

POLYNOMIAL PELL'S EQUATION

WILLIAM A. WEBB AND HISASHI YOKOTA

(Communicated by David E. Rohrlich)

ABSTRACT. Consider the polynomial Pell's equation $X^2 - DY^2 = 1$, where $D = A^2 + 2C$ is a monic polynomial in $\mathcal{Z}[x]$ and $\deg C < \deg A$. Then for $A, C \in \mathcal{Q}[x]$, $\deg C < 2$, and $B = A/C \in \mathcal{Q}[x]$, a necessary and sufficient condition for the polynomial Pell's equation to have a nontrivial solution in $\mathcal{Z}[x]$ is obtained.

1. INTRODUCTION

Let D be a nonconstant monic polynomial of even degree with integer coefficients. We consider the polynomial Pell's equation

$$(1) \quad X^2 - DY^2 = 1$$

where solutions X, Y are polynomials with integer coefficients. In 1976, Nathanson [5] proved that when $D = x^2 + d$, equation (1) has a nontrivial solution if and only if $d = \pm 1, \pm 2$. This is a special case of the open problem which asks to determine the polynomials D for which equation (1) has nontrivial solutions, and the special quadratics above is the only class of polynomials for which solutions of (1) have been completely characterized. We will characterize solutions of (1) for a much larger class of polynomials D , which includes all monic $D = A^2 + 2C$ where $\deg C \leq 1$ and $A/C \in \mathcal{Q}[x]$. In particular, this includes all monic quadratic polynomials since they can be written as $A^2 + 2C$ where $\deg C = 0$.

As we will see, solving (1) over $\mathcal{Q}[x]$ is relatively easy; determining when solutions in $\mathcal{Z}[x]$ exist is the more difficult question.

We note that equation (1) has no nontrivial solution if D is a perfect square. For $D = A^2$, we have $1 = (X + AY)(X - AY)$, which implies $X = \pm 1, Y = 0$. So, we assume \sqrt{D} is irrational.

We will call $W = U + V\sqrt{D}$ a rational solution of (1) if $U^2 - DV^2 = 1$ and $U, V \in \mathcal{Q}[x]$. We define

$$T = \{U + V\sqrt{D} : U^2 - DV^2 = 1, \operatorname{sgn} U > 0, \operatorname{sgn} V > 0, \text{ where } U, V \in \mathcal{Q}[x]\}$$

and T_0 to be the subset of T such that $U, V \in \mathcal{Z}[x]$. If W is any rational solution of (1), so are $\pm W$ and $\pm \overline{W}$. Among these four solutions, there is always one for which $\operatorname{sgn} U > 0$ and $\operatorname{sgn} V > 0$. Thus to determine all rational solutions of (1), it suffices to find all solutions in T .

Received by the editors April 3, 2001.

1991 *Mathematics Subject Classification*. Primary 11D25, 11A55.

Key words and phrases. Polynomial Pell's equation.

Among all rational solutions in T , we say $P+Q\sqrt{D}$ is a minimal (or fundamental) solution if and only if its nonarchimedean absolute value, defined below, satisfies the following condition:

$$|P + Q\sqrt{D}| \leq |U + V\sqrt{D}| \text{ for all } U + V\sqrt{D} \in T.$$

Then we can show (see Lemma 3 below) that a minimal solution is unique, and (see Lemma 4 below) every rational solution $W \in T$ can be expressed as $W = W_0^n$ for some $n \geq 1$, where W_0 is the minimal solution. So, to determine the polynomials D for which the polynomial Pell's equation (1) has nontrivial rational solutions, it suffices to find the minimal solution.

Let W_0 be the minimal solution. We ask the following questions:

- (1) When is W_0 in T_0 ?
- (2) Is it possible to have $W_0^n \in T_0$ even though $W_0 \notin T_0$?

Since $T_0 \subset T$, $W \in T_0$ implies $W = W_0^n$ for some $n \geq 1$, where W_0 is the minimal solution. Thus if the answer to the second question is negative, then every solution W of the polynomial Pell's equation (1) is expressed as $\pm W_0^n$ or $\pm \overline{W_0}^n$ for some $n \geq 1$, where $W_0 \in T_0$.

To answer these questions, we consider the continued fraction expansion of \sqrt{D} . Note that the continued fraction expansion of \sqrt{D} can be defined in many ways depending on the base field (see [1], [2], [3], [4], [6]). Let $\mathcal{K} = \mathcal{Q}((x^{-1}))$ be the field of formal Laurent series in x^{-1} over \mathcal{Q} . Then $\alpha \in \mathcal{K}$ implies that

$$\alpha = \sum_{j=t}^{\infty} a_j x^{-j}, \text{ where } a_j \in \mathcal{Q}, a_t \neq 0, \text{sgn } \alpha = a_t.$$

We define the nonarchimedean absolute value by

$$|\alpha| = e^{-t}.$$

So, $|A/B| = e^{\deg A - \deg B}$ for $A, B \in \mathcal{Q}[x]$. We use the symbol $[\alpha]$ to mean the integer part of α :

$$[\alpha] = \sum_{j=t}^0 a_j x^{-j} = a_t x^{-t} + \dots + a_0 \in \mathcal{Q}[x].$$

Note that for any $U + V\sqrt{D} \in T$, $|U + V\sqrt{D}| > 1$ and $|U - V\sqrt{D}| < 1$. Hence, $|U| = |V\sqrt{D}|$. Also, if W_1 and W_2 are rational solutions of (1), then so is $W_1 W_2$. Write $W_1 = U_1 + V_1\sqrt{D}$ and $W_2 = U_2 + V_2\sqrt{D}$. Then

$$1 = U_1^2 - DV_1^2 = W_1 \overline{W_1} = W_2 \overline{W_2} = U_2^2 - DV_2^2.$$

Hence $(W_1 W_2) \overline{(W_1 W_2)} = 1$ which implies $W_1 W_2$ is a rational solution of (1).

