

The polynominal Pell equation

Autor(en): **Dubickas, Artras / Steuding, Jörn**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **59 (2004)**

PDF erstellt am: **25.05.2024**

Persistenter Link: <https://doi.org/10.5169/seals-9316>

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

The polynomial Pell equation

Artūras Dubickas and Jörn Steuding

Artūras Dubickas received his Ph.D. from the Moscow State University in 1990. He then had a postdoctoral position at the University of Witwatersrand in Johannesburg. Since 1994 he has a position at Vilnius University (Lithuania), where he is now chief research fellow and professor in the Department of Mathematics and Informatics. His main fields of research are algebraic number theory and transcendence theory.

Jörn Steuding received his Ph.D. from the University of Hannover in 1999. Since then he has a postdoctoral position at the Department of Mathematics of the Johann Wolfgang Goethe-Universität in Frankfurt. His main fields of research are analytic number theory and diophantine analysis.

1 Introduction: a brief history

In a letter to Eratosthenes, Archimedes posed the so-called cattle problem in which he asks for the number of bulls and cows belonging to the Sun god, subject to certain arithmetical restrictions. This problem was already forgotten over the centuries until it was rediscovered by G.E. Lessing in the Wolfenbüttel library in 1773. Essentially, the cattle problem asks for solutions of the quadratic equation

$$X^2 - 410\,286\,423\,278\,424 \cdot Y^2 = 1$$

in positive integers, where $410\,286\,423\,278\,424 = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 29 \cdot 353 \cdot (2 \cdot 4657)^2$. It seems that the ancient Greeks were unable to solve this equation; see [8] for a nicely

Das klassische Problem der diophantischen Approximation besteht im Auffinden guter rationalzahliger Annäherungen quadratischer Irrationalitäten der Form \sqrt{d} , wobei d eine quadratfreie natürliche Zahl ist. Diese Fragestellung führt auf das Lösen der sogenannten Pellschen Gleichung $x^2 - dy^2 = 1$ in ganzen Zahlen x, y . Es stellt sich dabei heraus, dass sich alle Lösungen aus einer einzigen Lösung mit minimalem $x > 1$ erzeugen lassen, wobei diese Lösung mit Hilfe der Kettenbruchentwicklung von \sqrt{d} gefunden werden kann. In der vorliegenden Arbeit wird nun die entsprechende Problemstellung für Polynome betrachtet. Ausgehend von einem Polynom $D \in \mathbb{C}[X]$ wird die Frage nach der Lösbarkeit der Gleichung $P^2 - DQ^2 = 1$ in Polynomen $P, Q \in \mathbb{C}[X]$ untersucht. Als wesentliches Hilfsmittel wird die Gültigkeit der *abc*-Vermutung für Polynome herangezogen.

written survey on the cattle problem and its history. The quadratic equation above is an example of the so-called Pell equation

$$X^2 - dY^2 = 1,$$

where $d \in \mathbb{N}$ is not a perfect square. It should be noted that Pell was an English mathematician who lived in the seventeenth century, but he had nothing to do with this equation. This diophantine equation is closely related to unit norm equations in quadratic number fields. Geometrically, the set of integer solutions (x, y) is the set of intersections of a hyperbola with the lattice \mathbb{Z}^2 . Integer solutions of the Pell equation were well understood few centuries ago by the contributions of Euler, Lagrange and others. Obviously, $x = 1$ and $y = 0$ is always a solution, but are there more? By symmetry it suffices to look for solutions in positive integers. Assuming that (x, y) is such a solution, we may factor the left-hand side,

$$(x - y\sqrt{d})(x + y\sqrt{d}) = x^2 - dy^2 = 1,$$

which gives

$$\left| \sqrt{d} - \frac{x}{y} \right| = \frac{1}{y^2(\sqrt{d} + \frac{x}{y})} < \frac{1}{2y^2}.$$

