

The Matiyasevich Theorem. Preliminaries¹

Karol Pałk
Institute of Informatics
University of Białystok
Poland

Summary. *czkam rzewnie*

MSC: 03B35

Keywords:

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

$$x^2 - (a^2 - 1)y^2 = 1, \quad (0.1)$$

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 $x_0(a) = 1$, $y_0(a) = 0$ 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 them. In our case the $n + 1$ -solution $x_{n+1}(a)$, $y_{n+1}(a)$ can be simply determined in terms of the n -solution as follows:

$$\begin{aligned} x_{n+1}(a) &= a \cdot x_n(a) + (a^2 - 1) \cdot y_n(a) \\ y_{n+1}(a) &= x_n(a) + a \cdot y_n(a) \end{aligned} \quad (0.2)$$

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

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

$$\begin{aligned}
 & a > 1 \wedge y_1 \geq y \wedge A > y \wedge y \geq z \wedge \\
 & x^2 - (a^2 - 1)y^2 = 1 \wedge x_1^2 - (a^2 - 1)y_1^2 = 1 \wedge x_2^2 - (A^2 - 1)y_2^2 = 1 \wedge \\
 & y_2 \equiv y \pmod{x_1} \wedge A \equiv a \pmod{x_1} \wedge \\
 & y_2 \equiv z \pmod{2y} \wedge A \equiv 1 \pmod{2y} \wedge y_1 \equiv 0 \pmod{y^2}
 \end{aligned} \tag{0.3}$$

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

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

The formalization follows Z. Adamowicz, P. Zbierski [2] as well as M. Davis [8].

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 $1 < k \leq \text{len } F$ holds $F(k) \pmod n = 0$. Then $\sum F \pmod n = F(1) \pmod n$.

PROOF: Define \mathcal{P} [natural number] \equiv for every finite sequence F of elements of \mathbb{N} such that $\text{len } F = n$ and for every k such that $1 < k \leq \text{len } F$ holds $F(k) \pmod n = 0$ holds $\sum F \pmod n = F(1) \pmod n$. $\mathcal{P}[0]$ by [7, (72)]. If $\mathcal{P}[k]$, then $\mathcal{P}[k + 1]$ by [4, (40)], [6, (6), (10)], [7, (74)]. $\mathcal{P}[k]$ from [3, Sch. 2]. \square

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

- (i) $\text{len } e = \lfloor \frac{\text{len } f}{2} \rfloor$, and
- (ii) $\text{len } o = \lceil \frac{\text{len } f}{2} \rceil$, 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 $\text{len } f = \mathbb{S}_1$ there exist complex-valued finite sequences e, o such that $\text{len } e = \lfloor \frac{\text{len } f}{2} \rfloor$ and $\text{len } o = \lceil \frac{\text{len } f}{2} \rceil$ and $\sum f = \sum e + \sum o$ and for every n , $e(n) = f(2 \cdot n)$ and $o(n) = f(2 \cdot n - 1)$. $\mathcal{P}[0]$ by [15, (25), (30)], [7, (72)]. If $\mathcal{P}[n]$, then $\mathcal{P}[n + 1]$ by [16, (55)], [3, (13)], [4, (59)], [5, (16)]. $\mathcal{P}[n]$ from [3, Sch. 2]. \square

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

2. SOLUTIONS OF PELL'S EQUATION - SPECIAL CASE

Let a, n be natural numbers. Assume a is not trivial. The functor $\mathbf{x}_a(n)$ 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 $it + y \cdot \sqrt{b^2 - '1} = (((\text{the minimal Pell's solution of } (b^2 - '1)))_1)$

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

(Def. 2) for every non trivial natural number b such that $b = a$ holds $\mathbf{x}_b(n) + it \cdot \sqrt{b^2 - '1} = (((\text{the minimal Pell's solution of } (b^2 - '1)))_1) + (((\text{the minimal Pell's solution of } (b^2 - '1)))_2)$

Now we state the propositions:

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

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

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

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

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

The theorem is a consequence of (3).

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

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

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

The theorem is a consequence of (5).

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

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

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

The theorem is a consequence of (5).