A *continued fraction expansion* for \sqrt{D} is obtained by putting $\alpha_0 = \sqrt{D}$ and, recursively for $n \geq 0$, putting

$$A_n = [\alpha_n] \text{ and } \alpha_{n+1} = 1/(\alpha_n - A_n).$$

The algorithm terminates if, for some n , $\alpha_n = A_n$. This happens if and only if \sqrt{D} is a rational function. Thus \sqrt{D} can be expressed in the following way:

$$\begin{aligned} \sqrt{D} &= [\sqrt{D}] + \frac{1}{\alpha_1} \\ &= [\sqrt{D}] + \frac{1}{[\alpha_1] + \frac{1}{\alpha_2} + \dots}. \end{aligned}$$

For short, we write

$$\sqrt{D} = \langle [\sqrt{D}], [\alpha_1], \dots \rangle = \langle A_0, A_1, \dots \rangle, \text{ where } A_i \in \mathcal{Q}[x].$$

We write convergents to \sqrt{D} as $P_n/Q_n = \langle A_0, A_1, \dots, A_n \rangle$, where

$$\begin{pmatrix} P_n & Q_n \\ P_{n-1} & Q_{n-1} \end{pmatrix} = \begin{pmatrix} A_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} P_{n-1} & Q_{n-1} \\ P_{n-2} & Q_{n-2} \end{pmatrix} \text{ for } n \geq 0$$

and

$$\begin{pmatrix} P_{-1} & Q_{-1} \\ P_{-2} & Q_{-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then by looking at the determinant of the above matrix, we have for $n \geq 0$

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n+1}.$$

We note that since $\text{sgn } A_0 > 0$, $\sigma(P_n) = \sigma(Q_n)$ for all $n \geq 0$, where $\sigma(A)$ denote the sign of the leading coefficient of A .

Now write \sqrt{D} as

$$\sqrt{D} = \langle A_0, A_1, \dots, A_n, A_{n+1}, \dots \rangle = \langle A_0, A_1, \dots, A_n, \alpha_{n+1} \rangle.$$

Then

$$\sqrt{D} = \frac{\alpha_{n+1} P_n + P_{n-1}}{\alpha_{n+1} Q_n + Q_{n-1}}.$$

We say α_j is reduced if $|\alpha_j| > 1$ and $|\bar{\alpha}_j| < 1$.

Suppose $P + Q\sqrt{D}$ is the minimal solution. Then we can show (see Lemma 2 below) that $P + Q\sqrt{D} = \lambda(P_n + Q_n\sqrt{D})$ for some $\lambda \in \mathcal{Q}$. We note that if s is the least index satisfying $(\lambda P_s)^2 - D(\lambda Q_s)^2 = 1$, then since $\sigma(P_s) = \sigma(Q_s)$, $\sigma(\lambda Q_s)(\lambda P_s + \lambda Q_s\sqrt{D})$ is the minimal solution.

Let $D = A^2 + 2C$ be a polynomial in $\mathcal{Z}[x]$, where $A, C \in \mathcal{Q}[x]$, $\deg C < \deg A$, and $B = A/C \in \mathcal{Q}[x]$. Since

$$\sqrt{D} = [\sqrt{D}] + \frac{1}{\alpha_1} = A + \frac{1}{\alpha_1},$$

where

$$\alpha_1 = \frac{1}{\sqrt{D} - A} = \frac{\sqrt{D} + A}{2C} = \left[\frac{\sqrt{D} + A}{2C} \right] + \frac{1}{\alpha_2} = B + \frac{1}{\alpha_2}$$

and

$$\alpha_2 = \sqrt{D} + A = 2A + \sqrt{D} - A = 2A + \frac{1}{\alpha_1},$$

then $\sqrt{D} = \langle A, \overline{B}, 2A \rangle$ and

$$P_1^2 - DQ_1^2 = (AB + 1)^2 - DB^2 = (AB + 1)^2 - (A^2B^2 + 2AB) = 1.$$

Thus $\sigma(Q_1)(P_1 + Q_1\sqrt{D})$ is a nontrivial rational solution in T . Note that this may not be the minimal solution.

To see this, notice that

$$(kP_0)^2 - D(kQ_0)^2 = k^2(A^2 - (A^2 + 2C)) = k^2(-2C) = 1$$

if and only if $2C = -1/k^2$. Thus $W_0 = kP_0 + kQ_0\sqrt{D}$ with $\text{sgn}(kP_0) > 0$ is the minimal solution if and only if $2C = -1/k^2$, and $W_0 = \sigma(Q_1)(P_1 + Q_1\sqrt{D})$ is the

minimal solution if and only if $2C \neq -1/k^2$. Thus we are left to determine when $W_0^n \in T_0$ for $W_0 = kP_0 + kQ_0\sqrt{D}$ and $W_0 = \sigma(Q_1)(P_1 + Q_1\sqrt{D})$.

We will show

Theorem 1. *Let $D = A^2 + 2C$ be a monic polynomial in $\mathcal{Z}[x]$, where $\deg C < \deg A$ and $B = A/C \in \mathcal{Q}[x]$. Suppose either $A \in \mathcal{Z}[x]$ or $2A \in \mathcal{Z}[x]$. Then the following are equivalent:*

- (1) $W_0^n \in T_0$ for some $n \geq 1$.
- (2) $W_0 \in T_0$.
- (3) $W_0 = \begin{cases} A + \sqrt{D}, & \text{where } A \in \mathcal{Z}[x], 2C = -1, \\ 2A + 2\sqrt{D}, & \text{where } A \notin \mathcal{Z}[x], 2A \in \mathcal{Z}[x], \\ & 2C = -1/4, \\ \sigma(C)(B^2C + 1 + B\sqrt{D}), & \text{where } B, C \in \mathcal{Z}[x], \\ 2A^2 + 1 + 2A\sqrt{D}, & \text{where } A \in \mathcal{Z}[x], 2C = 1, \\ \sigma(C)(B^2C + 1 + B\sqrt{D}), & \text{where } A \in \mathcal{Z}[x], B = \pm 2B_1, \\ & B_1 \in \mathcal{Z}[x], \text{sgn } C = \pm \frac{1}{2}, \\ & 2C \in \mathcal{Z}[x], \deg C > 0. \end{cases}$

Theorem 2. *Let $D = A^2 + 2C$ be a monic polynomial in $\mathcal{Z}[x]$, where $\deg C < \deg A$ and $B = A/C \in \mathcal{Q}[x]$. Suppose $C = c_1x + c_0 \in \mathcal{Q}[x]$. Then either $A \in \mathcal{Z}[x]$ or $2A \in \mathcal{Z}[x]$.*

Hence the complete characterization of solutions of (1) for the monic polynomials of the form $D = A^2 + 2C = A^2 + c_1x + c_0$, where $\deg C < \deg A$ and $B = A/C \in \mathcal{Q}[x]$.

Before proving these, we need a few notations and lemmas.