Thus, x/y is an extraordinary good rational approximation to the irrational number \sqrt{d} . In view of a theorem of Lagrange from the theory of diophantine approximations, it follows that all solutions of the Pell equation can be found among the convergents to \sqrt{d} . For instance, the sequence of convergents p_n/q_n to $\sqrt{2}$ starts with

$$\frac{1}{1}, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \frac{99}{70}, \dots \rightarrow \sqrt{2} = [1, \overline{2}],$$

and, in fact, we get for $p_n^2 - 2q_n^2$ the values

$$1^2 - 2 \cdot 1^2 = -1, \quad 3^2 - 2 \cdot 2^2 = +1, \quad 7^2 - 2 \cdot 5^2 = -1,$$

$$17^2 - 2 \cdot 12^2 = +1, \quad 41^2 - 2 \cdot 29^2 = -1, \quad 99^2 - 2 \cdot 70^2 = +1.$$

Every second convergent to $\sqrt{2}$ gives a solution of $X^2 - 2 \cdot Y^2 = 1$ and can be obtained as a natural power of the solution (x, y) with minimal $x > 1$, e.g.,

$$17 + 12 \cdot \sqrt{2} = (3 + 2 \cdot \sqrt{2})^2.$$

This regularity is related to the minimal length of the period of the continued fraction expansion of $\sqrt{2}$. In general, for every integer d which is not a perfect square, there is a smallest solution (x, y) with $x > 1$. All other solutions can be expressed in terms of its natural power $(x + y\sqrt{d})^n$, and thus the set of integer solutions of the Pell equation form a cyclic group. All this is usually included in a standard introductory course in number theory. Recent Lenstra's survey [8] and Barbeau's monograph [3] contain many references on Pell's equation in general and on its smallest solution in particular.

In this paper we are interested in the polynomial solutions of the Pell equation which we rewrite as

$$P^2 - D \cdot Q^2 = 1, \quad (1)$$

where D is a fixed polynomial, P and Q are polynomials in the same variables as D and with coefficients in the same field or ring as those of D . We shall refer to this as the polynomial Pell equation. As we shall see below, many aspects of the Pell equation do not depend on the type of solutions we ask for. The solutions $(P, Q) = (1, 0)$ and $(-1, 0)$ are called *trivial*. All other solutions are called *non-trivial*. The main difficulty in solving polynomial Pell equations is to determine whether non-trivial solutions exist or not. In case, if there is at least one non-trivial solution of (1), all solutions are obtained as powers of the smallest non-trivial solution. In Section 3 we will prove this for polynomials $D(X)$ in one variable with coefficients in \mathbb{C} . The proof is purely algebraic and extends without change to arbitrary polynomials in several variables $D \in \mathbb{K}[X_1, \dots, X_s]$ over every field \mathbb{K} of characteristic $\neq 2$.

Clearly, for $\deg D = 0$, we have $\deg P = \deg Q = 0$. Since the set of solutions of Pell's equation in integers is well understood, we may assume in the sequel that $\deg D > 0$. Obviously, the polynomial Pell equation has no solutions if $\deg D$ is an odd number. Therefore, we assume that $\deg D$ is even, so that $\deg D \geq 2$. Also, if (P, Q) is a non-trivial solution, then so are $(P, -Q)$ and $(-P, \pm Q)$. Sometimes the expression $P + Q\sqrt{D}$, where (P, Q) is a solution of (1), is also called a solution of (1).

Chowla asked for the solutions of (1) in $\mathbb{Z}[X]$ for $D(X) = X^2 + d \in \mathbb{Z}[X]$. Nathanson [11] proved that there are no non-trivial solutions if $d \neq \pm 1, \pm 2$. For $d = 1$ or $d = \pm 2$, he found the sequences of polynomials given by $P_0 = 1, Q_0 = 0$ and, for $n \in \mathbb{N}$,

$$\begin{aligned} P_n(X) &= \left(\frac{2}{d}X^2 + 1\right) P_{n-1}(X) + \frac{2}{d}X(X^2 + d)Q_{n-1}(X), \\ Q_n(X) &= \frac{2}{d}XP_{n-1}(X) + \left(\frac{2}{d}X^2 + 1\right) Q_{n-1}(X), \end{aligned} \quad (2)$$

and showed that the only integer polynomials which satisfy (1) are of the form $(\pm P_n, \pm Q_n)$; for $d = -1$ he gave another family of solutions. These polynomials can be expressed via Chebyshev polynomials (see, e.g., [12] and Section 4 below). Gaunet [4] proved a similar result for a cubic analogue of (1).