- (9) There exist finite sequences F_2, F_1 of elements of \mathbb{N} such that
- (i) $\sum F_2 = y_a(n)$, and
 - (ii) $\text{len } F_2 = \lfloor \frac{n+1}{2} \rfloor$, and
 - (iii) for every i such that $1 \leq i \leq \frac{n+1}{2}$ holds $F_2(i) = \binom{n}{2 \cdot i - 1} \cdot (a^{n+1-2 \cdot i}) \cdot ((a^2 - 1)^{i-1})$, and
 - (iv) $a^n + \sum F_1 = x_a(n)$, and
 - (v) $\text{len } F_1 = \lfloor \frac{n}{2} \rfloor$, and
 - (vi) for every i such that $1 \leq i \leq \frac{n}{2}$ holds $F_1(i) = \binom{n}{2 \cdot i} \cdot (a^{n-2 \cdot i}) \cdot ((a^2 - 1)^i)$.

PROOF: Set $A = a^2 - 1$. Define $\mathcal{P}[\text{natural number}] \equiv$ there exist finite sequences F_2, F_1 of elements of \mathbb{N} such that $\sum F_2 = y_a(\$1)$ and $\text{len } F_2 = \lfloor \frac{\$1+1}{2} \rfloor$ and for every natural number i such that $1 \leq i \leq \frac{\$1+1}{2}$ holds $F_2(i) = \binom{\$1}{2 \cdot i - 1} \cdot (a^{\$1+1-2 \cdot i}) \cdot (A^{i-1})$ and $a^{\$1} + \sum F_1 = x_a(\$1)$ and $\text{len } F_1 = \lfloor \frac{\$1}{2} \rfloor$ and for every natural number i such that $1 \leq i \leq \frac{\$1}{2}$ holds $F_1(i) = \binom{\$1}{2 \cdot i} \cdot (a^{\$1-2 \cdot i}) \cdot (A^i)$. $\mathcal{P}[0]$ by (3), [7, (72)], [10, (4)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by (6), [10, (6)], [7, (87), (74), (76)]. For every n , $\mathcal{P}[n]$ from [3, Sch. 2]. \square

3. SOLUTIONS OF PELL'S EQUATION - INEQUALITIES

Now we state the proposition:

- (10) If $k \leq n$, then $x_a(k) \leq x_a(n)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv x_a(k) \leq x_a(k + \$1)$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by (6), [13, (29)]. $\mathcal{P}[n_1]$ from [3, Sch. 2]. \square

Let us consider a and k . One can verify that $x_a(k)$ is positive.

Now we state the propositions:

- (11) If $k < n$, then $y_a(k) < y_a(n)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$1 > 0$, then $y_a(k) < y_a(k + \$1)$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by (6), [13, (29)]. $\mathcal{P}[n_1]$ from [3, Sch. 2]. \square

- (12) If $y_a(k) = y_a(n)$, then $k = n$. The theorem is a consequence of (11).

- (13) $y_a(n) \geq n$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv y_a(\$1) \geq \$1$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$ by [3, (13)], (11). $\mathcal{P}[k]$ from [3, Sch. 2]. \square

Let us consider a . Let k be a non zero natural number. Observe that $y_a(k)$ 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 $k \leq n$, then $2 \cdot (y_a(k)) < x_a(n)$. The theorem is a consequence of (7) and (10).
- (15) If $a = 2$ and $k \leq n$, then $\sqrt{3} \cdot (y_a(k)) < x_a(n)$. The theorem is a consequence of (7) and (10).
- (16) If $a = 2$ and $k < n$, then $(3 + 2 \cdot \sqrt{3}) \cdot (y_a(k)) < x_a(n)$. The theorem is a consequence of (6) and (15).
- (17) (i) $(2 \cdot a - 1)^n \cdot (a - 1) \leq x_a(n + 1) \leq a \cdot (2 \cdot a^n)$, and
 (ii) $(2 \cdot a - 1)^n \leq y_a(n + 1) \leq 2 \cdot a^n$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv (2 \cdot a - 1)^{\$1} \leq y_a(\$1 + 1) \leq 2 \cdot a^{\$1}$ and $(2 \cdot a - 1)^{\$1} \cdot (a - 1) \leq x_a(\$1 + 1) \leq a \cdot (2 \cdot a^{\$1})$. $y_a(0) = 0$ and $x_a(0) = 1$. $y_a(1 + 0) = 1 + 0 \cdot a$ and $x_a(1 + 0) = 1 \cdot a + 0 \cdot (a^2 - 1)$. If $\mathcal{P}[k]$, then $\mathcal{P}[k + 1]$ by (6), [10, (6)], [3, (14)]. $\mathcal{P}[k]$ from [3, Sch. 2]. \square

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

- (18) $x^n \cdot ((1 - \frac{1}{2 \cdot a \cdot x})^n) \leq \frac{y_{a \cdot x}(n+1)}{y_a(n+1)} \leq x^n \cdot (\frac{1}{(1 - \frac{1}{2 \cdot a})^n})$. The theorem is a consequence of (17).
- (19) If $a > 2 \cdot n \cdot (x^n)$, then $x^n - \frac{1}{2} < \frac{y_{a \cdot x}(n+1)}{y_a(n+1)} < x^n + \frac{1}{2}$. The theorem is a consequence of (18).