Let $\nu_p(m/n) = i - j$, where $(m, n) = 1, p^i || m, p^j || n$. For $A = x^k + a_{k-1}x^{k-1} + \dots + a_1x + a_0$, define $\nu_p(A) = \min\{\nu_p(a_i) : 0 \leq i < k\}$. Denote the coefficient a_j of x^j in A by $[x^j]A$ and the Gaussian integer function of a by $[a]$.

2. LEMMAS

Lemma 1. *Let $D = A^2 + 2C$ be a monic polynomial in $\mathcal{Z}[x]$, where $\deg C < \deg A$. Suppose that $\sqrt{D} = \langle A_0, A_1, A_2, \dots, A_n, \alpha_{n+1} \rangle$. Then α_{n+1} is reduced, $\deg A_n \geq 1$, and $|P_n/Q_n - \sqrt{D}| = |1/Q_n Q_{n+1}|$ for all $n \geq 0$.*

Proof. We first show by using induction on n that α_n is reduced and $\deg A_n \geq 1$ for all $n > 0$.

Since $D = A^2 + 2C$ with $\deg C < \deg A$, $[\sqrt{A^2 + 2C}] = A$. Thus if $\sqrt{D} = \langle A_0, \dots, A_n, \alpha_{n+1} \rangle$, then $A_0 = A$ and $\deg A_0 \geq 1$. Now since D is monic, $\text{sgn } A > 0$ and $|\sqrt{D} + A| = e^{\deg A}$. Then

$$|\sqrt{D} - A| = \left| \frac{D - A^2}{\sqrt{D} + A} \right| = \left| \frac{2C}{\sqrt{D} + A} \right| < 1.$$

Thus

$$|\alpha_1| = \left| \frac{1}{\sqrt{D} - A} \right| = \left| \frac{A + \sqrt{D}}{2C} \right| > 1 \text{ and } |\bar{\alpha}_1| = \left| \frac{1}{\sqrt{D} + A} \right| < 1.$$

This shows that α_1 is reduced and $\deg A_1 = \deg [\alpha_1] \geq 1$.

Suppose $|\alpha_k| > 1, |\bar{\alpha}_k| < 1$ and $\deg A_k \geq 1$. Then since $|\alpha_k - A_k| = |\alpha_k - [\alpha_k]| < 1$, we have

$$|\alpha_{k+1}| = \left| \frac{1}{\alpha_k - A_k} \right| > 1$$

and since $|\bar{\alpha}_k - A_k| = |A_k| > 1$, we have

$$|\bar{\alpha}_{k+1}| = \left| \frac{1}{\bar{\alpha}_k - A_k} \right| < 1.$$

Thus α_{k+1} is reduced and $\deg A_{k+1} = \deg [\alpha_{k+1}] \geq 1$.

Next we show $|P_n/Q_n - \sqrt{D}| = |1/Q_n Q_{n+1}|$ for all $n \geq 0$. By the first part, we can assume that $|\alpha_{n+2}| > 1$. Then since $|Q_n^2/\alpha_{n+2}| < |Q_n Q_{n+1}|$, we have

$$\begin{aligned} \left| \frac{P_n}{Q_n} - \sqrt{D} \right| &= \left| \frac{P_n}{Q_n} - \frac{\alpha_{n+1}P_n + P_{n-1}}{\alpha_{n+1}Q_n + Q_{n-1}} \right| = \left| \frac{P_n Q_{n-1} - Q_n P_{n-1}}{Q_n(\alpha_{n+1}Q_n + Q_{n-1})} \right| \\ &= \left| \frac{1}{Q_n((A_{n+1} + \frac{1}{\alpha_{n+2}})Q_n + Q_{n-1})} \right| = \left| \frac{1}{Q_n Q_{n+1} + \frac{Q_n^2}{\alpha_{n+2}}} \right| \\ &= \left| \frac{1}{Q_n Q_{n+1}} \right|. \end{aligned}$$

□

Lemma 2. *If $U + V\sqrt{D} \in T$, then $U = \lambda P_n$ and $V = \lambda Q_n$ for some $n \geq 0$ and $\lambda \in \mathcal{Q}$.*

Proof. We have

$$\left| \frac{U}{V} - \sqrt{D} \right| = \left| \frac{1}{V(U + V\sqrt{D})} \right| = \left| \frac{1}{V^2(U/V + \sqrt{D})} \right| < \left| \frac{1}{V} \right|^2.$$

Then choose n so that $|Q_n| \leq |V| < |Q_{n+1}|$, so by Lemma 1,

$$\left| \frac{U}{V} - \sqrt{D} \right| < \left| \frac{1}{VQ_n} \right| \text{ and } \left| \frac{P_n}{Q_n} - \sqrt{D} \right| < \left| \frac{1}{VQ_n} \right|.$$

If $U/V \neq P_n/Q_n$, then

$$\begin{aligned} \left| \frac{1}{Q_n V} \right| &\leq \left| \frac{P_n V - Q_n U}{Q_n V} \right| = \left| \frac{P_n}{Q_n} - \frac{U}{V} \right| = \left| \frac{P_n}{Q_n} - \sqrt{D} + \sqrt{D} - \frac{U}{V} \right| \\ &\leq \max\{ \left| \frac{P_n}{Q_n} - \sqrt{D} \right|, \left| \sqrt{D} - \frac{U}{V} \right| \} < \left| \frac{1}{Q_n V} \right|, \end{aligned}$$

a contradiction. Thus $U/V = P_n/Q_n$. Note that $P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n+1}$ implies P_n and Q_n are relatively prime, and $U^2 - DV^2 = 1$ implies U and V are relatively prime, which in turn imply $U = \lambda P_n, V = \lambda Q_n$ for some $n \geq 0$ and $\lambda \in \mathcal{Q}$. □

Lemma 3. *If $W_1, W_2 \in T$ and $|W_1| = |W_2|$, then $W_1 = W_2$. In particular, the minimum solution is unique.*

Proof. Let $W_1 = U_1 + V_1\sqrt{D}$ and $W_2 = U_2 + V_2\sqrt{D}$. Then by Lemma 2, $W_1 = \lambda P_m + \lambda Q_m\sqrt{D}$ and $W_2 = \mu P_n + \mu Q_n\sqrt{D}$ for some $m, n \geq 0$ and $\lambda, \mu \in \mathcal{Q}$. Since $|W_1| = |W_2|$, $\deg P_m = \deg P_n$ so $m = n$. Thus

$$\lambda^2(P_m^2 - DQ_m^2) = \mu^2(P_m^2 - DQ_m^2).$$

Since \sqrt{D} is irrational, $\lambda = \pm\mu$ and by the definition of T , $W_1 = W_2$.