The quest for polynomial solutions of the Pell equation is rather old. Abel [1] observed in 1826 that any non-trivial solution (P, Q) of (1) produces a surprising integral of the shape

$$\int \frac{P'(t)dt}{Q(t)\sqrt{D(t)}} = \log \left(P(t) + Q(t)\sqrt{D(t)} \right).$$

Here, Q divides P' which follows immediately by differentiating both sides of (1). Recently, van der Poorten and Tran [13] gave applications of these generalizations of abelian and quasi-elliptic integrals to units in hyperelliptic function fields.

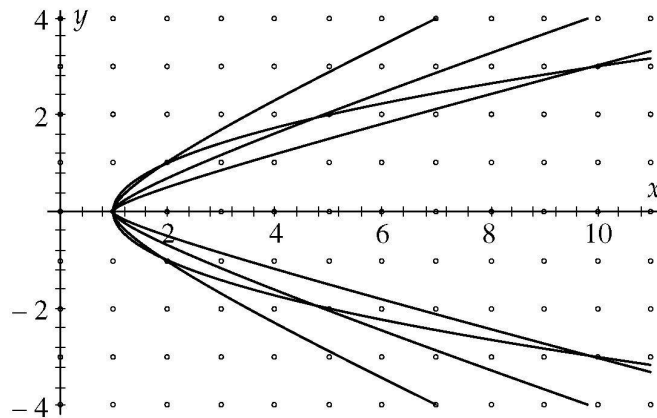


Fig. 1 The hyperbolas $x^2 - Dy^2 = 1$ with $D = D(X) = X^2 + 1$ for $X = 1, 2, 3$ in the range $0 < x \leq 11$ and the curve $x = D(y)$ (resp., $Q_1(x) = P_1(y)$ with $d = 2$ in terms of Nathanson's polynomials). Polynomial solutions with integer coefficients generate solutions in integers.

Shabat and Zvonkin [14] gave certain conditions for the solvability of (1) in terms of the representability of certain integrals by elementary functions and some properties of graphs associated with coverings of Riemann spheres. Let \mathbb{K} be a field of characteristic zero. Avanzi and Zannier [2] proved that if $D \in \mathbb{K}[X]$ is a separable polynomial of degree four, then the polynomial Pell equation (1) has a solution (P, Q) , if and only if the two points at infinity of the elliptic curve

$$Y^2 = D(X) \quad (3)$$

differ by a torsion point (see also [13, pp. 165 and 167]). If this is the case, the solutions (P, Q) of (1) have a parametrization in terms of Chebyshev polynomials. For arbitrary $D \in \mathbb{K}[X]$, Hazama [6] described how the polynomial solutions of (1) may be analyzed via the generalized Jacobian of the affine hyperelliptic curve (3). For $\deg D = 2$, this gives a concrete characterization by treating (1) as a twist of a conic by a conic. Recently, Webb and Yokota [17] and McLaughlin [10] studied the polynomial Pell equation via the continued fraction expansions of polynomials. Their analytical approach seems to be rather technical.

