FORMALIZED MATHEMATICS
Vol. 25, No. 3, Pages 201–206, 2017
DOI: 10.1515/forma-2017-0019

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

The Pell's Equation

Marcin Acewicz
Institute of Informatics
University of Białystok
Poland

Karol Pąk
Institute of Informatics
University of Białystok
Poland

Summary. In this article we prove several basic theorems that correspond to the Pell's Equation. First we focus on the theorem that the Pell's equation $x^2 - Dy^2 = 1$ has infinitely many solutions in positive integers for a given non square natural number D. We present also a formalization of a theorem that based on the least fundamental solution of the equation we can simply calculate algebraically each remaining solution.

The formalization follows W. Sierpiński [**?**]. Solutions to Pell's Equation are listed as #39 at Freek Wiedijk's list of "Top 100 mathematical theorems" [13].

MSC: 11D45 03B35

Keywords:

MML identifier: PELLS_EQ, version: 8.1.06 5.44.1305

1. Preliminaries

From now on n, n_1, n_2, k, D denote natural numbers, r, r_1, r_2 denote real numbers, and x, y denote integers.

Now we state the propositions:

(1) Let us consider integers i, j. If $j < 0$, then $j < i \bmod j \leqslant 0$.

(2) Let us consider integers i, j. If $j \neq 0$, then $|i \bmod j| < |j|$. The theorem is a consequence of (1).

(3) Let us consider a natural number D, and integers a, b, c, d. If $a + (b \cdot \sqrt{D}) = c + (d \cdot \sqrt{D})$, then $a = c$ and $b = d$.

(4) Let us consider natural numbers c, d, n. Then there exist natural numbers a, b such that $a + (b \cdot \sqrt{D}) = (c + (d \cdot \sqrt{D}))^n$.

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

PROOF: Set $c_1 = c + (d \cdot \sqrt{D})$. Define $\mathcal{P}$[natural number] $\equiv$ there exist natural numbers a, b such that $a + (b \cdot \sqrt{D}) = {c_1}^{\$_1}$. $\mathcal{P}[0]$ by [7, (4)]. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$ by [7, (6)]. $\mathcal{P}[n]$ from [2, Sch. 2]. □

(5) Let us consider integers c, d, and a natural number n. Then there exist integers a, b such that $a + (b \cdot \sqrt{D}) = (c + (d \cdot \sqrt{D}))^n$.

PROOF: Set $c_1 = c + (d \cdot \sqrt{D})$. Define $\mathcal{P}$[natural number] $\equiv$ there exist integers a, b such that $a + (b \cdot \sqrt{D}) = {c_1}^{\$_1}$. $\mathcal{P}[0]$ by [7, (4)]. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$ by [7, (6)]. $\mathcal{P}[n]$ from [2, Sch. 2]. □

(6) Let us consider a natural number D, integers a, b, c, d, and a natural number n. Suppose $a + (b \cdot \sqrt{D}) = (c + (d \cdot \sqrt{D}))^n$. Then $a - (b \cdot \sqrt{D}) = (c - (d \cdot \sqrt{D}))^n$.

PROOF: Set $S = \sqrt{D}$. Define $\mathcal{P}$[natural number] $\equiv$ for every integers a, b, c, d such that $a + (b \cdot S) = (c + (d \cdot S))^{\$_1}$ holds $a - (b \cdot S) = (c - (d \cdot S))^{\$_1}$. $\mathcal{P}[0]$ by [7, (4)], (3). If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$ by (5), [7, (6)], (3). $\mathcal{P}[n]$ from [2, Sch. 2]. □

2. Solutions to Pell's Equation – Construction

Now we state the propositions:

(7) There exists a finite sequence F of elements of $\mathbb{N}$ such that

(i) $\operatorname{len} F = n + 1$, and

(ii) for every k such that $k \in \operatorname{dom} F$ holds $F(k) = \lfloor k - 1 \cdot \sqrt{D} \rfloor + 1$, and

(iii) if D is not square, then F is one-to-one.