If, in particular, W_1 and W_2 are minimum solutions, then by the definition of a minimum solution, we have $|W_1| = |W_2|$, which implies $W_1 = W_2$. □

Lemma 4. *If W_0 is the minimal solution, then for any $W \in T$, $W = W_0^n$ for some $n \geq 1$.*

Proof. If $|W| = |W_0|^n = |W_0^n|$, then by Lemma 3, $W = W_0^n$. Otherwise choose $n \geq 1$ so that

$$|W_0|^n < |W| < |W_0|^{n+1}.$$

Then

$$1 < |\overline{W_0}^n W| < |W_0|$$

and $\overline{W_0}^n W$ is a solution of (1). Since $|\overline{W_0}^n W| > 1$, either $\overline{W_0}^n W$ or $-\overline{W_0}^n W$ is in T , which is impossible since $|\overline{W_0}^n W| < |W_0|$. \square

Lemma 5. *Let $D = A^2 + 2C$ be a monic polynomial in $\mathcal{Z}[x]$, where $A, C \in \mathcal{Q}[x]$ and $\deg C < \deg A$. If $p > 2$, then $\nu_p(A) \geq 0$ and $\nu_p(C) \geq 0$.*

Proof. Since D is monic, we write $A = x^k + a_{k-1}x^{k-1} + \dots + a_0$. Suppose r is the largest index so that $\nu_p(a_r) \leq -1$. Then

$$[x^{k+r}]D = [x^{k+r}]A^2 = 2a_r + \sum_{\substack{i+j=k+r \\ r < i, j < k}} a_i a_j \in \mathcal{Z}.$$

Since $\nu_p(a_j) \geq 0$ for $j > r$, $\nu_p\left(\sum_{\substack{i+j=k+r \\ r < i, j < k}} a_i a_j\right) \geq 0$, and so $\nu_p(a_r) = \nu_p(2a_r) \geq 0$, a contradiction. \square

Lemma 6. *Let $f(m) = \sum_{i=1}^{\infty} \lfloor \frac{m}{2^i} \rfloor$. Then for $m > 0$,*

- (1) $2f(m) \leq f(2m) - 1$.
- (2) $f(m) \geq f(m - j) + f(j)$ for $1 \leq j \leq m - 1$.

Proof. Since $f(m) < \sum_{i=1}^{\infty} \frac{m}{2^i} = m$,

$$f(2m) = \sum_{i=1}^{\infty} \lfloor \frac{2m}{2^i} \rfloor = \sum_{i=0}^{\infty} \lfloor \frac{m}{2^i} \rfloor = m + f(m) > 2f(m).$$

Inequality (2) follows from the well-known fact that $f(m)$ is the largest power of 2 which divides $m!$. \square

Lemma 7. *Let $D = A^2 + 2C = (x^k + a_{k-1}x^{k-1} + \dots + a_0)^2 + 2C$ be a monic polynomial in $\mathcal{Z}[x]$, where $\deg C < k$. If $A \notin \mathcal{Z}[x]$, then let $k - m > 1$ be the largest index such that $\nu_2(a_{k-m}) \leq -1$. Then $\nu_2(a_{k-m}) = -1$. Furthermore, for $qm \leq j < (q + 1)m$,*

$$\nu_2(a_{k-j}) \geq -q - f(q),$$

where $f(q) = \sum_{i=1}^{\infty} \lfloor \frac{q}{2^i} \rfloor$.

Proof. Since $k - m$ is the largest index such that $\nu_2(a_{k-m}) \leq -1$, suppose that $\nu_2(a_{k-m}) \leq -2$ and $\nu_2(a_{k-j}) \geq 0$ for $j < m$. Then consider

$$[x^{k+k-m}]D = [x^{2k-m}]A^2 = 2a_{k-m} + \sum_{\substack{i+j=m \\ 0 < i, j < m}} a_{k-i} a_{k-j} \in \mathcal{Z}.$$

Since $\nu_2\left(\sum_{\substack{i+j=m \\ 0 < i, j < m}} a_{k-i} a_{k-j}\right) \geq 0$, $\nu_2(2a_{k-m}) \geq 0$, a contradiction. Hence $\nu_2(a_{k-m}) = -1$.

Next we show for all j with $qm \leq j < (q + 1)m$, $\nu_2(a_{k-j}) \geq -q - f(q)$. We use induction on q . For $q = 0$, we have $0 \leq j < m$ and $\nu_2(a_{k-j}) \geq 0$.

Assume that the induction hypothesis is true for all values less than q , where $q \geq 1$. Suppose $k - m_q$, $qm \leq m_q < (q + 1)m$ is the largest index such that $\nu_2(a_{k-m_q}) < -q - f(q)$. Then consider

$$[x^{k+k-m_q}]D = [x^{2k-m_q}]A^2 = 2a_{k-m_q} + \sum_{\substack{i+j=m_q \\ 0 < i, j < m_q}} a_{k-i}a_{k-j} \in \mathcal{Z}.$$

Let $sm \leq i < (s + 1)m$. Then since $i + j = m_q < (q + 1)m$, $j < (q - s + 1)m$. By the induction hypothesis, $\nu_2(a_{k-i}) \geq -s - f(s)$ and $\nu_2(a_{k-j}) \geq -(q - s) - f(q - s)$. Thus by Lemma 6,

$$\nu_2(2a_{k-i}a_{k-j}) \geq -q - (f(s) + f(q - s)) + 1 \geq -q - f(q) + 1.$$

Now for m_q even, since $qm \leq m_q < (q + 1)m$, we have

$$\lfloor \frac{q}{2} \rfloor m \leq \frac{m_q}{2} < (\lfloor \frac{q}{2} \rfloor + 1)m.$$

Thus

$$\begin{aligned} \nu_2(a_{k-m_q/2}^2) &= 2\nu_2(a_{k-m_q/2}) \geq 2(-\lfloor q/2 \rfloor - f(\lfloor q/2 \rfloor)) \\ &\geq \begin{cases} -2\lfloor \frac{q}{2} \rfloor - f(2\lfloor \frac{q}{2} \rfloor) + 1 & \text{for } q \geq 1, \\ -2\lfloor \frac{1}{2} \rfloor - 2f(\lfloor \frac{1}{2} \rfloor) = 0 & \text{for } q = 1 \end{cases} \\ &\geq \begin{cases} -q - f(q) + 1 & \text{for } q \geq 1, \\ -1 - f(1) + 1 & \text{for } q = 1. \end{cases} \end{aligned}$$