The aim of this paper is to show, that there is nothing mysterious with the solutions of (1) in $\mathbb{Z}[X]$ once we have a solution of the same equation, i.e., with the same $D \in \mathbb{Z}[X]$, in polynomials $P, Q \in \mathbb{C}[X]$. Then all solutions of (1) in $\mathbb{Z}[X]$ are certain powers of the minimal complex solution and can be given in terms of Chebyshev polynomials. We shall study (1) by purely algebraic methods, so our result holds for polynomials in several variables over any field of characteristic $\neq 2$. In the following section we shall give a simple necessary condition for the solvability of the polynomial Pell equation which turns out to be also a sufficient condition if D is quadratic. In Section 3 we give a complete characterization of the solutions of the polynomial Pell equation (1) in case it

has a non-trivial solution. A very simple proof of Nathanson's result and the connections with few of the results mentioned above will also be given.

2 ABC for polynomials: application to Pell's equation

Let $n(P)$ denote the number of distinct complex zeros of a polynomial P (which does not vanish identically). Stothers [16] and Mason [9] (independently) proved that if A, B, C are coprime polynomials over \mathbb{C} , not all constant, which satisfy

$$A + B = C,$$

then

$$\max\{\deg A, \deg B, \deg C\} < n(ABC). \quad (4)$$

The proof is elementary and relies mainly on certain simple properties of logarithmic derivatives. A slightly alternative proof is due to Snyder [15]. A further different proof, using the Riemann-Hurwitz formula, was given by Silverman; the details can be found in [5]. It is easily seen, that (4) implies the truth of Fermat's last theorem for polynomials; see, for example, Lang's survey [7]. Soon after the discovery of the ABC-theorem for polynomials (4) first attempts for a corresponding result with numbers instead of polynomials were started. The well-known *abc*-conjecture due to Masser and Oesterlé claims that if a, b, c are coprime integers which satisfy $a + b = c$, then, for any $\epsilon > 0$,

$$\max\{|a|, |b|, |c|\} \leq \nu(\epsilon) \left(\prod_{p|abc} p \right)^{1+\epsilon},$$

where $\nu(\epsilon)$ is a constant depending on ϵ only; a proof seems to be out of reach with present day methods.

Let us return to the ABC-theorem for polynomials and apply it to the polynomial Pell equation. Suppose that the polynomials $P, Q, D \in \mathbb{C}[X]$ satisfy (1). Then (4) applied with $A = P^2, B = -DQ^2$ and $C = 1$ yields

$$\deg D + 2 \deg Q = \deg DQ^2 < n(P^2DQ^2).$$

Since $n(P^2DQ^2) = n(PDQ) \leq \deg P + n(D) + \deg Q$ and $\deg D = 2 \deg P - 2 \deg Q$, we get

$$n(D) > \deg P - \deg Q = \frac{1}{2} \deg D.$$

Thus, we have shown

Theorem 1 *If the number $n(D)$ of distinct zeros of $D \in \mathbb{C}[X]$ is less than or equal to $\frac{1}{2} \deg D$, then the polynomial Pell equation (1) has no non-trivial solution in $\mathbb{C}[X]$.*

The bound of the theorem is sharp, i.e., it cannot be improved for any $\deg D$. For example, the identity

$$(X^k + 1)^2 - (X^{2k} + 2X^k) \cdot 1^2 = 1$$

shows that there is a non-trivial solution with $D(X) = X^{2k} + 2X^k$, where $\deg D = 2k$ and $n(D) = k + 1$.

In the following section we shall give a complete characterization of the solutions of the polynomial Pell equation (1) with complex coefficients in case it is solvable.

3 Characterization of complex solutions

Pastor [12] studied generalized Chebyshev polynomials and corresponding trees. As an application of his structural theorem he found a polynomial analogue of the structure of the set of solutions of Pell's equation in numbers in case of unitary square-free D . We prove slightly more.

Let R be a subring of \mathbb{C} , and let $D \in \mathbb{C}[X]$ (or $D \in R[X]$). We are interested in polynomials $P, Q \in \mathbb{C}[X]$ (or in $R[X]$, respectively) satisfying the Pell equation (1). We call the solution (p, q) of (1) minimal if $p, q \in \mathbb{C}[X]$ and p has the smallest degree among all non-trivial solutions of (1) (with fixed D). Since $2 \deg p = \deg D + 2 \deg q$, the polynomial q has the smallest non-negative degree among all Q in non-trivial solutions (P, Q) . The set of polynomial solutions of the polynomial Pell equation forms an abelian group generated by one of the minimal solutions and $(-1, 0)$. (The multiplication in the abelian group corresponds to the multiplication of two expressions of the form $P + Q\sqrt{D}$.)