PROOF: Define $\mathcal{F}$(natural number) $= \lfloor \$_1 - 1 \cdot \sqrt{D} \rfloor + 1$. Consider p being a finite sequence such that $\operatorname{len} p = n+1$ and for every k such that $k \in \operatorname{dom} p$ holds $p(k) = \mathcal{F}(k)$ from [3, Sch. 2]. $\operatorname{rng} p \subseteq \mathbb{N}$ by [12, (25)], [10, (25)], [11, (29), (3)]. □

(8) Let us consider real numbers a, b, and a finite sequence F of elements of $\mathbb{R}$. Suppose $n > 1$ and $\operatorname{len} F = n + 1$ and for every k such that $k \in \operatorname{dom} F$ holds $a < F(k) \leqslant b$. Then there exist natural numbers i, j such that

(i) i, $j \in \operatorname{dom} F$, and

(ii) $i \neq j$, and

(iii) $F(i) \leqslant F(j)$, and

(iv) $F(j) - F(i) < \frac{b-a}{n}$.

PROOF: Define $\mathcal{P}$(natural number) $=]a + \frac{\$_1 - 1 \cdot (b-a)}{n}, a + \frac{\$_1 \cdot (b-a)}{n}]$. Define $\mathcal{H}$[object, object] $\equiv$ for every natural number k such that $\$_1 \in \mathcal{P}(k)$ holds

$k = \$_2$. For every object x such that $x \in]a, b]$ there exists a natural number k such that $x \in \mathcal{P}(k)$ and $k \in \operatorname{Seg} n$ by [2, (14)], [11, (3)], [2, (13)], [3, (1)]. For every object x such that $x \in]a, b]$ there exists an object y such that $\mathcal{H}[x, y]$ by [2, (11)], [12, (25)], [2, (13)]. Consider f being a function such that $\operatorname{dom} f =]a, b]$ and for every object x such that $x \in]a, b]$ holds $\mathcal{H}[x, f(x)]$ from [1, Sch. 1]. Set $f_1 = f \cdot F$. $\operatorname{rng} F \subseteq \operatorname{dom} f$. $\operatorname{rng} f_1 \subseteq \operatorname{Seg} n$ by [4, (11), (12)]. f_1 is one-to-one by [4, (11), (12)]. □

(9) If D is not square and $n > 1$, then there exist integers x, y such that $y \neq 0$ and $|y| \leqslant n$ and $0 < x - (y \cdot \sqrt{D}) < \frac{1}{n}$.
PROOF: Consider x being a finite sequence of elements of $\mathbb{N}$ such that $\operatorname{len} x = n + 1$ and for every k such that $k \in \operatorname{dom} x$ holds $x(k) = \lfloor k - 1 \cdot \sqrt{D} \rfloor + 1$ and if D is not square, then x is one-to-one. Define $\mathcal{U}$(natural number) $= x(\$_1) - (\$_1 - 1 \cdot \sqrt{D})$. Consider u being a finite sequence such that $\operatorname{len} u = n + 1$ and for every k such that $k \in \operatorname{dom} u$ holds $u(k) = \mathcal{U}(k)$ from [3, Sch. 2]. $\operatorname{rng} u \subseteq \mathbb{R}$. For every k such that $k \in \operatorname{dom} u$ holds $0 < u(k) \leqslant 1$. Consider n_1, n_2 being natural numbers such that n_1, $n_2 \in \operatorname{dom} u$ and $n_1 \neq n_2$ and $u(n_1) \leqslant u(n_2)$ and $u(n_2) - u(n_1) < \frac{1-0}{n}$. $u(n_1) \neq u(n_2)$. □

(10) Suppose D is not square and $n \neq 0$ and $|y| \leqslant n$ and $0 < x - (y \cdot \sqrt{D}) < \frac{1}{n}$. Then $|x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}})| \leqslant 2 \cdot \sqrt{D} + \frac{1}{n^{\mathbf{2}}}$.

