

The Catalan Conjecture

Martin Klazar

October 13, 2026

In this lecture

- 1 Diophantine equations
- 2 The Catalan conjecture
- 3 The Catalan conjecture = P. Mihăilescu's theorem
- 4 Solving the Diophantine equation $x^2 - y^3 = 1$

Systems are equivalent to single equations

A Diophantine equation is any equation

$$f(\bar{x}) = f(x_1, \dots, x_n) = 0$$

where $f \in \mathbb{Z}[\bar{x}]$ is a polynomial with integral coefficients. We are usually interested in integral solutions $\bar{x} \in \mathbb{Z}^n$, but sometimes also in rational solutions $\bar{x} \in \mathbb{Q}^n$. Systems of D. equations are in fact equivalent to single equations.

Proposition

The solution set of a D. system $f_1(\bar{x}) = \dots = f_m(\bar{x}) = 0$ is the same as the solution set of the single D. equation $g(\bar{x}) = 0$, where

$$g(\bar{x}) = \sum_{i=1}^m f_i(\bar{x})^2.$$

Proof.

If $z_i \in \mathbb{R}$, then $z_1 = \dots = z_m = 0 \iff \sum_{i=1}^m z_i^2 = 0$. □

Skolem's reductions of degrees

The Norwegian logician and number theorist *Thoralf Skolem* (1887–1963) invented the following reductions to degrees ≤ 4 .

Proposition

For every polynomial $f \in \mathbb{Z}[x_1, \dots, x_n]$, one can easily construct polynomials $f_1, \dots, f_m$ in $\mathbb{Z}[y_1, \dots, y_N]$ such that $\deg(f_i) \leq 2$ and the solution set of the D. equation

$$f(\bar{x}) = 0$$

can be easily obtained from the solution set of the D. system $f_1(\bar{y}) = \dots = f_m(\bar{y}) = 0$.

Proof.

Let $f(\bar{x}) = ax_1^{m_1} \dots x_n^{m_n} + g(\bar{x})$, where $m_1 + \dots + m_n \geq 3$, $m_1 \geq 1$, and $g \in \mathbb{Z}[\bar{x}]$. Then $f(\bar{x}) = 0 \iff y_1 = x_1^{m_1-1} x_2^{m_2} \dots x_n^{m_n}$ and $ax_1 y_1 + g(\bar{x}) = 0$. Repeat this elementary reduction, which introduces the new variables $y_1, y_2, \dots$, as long as possible. □

Skolem's reductions of degrees. Hilbert's tenth problem

Corollary

For every polynomial $f \in \mathbb{Z}[x_1, \dots, x_n]$, one can easily construct another polynomial $g \in \mathbb{Z}[y_1, \dots, y_N]$ such that $\deg(g) \leq 4$ and the solution set of the D. equation $f(\bar{x}) = 0$ can be easily obtained from the solution set of the D. equation $g(\bar{y}) = 0$.

Proof.

Use the two previous propositions. □

In 1900, *David Hilbert* (1862–1943) included in his famous list of 23 mathematical problems for the 20th century the following *tenth problem*.

Problem (Hilbert's 10th problem)

Find an algorithm $\mathcal{A}$ such that for every input polynomial $f \in \mathbb{Z}[x_1, \dots, x_n]$, the algorithm $\mathcal{A}$ decides if the D. equation $f(\bar{x}) = 0$ has a solution $\bar{x} \in \mathbb{Z}^n$.

Hilbert's tenth problem. Halting problem

Mathematical algorithms were introduced by *Alan M. Turing* (1912–1954) only in 1936, and in 1900–1940 there was zero interest in Hilbert's 10th problem. (I explain orally how D. Hilbert formulated his 10th problem.) But from 1940 on, American mathematical logicians started to be interested in the problem.

We say that a set $X \subset \mathbb{Z}^n$ is

- *decidable*, if there is an algorithm $\mathcal{A}: \mathbb{Z}^n \rightarrow \{0, 1\}$ (inputs in $\mathbb{Z}^n$ and outputs 0 or 1) such that $\mathcal{A}$ always terminates and $\bar{x} \in X \iff \mathcal{A}(\bar{x}) = 1$;
- *half-decidable*, if there is an algorithm $\mathcal{A}: \mathbb{Z}^n \rightarrow \{0, 1\}$ such that $\bar{x} \in X \iff$ the computation $\mathcal{A}(\bar{x})$ terminates.