Theorem 2 Suppose that $D \in \mathbb{C}[X]$. If (1) has a non-trivial solution in $\mathbb{C}[X]$, then it has precisely four minimal solutions. If (p, q) is one of these, then all non-trivial solutions of (1) are obtained as $(\pm P, \pm Q)$, where

$$P + Q\sqrt{D} = (p + q\sqrt{D})^n$$

for some $n \in \mathbb{N}$.

Furthermore, if $D \in R[X]$, where R is a subring of \mathbb{C} , is such that (1) has a non-trivial solution in $R[X]$, then there is a positive integer m such that every non-trivial solution of (1) in $R[X]$ is of the form $(\pm P, \pm Q)$, where

$$P + Q\sqrt{D} = (p + q\sqrt{D})^{mn}$$

for some $n \in \mathbb{N}$.

Proof. Note, that if (p, q) and (P, Q) are two solutions of (1), then so are

$$(Pp + DQq, Pq + Qp) \quad \text{and} \quad (Pp - DQq, Qp - Pq). \quad (5)$$

Clearly,

$$(Pq + Qp)(Qp - Pq) = \begin{vmatrix} p^2 & q^2 \\ p^2 & Q^2 \end{vmatrix} = \begin{vmatrix} 1 & q^2 \\ 1 & Q^2 \end{vmatrix} = Q^2 - q^2. \quad (6)$$

Assume that (p, q) and (P, Q) are two minimal solutions. Let $s = \deg Q = \deg q$. Then (6) implies that

$$\deg(Pq + Qp) + \deg(Qp - Pq) \leq 2s.$$

If both degrees on the left-hand side would be equal to s , then

$$Pq + Qp + Qp - Pq = 2Qp$$

would be of degree $\leq s$, so $\deg p = 0$, a contradiction. Hence, for instance, $\deg(Qp - Pq) < s$ (the other case can be treated in the same way). Then the second solution in (5) must be trivial, so $Qp = Pq$ and $Pp = \pm 1 + DQq$. Setting

$$\lambda = \lambda(X) = \frac{P(X)}{p(X)} = \frac{Q(X)}{q(X)},$$

we have $\lambda p^2 = \pm 1 + \lambda Dq^2$. Thus $\lambda = \lambda(p^2 - Dq^2) = \pm 1$, giving $(P, Q) = (p, q)$ or $(-p, -q)$ (the other case yields $(P, Q) = (-p, q)$ or $(p, -q)$). This proves the first assertion of the theorem.

Assume that all solutions of (1) with Q of degree $< \ell$ are of the form $(\pm P, \pm Q)$, where $P + Q\sqrt{D} = (p + q\sqrt{D})^n$ with some $n \in \mathbb{N}$. Consider a solution (P, Q) of (1) with $\deg Q = \ell$. Again (6) shows, by the same reasoning as above, that either $\deg(Pq + Qp) < \ell$ or $\deg(Qp - Pq) < \ell$. In the first case, using (5) we get by induction that (up to a sign)

$$Pp + DQq + (Pq + Qp)\sqrt{D} = (p + q\sqrt{D})^n,$$

which yields

$$P + Q\sqrt{D} = (p + q\sqrt{D})^{n-1},$$

and so (P, Q) is as required. The other case can be treated in the same way. This proves the ‘complex’ case of the theorem.