4. SOLUTIONS OF PELL'S EQUATION - EQUALITY

Now we state the propositions:

- (20) If $x \geq 0$, then $(\text{sgn } x) \cdot (y_a(|x|)) = y_a(|x|)$. The theorem is a consequence of (3).
- (21) If $x \leq 0$, then $(\text{sgn } x) \cdot (y_a(|x|)) = -y_a(|x|)$. The theorem is a consequence of (3).
- (22) (i) $x_a(|x + y|) = (x_a(|x|)) \cdot (x_a(|y|)) + (a^2 - 1) \cdot (\text{sgn } x) \cdot (y_a(|x|)) \cdot (\text{sgn } y) \cdot (y_a(|y|))$, and
 (ii) $(\text{sgn}(x + y)) \cdot (y_a(|x + y|)) = (x_a(|x|)) \cdot (\text{sgn } y) \cdot (y_a(|y|)) + (\text{sgn } x) \cdot (y_a(|x|)) \cdot (x_a(|y|))$.

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

5. SOLUTIONS OF PELL'S EQUATION - CONGRUENCES

Now we state the propositions:

(23) $x_a(n)$ and $y_a(n)$ are relatively prime.

PROOF: Define \mathcal{P} [natural number] $\equiv \gcd(x_a(\$1), y_a(\$1)) = 1$. $x_a(0) = 1$ and $y_a(0) = 0$. For every n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [3, (14)], (6), [9, (8)], [17, (1), (5)]. For every n , $\mathcal{P}[n]$ from [3, Sch. 2]. \square

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

(25) (i) $x_a(n) \equiv x_b(n) \pmod{a-b}$, and

(ii) $y_a(n) \equiv y_b(n) \pmod{a-b}$.

PROOF: Define \mathcal{P} [natural number] $\equiv x_a(\$1) \equiv x_b(\$1) \pmod{a-b}$ and $y_a(\$1) \equiv y_b(\$1) \pmod{a-b}$. $x_a(0) = 1 = x_b(0)$ and $y_a(0) = 0 = y_b(0)$. For every n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [3, (14)], (6), [15, (18), (16)]. For every n , $\mathcal{P}[n]$ from [3, Sch. 2]. \square

(26) If $a \equiv b \pmod{k}$, then $y_a(n) \equiv y_b(n) \pmod{k}$. The theorem is a consequence of (25).

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

(28) $(\operatorname{sgn}(4 \cdot x \cdot n + y)) \cdot (y_a(|4 \cdot x \cdot n + y|)) \equiv (\operatorname{sgn} y) \cdot (y_a(|y|)) \pmod{x_a(|x|)}$.

PROOF: Define \mathcal{P} [natural number] $\equiv (\operatorname{sgn}(4 \cdot x \cdot \$1 + y)) \cdot (y_a(|4 \cdot x \cdot \$1 + y|)) \equiv (\operatorname{sgn} y) \cdot (y_a(|y|)) \pmod{x_a(|x|)}$. For every n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [15, (15)]. For every n , $\mathcal{P}[n]$ from [3, Sch. 2]. \square

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

(30) If $n_1 < n_2 \leq n$ and $|x| = y_a(n_1)$ and $|y| = y_a(n_2)$ and $x \equiv y \pmod{x_a(n)}$, then $x = y$.

PROOF: Consider i being an integer such that $x - y = (x_a(n)) \cdot i$. $-x_a(n) < x - y < x_a(n)$ by [14, (25)], (16), (15), (14). \square

(31) Suppose $n_1 \leq 2 \cdot n$ and $n_2 \leq 2 \cdot n$ and $|x| = y_a(n_1)$ and $|y| = y_a(n_2)$ and $x \equiv y \pmod{x_a(n)}$. Then

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

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

(32) Suppose $n_1 \leq 4 \cdot n$ and $n_2 \leq 4 \cdot n$ and $|x| = y_a(n_1)$ and $|y| = y_a(n_2)$ and $x \equiv y \pmod{x_a(n)}$. 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 $y_a(n_1) \equiv y_a(n_2) \pmod{x_a(n)}$ 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) $y_a(n) \mid y_a(n \cdot k)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv y_a(n) \mid y_a(n \cdot \mathcal{S}_1)$. $(y_a(n)) \cdot 0 = y_a(n \cdot 0)$. For every k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by (20), (22), [11, (2)]. For every k , $\mathcal{P}[k]$ from [3, Sch. 2]. \square

(35) $y_a(n \cdot k) \equiv k \cdot ((x_a(n))^{k-1}) \cdot (y_a(n)) \pmod{(y_a(n))^2}$. The theorem is a consequence of (3), (2), and (1).

