FORMALIZED MATHEMATICS
Vol. 25, No. 4, Pages 315–322, 2017
DOI: 10.1515/forma-2017-0029

DE GRUYTER OPEN
degruyter.com/view/j/forma

# The Matiyasevich Theorem. Preliminaries[1]

Karol Pąk
Institute of Informatics
University of Białystok
Poland

**Summary.** In this article, we prove selected properties of Pell's equation that are essential to finally prove the Diophantine property of two equations. These equations are explored in the proof of Matiyasevich's negative solution of Hilbert's tenth problem.

MSC: 11D45 03B35

Keywords: Pell's equation; Diophantine equation; Hilbert's 10th problem

MML identifier: HILB10_1, version: 8.1.06 5.45.1311

## 0. Introduction

In this article, we prove, using the Mizar formalism, a number of properties that correspond to the Pell's Equation to prove finally two basic lemmas that are essential in the proof of Matiyasevich's negative solution of Hilbert's tenth problem.

For this purpose, first, we focus on a special case of the Pell's Equation, which has the form

$$x^2 - (a^2 - 1)y^2 = 1, \tag{0.1}$$

where $a > 1$ and integer numerical solutions are sought for $x$ and $y$. We develop the Pell's Equation theory formalized for the general case in [1]. Note that $\mathtt{x}_a(0) = 1$, $\mathtt{y}_a(0) = 0$ is an obvious solution. Additionally, if we know a solution of the Pell's equation, we can determine all solutions as well as we can order

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




ISSN 1426–2630(Print), 1898-9934(Online)

them. In our case the $n+1$-solution $\mathtt{x}_a(n+1)$, $\mathtt{y}_a(n+1)$ as shown Theorem 6 can be simply determined in terms of the $n$-solution as follows:

$$\begin{array}{rcl} \mathtt{x}_a(n+1) & = & a \cdot \mathtt{x}_a(n) + (a^2-1) \cdot \mathtt{y}_a(n) \\ \mathtt{y}_a(n+1) & = & \mathtt{x}_a(n) + a \cdot \mathtt{y}_a(n) \end{array} \tag{0.2}$$

We show a number of dependency between the elements of these sequences to provide that the equality $\mathtt{y}_a(z) = y$ is Diophantine. For this purpose we justify in Theorem 38 that for a given $a$, $z$, $y$ holds $\mathtt{y}_a(z) = y$ if and only if the following system has a solution for natural numbers $x$, $x_1$, $y_1$, $A$, $x_2$, $y_2$:

$$\begin{array}{l} a > 1 \ \wedge \ y_1 \geqslant y \ \wedge \ A > y \ \wedge \ y \geqslant z \ \wedge \\ x^2 - (a^2-1)y^2 = 1 \ \wedge \ x_1^2 - (a^2-1)y_1^2 = 1 \ \wedge \\ x_2^2 - (A^2-1)y_2^2 = 1 \ \wedge \ y_2 \equiv y \bmod x_1 \ \wedge \ A \equiv a \bmod x_1 \ \wedge \\ y_2 \equiv z \bmod 2y \ \wedge \ A \equiv 1 \bmod 2y \ \wedge \ y_1 \equiv 0 \bmod y^2 \end{array} \tag{0.3}$$

Based on this result we prove in Theorem 39 that the equality $y = x^z$ is Diophantine. For this purpose we justify that for a given $x$, $y$, $z$ that $y = x^z$ if and only if

$$\begin{array}{l} (y = 1 \wedge z = 0) \vee \\ (x = 0 \wedge y = 0 \wedge z > 0) \ \vee \ (x = 1 \wedge y = 1 \wedge z > 0) \vee \\ (x > 1 \wedge z > 0 \wedge \exists_{y_1,y_2,y_3,K \in \mathbb{N}} \\ \qquad y_1 = y_{z+1}(x) \wedge K > 2zy_1 \wedge y_2 = y_{z+1}(K) \wedge y_3 = y_{z+1}(Kx) \wedge \\ \qquad (0 \leqslant y - \frac{y_3}{y_2} < \frac{1}{2} \vee 0 \leqslant \frac{y_3}{y_2} - y < \frac{1}{2})). \end{array} \tag{0.4}$$

The formalization follows Z.Adamowicz, P.Zbierski [2] as well as M.Davis [3].

