheme *SubstitutionInt* deals with a ternary predicate  $\mathcal{P}$  and a ternary functor  $\mathcal{F}$  yielding an integer and states that

(Sch. 5) For every  $i_1, i_2, i_3, i_4$ , and  $i_5$ ,  $\{p : \mathcal{P}[p(i_1), p(i_2), \mathcal{F}(p(i_3), p(i_4), p(i_5))]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$

provided

- for every  $i_1, i_2, i_3$ , and  $a$ ,  $\{p : \mathcal{P}[p(i_1), p(i_2), a \cdot p(i_3)]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$  and
- for every  $i_1, i_2, i_3, i_4$ , and  $a$ ,  $\{p : \mathcal{F}(p(i_1), p(i_2), p(i_3)) = a \cdot p(i_4)\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .

Now we state the propositions:

(11)  $\{p : a \cdot p(i_1) = b \cdot p(i_2) + c \cdot p(i_3) + d\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ . The theorem is a consequence of (1).

(12)  $\{p : p(i_1) = a \cdot p(i_2)\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ . The theorem is a consequence of (6).

(13)  $\{p : a \cdot p(i_1) = b\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .

PROOF: Set  $i_2 =$  the element of  $n$ . Define  $\mathcal{P}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv a \cdot \$_1(i_1) = b$ . Define  $\mathcal{Q}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv a \cdot \$_1(i_1) = 0 \cdot \$_1(i_2) + b$ .  $\{p : \mathcal{P}[p]\} = \{q : \mathcal{Q}[q]\}$ .  $\square$

(14)  $\{p : p(i_1) = a\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .

PROOF: Set  $i_2 =$  the element of  $n$ . Define  $\mathcal{P}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv \$_1(i_1) = a$ . Define  $\mathcal{Q}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv 1 \cdot \$_1(i_1) = 0 \cdot \$_1(i_2) + a$ .  $\{p : \mathcal{P}[p]\} = \{q : \mathcal{Q}[q]\}$ .  $\square$

(15)  $\{p : p(i_1) = a \cdot p(i_2) + b\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .

PROOF: Define  $\mathcal{P}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv \$_1(i_1) = a \cdot \$_1(i_2) + b$ . Define  $\mathcal{Q}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv 1 \cdot \$_1(i_1) = a \cdot \$_1(i_2) + b$ .  $\{p : \mathcal{P}[p]\} = \{q : \mathcal{Q}[q]\}$ .  $\square$

(16)  $\{p : a \cdot p(i_1) \neq b \cdot p(i_2) + c\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .

PROOF: Define  $\mathcal{P}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv a \cdot \$_1(i_1) > b \cdot \$_1(i_2) + c$ . Define  $\mathcal{Q}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv a \cdot \$_1(i_1) + -c < b \cdot \$_1(i_2)$ . Define  $\mathcal{R}$ [finite

0-sequence of  $\mathbb{N}$ ]  $\equiv \mathcal{P}[\$1]$  or  $\mathcal{Q}[\$1]$ . Define  $\mathcal{S}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv a \cdot \$1(i_1) \neq b \cdot \$1(i_2) + c$ .  $\{p : \mathcal{P}[p]\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$ .  $\{p : \mathcal{Q}[p]\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$ .  $\{p : \mathcal{P}[p]$  or  $\mathcal{Q}[p]\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$ .  $\mathcal{R}[p]$  iff  $\mathcal{S}[p]$ .  $\{p : \mathcal{R}[p]\} = \{q : \mathcal{S}[q]\}$ .  $\square$

- (17)  $\{p : a \cdot p(i_1) > b \cdot p(i_2) \cdot p(i_3)\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$ .

PROOF: Define  $\mathcal{P}$ [natural number, natural number, integer]  $\equiv a \cdot \$1 > \$3 + 0$ . Define  $\mathcal{F}$ (natural number, natural number, natural number)  $= b \cdot \$2 \cdot \$3$ . Define  $\mathcal{Q}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv a \cdot \$1(i_1) > b \cdot \$1(i_2) \cdot \$1(i_3) + 0$ . Define  $\mathcal{R}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv a \cdot \$1(i_1) > b \cdot \$1(i_2) \cdot \$1(i_3)$ .