(11) If D is not square, then there exist integers x, y such that $y \neq 0$ and $0 < x - (y \cdot \sqrt{D})$ and $|x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}})| < 2 \cdot \sqrt{D} + 1$. The theorem is a consequence of (9) and (10).

(12) Suppose D is not square. Then $\{\langle x, y\rangle$, where x, y are integers : $y \neq 0$ and $|x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}})| < 2 \cdot \sqrt{D} + 1$ and $0 < x - (y \cdot \sqrt{D})\}$ is infinite.
PROOF: Set $S = \{\langle x, y\rangle$, where x, y are integers : $y \neq 0$ and $|x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}})| < 2 \cdot \sqrt{D} + 1$ and $0 < x - (y \cdot \sqrt{D})\}$. There exists a function f from S into $\mathbb{R}$ such that for every integers x, y such that $\langle x, y\rangle \in S$ holds $f(\langle x, y\rangle) = x - (y \cdot \sqrt{D})$ by [5, (2)]. Consider f being a function from S into $\mathbb{R}$ such that for every integers x, y such that $\langle x, y\rangle \in S$ holds $f(\langle x, y\rangle) = x - (y \cdot \sqrt{D})$. S is not empty. Reconsider $R = \operatorname{rng} f$ as a finite, non empty subset of $\mathbb{R}$. $\inf R > 0$. Consider n being a natural number such that $\frac{1}{n} < \inf R$ and $n > 1$. Consider x, y being integers such that $y \neq 0$ and $|y| \leqslant n$ and $0 < x - (y \cdot \sqrt{D}) < \frac{1}{n}$. $|x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}})| \leqslant 2 \cdot \sqrt{D} + \frac{1}{n^{\mathbf{2}}}$. $2 \cdot \sqrt{D} + \frac{1}{n^{\mathbf{2}}} < 2 \cdot \sqrt{D} + 1$. □

(13) Suppose D is not square. Then there exist integers k, a, b, c, d such that
(i) $0 \neq k$, and
(ii) $a^{\mathbf{2}} - (D \cdot b^{\mathbf{2}}) = k = c^{\mathbf{2}} - (D \cdot d^{\mathbf{2}})$, and
(iii) $a \equiv c \pmod{k}$, and

(iv) $b \equiv d \pmod{k}$, and

(v) $|a| \neq |c|$ or $|b| \neq |d|$.