## 1. Preliminaries

From now on $i$, $j$, $n$, $n_1$, $n_2$, $m$, $k$, $u$ denote natural numbers, $r$, $r_1$, $r_2$ denote real numbers, $x$, $y$ denote integers, and $a$, $b$ denote non trivial natural numbers.

Now we state the propositions:

(1) Let us consider a finite sequence $F$ of elements of $\mathbb{N}$. Suppose for every $k$ such that $1 < k \leqslant \operatorname{len} F$ holds $F(k) \bmod n = 0$. Then $\sum F \bmod n = F(1) \bmod n$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence $F$ of elements of $\mathbb{N}$ such that $\operatorname{len} F = \$_1$ and for every $k$ such that $1 < k \leqslant \operatorname{len} F$ holds $F(k) \bmod n = 0$ holds $\sum F \bmod n = F(1) \bmod n$. $\mathcal{P}[0]$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. $\square$

(2) Let us consider a complex-valued finite sequence $f$. Then there exist complex-valued finite sequences $e$, $o$ such that

(i) $\operatorname{len} e = \lfloor \frac{\operatorname{len} f}{2} \rfloor$, and

(ii) $\operatorname{len} o = \lceil \frac{\operatorname{len} f}{2} \rceil$, and

(iii) $\sum f = \sum e + \sum o$, and

(iv) for every $n$, $e(n) = f(2 \cdot n)$ and $o(n) = f(2 \cdot n - 1)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every complex-valued finite sequence $f$ such that $\operatorname{len} f = \$_1$ there exist complex-valued finite sequences $e$, $o$ such that $\operatorname{len} e = \lfloor \frac{\operatorname{len} f}{2} \rfloor$ and $\operatorname{len} o = \lceil \frac{\operatorname{len} f}{2} \rceil$ and $\sum f = \sum e + \sum o$ and for every $n$, $e(n) = f(2 \cdot n)$ and $o(n) = f(2 \cdot n - 1)$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. $\square$

Let us consider $a$. Let us observe that $a^{\mathbf{2}} -' 1$ is non square.

## 2. SOLUTIONS OF PELL'S EQUATION – SPECIAL CASE

Let $a$, $n$ be natural numbers. Assume $a$ is not trivial. The functor $\mathtt{x}_a(n)$ yielding a natural number is defined by

(Def. 1) for every non trivial natural number $b$ such that $b = a$ there exists a natural number $y$ such that
$it + y \cdot \sqrt{b^{\mathbf{2}} -' 1} = ((\text{the minimal Pell's solution of } (b^{\mathbf{2}} -' 1))_{\mathbf{1}} +$
$(\text{the minimal Pell's solution of } (b^{\mathbf{2}} -' 1))_{\mathbf{2}} \cdot \sqrt{b^{\mathbf{2}} -' 1})^n$.

Assume $a$ is not trivial. The functor $\mathtt{y}_a(n)$ yielding a natural number is defined by

(Def. 2) for every non trivial natural number $b$ such that $b = a$ holds $\mathtt{x}_b(n) + it \cdot \sqrt{b^{\mathbf{2}} -' 1} = ((\text{the minimal Pell's solution of } (b^{\mathbf{2}} -' 1))_{\mathbf{1}} +$
$(\text{the minimal Pell's solution of } (b^{\mathbf{2}} -' 1))_{\mathbf{2}} \cdot \sqrt{b^{\mathbf{2}} -' 1})^n$.

Now we state the propositions:

(3) (i) $\mathtt{x}_a(0) = 1$, and

(ii) $\mathtt{y}_a(0) = 0$.

(4) Suppose $\langle n_1, n_2 \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$. Then there exists $n$ such that

(i) $n_1 = \mathtt{x}_a(n)$, and

(ii) $n_2 = \mathtt{y}_a(n)$.

The theorem is a consequence of (3).