For every  $n, i_1, i_2, i_3$ , and  $c$ ,  $\{p : \mathcal{P}[p(i_1), p(i_2), c \cdot p(i_3)]\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$ . For every  $n, i_1, i_2, i_3, i_4$ , and  $c$ ,  $\{p : \mathcal{F}(p(i_1), p(i_2), p(i_3)) = c \cdot p(i_4)\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$ . For every  $n, i_1, i_2, i_3, i_4$ , and  $i_5$ ,  $\{p : \mathcal{P}[p(i_1), p(i_2), \mathcal{F}(p(i_3), p(i_4), p(i_5))]\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$ .  $\{p : \mathcal{Q}[p]\} = \{q : \mathcal{R}[q]\}$ .  $\square$

Let us consider  $a, b, c, i_1, i_2$ , and  $i_3$ . Now we state the propositions:

- (18)  $\{p : a \cdot p(i_1) < b \cdot p(i_2) + c \cdot p(i_3)\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$ .

PROOF: Define  $\mathcal{P}$ [natural number, natural number, integer]  $\equiv a \cdot \$1 + 0 < \$3$ . Define  $\mathcal{F}$ (natural number, natural number, natural number)  $= b \cdot \$2 + c \cdot \$3 + 0$ . Define  $\mathcal{Q}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv a \cdot \$1(i_1) + 0 < b \cdot \$1(i_2) + c \cdot \$1(i_3) + 0$ . Define  $\mathcal{R}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv a \cdot \$1(i_1) < b \cdot \$1(i_2) + c \cdot \$1(i_3)$ . For every  $n, i_1, i_2, i_3$ , and  $d$ ,  $\{p : \mathcal{P}[p(i_1), p(i_2), d \cdot p(i_3)]\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$ .

For every  $n, i_1, i_2, i_3, i_4$ , and  $d$ ,  $\{p : \mathcal{F}(p(i_1), p(i_2), p(i_3)) = d \cdot p(i_4)\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$ . For every  $n, i_1, i_2, i_3, i_4$ , and  $i_5$ ,  $\{p : \mathcal{P}[p(i_1), p(i_2), \mathcal{F}(p(i_3), p(i_4), p(i_5))]\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$ .  $\{p : \mathcal{Q}[p]\} = \{q : \mathcal{R}[q]\}$ .  $\square$

- (19)  $\{p : a \cdot p(i_1) = b \cdot p(i_2) - c \cdot p(i_3)\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$ .

PROOF: Define  $\mathcal{P}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv a \cdot \$1(i_1) = b \cdot \$1(i_2) + (-c) \cdot \$1(i_3) + 0$ . Define  $\mathcal{Q}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv b \cdot \$1(i_2) \geq c \cdot \$1(i_3) + 0$ . Define  $\mathcal{R}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv a \cdot \$1(i_1) = 0 \cdot \$1(i_2) \cdot \$1(i_3)$ . Define  $\mathcal{S}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv b \cdot \$1(i_2) + 0 < c \cdot \$1(i_3)$ . Define  $\mathcal{U}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv \mathcal{P}[\$1]$  and  $\mathcal{Q}[\$1]$ .  $\{p : \mathcal{P}[p]\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$ .  $\{p : \mathcal{Q}[p]\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$ .  $\{p : \mathcal{P}[p]$  and  $\mathcal{Q}[p]\}$  is a diophantine subset of the  $n$ -xtuples of  $\mathbb{N}$ .

Define  $\mathcal{W}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv \mathcal{R}[\$1]$  and  $\mathcal{S}[\$1]$ .  $\{p : \mathcal{R}[p]\}$  is

a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .  $\{p : \mathcal{S}[p]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .  $\{p : \mathcal{R}[p] \text{ and } \mathcal{S}[p]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ . Define  $\mathcal{V}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv \mathcal{U}[\$1]$  or  $\mathcal{W}[\$1]$ . Define  $\mathcal{T}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv a \cdot \$1(i_1) = b \cdot \$1(i_2) -' c \cdot \$1(i_3)$ .  $\{p : \mathcal{U}[p] \text{ or } \mathcal{W}[p]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .  $\mathcal{V}[p]$  iff  $\mathcal{T}[p]$ .  $\{p : \mathcal{V}[p]\} = \{q : \mathcal{T}[q]\}$ .  $\square$

(20)  $\{p : a \cdot p(i_1) = b \cdot p(i_2) -' c\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .

PROOF: Define  $\mathcal{P}$ [natural number, natural number, integer]  $\equiv a \cdot \$1 = b \cdot \$2 -' \$3$ . For every  $n, i_1, i_2, i_3$ , and  $d$ ,  $\{p : \mathcal{P}[p(i_1), p(i_2), d \cdot p(i_3)]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ . Define  $\mathcal{F}$ (natural number, natural number, natural number)  $= c$ . For every  $n, i_1, i_2, i_3, i_4$ , and  $d$ ,  $\{p : \mathcal{F}(p(i_1), p(i_2), p(i_3)) = d \cdot p(i_4)\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ . For every  $n, i_1, i_2, i_3, i_4$ , and  $i_5$ ,  $\{p : \mathcal{P}[p(i_1), p(i_2), \mathcal{F}(p(i_3), p(i_4), p(i_5))]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .  $\square$

(21)  $\{p : a \cdot p(i_1) \equiv b \cdot p(i_2) \pmod{c \cdot p(i_3)}\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .

PROOF: Define  $\mathcal{P}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv$  there exists a natural number  $z$  such that  $a \cdot \$1(i_1) = b \cdot \$1(i_2) + z \cdot c \cdot \$1(i_3)$ . Define  $\mathcal{Q}$ [finite 0-sequence of  $\mathbb{N}$ ]  $\equiv$  there exists a natural number  $z$  such that  $b \cdot \$1(i_2) = a \cdot \$1(i_1) + z \cdot c \cdot \$1(i_3)$ .  $\{p : \mathcal{P}[p]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .  $\{p : \mathcal{Q}[p]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ .  $\{p : \mathcal{P}[p] \text{ or } \mathcal{Q}[p]\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ . Set  $P = \{p : a \cdot p(i_1) \equiv b \cdot p(i_2) \pmod{c \cdot p(i_3)}\}$ .  $P \subseteq \{p : \mathcal{P}[p] \text{ or } \mathcal{Q}[p]\}$ .  $\{p : \mathcal{P}[p] \text{ or } \mathcal{Q}[p]\} \subseteq P$ .  $\square$

(22)  $\{p : \langle a \cdot p(i_1), b \cdot p(i_2) \rangle$  is Pell's solution of  $(c \cdot p(i_3))^2 -' 1\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ . The theorem is a consequence of (2), (3), (9), (20), (6), (5), and (4).

### 3. MAIN LEMMAS

Let us consider  $i_1, i_2$ , and  $i_3$ . Now we state the propositions:

(23)  $\{p : p(i_1) = y_{p(i_2)}(p(i_3)) \text{ and } p(i_2) > 1\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ . The theorem is a consequence of (2), (3), (7), (22), (8), (21), (14), (12), (9), (5), and (4).

(24)  $\{p : p(i_2) = p(i_1)^{p(i_3)}\}$  is a diophantine subset of the  $n$ -tuples of  $\mathbb{N}$ . The theorem is a consequence of (2), (3), (14), (7), (6), (9), (23), (17), (8), (18), (5), and (4).

## REFERENCES

- [1] Zofia Adamowicz and Paweł Zbierski. *Logic of Mathematics: A Modern Course of Classical Logic*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley-Interscience, 1997.
- [2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Kornilowicz, Roman Matuszewski, Adam Naumowicz, Karol Pał, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8\_17.
- [3] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Kornilowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pał. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.
- [4] Martin Davis. Hilbert’s tenth problem is unsolvable. *The American Mathematical Monthly, Mathematical Association of America*, 80(3):233–269, 1973. doi:10.2307/2318447.
- [5] Yatsuka Nakamura and Hisashi Ito. Basic properties and concept of selected subsequence of zero based finite sequences. *Formalized Mathematics*, 16(3):283–288, 2008. doi:10.2478/v10037-008-0034-y.
- [6] Karol Pał. The Matiyasevich theorem. Preliminaries. *Formalized Mathematics*, 25(4):315–322, 2017. doi:10.1515/forma-2017-0029.
- [7] Karol Pał. Diophantine sets. Preliminaries. *Formalized Mathematics*, 26(1):81–90, 2018. doi:10.2478/forma-2018-0007.
- [8] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(4):825–829, 2001.

Accepted June 29, 2018

---