PROOF: Set $S = \{\langle x, y\rangle$, where x is an integer, y is an integer : $y \neq 0$ and $|x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}})| < 2 \cdot \sqrt{D} + 1$ and $0 < x - (y \cdot \sqrt{D})\}$. Reconsider $M = \lceil 2 \cdot \sqrt{D} + 1 \rceil$ as an element of $\mathbb{N}$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ for every integers x, y such that $\langle x, y\rangle = \$_1$ holds $\$_2 = x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}})$. For every object x_1 such that $x_1 \in S$ there exists an object u such that $\mathcal{P}[x_1, u]$. Consider f being a function such that $\operatorname{dom} f = S$ and for every object x_1 such that $x_1 \in S$ holds $\mathcal{P}[x_1, f(x_1)]$ from [1, Sch. 1]. Reconsider $M = \lceil 2 \cdot \sqrt{D} + 1 \rceil$ as an element of $\mathbb{N}$. Define $\mathcal{P}[\text{integer}] \equiv \$_1 \neq 0$. Define $\mathcal{F}(\text{set}) = \$_1$. Set $S_1 = \{\mathcal{F}(i)$, where i is an element of $\mathbb{Z} : -M \leqslant i \leqslant M$ and $\mathcal{P}[i]\}$. S_1 is finite. $\operatorname{rng} f \subseteq S_1$ by [8, (5)]. Consider k_1 being an object such that $k_1 \in \operatorname{rng} f$ and $f^{-1}(\{k_1\})$ is infinite. Consider k being an element of $\mathbb{Z}$ such that $k = k_1$ and $-M \leqslant k \leqslant M$ and $\mathcal{P}[k]$. Set $Z = f^{-1}(\{k\})$. Define $\mathcal{R}[\text{object}, \text{object}] \equiv$ for every integers x, y such that $\langle x, y\rangle = \$_1$ holds $\$_2 = \langle x \bmod k, y \bmod k\rangle$. For every object x_1 such that $x_1 \in Z$ there exists an object u such that $\mathcal{R}[x_1, u]$. Consider g being a function such that $\operatorname{dom} g = Z$ and for every object x_1 such that $x_1 \in Z$ holds $\mathcal{R}[x_1, g(x_1)]$ from [1, Sch. 1]. Define $\mathcal{R}[\text{object}] \equiv$ not contradiction. Set $K = \{\mathcal{F}(i)$, where i is an element of $\mathbb{Z} : -|k| \leqslant i \leqslant |k|$ and $\mathcal{R}[i]\}$. K is finite. $\operatorname{rng} g \subseteq K \times K$ by (2), [8, (5)], [6, (87)]. Consider a_1 being an object such that $a_1 \in \operatorname{rng} g$ and $g^{-1}(\{a_1\})$ is infinite. Consider X being an object such that $X \in g^{-1}(\{a_1\})$. Consider x, y being integers such that $X = \langle x, y\rangle$ and $y \neq 0$ and $|x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}})| < 2 \cdot \sqrt{D} + 1$ and $0 < x - (y \cdot \sqrt{D})$. There exist integers a, b, c, d such that $a^{\mathbf{2}} - (D \cdot b^{\mathbf{2}}) = k = c^{\mathbf{2}} - (D \cdot d^{\mathbf{2}})$ and $a \equiv c \pmod{k}$ and $b \equiv d \pmod{k}$ and ($|a| \neq |c|$ or $|b| \neq |d|$) by [11, (59)], [8, (28)]. □

3. Pell's Equation

Now we state the proposition:

(14) 39 SOLUTIONS TO PELL'S EQUATION:
If D is not square, then there exist natural numbers x, y such that $x^{\mathbf{2}} - (D \cdot y^{\mathbf{2}}) = 1$ and $y \neq 0$. The theorem is a consequence of (13).

Let D be a natural number.

A Pell's solution of D is an element of $\mathbb{Z} \times \mathbb{Z}$ and is defined by

(Def. 1) $((it)_{\mathbf{1}})^{\mathbf{2}} - (D \cdot ((it)_{\mathbf{2}})^{\mathbf{2}}) = 1$.

Let D_1, D_2 be real-membered, non empty sets and p be an element of $D_1 \times D_2$. We say that p is positive if and only if

(Def. 2) $(p)_{\mathbf{1}}$ is positive and $(p)_{\mathbf{2}}$ is positive.

One can check that there exists an element of $\mathbb{Z} \times \mathbb{Z}$ which is positive.

Let p be a positive element of $\mathbb{Z} \times \mathbb{Z}$. Observe that $(p)_{\mathbf{1}}$ is positive as an integer and $(p)_{\mathbf{2}}$ is positive as an integer.

Now we state the propositions:

(15) Let us consider square natural number D, and a positive element p of $\mathbb{Z} \times \mathbb{Z}$. If $D > 0$, then p is not a Pell's solution of D.

(16) If D is not square, then there exists a Pell's solution p of D such that p is positive. The theorem is a consequence of (14).

Let D be a natural number. One can verify that there exists a Pell's solution of D which is positive.