(5) $\langle a, 1 \rangle =$ the minimal Pell's solution of $(a^{\mathbf{2}} -' 1)$.

(6) (i) $\mathtt{x}_a(n+1) = \mathtt{x}_a(n) \cdot a + \mathtt{y}_a(n) \cdot (a^{\mathbf{2}} -' 1)$, and

(ii) $\mathtt{y}_a(n+1) = \mathtt{x}_a(n) + \mathtt{y}_a(n) \cdot a$.

The theorem is a consequence of (5).

(7) $(\mathtt{x}_a(n))^{\mathbf{2}} - (a^{\mathbf{2}} -' 1) \cdot (\mathtt{y}_a(n))^{\mathbf{2}} = 1$. The theorem is a consequence of (3).

(8) (i) $\mathtt{x}_a(n) + \mathtt{y}_a(n) \cdot \sqrt{a^{\mathbf{2}} -' 1} = (a + \sqrt{a^{\mathbf{2}} -' 1})^n$, and

(ii) $\mathtt{x}_a(n) + -\mathtt{y}_a(n) \cdot \sqrt{a^{\mathbf{2}} -' 1} = (a - \sqrt{a^{\mathbf{2}} -' 1})^n$.

The theorem is a consequence of (5).

(9) There exist finite sequences $F_2$, $F_1$ of elements of $\mathbb{N}$ such that

(i) $\sum F_2 = \mathtt{y}_a(n)$, and

(ii) $\operatorname{len} F_2 = \lfloor \frac{n+1}{2} \rfloor$, and

(iii) for every $i$ such that $1 \leqslant i \leqslant \frac{n+1}{2}$ holds $F_2(i) = \binom{n}{2 \cdot i -' 1} \cdot (a^{n+1-'2 \cdot i}) \cdot (a^{\mathbf{2}} -' 1)^{i-'1}$, and

(iv) $a^n + \sum F_1 = \mathtt{x}_a(n)$, and

(v) $\operatorname{len} F_1 = \lfloor \frac{n}{2} \rfloor$, and

(vi) for every $i$ such that $1 \leqslant i \leqslant \frac{n}{2}$ holds $F_1(i) = \binom{n}{2 \cdot i} \cdot (a^{n-'2 \cdot i}) \cdot (a^{\mathbf{2}} -' 1)^i$.

PROOF: Set $A = a^{\mathbf{2}} -' 1$. Define $\mathcal{P}[\text{natural number}] \equiv$ there exist finite sequences $F_2$, $F_1$ of elements of $\mathbb{N}$ such that $\sum F_2 = \mathtt{y}_a(\$_1)$ and $\operatorname{len} F_2 = \lfloor \frac{\$_1+1}{2} \rfloor$ and for every natural number $i$ such that $1 \leqslant i \leqslant \frac{\$_1+1}{2}$ holds $F_2(i) = \binom{\$_1}{2 \cdot i -' 1} \cdot (a^{\$_1+1-'2 \cdot i}) \cdot (A^{i-'1})$ and $a^{\$_1} + \sum F_1 = \mathtt{x}_a(\$_1)$ and $\operatorname{len} F_1 = \lfloor \frac{\$_1}{2} \rfloor$ and for every natural number $i$ such that $1 \leqslant i \leqslant \frac{\$_1}{2}$ holds $F_1(i) = \binom{\$_1}{2 \cdot i} \cdot (a^{\$_1-'2 \cdot i}) \cdot (A^i)$. $\mathcal{P}[0]$. For every natural number $n$ such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every $n$, $\mathcal{P}[n]$. □

## 3. Solutions of Pell's Equation – Inequalities

Now we state the proposition:

(10) If $k \leqslant n$, then $\mathtt{x}_a(k) \leqslant \mathtt{x}_a(n)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \mathtt{x}_a(k) \leqslant \mathtt{x}_a(k + \$_1)$. For every natural number $i$ such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by (6), [6, (29)]. $\mathcal{P}[n_1]$. □

Let us consider $a$ and $k$. One can verify that $\mathtt{x}_a(k)$ is positive.