Therefore, $\nu_2\left(\sum_{\substack{i+j=m_q \\ 0 < i, j < m_q}} a_{k-i}a_{k-j}\right) \geq -q - f(q) + 1$ which implies that $\nu_2(a_{k-m_q}) \geq -q - f(q)$, a contradiction. Thus for $qm \leq j < (q + 1)m$, $\nu_2(a_{k-j}) \geq -q - f(q)$. \square

3. MAIN THEOREMS

Proof of Theorem 1. We break Theorem 1 into two cases according to whether $2C = -1/k^2$ or not. We first treat the case $2C = -1/k^2$. Note that in this case, the minimal solution is $W_0 = kP_0 + kQ_0\sqrt{D} = kA + k\sqrt{D}$ with $k > 0$. \square

Proposition 1. *Let $D = A^2 + 2C$ be a monic polynomial in $\mathcal{Z}[x]$, where $2C = -1/k^2, k \in \mathcal{Q}$. Suppose either $A \in \mathcal{Z}[x]$ or $2A \in \mathcal{Z}[x]$. Then the following are equivalent:*

- (1) $W_0^n \in T_0$ for some $n \geq 1$.
- (2) $W_0 \in T_0$.
- (3) $W_0 = \begin{cases} A + \sqrt{D}, & \text{where } A \in \mathcal{Z}[x], 2C = -1, \\ 2A + 2\sqrt{D}, & \text{where } A \notin \mathcal{Z}[x], 2A \in \mathcal{Z}[x], 2C = -1/4. \end{cases}$

Proof. The implications (3) \Rightarrow (2) and (2) \Rightarrow (1) are clear. So, we show (1) \Rightarrow (3).

Case 1. $A \in \mathcal{Z}[x]$.

Note that $2C = D - A^2 = -1/k^2 \in \mathcal{Z}[x]$ implies $1/k = u, u \in \mathcal{Z}$. Suppose that $W_0^n = (kA + k\sqrt{D})^n = X_{n-1} + Y_{n-1}\sqrt{D} \in T_0$, where $k > 0$. Then

$$X_{n-1} = \sum_j \binom{n}{2j} (kA)^{n-2j} k^{2j} D^j = \sum_j \binom{n}{2j} (kA)^{n-2j} k^{2j} (A^2 + 2C)^j$$

has the leading coefficient of A^n :

$$\sum_j \binom{n}{2j} k^n = 2^{n-1} k^n = 2^{n-1}/u^n$$

which is in \mathcal{Z} only if $k = u = 1$. Thus, we have $W_0 = A + \sqrt{D}$, where $A \in \mathcal{Z}[x]$ and $2C = -1$.

Case 2. $A \notin \mathcal{Z}[x], 2A \in \mathcal{Z}[x]$.

Note that $8C = 4D - (2A)^2 = -4/k^2 \in \mathcal{Z}[x]$ implies $1/k = u/2, u \in \mathcal{Z}$. Suppose that $W_0^n = (kA + k\sqrt{D})^n = X_{n-1} + Y_{n-1}\sqrt{D} \in T_0$, where $k > 0$. Then

$$X_{n-1} = \sum_j \binom{n}{2j} (kA)^{n-2j} k^{2j} D^j$$

has the leading coefficient of A^n :

$$\sum_j \binom{n}{2j} k^n = 2^{n-1} k^n = 2^{2n-1}/u^n$$

which is in \mathcal{Z} only if $k = 1, 2$. But $k = 1$ implies $2C \in \mathcal{Z}$, which implies $A = D^2 - 2C \in \mathcal{Z}[x]$, a contradiction.

Thus, we have $W_0 = 2A + 2\sqrt{D}$, where $A \notin \mathcal{Z}[x], 2A \in \mathcal{Z}[x]$, and $2C = -1/4$. \square

Proposition 2. *Let $D = A^2 + 2C$ be a monic polynomial in $\mathcal{Z}[x]$, where $\deg C < \deg A, B = A/C \in \mathcal{Q}[x]$, and $2C \neq -1/k^2$. Suppose either $A \in \mathcal{Z}[x]$ or $2A \in \mathcal{Z}[x]$. Then the following are equivalent:*

- (1) $W_0^n \in T_0$ for some $n \geq 1$.
- (2) $W_0 \in T_0$.
- (3) $W_0 = \begin{cases} \sigma(C)(B^2C + 1 + B\sqrt{D}), & \text{where } B, C \in \mathcal{Z}[x], \\ 2A^2 + 1 + 2A\sqrt{D}, & \text{where } A \in \mathcal{Z}[x], 2C = 1, \\ \sigma(C)(B^2C + 1 + B\sqrt{D}), & \text{where } A \in \mathcal{Z}[x], B = \pm 2B_1, \\ & B_1 \in \mathcal{Z}[x], \text{sgn } C = \pm \frac{1}{2}, \\ & 2C \in \mathcal{Z}[x], \deg C > 0. \end{cases}$

Proof. The implications (3) \Rightarrow (2) and (2) \Rightarrow (1) are clear. So, we show (1) \Rightarrow (3).

Since $B = A/C \in \mathcal{Q}[x]$, we have

$$\sqrt{D} = \langle BC, \overline{B}, 2BC \rangle \quad \text{and} \quad W_0 = \sigma(C)(B^2C + 1 + B\sqrt{D}) \in T.$$

Assume $W_0^n \in T_0$. If $t = \text{sgn } B$, then we can write $B = tB_1, C = \frac{1}{t}C_1$, where $t \in \mathcal{Q}$ and $A = B_1C_1$. If $\nu_p(B_1) = e, \nu_p(C_1) = f$, then since B_1 and C_1 are monic, $e, f \leq 0$ and $\nu_p(A) = \nu_p(B_1C_1) = \nu_p(B_1) + \nu_p(C_1) = e + f$. But $2A \in \mathcal{Z}[x]$, so if $p \neq 2$, then $e = f = 0$. If $p = 2$, then $e + f$ is equal to either 0 or -1 depending on whether $A \in \mathcal{Z}[x]$ or not.

Case 1. $A \in \mathcal{Z}[x]$.