For the ‘subring’ part note that every solution in $R[X]$ must be certain natural power of a minimal complex solution. Take the smallest power m for which $(p + q\sqrt{D})^m$ gives the expression $P + Q\sqrt{D}$ with $P, Q \in R[X]$. It follows that $(p + q\sqrt{D})^{mn}$ are solutions of (1) for every $n \in \mathbb{N}$. If there would be a solution in $R[X]$ different from $(p + q\sqrt{D})^{mn}$, say $(p + q\sqrt{D})^{mn+r}$ with $0 < r < m$, then $(p + q\sqrt{D})^r = (p + q\sqrt{D})^{mn+r} (p - q\sqrt{D})^{mn}$ would give a solution of (1) in $R[X]$, a contradiction with the minimality of m . This completes the proof of the theorem. \square

This proof carries over without change for every polynomial in several variables $D \in \mathbb{K}[X_1, \dots, X_s]$ over a field \mathbb{K} of characteristic $\neq 2$ (instead of \mathbb{C}) and for every subring R of \mathbb{K} . Note that the equality $P + Q\sqrt{D} = (p + q\sqrt{D})^n$ can be rewritten as

$$P = \frac{1}{2} \left((p + q\sqrt{D})^n + (p - q\sqrt{D})^n \right), \quad Q = \frac{1}{2\sqrt{D}} \left((p + q\sqrt{D})^n - (p - q\sqrt{D})^n \right).$$

Corollary 3 *The solution (P, Q) of (1) satisfying $\deg P = \frac{1}{2} \deg D$ and $\deg Q = 0$ is minimal.*

It follows from Theorem 1 that, for $\deg D = 2$, non-trivial solutions exist only if both roots of D are distinct. This condition is not only necessary, but also sufficient. Indeed, assume that

$$D(X) = c(X - \alpha)(X - \beta) \in \mathbb{C}[X]$$

with complex numbers $c \neq 0$ and $\alpha \neq \beta$. Set

$$P(X) = \frac{2X - (\alpha + \beta)}{\alpha - \beta} \quad \text{and} \quad Q(X) = \frac{2}{\sqrt{c}(\alpha - \beta)}.$$

A simple computation shows that equation (1) holds and, by Corollary 3, this solution is minimal. We obtain

Corollary 4 *If $D \in \mathbb{C}[X]$ is a quadratic polynomial, then the Pell equation (1) has a non-trivial solution in $\mathbb{C}[X]$ if and only if D is separable.*

The case of quartic D is much more difficult. We shall return to this topic in the following section.

4 Families of solutions

As an application of Theorem 2 and Corollary 3, we prove a generalization of Nathanson's result [11]. Consider $D(X) = X^{2k} + d$ with $k \in \mathbb{N}$ and non-zero $d \in \mathbb{C}$. (By Theorem 1, there are no non-trivial solutions for $d = 0$.) By Corollary 3

$$\left(\frac{X^k}{\sqrt{-d}}, \frac{1}{\sqrt{-d}} \right)$$

is the minimal solution of (1). By Theorem 2 all non-trivial solutions of (1) in complex polynomials are given by

$$\left(\frac{X^k + \sqrt{X^{2k} + d}}{\sqrt{-d}} \right)^n \quad \text{for } n \in \mathbb{N}.$$

Let d be a non-zero integer. Note that the coefficient for X^{kn} in P equals

$$\frac{1}{(-d)^{n/2}} \left(1 + \binom{n}{2} + \binom{n}{4} + \dots \right) = \frac{2^{n-1}}{(-d)^{n/2}}.$$

Consequently, if (1) has a non-trivial solution in $\mathbb{Z}[X]$, then there is some $n \in \mathbb{N}$ for which

$$\frac{2^{n-1}}{(-d)^{n/2}} \in \mathbb{Z}.$$

This is the case if and only if $d \in \{\pm 1, \pm 2\}$. This leads to Theorem 1 in [11]. Now, if $d = -1$ we have $m = 1$, giving Theorem 3 in [11], and if $d \in \{1, \pm 2\}$ we have $m = 2$, since

$$-\left(\frac{X^k + \sqrt{X^{2k} + d}}{\sqrt{-d}} \right)^2 = \frac{2}{d}X^{2k} + 1 + \frac{2}{d}X^k\sqrt{X^{2k} + d}$$

give polynomials

$$\frac{2}{d}X^{2k} + 1 \quad \text{and} \quad \frac{2}{d}X^k$$

with integer coefficients, which leads to Theorem 3 of [11].