Now we state the propositions:

(11) If $k < n$, then $\mathtt{y}_a(k) < \mathtt{y}_a(n)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 > 0$, then $\mathtt{y}_a(k) < \mathtt{y}_a(k + \$_1)$. For every natural number $i$ such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. $\mathcal{P}[n_1]$. □

(12) If $\mathtt{y}_a(k) = \mathtt{y}_a(n)$, then $k = n$. The theorem is a consequence of (11).

(13) $\mathtt{y}_a(n) \geqslant n$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \mathtt{y}_a(\$_1) \geqslant \$_1$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. □

Let us consider $a$. Let $k$ be a non zero natural number. Observe that $\mathtt{y}_a(k)$ is non zero.

Let $a$ be a non trivial natural number and $x$ be a positive natural number. Note that $a \cdot x$ is non trivial.

Now we state the propositions:

(14) If $a \neq 2$ and $k \leqslant n$, then $2 \cdot (\mathtt{y}_a(k)) < \mathtt{x}_a(n)$. The theorem is a consequence of (7) and (10).

(15) If $a = 2$ and $k \leqslant n$, then $\sqrt{3} \cdot (\mathtt{y}_a(k)) < \mathtt{x}_a(n)$. The theorem is a consequence of (7) and (10).

(16) If $a = 2$ and $k < n$, then $(3 + 2 \cdot \sqrt{3}) \cdot \mathtt{y}_a(k) < \mathtt{x}_a(n)$. The theorem is a consequence of (6) and (15).

(17) (i) $(2 \cdot a - 1)^n \cdot (a - 1) \leqslant \mathtt{x}_a(n + 1) \leqslant a \cdot (2 \cdot a)^n$, and

(ii) $(2 \cdot a - 1)^n \leqslant \mathtt{y}_a(n + 1) \leqslant 2 \cdot a^n$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv (2 \cdot a - 1)^{\$_1} \leqslant \mathtt{y}_a(\$_1 + 1) \leqslant 2 \cdot a^{\$_1}$ and $(2 \cdot a - 1)^{\$_1} \cdot (a-1) \leqslant \mathtt{x}_a(\$_1+1) \leqslant a \cdot (2 \cdot a^{\$_1})$. $\mathtt{y}_a(0) = 0$ and $\mathtt{x}_a(0) = 1$. $\mathtt{y}_a(1 + 0) = 1 + 0 \cdot a$ and $\mathtt{x}_a(1 + 0) = 1 \cdot a + 0 \cdot (a^{\mathbf{2}} -' 1)$. If $\mathcal{P}[k]$, then $\mathcal{P}[k + 1]$. $\mathcal{P}[k]$. $\square$

Let us consider a positive natural number $x$. Now we state the propositions:

(18) $x^n \cdot (1 - \frac{1}{2 \cdot a \cdot x})^n \leqslant \frac{\mathtt{y}_{a \cdot x}(n+1)}{\mathtt{y}_a(n+1)} \leqslant x^n \cdot \frac{1}{(1 - \frac{1}{2 \cdot a})^n}$. The theorem is a consequence of (17).

(19) If $a > 2 \cdot n \cdot x^n$, then $x^n - \frac{1}{2} < \frac{\mathtt{y}_{a \cdot x}(n+1)}{\mathtt{y}_a(n+1)} < x^n + \frac{1}{2}$. The theorem is a consequence of (18).

## 4. SOLUTIONS OF PELL'S EQUATION – EQUALITY

Now we state the propositions:

(20) If $x \geqslant 0$, then $(\operatorname{sgn} x) \cdot (\mathtt{y}_a(|x|)) = \mathtt{y}_a(|x|)$. The theorem is a consequence of (3).

(21) If $x \leqslant 0$, then $(\operatorname{sgn} x) \cdot (\mathtt{y}_a(|x|)) = -\mathtt{y}_a(|x|)$. The theorem is a consequence of (3).