(36) If $k > 0$ and $y_a(k) \mid y_a(n)$, then $k \mid n$.

PROOF: Set $P = y_a(k)$. Set $r = n \bmod k$. Set $q = n \operatorname{div} k$. $(\operatorname{sgn} n) \cdot (y_a(|n|)) = (x_a(|r|)) \cdot (\operatorname{sgn} q \cdot k) \cdot (y_a(|q \cdot k|)) + (\operatorname{sgn} r) \cdot (y_a(|r|)) \cdot (x_a(|q \cdot k|))$. $y_a(n) = (x_a(|r|)) \cdot ((\operatorname{sgn} q \cdot k) \cdot (y_a(|q \cdot k|))) + (\operatorname{sgn} r) \cdot (y_a(|r|)) \cdot (x_a(|q \cdot k|))$. $P \mid y_a(q \cdot k)$. $P \mid (x_a(r)) \cdot (y_a(q \cdot k))$. P and $x_a(k \cdot q)$ are relatively prime by [11, (9), (22)], (23), [11, (13)]. $r = 0$ by [12, (6)], [11, (25)], (11), [15, (58)]. \square

(37) If $(y_a(k))^2 \mid y_a(n)$, then $y_a(k) \mid n$. The theorem is a consequence of (3), (36), (35), and (23).

7. SPECIAL CASE OF PELL'S EQUATION IS DIOPHANTIN

Now we state the proposition:

(38) Let us consider natural numbers y, z, a . Then $y = y_a(z)$ 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 $a^2 - 1$ and $\langle x_1, y_1 \rangle$ is a Pell's solution of $a^2 - 1$ and $y_1 \geq y$ and $A > y \geq z$ and $\langle x_2, y_2 \rangle$ is a Pell's solution of $A^2 - 1$ 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 $y_1 \equiv 0 \pmod{y^2}$.

PROOF: If $y = y_a(z)$ 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 $a^2 - 1$ and $\langle x_1, y_1 \rangle$ is a Pell's solution of $a^2 - 1$ and $y_1 \geq y$ and $A > y \geq z$ and $\langle x_2,$

y_2) is a Pell's solution of $A^2 - 1$ 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 $y_1 \equiv 0 \pmod{y^2}$ by [13, (28)], [3, (13), (14)], (7). \square

8. EXPONENTIAL FUNCTION IS DIOPHANTIN

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 $y_1 = \mathcal{Y}_x(z+1)$ and $K > 2 \cdot z \cdot y_1$ and $y_2 = \mathcal{Y}_K(z+1)$ and $y_3 = \mathcal{Y}_{K \cdot x}(z+1)$ and $(0 \leq y - \frac{y_3}{y_2} < \frac{1}{2}$ or $0 \leq \frac{y_3}{y_2} - y < \frac{1}{2})$.
 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 $y_1 = \mathcal{Y}_x(z+1)$ and $K > 2 \cdot z \cdot y_1$ and $y_2 = \mathcal{Y}_K(z+1)$ and $y_3 = \mathcal{Y}_{K \cdot x}(z+1)$ and $(0 \leq y - \frac{y_3}{y_2} < \frac{1}{2}$ or $0 \leq \frac{y_3}{y_2} - y < \frac{1}{2})$ by [10, (4)], [3, (53), (14)], [10, (11)]. \square

REFERENCES

- [1] Marcin Acewicz and Karol Pałk. 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] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(1):41–46, 1990.
- [4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(1):107–114, 1990.
- [5] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(3):529–536, 1990.
- [6] Czesław Byliński. Some properties of restrictions of finite sequences. *Formalized Mathematics*, 5(2):241–245, 1996.
- [7] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(4):661–668, 1990.
- [8] 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.
- [9] Yoshinori Fujisawa and Yasushi Fuwa. The Euler's function. *Formalized Mathematics*, 6(4):549–551, 1997.
- [10] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(5):887–890, 1990.
- [11] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(5):829–832, 1990.
- [12] 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.
- [13] Robert Milewski. Natural numbers. *Formalized Mathematics*, 7(1):19–22, 1998.
- [14] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(3):445–449, 1990.

- [15] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
- [16] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.
- [17] 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.