For example, for $d = k = 1$, i.e., $D(X) = X^2 + 1$, we have two series of solutions of (1) in $\mathbb{C}[X]$. The integer solutions of the Pell equation are integral lattice points on a hyperbola, and so it is not at all surprising that the polynomial solutions of (1) can be parametrized by the hyperbolic sine and cosine functions. Let

$$t = \operatorname{arsinh}(X) = \log(X + \sqrt{X^2 + 1}).$$

Then these series are

$$\left(\pm \cosh(nt), \pm \frac{\sinh(nt)}{\cosh(t)} \right) \quad \text{for } n = 0, 2, 4, \dots, \quad (7)$$

and

$$\left(\pm i \sinh(nt), \pm i \frac{\cosh(nt)}{\cosh(t)} \right) \quad \text{for } n = 1, 3, 5, \dots \quad (8)$$

These are solutions of (1) since

$$\cosh(nt)^2 - \sinh(nt)^2 = 1.$$

It is easily seen, that the expressions (7) and (8) are, in fact, polynomials in X for the corresponding parity of n , and by Theorem 2 for every $n \in \mathbb{N}$ there are at most four solutions (P, Q) with $\deg P = n$. Thus, (7) and (8) give all complex solutions of $P(X)^2 - (X^2 + 1)Q(X)^2 = 1$. In fact, the series (7) must be identical to the polynomials found by Nathanson (2). They consist of polynomials with integer coefficients. Similarly, the series (8) consist of integer polynomials multiplied by $\pm i$. (These correspond to the solutions of the equation $P(X)^2 - (X^2 + 1)Q(X)^2 = -1$.)

In particular, this implies that for quartic polynomials D the condition of Theorem 1 is necessary but not sufficient. We give a simple example. Set

$$D(X) = (X^2 + 1)(X - a)^2,$$

where a is a positive real number. Then $n(D) = 3 > 2 = \frac{1}{2} \deg D$, but the Pell equation has no non-trivial solutions. Indeed, assume it has. Then there exist polynomials $P \in \mathbb{C}[X]$, $\deg P > 0$, and $Q \in \mathbb{C}[X]$, $Q(a) = 0$, such that

$$P(X)^2 - (X^2 + 1)Q(X)^2 = 1. \quad (9)$$

All solutions of (9) are, however, described by (7) and (8). Every polynomial $Q(X)$ of the form $\sinh(nt)/\cosh(t)$, $n = 2, 4, 6, \dots$, or $i \cosh(nt)/\cosh(t)$, $n = 1, 3, 5, \dots$, where $t = \log(X + \sqrt{X^2 + 1})$, satisfies $Q(a) \neq 0$, giving the desired contradiction. Similarly,

setting $D(X) = (X^{2k} + 1)(X - a)^2$, $a > 0$, we obtain examples with $\deg D = 2k + 2$ for every $k \in \mathbb{N}$.

We conclude with a look on quartic D . Consider

$$S(X) = X^2 + uX + v \in \mathbb{Z}[X].$$

By Corollary 3, $(S(X), 1)$ is a minimal solution of (1) for

$$D(X) = S(X)^2 - 1 = X^4 + 2uX^3 + (u^2 + 2v)X^2 + 2uvX + v^2 - 1,$$

which gives formula (1) on p. 1006 of [17]. Similarly, $(2S(X) \pm 1, 2)$ is the minimal solution of (1) for $D(X) = S(X)^2 \pm S(X)$ (see (2) in [17]) and $(S(X)^2 + D(X), 2S(X))$ is the minimal solution of (1) for $D(X) = S(X)^2 + 1$, which gives formula (4) in [17], because

$$-\left(iS(X) + i\sqrt{D(X)}\right)^2 = S(X)^2 + D(X) + 2S(X)\sqrt{D(X)},$$

and $(iS(X), i)$ is a minimal complex solution by Corollary 3.