Theorem (A. M. Turing)

There exists a half-decidable set $X \subset \mathbb{Z}^n$ that is not decidable.

Proof.

Set $X = \{\text{codes of Turing machines and inputs on which they halt (terminate)}\}$. □

The DPRM theorem on Hilbert's tenth problem

A set $X \subset \mathbb{Z}^n$ is *Diophantine* if there exists a polynomial $f \in \mathbb{Z}[x_1, \dots, x_n, y_1, \dots, y_m]$ such that $\bar{x} \in X \iff \exists \bar{y} \in \mathbb{Z}^m: f(\bar{x}, \bar{y}) = 0$. In view of Turing's theorem, Hilbert's 10th problem is resolved in the negative — no algorithm $\mathcal{A}$ as asked for by Hilbert exists — by the following theorem.

Theorem (DPRM, 1970)

Every half-decidable set $X \subset \mathbb{Z}^n$ is Diophantine. (The converse is trivial.)

Proof.

Program in terms of Diophantine sets; use Pell D. equations. □

D stands for *Martin Davis* (1928–2023), H for *Hilary Putnam* (1926–2016), R for *Julia Robinson* (Bowman) (1919–1985), and M for *Jurij Vladimirovič Matijasevič* (1947).

Pythagorean triples

Pythagorean triples are solutions $x, y, z \in \mathbb{Z}$ of the D. equation $x^2 + y^2 = z^2$, for example $\pm 3, \pm 4, \pm 5$ or $\pm 5, \pm 12, \pm 13$.

Theorem (T, parametric description of all Pythagorean triples)

$$\{\langle x, y, z \rangle \in \mathbb{Z}^3 : x^2 + y^2 = z^2\} = \{\langle \underbrace{\pm 2abc, \pm(a^2 - b^2)c}_{\longleftrightarrow}, \pm(a^2 + b^2)c \rangle : a, b, c \in \mathbb{N}_0\}.$$

Proof.

$\supset$ is trivial. We prove $\subset$. Let x, y, z be a P. triple. If $z = 0$ then $x = y = 0$ and we set $a = b = 0$. Let $z > 0$. We cancel a common factor, if any, and have $(x, y) = 1$. Mod 4 implies that one of x and y is odd and the other is even. Let $x > 0$ be odd and $y \geq 0$ be even. Then z is odd, $(y/2)^2 = \frac{z-x}{2} \cdot \frac{z+x}{2}$, and $(\frac{z-x}{2}, \frac{z+x}{2}) = 1$. If $y = 0$ then $x = 1$, and we set $a = 1$ and $b = 0$. Finally, if $y > 0$ then (by the FTAr) $\frac{z-x}{2} = b^2$, $\frac{z+x}{2} = a^2$, $z = a^2 + b^2$, $x = a^2 - b^2$, and $y = 2ab$ for some $a, b \in \mathbb{N}$. □

Pythagorean triples and AI

The following problem is due to *Paul Erdős (1913–1996)* and the American mathematician *Ron Graham (1935–2020)*.

Problem

Let $k \in \mathbb{N}$ with $k \geq 2$ and $\chi: \mathbb{N} \rightarrow \{1, \dots, k\}$. Does there always exist a monochromatic Pythagorean triple, i.e. numbers $x, y, z \in \mathbb{N}$ such that $x^2 + y^2 = z^2$ and $\chi(x) = \chi(y) = \chi(z)$?

For $k \geq 3$ this is still an open problem. For $k = 2$, it was solved, in the positive, first by Heule, Kullmann and Marek in 2017 who proved by a computation using 200 TB of data that every 2-coloring of $\{1, 2, \dots, 7825\}$ contains a monochromatic P. triple, but that it ceases to be true for 7824 in place of 7825.

- In 2026, AI found an analytical proof of the $k = 2$ case. J. Leng (arXiv:2609.3467v1): “...this proof was essentially found using ChatGPT Astra Ultra on the Codex app [1]”.

Fermat's Last Theorem (FLT)

Conjecture: $\neg \exists$ a talk on D. equations not mentioning FLT.

- Around 1637, *Pierre de Fermat* (1601–1665) stated (in print) that he could prove that no D. equation $x^n + y^n = z^n$, where $n \geq 3$, has a solution $x, y, z \in \mathbb{N}$ ($= \{1, 2, \dots\}$).