Then $e + f = 0$ and $B_1, C_1 \in \mathcal{Z}[x]$. Since $2C = D - A^2 \in \mathcal{Z}[x], \frac{2}{t}C_1 \in \mathcal{Z}[x]$. Thus $2/t \in \mathcal{Z}$ which in turn implies that $t = 1/u$ or $2/u$ for some $u \in \mathcal{Z}$. Write $(P_1 + Q_1\sqrt{D})^n = (tB_1^2C_1 + 1 + tB_1\sqrt{D})^n = X_n + Y_n\sqrt{D}$. Then

$$X_n = \sum_j \binom{n}{2j} (tB_1^2C_1 + 1)^{n-2j} (tB_1)^{2j} D^j$$

has the leading coefficient

$$\sum_j \binom{n}{2j} t^n = 2^{n-1} t^n = \begin{cases} 2^{n-1}/u^n & \text{if } t = 1/u, \\ 2^{2n-1}/u^n & \text{if } t = 2/u \end{cases}$$

which is in \mathcal{Z} only if $|t| = 1, 2$.

If $|t| = 1$, then $B = tB_1 \in \mathcal{Z}[x]$, $C = C_1/t \in \mathcal{Z}[x]$, and

$$W_0 = \sigma(C)(B^2C + 1 + B\sqrt{D}).$$

If $|t| = 2$, then $B = tB_1 \in \mathcal{Z}[x]$ and $2C = \pm C_1 \in \mathcal{Z}[x]$. Since C_1 is monic, $C = \frac{1}{t}C_1$ implies $\text{sgn } C = \pm 1/2$. Note that for $\deg C = 0$, $\text{sgn } C = -1/2$ implies $2C = -1$ which is impossible since $2C \neq -1/k^2$. Thus for $\deg C = 0$, we have $2C = 1$. Then $B = A/C = 2A$ and $W_0 = 2A^2 + 1 + 2A\sqrt{D}$. For $\deg C > 0$, $W_0 = \sigma(C)(B^2C + 1 + B\sqrt{D})$, where $\text{sgn } C = \pm 1/2$, $B = \pm 2B_1$, $B_1, 2C \in \mathcal{Z}[x]$.

Case 2. $A \notin \mathcal{Z}[x]$, $2A \in \mathcal{Z}[x]$.

We will show that $W_0^n \notin \mathcal{Z}[x]$. Let $p = 2$. Then $e + f = -1$. Thus either $f = 0$ or $f = -1$ which implies either $C_1 \in \mathcal{Z}[x]$ or $2C_1 \in \mathcal{Z}[x]$. Since $8C = 4D - (2A)^2 \in \mathcal{Z}[x]$, $\frac{8}{t}C_1 \in \mathcal{Z}[x]$. Thus $8/t \in \mathcal{Z}$ and we can write $t = 2^g/u$, $0 \leq g \leq 3$, where u is an integer.

Now as above, the leading coefficient of X_n is $2^{(g+1)n-1}/u^n$, which is in \mathcal{Z} only if $u|2^g$. Thus $t|8$. Recalling that $e + f = -1$ and $e, f \leq 0$, we see

- (1) $t = \pm 1, \pm 2$ implies $f = \nu_2(C_1) = \nu_2(tC) \leq -2$ which is impossible.
- (2) $t = \pm 4$ implies $e = 0$ and $f = -1$ which in turn implies

$$W_0 = \sigma(C)(B^2C + 1 + B\sqrt{D}) = 4B_1^2C_1 \pm 1 + 4B_1\sqrt{D} \in T_0,$$

where $B_1, 2C_1 \in \mathcal{Z}[x]$.

- (3) $t = \pm 8$ implies $e = -1$ and $f = 0$ which in turn implies

$$W_0 = \sigma(C)(B^2C + 1 + B\sqrt{D}) = 8B_1^2C_1 \pm 1 + 8B_1\sqrt{D} \in T_0,$$

where $2B_1, C_1 \in \mathcal{Z}[x]$.

Thus in either case, $8C \in \mathcal{Z}[x]$ and $B \in \mathcal{Z}[x]$. So, we let

$$\begin{aligned} A &= x^k + a_{k-1}x^{k-1} + \dots + a_0, \text{ where } 2a_i \in \mathcal{Z} \text{ for all } i, \\ C &= \frac{1}{8}(c_sx^s + c_{s-1}x^{s-1} + \dots + c_0), \text{ where } c_i \in \mathcal{Z} \text{ for all } i, \\ B &= 8(b_rx^r + b_{r-1}x^{r-1} + \dots + b_0), \text{ where } 8b_i \in \mathcal{Z} \text{ for all } i. \end{aligned}$$

Let m be the largest index so that $\nu_2(a_m) = -1$. If $2m > s$, then

$$[x^{2m}]D = [x^{2m}]A^2 = 2(a_0a_{2m} + a_1a_{2m-1} + \dots + a_{m+1}a_{m-1}) + a_m^2 \in \mathcal{Z},$$

which is impossible since $\nu_2(2a_i a_j) \geq 0$ for $i \neq j$ and $\nu_2(a_m^2) = -2$. So, assume $2m \leq s$. Thus

$$\begin{aligned} A^2 &= x^{2k} + d_{2k-1}x^{2k-1} + \dots + d_sx^s + \dots + d_{2m}x^{2m} + \dots, \\ 2C &= \frac{c_s}{4}x^s + \dots + \frac{c_{2m}}{4}x^{2m} + \dots, \end{aligned}$$

where $\nu_2(d_j) \geq 0$ for all $j > 2m$. Then $c_j/4 \in \mathcal{Z}$ for $j > 2m$. Also, $[x^{2m}](A^2 + 2C) \in \mathcal{Z}$ implies that $\nu_2(c_{2m}/4) = -2$ which in turn implies that c_{2m} is odd.

Now write A as

$$\begin{aligned} A &= BC \\ &= b_r c_s x^{r+s} + (b_r c_{s-1} + c_s b_{r-1}) x^{r+s-1} + \dots \\ &\quad + (b_r c_{2m} + b_{r-1} c_{2m+1} + \dots + b_{r+2m-s} c_s) x^{r+2m} + \dots \end{aligned}$$

Suppose that $s > 2m$. Then since $4|c_s$ and $b_r c_s = 1$, we have $\nu_2(b_r) \leq -2$. We also note that since $8b_i \in \mathcal{Z}$ for all i and $c_j/4 \in \mathcal{Z}$ for $j > 2m$, $\nu_2(b_{r-i} c_{2m+i}) \geq -1$ for $i > 0$, which implies that $\nu_2([x^{r+2m}]A) \leq -2$, a contradiction.