Now we state the proposition:

(17) THE CARDINALITY OF THE PELL'S SOLUTIONS:
Let us consider a natural number D. Then the set of all a_1 where a_1 is a positive Pell's solution of D is infinite.
PROOF: Set $P =$ the set of all a_1 where a_1 is a positive Pell's solution of D. Set $a_1 =$ the positive Pell's solution of D. $\pi_2(P) \subseteq \mathbb{N}$ by [11, (3)]. Reconsider $P_2 = \pi_2(P)$ as a finite, non empty subset of $\mathbb{N}$. Set $b = \max P_2$. Consider a being an object such that $\langle a, b \rangle \in P$. Consider a_1 being a positive Pell's solution of D such that $\langle a, b \rangle = a_1$. □

4. SOLUTIONS TO PELL'S EQUATION – SHAPE

In the sequel p, p_1, p_2 denote Pell's solutions of D.

Now we state the propositions:

(18) If D is not square, then p is positive iff $(p)_{\mathbf{1}} + ((p)_{\mathbf{2}} \cdot \sqrt{D}) > 1$.
PROOF: If p is positive, then $(p)_{\mathbf{1}} + ((p)_{\mathbf{2}} \cdot \sqrt{D}) > 1$ by [10, (27)], [2, (25)], [10, (18)], [11, (7)]. □

(19) Suppose $1 < (p_1)_{\mathbf{1}} + ((p_1)_{\mathbf{2}} \cdot \sqrt{D}) < (p_2)_{\mathbf{1}} + ((p_2)_{\mathbf{2}} \cdot \sqrt{D})$ and D is not square. Then

(i) $(p_1)_{\mathbf{1}} < (p_2)_{\mathbf{1}}$, and

(ii) $(p_1)_{\mathbf{2}} < (p_2)_{\mathbf{2}}$.

The theorem is a consequence of (18).

(20) Let us consider a natural number D, a positive Pell's solution p of D, integers a, b, and a natural number n. Suppose $n > 0$ and $a + (b \cdot \sqrt{D}) = ((p)_{\mathbf{1}} + ((p)_{\mathbf{2}} \cdot \sqrt{D}))^n$. Then $\langle a, b \rangle$ is a positive Pell's solution of D. The theorem is a consequence of (6) and (18).

Let D be a natural number. The minimal Pell's solution of D yielding a positive Pell's solution of D is defined by

(Def. 3) for every positive Pell's solution p of D, $(it)_{\mathbf{1}} \leqslant (p)_{\mathbf{1}}$ and $(it)_{\mathbf{2}} \leqslant (p)_{\mathbf{2}}$.

Now we state the proposition:

(21) Let us consider a natural number D, and an element p of $\mathbb{Z} \times \mathbb{Z}$. Then p is a positive Pell's solution of D if and only if there exists a positive natural number n such that $(p)_{\mathbf{1}}+((p)_{\mathbf{2}}\cdot\sqrt{D}) = (((\text{the minimal Pell's solution of } D))_{\mathbf{1}} + (((\text{t}$

PROOF: Set $m =$ the minimal Pell's solution of D. Set $t = (m)_{\mathbf{1}}$. Set $u = (m)_{\mathbf{2}}$. Set $S = \sqrt{D}$. Set $x = (p)_{\mathbf{1}}$. Set $y = (p)_{\mathbf{2}}$. If p is a positive Pell's solution of D, then there exists a positive natural number n such that $x + (y \cdot S) = (t + (u \cdot S))^n$ by (18), (19), [9, (51), (57)]. $\langle x, y \rangle$ is a positive Pell's solution of D. □

REFERENCES

[1] Grzegorz Bancerek. Tarski's classes and ranks. *Formalized Mathematics*, 1(**3**):563–567, 1990.

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[6] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[7] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[8] Jan Popiołek. Some properties of functions modul and signum. *Formalized Mathematics*, 1(**2**):263–264, 1990.

[9] Konrad Raczkowski and Andrzej Nędzusiak. Real exponents and logarithms. *Formalized Mathematics*, 2(**2**):213–216, 1991.

[10] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

[11] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[12] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

[13] Freek Wiedijk. Formalizing 100 theorems.

Received August 30, 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.