We may assume that $n = p \geq 3$ is a prime number or that $n = 4$. The latter case was proved by Fermat. Many partial results followed, for example:

- for $p = 3$ by *Leonhard Euler* (1707–1783) around 1770 (the proof was incomplete);
- for $p = 5$ by *Adrien-Marie Legendre* (1752–1833) (of the portrait debacle fame) and, independently, by *Peter Lejeune Dirichlet* (1805–1859) around 1825;
- for $p = 7$ by *Gabriel Lamé* (1795–1870) around 1839;
- for all primes $3 \leq p \leq 100$ except 37, 59, and 67 by *Ernst E. Kummer* (1810–1893) around 1850; in this attack on FLT, E. E. Kummer founded algebraic number theory.
- The American mathematician *Harry S. Vandiver* (1882–1973) and the Swiss-Russian mathematician *Dmitry S. Mirimanoff* (1861–1945) considerably extended Kummer's range of exponents p .

Fermat's Last Theorem and AI

- *Yves Hellegouarch (1936–1922)* in 1972 and, independently, *Gerhard Frey (1944)* in 1985, discovered the connection between FLT and elliptic curves. An elliptic curve is the solution set, in $\mathbb{C}^2$, $\mathbb{Q}^2$, $\dots$, of the D. equation $y^2 = x^3 + ax + b$.
- Using this connection, *Sir Andrew Wiles (1953)* and *Richard Taylor (1962)* proved FLT in 1995. See the articles AW, *Ann. Math.* **141** (1995), 443–551 and RT & AW, *Ann. Math.* **141** (1995), 553–572; the original approach of AW contained a gap, hence the latter article.
- So the proof has 129 pages. How hard would it be to formalize it, say in the proof assistant Lean? The proof of the Feit–Thompson theorem in group theory has 255 pages, see WF & JT, *Pacific J. Math.* **13** (1963) 775–1029, and it was formalized in 2012 in Rocq after six-years effort by a team led by *Georges Gonthier (1962)*.
- From the web (October 2026): “An autonomous AI agent developed by Anthropic (using Claude and the Lean proof assistant) completed the first end-to-end, machine-checked formal proof of Fermat's Last Theorem (FLT) in 11 days”.

The Catalan conjecture

In 1844, the French-Belgian mathematician *Eugène Catalan* (1814–1894) published the following conjecture.

Conjecture

Let $m, n \in \mathbb{N}$ with $m, n \geq 2$. Then the only solution $x, y \in \mathbb{N} \setminus \{1\}$ of the D. equation $x^m - y^n = 1$ is given by $3^2 - 2^3 = 1$ (i.e., when $x = n = 3$ and $y = m = 2$).

In other words, the only two consecutive *pure powers* (marked **bold**) in the sequence of natural numbers 1, 2, 3, **4**, 5, 6, 7, **8**, **9**, 10, 11, 12, 13, 14, 15, **16**, 17, 18, 19, 20, 21, 22, 23, 24, **25**, 26, **27**, 28, 29, 30, ... are the numbers 8 and 9.

- Similarly to FLT, we can restrict the exponents to primes: $m = p$ and $n = q$.
- The Catalan numbers $C_n = \frac{1}{n+1} \binom{2n}{n}$ counting, for example, proper bracketings — $()()()$, $((()))$, $()(())$, $((()))$, and $((()))$ for $n = 3$ pairs $(,)$ — are also named after E. Catalan.
- The Catalan opening in chess, 1. d4 Nf6, 2. c4 e6, and 3. g3, is not named after him.

Partial results on the Catalan conjecture 1

The D. equation $x^2 - y^2 = (x - y)(x + y) = 1$ is trivial: the only solutions are $x = \pm 1, y = 0$. Let us have a look at more interesting partial results on solutions of $x^m - y^n = 1$ in the cases $m = 2$ or $n = 2$. The latter case was solved by *Victor-Amédée Lebesgue (1791–1875)* in 1850.

Theorem (Lebesgue)

Let $p \geq 3$ be a prime number. Then $x^p - y^2 = 1$ has only the trivial solution $x = 1, y = 0$.

Proof.

Factorize $x^p = (1 + iy)(1 - iy)$, work in $\mathbb{Z}[i]$, and use a 2-adic argument. □

The case $m = 2$ is harder. For $n = 3$ we have an old result of L. Euler from 1738.