Thus we assume that $s = 2m$. Then since c_{2m} is odd, $8b_r \in \mathcal{Z}$, and $b_r c_{2m} = 1$ imply that $c_{2m} = b_r = \pm 1$. Now write A as

$$\begin{aligned} A &= BC \\ &= x^{r+2m} + (b_{r-1} + c_{2m-1}) x^{r+2m-1} + \dots \\ &\quad + (b_0 + b_1 c_{2m-1} + \dots + b_{2m} c_0) x^{2m} + \dots \end{aligned}$$

We divide this into cases $m > 0$ and $m = 0$.

If $m > 0$, then since $\nu_2(a_j) \geq 0$ for $j > m$, all coefficients of x^t for $t \geq 2m$ are integers. But then $c_i \in \mathcal{Z}$ implies that $b_j \in \mathcal{Z}$ for all $j \geq 0$. Then $A = BC \in \mathcal{Z}[x]$ which is a contradiction.

So, we suppose that $m = 0$, $C = c_0/8$, and $c_0 = \pm 1$. Since $D = A^2 + 2C = x^{2k} + \dots + a_0^2 + c_0/4 \in \mathcal{Z}[x]$, $a_0^2 + c_0/4 \in \mathcal{Z}$. Then $a_0^2 + c_0/4 \in \mathcal{Z}$ and $c_0 = \pm 1$ imply that $c_0 = -1$, which in turn implies $2C = -1/4 = -1/k^2$, a contradiction. Thus for $A \notin \mathcal{Z}[x]$ and $2A \in \mathcal{Z}[x]$, $W_0^n \notin T_0$ for all $n \geq 1$. □

Proof of Theorem 2. Since D is monic, we write $A = x^k + a_{k-1}x^{k-1} + \dots + a_0$. We first treat the case $c_1 = 0$. Since $D \in \mathcal{Z}[x]$, if either $A \in \mathcal{Z}[x]$ or $2C \in \mathcal{Z}[x]$, then both are. Otherwise, by Lemma 5, we may suppose that $\nu_2(2c_0) \leq -1$ and since $a_0^2 + 2c_0 \in \mathcal{Z}$, $\nu_2(a_0) \leq -1$. Suppose that $l \geq 1$ is the smallest index satisfying $\nu_2(a_l) \leq -1$. Then

$$[x^l]D = [x^l]A^2 = 2a_l a_0 + \sum_{\substack{i+j=l \\ 0 < i, j < l}} a_i a_j \in \mathcal{Z}.$$

Since $\nu_2\left(\sum_{\substack{i+j=l \\ 0 < i, j < l}} a_i a_j\right) \geq 0$, $\nu_2(2a_l a_0) \geq 0$ which implies that $\nu_2(a_l) \geq 0$, a contradiction. Hence $a_i \in \mathcal{Z}$ for $i \geq 1$. Now

$$[x^k]D = [x^k]A^2 = 2a_0 + \sum_{\substack{i+j=k \\ 0 < i, j < k}} a_i a_j \in \mathcal{Z}$$

and $\nu_2\left(\sum_{\substack{i+j=k \\ 0 < i, j < k}} a_i a_j\right) \geq 0$ imply that $\nu_2(2a_0) = 1 + \nu_2(a_0) \geq 0$, which in turn implies that $\nu_2(a_0) \geq -1$. So $\nu_2(a_0) = -1$ and $2A \in \mathcal{Z}[x]$.

We next treat the case $c_1 \neq 0$. We will divide the proof into two cases according to whether $\nu_2(a_0) \geq 0$ or $\nu_2(a_0) < 0$.

Case 1. $\nu_2(a_0) \geq 0$.

Suppose that $\nu_2(a_1) = -t \leq -1$. Then since $\nu_2(a_0) \geq 0$, $[x^0]D = a_0^2 + 2c_0 \in \mathcal{Z}$ and $[x^1]D = 2a_1 a_0 + 2c_1 \in \mathcal{Z}$ imply that $\nu_2(2c_0) \geq 0$ and $\nu_2(c_1) \geq -t$. Thus $2^t c_1 \in \mathcal{Z}[x]$. Since $D = A^2 + 2C \in \mathcal{Z}[x]$, $2^{t-1}D = 2^{t-1}A^2 + 2^t C \in \mathcal{Z}[x]$, which implies that $2^{t-1}A^2 \in \mathcal{Z}[x]$. Thus $\nu_2(A) \geq -\frac{t-1}{2} > -t = \nu_2(a_1)$, a contradiction.

Therefore, if $\nu_2(a_0) \geq 0$, then $\nu_2(a_1) \geq 0$. But then $a_0^2 + 2c_0 \in \mathcal{Z}$ and $2a_1a_0 + 2c_1 \in \mathcal{Z}$ imply that $2C = 2c_1x + 2c_0 \in \mathcal{Z}[x]$, which in turn implies that $A \in \mathcal{Z}[x]$.

Case 2. $\nu_2(a_0) < 0$.

Suppose first that $\nu_2(a_1) < \nu_2(a_0)$. Let $\nu_2(a_1) = -t$ and $\nu_2(a_0) = -u$. Then $a_0^2 + 2c_0 \in \mathcal{Z}$ and $2a_1a_0 + 2c_1 \in \mathcal{Z}$ imply that $\nu_2(c_0) = -2u - 1$ and $\nu_2(c_1) = -t - u$. Since $-t < -u$, we have $2^{t+u}C \in \mathcal{Z}[x]$. Then $2^{t+u-1}D = 2^{t+u-1}A^2 + 2^{t+u}C \in \mathcal{Z}[x]$ which implies that $2^{t+u-1}A^2 \in \mathcal{Z}[x]$. Thus $\nu_2(A) \geq -\frac{t+u-1}{2} > -u = \nu_2(a_1)$, a contradiction.