(22) (i) $\mathtt{x}_a(|x+y|) = (\mathtt{x}_a(|x|)) \cdot (\mathtt{x}_a(|y|)) + (a^{\mathbf{2}} -' 1) \cdot (\operatorname{sgn} x) \cdot (\mathtt{y}_a(|x|)) \cdot (\operatorname{sgn} y) \cdot (\mathtt{y}_a(|y|))$, and

(ii) $(\operatorname{sgn}(x + y)) \cdot (\mathtt{y}_a(|x + y|)) = (\mathtt{x}_a(|x|)) \cdot (\operatorname{sgn} y) \cdot (\mathtt{y}_a(|y|)) + (\operatorname{sgn} x) \cdot (\mathtt{y}_a(|x|)) \cdot (\mathtt{x}_a(|y|))$.

The theorem is a consequence of (20), (8), and (21).

## 5. Solutions of Pell's Equation – Congruences

Now we state the propositions:

(23) $\mathtt{x}_a(n)$ and $\mathtt{y}_a(n)$ are relatively prime.
PROOF: Define $\mathcal{P}$[natural number] $\equiv \gcd(\mathtt{x}_a(\$_1), \mathtt{y}_a(\$_1)) = 1$. $\mathtt{x}_a(0) = 1$ and $\mathtt{y}_a(0) = 0$. For every $n$ such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by (6), [4, (8)], [7, (1), (5)]. For every $n$, $\mathcal{P}[n]$. □

(24) $\mathtt{y}_a(n) \equiv n \pmod{a-1}$. The theorem is a consequence of (9), (3), and (1).

(25) (i) $\mathtt{x}_a(n) \equiv \mathtt{x}_b(n) \pmod{a-b}$, and
(ii) $\mathtt{y}_a(n) \equiv \mathtt{y}_b(n) \pmod{a-b}$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv \mathtt{x}_a(\$_1) \equiv \mathtt{x}_b(\$_1) \pmod{a-b}$ and $\mathtt{y}_a(\$_1) \equiv \mathtt{y}_b(\$_1) \pmod{a-b}$. $\mathtt{x}_a(0) = 1 = \mathtt{x}_b(0)$ and $\mathtt{y}_a(0) = 0 = \mathtt{y}_b(0)$. For every $n$ such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every $n$, $\mathcal{P}[n]$. □

(26) If $a \equiv b \pmod{k}$, then $\mathtt{y}_a(n) \equiv \mathtt{y}_b(n) \pmod{k}$. The theorem is a consequence of (25).

(27) $\operatorname{sgn}(2\cdot x+y)\cdot \mathtt{y}_a(|2\cdot x+y|) \equiv -(\operatorname{sgn} y)\cdot \mathtt{y}_a(|y|) \pmod{\mathtt{x}_a(|x|)}$. The theorem is a consequence of (22) and (7).

(28) $(\operatorname{sgn}(4\cdot x\cdot n+y))\cdot(\mathtt{y}_a(|4\cdot x\cdot n+y|)) \equiv (\operatorname{sgn} y)\cdot(\mathtt{y}_a(|y|)) \pmod{\mathtt{x}_a(|x|)}$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv (\operatorname{sgn}(4\cdot x\cdot \$_1+y))\cdot(\mathtt{y}_a(|4\cdot x\cdot \$_1+y|)) \equiv (\operatorname{sgn} y)\cdot(\mathtt{y}_a(|y|)) \pmod{\mathtt{x}_a(|x|)}$. For every $n$ such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every $n$, $\mathcal{P}[n]$. □

(29) $(\operatorname{sgn}(x+y))\cdot(\mathtt{y}_a(|x+y|)) \equiv (\operatorname{sgn}(x-y))\cdot(\mathtt{y}_a(|x-y|)) \pmod{\mathtt{x}_a(|x|)}$. The theorem is a consequence of (27).