Theorem (Euler)

The only rational solutions of $x^2 - y^3 = 1$ are $\langle \pm 3, 2 \rangle$, $\langle \pm 1, 0 \rangle$, and $\langle 0, -1 \rangle$.

Partial results on the Catalan conjecture 2

Proof.

The solution set of $x^2 - y^3 = 1$ in $\mathbb{Q}^2$ is an elliptic curve. We can use the Abelian group structure on this set. □

The remaining case $m = 2$ and $n = q \geq 5$ was solved only in 1965 by the Chinese mathematician *Chao Ko (Ke Zhao) (1910–2002)*. In 1976, his proof was simplified by the American mathematician E. Z. Chein.

Theorem (Chao Ko)

Let $q \geq 5$ be a prime number. Then $x^2 - y^q = 1$ has only the trivial solutions $x = \pm 1, y = 0$ and $x = 0, y = -1$.

Proof.

The main tool in the proof is the parametric description of the solution set of Pell D. equation, which we state and prove below. □

Partial results on the Catalan conjecture 3

In two articles, published in 1953 and in 1960, the British mathematician *John W. S. Cassels* (1922–2015) proved two congruences for the hypothetical (and actually non-existing) nonzero solutions of $x^p - y^q = 1$.

Theorem (Cassels)

Let $p, q \geq 3$ be primes and let $x, y \in \mathbb{Z} \setminus \{0\}$ be integers such that $x^p - y^q = 1$. Then q divides x and p divides y .

Proof.

Interestingly, one works with the function $F(t) = ((1+t)^p - t^p)^{1/q}$, $t \in (-1, 1)$, and with the arithmetic properties of the (rational) coefficients in its Taylor expansion. $\square$

The congruences of Cassels are one of the main tools in Mihălescu's proof of the Catalan conjecture.

Partial results on the Catalan conjecture 4

In 1976, the Dutch mathematician *Robert Tijdeman (1943)* proved that the Catalan D. equation has only finitely many solutions, and even more. Recall that a pure power is a power a^b with $a, b \in \mathbb{N} \setminus \{1\}$.

Theorem (Tijdeman)

There exists an effectively computable constant $C \in \mathbb{N}$ with the property that if $n \in \mathbb{N}$ is such that both n and $n + 1$ are pure powers, then $n \leq C$.

Proof.

The proof uses, besides Cassels's congruences, the *method of estimates of linear forms in logarithms of algebraic numbers*. This method was invented by the British mathematician *Alan Baker (1939–2018)*, who was awarded for it in 1970 the Fields medal. □

What if n and $n + 2$ are pure powers, like 25 and 27? Now it is an open problem to bound n since no analog of Cassels's congruences for the RHS 2 is known.

The theorem of Preda Mihăilescu

In three articles, published in 2003, 2004, and 2006, the German-Swiss-Romanian mathematician *Preda Mihăilescu* (1955) completely proved the Catalan conjecture (by the old pen-and-paper method, no computer assistance). Thus now we have

Theorem (Mihăilescu)

If the number $n \in \mathbb{N}$ is such that both n and $n + 1$ are pure powers, then $n = 8$.

Proof.

Heavy algebraic number theory. Compared to (the proof of) FLT, there is practically no analytic component in Mihăilescu's proof (in FLT this component is modular forms) and it is, say, one order of magnitude simpler than FLT, but it is still quite complicated. □

In the preceding (and in my course on the topic) I relied on the nice booklet by *René Schoof* (1955), *Catalan's Conjecture*, Universitext. Springer-Verlag, London 2008, ix+124 pp.

Square minus cube is one 1

Let us return to the (weak form of the) result of L. Euler concerning the first nontrivial case $m = 2$ and $n = 3$ of the Catalan conjecture.

Theorem (Euler, 1738)

The only integral solutions of the D. equation $x^2 - y^3 = 1$ are $\langle \pm 3, 2 \rangle$, $\langle \pm 1, 0 \rangle$, and $\langle 0, -1 \rangle$.

Several modern proofs of this theorem (using arguments different from Euler's and proving also other results) have been published. In the rest of my talk I want to show you the proof which I had devised 37 years ago in M. Klazar, O řešení diofantické rovnice $x^2 - y^3 = \pm 1$, *Matematické obzory* **32** (1989), 47–53 (Solving the Diophantine equation $x^2 - y^3 = \pm 1$). Basically the same proof was published later in Ch. Notari, Une résolution élémentaire de l'équation diophantienne $x^3 = y^2 - 1$, *Expositiones Mathematicae* **21** (2003), 279–283. We have to start from Pell equations.