All these quartic examples come from the following more general example. Let R be a ring of characteristic $\neq 2$ and let $S(X), L(X)$ be non-zero polynomials such that $S(X), L(X), 2S(X)/L(X) \in R[X]$. Then, with $D(X) = S(X)^2 + L(X) \in R[X]$, Pell's equation (1) has non-trivial solutions in $R[X]$, because

$$\left(1 + 2\frac{S^2}{L}\right)^2 - (S^2 + L)\left(2\frac{S}{L}\right)^2 = 1.$$

Acknowledgements. The first named author was supported by the exchange program between the universities of Vilnius and Frankfurt; main parts of the paper were done during his stay at Frankfurt University in 2003. He was also supported by the Lithuanian State Science and Studies Foundation.

References

- [1] Abel, N.H.: *Sur l'intégration de la formule différentielle $\rho dx/\sqrt{R}$, R et ρ étant des fonctions entières.* In: *Oeuvres Complètes de Niels Henrik Abel*. Sylow, L.; Lie, S. (eds.), Christiania, t. 1 (1881), 104–144.
- [2] Avanzi, R.M.; Zannier, U.M.: Genus one curves defined by separated variable polynomials and a polynomial Pell equation. *Acta Arith.* 99 (2001), 227–256.
- [3] Barbeau, E.J.: *Pell's equation*. Springer, 2003.
- [4] Gaunet, M.-L.: Formes cubiques polynomiales. *C.R. Acad. Sci. Paris* 311 (1990), 491–494.
- [5] Granville, A.; Tucker, T.J.: It's as easy as abc. *Notices Amer. Math. Soc.* 49 (2002), 1224–1231.
- [6] Hazama, F.: Pell equations for polynomials. *Indag. Math.* 8 (1997), 387–397.
- [7] Lang, S.: Die abc-Vermutung. *Elem. Math.* 48 (1993), 89–99.
- [8] Lenstra, H.W.: Solving the Pell equation. *Notices Amer. Math. Soc.* 49 (2002), 182–192.

-
- [9] Mason, R.C.: *Diophantine equations over function fields*. LMS Lecture Notes 96, Cambridge University Press, 1984.
 - [10] McLaughlin, J.: Polynomial solutions of Pell's equation and fundamental units in real quadratic fields. *J. London Math. Soc.* 67 (2003), 16–28.
 - [11] Nathanson, M.B.: Polynomial Pell equations. *Proc. Amer. Math. Soc.* 56 (1976), 89–92.
 - [12] Pastor, A.V.: Generalized Chebyshev polynomials and the Pell-Abel equation. *Fundam. Prikl. Mat.* 7 (2001), 1123–1145.
 - [13] van der Poorten, A.J.; Tran, X.C.: Quasi-elliptic integrals and periodic continued fractions. *Monatsh. Math.* 131 (2000), 155–169.
 - [14] Shabat, G.; Zvonkin, A.: Plane trees and algebraic numbers. *Contemp. Math.* 178 (1994), 233–275.
 - [15] Snyder, N.: An alternate proof of Mason's theorem. *Elem. Math.* 55 (2000), 93–94.
 - [16] Stothers, W.W.: Polynomial identities and Hauptmoduln. *Quart. J. Math.* 32 (1981), 349–370.
 - [17] Webb, W.A.; Yokota, H.: Polynomial Pell's equation. *Proc. Amer. Math. Soc.* 131 (2002), 993–1006.

Artūras Dubickas

Department of Mathematics

Vilnius University

Naugarduko 24

03225 Vilnius, Lithuania

e-mail: arturas.dubickas@maf.vu.lt

Jörn Steuding

Department of Mathematics

J.W. Goethe-Universität Frankfurt

Robert-Mayer-Str. 10

60054 Frankfurt, Germany

e-mail: steuding@math.uni-frankfurt.de