(30) If $n_1 < n_2 \leqslant n$ and $|x| = \mathtt{y}_a(n_1)$ and $|y| = \mathtt{y}_a(n_2)$ and $x \equiv y \pmod{\mathtt{x}_a(n)}$, then $x = y$.
PROOF: Consider $i$ being an integer such that $x-y = (\mathtt{x}_a(n))\cdot i$. $-\mathtt{x}_a(n) < x-y < \mathtt{x}_a(n)$. □

(31) Suppose $n_1 \leqslant 2\cdot n$ and $n_2 \leqslant 2\cdot n$ and $|x| = \mathtt{y}_a(n_1)$ and $|y| = \mathtt{y}_a(n_2)$ and $x \equiv y \pmod{\mathtt{x}_a(n)}$. Then
(i) $n_1 \equiv n_2 \pmod{2\cdot n}$, or
(ii) $n_1 \equiv -n_2 \pmod{2\cdot n}$.

(32) Suppose $n_1 \leqslant 4\cdot n$ and $n_2 \leqslant 4\cdot n$ and $|x| = \mathtt{y}_a(n_1)$ and $|y| = \mathtt{y}_a(n_2)$ and $x \equiv y \pmod{\mathtt{x}_a(n)}$. Then
(i) $n_1 \equiv n_2 \pmod{2\cdot n}$, or
(ii) $n_1 \equiv -n_2 \pmod{2\cdot n}$.
The theorem is a consequence of (31).

(33) Suppose $\mathtt{y}_a(n_1) \equiv \mathtt{y}_a(n_2) \pmod{\mathtt{x}_a(n)}$ and $n > 0$. Then

(i) $n_1 \equiv n_2 \pmod{2 \cdot n}$, or

(ii) $n_1 \equiv -n_2 \pmod{2 \cdot n}$.

The theorem is a consequence of (28), (20), and (32).

## 6. Solutions of Pell's Equation – Divisibility

Now we state the propositions:

(34) $\mathtt{y}_a(n) \mid \mathtt{y}_a(n \cdot k)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv \mathtt{y}_a(n) \mid \mathtt{y}_a(n \cdot \$_1)$. $(\mathtt{y}_a(n)) \cdot 0 = \mathtt{y}_a(n \cdot 0)$. For every $k$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every $k$, $\mathcal{P}[k]$. $\square$

(35) $\mathtt{y}_a(n \cdot k) \equiv k \cdot ((\mathtt{x}_a(n))^{k-'1}) \cdot (\mathtt{y}_a(n)) \pmod{(\mathtt{y}_a(n))^{\mathbf{2}}}$. The theorem is a consequence of (3), (2), and (1).

(36) If $k > 0$ and $\mathtt{y}_a(k) \mid \mathtt{y}_a(n)$, then $k \mid n$.

PROOF: Set $P = \mathtt{y}_a(k)$. Set $r = n \bmod k$. Set $q = n \operatorname{div} k$. $(\operatorname{sgn} n) \cdot (\mathtt{y}_a(|n|)) = (\mathtt{x}_a(|r|)) \cdot (\operatorname{sgn} q \cdot k) \cdot (\mathtt{y}_a(|q \cdot k|)) + (\operatorname{sgn} r) \cdot (\mathtt{y}_a(|r|)) \cdot (\mathtt{x}_a(|q \cdot k|))$. $\mathtt{y}_a(n) = (\mathtt{x}_a(|r|)) \cdot ((\operatorname{sgn} q \cdot k) \cdot (\mathtt{y}_a(|q \cdot k|))) + (\operatorname{sgn} r) \cdot (\mathtt{y}_a(|r|)) \cdot (\mathtt{x}_a(|q \cdot k|))$. $P \mid \mathtt{y}_a(q \cdot k)$. $P \mid (\mathtt{x}_a(r)) \cdot (\mathtt{y}_a(q \cdot k))$. $P$ and $\mathtt{x}_a(k \cdot q)$ are relatively prime. $r = 0$ by [5, (6)], (11). $\square$

(37) If $(\mathtt{y}_a(k))^{\mathbf{2}} \mid \mathtt{y}_a(n)$, then $\mathtt{y}_a(k) \mid n$. The theorem is a consequence of (3), (36), (35), and (23).