Pell equations 1

A *Pell equation* is any D. equation with unknowns x and y and of the form

$$x^2 - dy^2 = 1, \text{ where } d \in \mathbb{N} \text{ and is not a square.}$$

Thus $x^2 - 2y^2 = 1$, $x^2 - 3y^2 = 1$, $x^2 - 5y^2 = 1$, and so on are Pell equations. We call $\pm 1, 0$ the *trivial solution*. *Joseph-Louis Lagrange (1736–1813)* proved in 1770 the following theorem.

Theorem (J. L. Lagrange)

Every Pell equation $x^2 - dy^2 = 1$ has a nontrivial solution.

Proof.

Use the (periodic!) expansion of $\sqrt{d}$ into a cont. fraction, as JLL did, or apply the theorem of Dirichlet and work with the infinitely many fractions $\frac{m}{n}$ such that $|\sqrt{d} - \frac{m}{n}| < \frac{1}{n^2}$. $\square$

For example, the three Pell equations above have respective nontrivial solutions $\langle \pm 3, \pm 2 \rangle$, $\langle \pm 2, \pm 1 \rangle$, and $\langle \pm 9, \pm 4 \rangle$.

Pell equations 2

Corollary

Every Pell equation $x^2 - dy^2 = 1$ has infinitely many solutions.

Proof.

Let $\langle a, b \rangle \in \mathbb{Z}^2$ be a nontrivial solution of $x^2 - dy^2 = 1$. Then $(\langle x_n, y_n \rangle) \subset \mathbb{Z}^2$, given by the relation $x_n + y_n\sqrt{d} = (a + b\sqrt{d})^n$, $n \in \mathbb{N}$, is an infinite sequence of distinct solutions. $\square$

For example, the nontrivial solution $\langle 3, 2 \rangle$ of $x^2 - 2y^2 = 1$ generates solutions $\langle 17, 12 \rangle$, $\langle 99, 70 \rangle$, and so on. A nontrivial solution $\langle a, b \rangle \in \mathbb{N}^2$ of $x^2 - dy^2 = 1$ is a *minimum solution* if there is no nontrivial solution $\langle a', b' \rangle \in \mathbb{N}^2$ such that $a' < a$ (equivalently, $b' < b$).

Theorem (P, parametric description of all solutions of a Pell equation)

Let $\langle a, b \rangle \in \mathbb{N}^2$ be the min. solution of $x^2 - dy^2 = 1$ (it exists due to Lagrange's theorem). Then $\{\langle x, y \rangle \in \mathbb{Z}^2 : x^2 - dy^2 = 1\} = \{\langle \pm x_n, \pm y_n \rangle : x_n + y_n\sqrt{d} = (a + b\sqrt{d})^n, n \in \mathbb{N}_0\}$.

Pell equations 3

Proof.

This follows from the closedness of the solution set to multiplication and division. If $x_0 + y_0\sqrt{d}$ and $x_1 + y_1\sqrt{d}$ are solutions of $x^2 - dy^2 = 1$, then $x_2 + y_2\sqrt{d} = (x_0 + y_0\sqrt{d})(x_1 + y_1\sqrt{d})$ is another solution, and so is $1/(x_0 + y_0\sqrt{d}) = x_0 - y_0\sqrt{d}$. $\square$

The minimum solution may be large. For example, for $x^2 - 61y^2 = 1$ it is

$$\langle a, b \rangle = \langle 1766319049, 226153980 \rangle.$$

On the other hand, it is easy to define an infinite family of Pell equations with obvious minimum solutions: the minimum solution of $x^2 - (k^2 - 1)y^2 = 1$, where $k = 2, 3, \dots$, is $\langle k, 1 \rangle$, and we can easily control the solution set of each of these Pell equations. This is one of the key steps in the proof of the DPRM theorem. The previous theorem can be used also for resolution of other D. equations; for example, we will solve the equation $x^4 - 3y^2 = 1$.

Square minus cube is one 2

I follow my article mentioned above.

Proposition (0)

The following holds.