## 7. Special Case of Pell's Equation is Diophantine

Now we state the proposition:

(38) Let us consider natural numbers $y$, $z$, $a$. Then $y = \mathtt{y}_a(z)$ and $a > 1$ if and only if there exist natural numbers $x$, $x_1$, $y_1$, $A$, $x_2$, $y_2$ such that $a > 1$ and $\langle x, y \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$ and $\langle x_1, y_1 \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$ and $y_1 \geqslant y$ and $A > y \geqslant z$ and $\langle x_2, y_2 \rangle$ is a Pell's solution of $A^{\mathbf{2}} -' 1$ and $y_2 \equiv y \pmod{x_1}$ and $A \equiv a \pmod{x_1}$ and $y_2 \equiv z \pmod{2 \cdot y}$ and $A \equiv 1 \pmod{2 \cdot y}$ and $y_1 \equiv 0 \pmod{y^{\mathbf{2}}}$.

PROOF: If $y = \mathtt{y}_a(z)$ and $a > 1$, then there exist natural numbers $x$, $x_1$, $y_1$, $A$, $x_2$, $y_2$ such that $a > 1$ and $\langle x, y \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$ and $\langle x_1, y_1 \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$ and $y_1 \geqslant y$ and $A > y \geqslant z$ and $\langle x_2, y_2 \rangle$ is a Pell's solution of $A^{\mathbf{2}} -' 1$ and $y_2 \equiv y \pmod{x_1}$ and $A \equiv a \pmod{x_1}$ and $y_2 \equiv z \pmod{2 \cdot y}$ and $A \equiv 1 \pmod{2 \cdot y}$ and $y_1 \equiv 0 \pmod{y^{\mathbf{2}}}$. $\square$

## 8. Exponential Function is Diophantine

Now we state the proposition:

(39) Let us consider natural numbers $x$, $y$, $z$. Then $y = x^z$ if and only if $y = 1$ and $z = 0$ or $x = 0$ and $y = 0$ and $z > 0$ or $x = 1$ and $y = 1$ and $z > 0$ or $x > 1$ and $z > 0$ and there exist natural numbers $y_1$, $y_2$, $y_3$, $K$ such that $y_1 = \mathtt{y}_x(z+1)$ and $K > 2 \cdot z \cdot y_1$ and $y_2 = \mathtt{y}_K(z+1)$ and $y_3 = \mathtt{y}_{K \cdot x}(z+1)$ and $(0 \leqslant y - \frac{y_3}{y_2} < \frac{1}{2}$ or $0 \leqslant \frac{y_3}{y_2} - y < \frac{1}{2})$.

Proof: If $y = x^z$, then $y = 1$ and $z = 0$ or $x = 0$ and $y = 0$ and $z > 0$ or $x = 1$ and $y = 1$ and $z > 0$ or $x > 1$ and $z > 0$ and there exist natural numbers $y_1$, $y_2$, $y_3$, $K$ such that $y_1 = \mathtt{y}_x(z+1)$ and $K > 2 \cdot z \cdot y_1$ and $y_2 = \mathtt{y}_K(z+1)$ and $y_3 = \mathtt{y}_{K \cdot x}(z+1)$ and $(0 \leqslant y - \frac{y_3}{y_2} < \frac{1}{2}$ or $0 \leqslant \frac{y_3}{y_2} - y < \frac{1}{2})$. □

## References


[1] Marcin Acewicz and Karol Pąk. Pell's equation. *Formalized Mathematics*, 25(**3**):197–204, 2017. doi:10.1515/forma-2017-0019.

[2] 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.

[3] 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.

[4] Yoshinori Fujisawa and Yasushi Fuwa. The Euler's function. *Formalized Mathematics*, 6 (**4**):549–551, 1997.

[5] Xiquan Liang, Li Yan, and Junjie Zhao. Linear congruence relation and complete residue systems. *Formalized Mathematics*, 15(**4**):181–187, 2007. doi:10.2478/v10037-007-0022-7.

[6] Robert Milewski. Natural numbers. *Formalized Mathematics*, 7(**1**):19–22, 1998.

[7] Rafał Ziobro. Fermat's Little Theorem via divisibility of Newton's binomial. *Formalized Mathematics*, 23(**3**):215–229, 2015. doi:10.1515/forma-2015-0018.


*Received November 29, 2017*

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.