- ① *The solutions of $x^2 - 3y^2 = 1$ are $\langle \pm x_n, \pm y_n \rangle$, where $x_n + y_n\sqrt{3} = (2 + \sqrt{3})^n$ for $n \in \mathbb{N}_0$. In particular, $x_0 = 1$, $y_0 = 0$, $x_{n+1} = 2x_n + 3y_n$, and $y_{n+1} = x_n + 2y_n$.*
- ② *$x_{2n} = 2x_n^2 - 1$, $y_{2n} = 2x_n y_n$, $x_{2n+1} = (y_n + y_{n+1})^2 + 1$, $y_{2n+1} = 2x_n y_{n+1} - 1$.*

Proof.

1. By Theorem P above, since $a = 2$, $b = 1$. 2. By induction. □

Proposition (1)

If $\langle x, y, z \rangle \in \mathbb{N}_0^3$ is a Pythagorean triple with $(x, y) = 1$, then we have $z = u^2 + v^2$ and $\{x, y\} = \{u^2 - v^2, 2uv\}$ for some coprime numbers $u, v \in \mathbb{N}_0$.

Square minus cube is one 3

Proof.

By the above Theorem T. □

Corollary (2)

Let $x, y \in \mathbb{N}_0$ be such that $2x^2 - y^2 = 1$. Then $x = 2a^2 - 1 \pm 2ab$ for some $a, b \in \mathbb{N}_0$ such that $a^2 - 2b^2 = 1$.

Proof.

Then $y = 2y_0 + 1$ for $y_0 \in \mathbb{N}_0$, $x^2 = y_0^2 + (y_0 + 1)^2$, and we use P1. □

I took the following neat result from a textbook of NT by *Wacław Sierpinski (1882–1969)*.

Proposition (3)

The only solutions of $x^4 - 2y^2 = 1$ are $x = \pm 1$ and $y = 0$.

Square minus cube is one 4

Proof.

It follows that x is odd and $x^2 = 1 + 4k$. We have $(x^2 - 1)(x^2 + 1) = 2y^2$ and $4k(2k + 1) = y^2$. By the FTAr, $4k$ is a square and we are done. □

Theorem (4)

The only solutions of $x^4 - 3y^2 = 1$ are $x = \pm 1$ and $y = 0$.

Proof.

We need to solve $x_n = m^2$ for $n, m \in \mathbb{N}_0$, where x_n are as in P0. If $n = 2n_0 + 1$, then by 2 of P0 we get the relation $u^2 - v^2 = 1$ and are done. If $n = 2n_0$, then by 2 of P0 we have $m^2 = 2x_{n_0}^2 - 1$. Mod 4 show that x_{n_0} is odd and we have $x_{n_0} = x_{2n_1} = 2x_{n_1}^2 - 1$. By C2, we have $2x_{n_1}^2 - 1 = x_{n_0} = 2a^2 - 1 \pm 2ab$ for some $a, b \in \mathbb{N}_0$ with $a^2 - 2b^2 = 1$. Hence $x_{n_1}^2 = a(a \pm b)$. Since a and $a \pm b$ are coprime, a is a square. P3: $a = 1$, $x = \pm 1$, $y = 0$. □

Square minus cube is one 5

We prove the main result

Theorem (Euler, 1738)

The only integral solutions of the D. equation $x^2 - y^3 = 1$ are $\langle \pm 3, 2 \rangle$, $\langle \pm 1, 0 \rangle$, and $\langle 0, -1 \rangle$.

Proof.

(MK) Let $x, y \in \mathbb{Z}$ be such that $x^2 - y^3 = 1$. For $x = 0$ we get the last solution $\langle 0, -1 \rangle$. So let $x > 0$. We write $x^2 = (y + 1) \cdot (y^2 - y + 1) =: a \cdot b$ and see that $(a, b) = 1$ or 3 . In the former case, $b = c^2$ and we get the trivial D. equation $(2c)^2 - (2y - 1)^2 = 3$ leading to the solution $\langle \pm 1, 0 \rangle$. In the latter case, $(a, b) = 3$ and $a = 3c^2$, $b = 3d^2$. We arrive at the Pell equation $X^2 - 3Y^2 = 1$, where $X = 2d$ and $3Y = 2y - 1$. We see that $Y = 2c^2 - 1$. By 2 of P0, $c^2 = x_m y_{m+1}$. We have $(x_m, y_{m+1}) = 1$ or 2 . The former case leads, by T4, to the solution $\langle \pm 3, 2 \rangle$. The latter case is excluded by means of 2 of P0 and T4. □

THANK YOU FOR YOUR ATTENTION!