Suppose next that $\nu_2(a_0) = \nu_2(a_1) = -t \leq -1$. Then $a_0^2 + 2c_0 \in \mathcal{Z}$ and $2a_1a_0 + 2c_1 \in \mathcal{Z}$ imply that $\nu_2(c_0) = \nu_2(a_0^2) - 1 = -2t - 1$ and $\nu_2(c_1) = \nu_2(a_1) + \nu_2(a_0) = -2t$. Thus $2^{2t+1}C \in \mathcal{Z}[x]$. Since $D = A^2 + 2C$, we have $2^{2t}D = 2^{2t}A^2 + 2^{2t+1}C \in \mathcal{Z}[x]$, which implies that $2^tA \in \mathcal{Z}[x]$. Thus $\nu_2(A) \geq -t$. Now consider $[x^2]D = [x^2]A^2 = a_1^2 + 2a_2a_0 \in \mathcal{Z}$. Then $\nu_2(2a_2a_0) = \nu_2(a_1^2) = -2t$ implies that $\nu_2(a_2) = -t - 1 < -t \leq \nu_2(A)$, a contradiction.

Finally suppose $\nu_2(a_0) < \nu_2(a_1)$.

Suppose $\nu_2(a_1) \geq 0$ and consider $[x^l]A^2$ for $l \geq 2$. For $l = 2$, we have $2a_2a_0 + a_1^2 \in \mathcal{Z}$ and $\nu_2(a_2) \geq 0$. For $l = 3$, we have $2a_3a_0 + 2a_2a_1 \in \mathcal{Z}$ and $\nu_2(a_3) \geq 0$. Continuing this, we have $\nu_2(a_i) \geq 0$ for all $0 < i < k$. Then

$$[x^k]D = [x^k]A^2 = 2a_0 + \sum_{\substack{i+j=k \\ 0 < i, j < k}} a_i a_j \in \mathcal{Z}$$

which implies that $\nu_2(2a_0) \geq 0$. Thus $\nu_2(a_0) \geq -1$ and $2A \in \mathcal{Z}[x]$.

Suppose $\nu_2(a_1) \leq -1$ and let $\nu_2(a_1) - \nu_2(a_0) = t \geq 1$. Then since $a_0^2 + 2c_0 \in \mathcal{Z}$, $\nu_2(2c_0) = \nu_2(a_0^2) = 2\nu_2(a_0) = 2(\nu_2(a_1) - t)$. Also since $2a_1a_0 + 2c_1 \in \mathcal{Z}$, $\nu_2(2c_1) = \nu_2(2a_1a_0) = \nu_2(a_1) + \nu_2(a_0) + 1 = 2\nu_2(a_1) - t + 1$. Then

$$\nu_2\left(\frac{2c_0}{2c_1}\right) = 2\nu_2(a_1) - 2t - 2\nu_2(a_1) + t - 1 = -t - 1.$$

Thus $-c_0/c_1 = u/2^{t+1}$, where $u \in \mathcal{Q}$ and $\nu_2(u) = 0$. Since $A(x) = B(x)C(x) = B(x)(c_1x + c_0)$,

$$\begin{aligned} 0 &= A\left(-\frac{c_0}{c_1}\right) = A\left(\frac{u}{2^{t+1}}\right) \\ &= \left(\frac{u}{2^{t+1}}\right)^k + a_{k-1}\left(\frac{u}{2^{t+1}}\right)^{k-1} + \dots + a_1\left(\frac{u}{2^{t+1}}\right) + a_0. \end{aligned}$$

Let $k - m$ be the largest index such that $\nu_2(a_{k-m}) \leq -1$. Then by Lemma 7, $\nu_2(a_{k-m}) = -1$. Thus for $1 \leq j < m$,

$$\nu_2\left(a_{k-j}\left(\frac{u}{2^{t+1}}\right)^{k-j}\right) > \nu_2\left(\left(\frac{u}{2^{t+1}}\right)^k\right).$$

Now we evaluate $\nu_2\left(a_{k-j}\left(\frac{u}{2^{t+1}}\right)^{k-j}\right)$ for $j \geq m$. By Lemma 7, for $qm \leq j < (q + 1)m$, we have

$$\nu_2(a_{k-j}) \geq -q - f(q).$$

Thus for $qm \leq j < (q + 1)m$,

$$\begin{aligned} \nu_2 \left(a_{k-j} \left(\frac{u}{2^{t+1}} \right)^{k-j} \right) &= \nu_2(a_{k-j}) - (t + 1)(k - j) \\ &\geq -q - f(q) - (t + 1)(k - j) \\ &= -q - f(q) + j(t + 1) - k(t + 1) \\ &\geq -q - f(q) + qm(t + 1) - k(t + 1). \end{aligned}$$

Since $m \geq 1$ and $t \geq 1$, $-q - f(q) + qm(t + 1) - k(t + 1) \geq -q - f(q) + 2q - k(t + 1) \geq 1 - k(t + 1)$. Then since $\nu_2 \left(\left(\frac{u}{2^{t+1}} \right)^k \right) = -(t + 1)k$, we have

$$\nu_2 \left(a_{k-j} \left(\frac{u}{2^{t+1}} \right)^{k-j} \right) > \nu_2 \left(\left(\frac{u}{2^{t+1}} \right)^k \right)$$

for $j \geq m$. Thus we have

$$\nu_2 \left(a_{k-j} \left(\frac{u}{2^{t+1}} \right)^{k-j} \right) > \nu_2 \left(\left(\frac{u}{2^{t+1}} \right)^k \right)$$

for all $j \geq 1$, which implies that $A(-\frac{ca}{c_1}) \neq 0$, a contradiction. □

As a corollary to Theorems 1 and 2, we characterize the solutions of the polynomial Pell’s equation (1) for a class of quartic polynomials D .

Corollary 1. *Let $D = x^4 + ax^3 + bx^2 + cx + d \in \mathcal{Z}[x]$. Suppose $D = A^2 + 2C$, where $B = A/C \in \mathcal{Q}[x]$. Then $W_0 \in T_0$ if and only if*

- (1) $W_0 = x^2 + a_1x + l + \sqrt{D}$, where $a = 2a_1, a_1 \in \mathcal{Z}, b = a_1^2 + 2l, l \in \mathcal{Z}, c = 2a_1l$, and $d = l^2 - 1$.
- (2) $W_0 = 2(x^2 + a_1x + l + \frac{1}{2}) + 2\sqrt{D}$, where $a = 2a_1, a_1 \in \mathcal{Z}, b = a_1^2 + 2l + 1, l \in \mathcal{Z}, c = 2a_1l + a_1$, and $d = l^2 + l$.
- (3) $W_0 = (x + a_1 \mp t)^2(x \pm t) \pm 1 + (x + a_1 \mp t)\sqrt{D}$, where $a = 2a_1, a_1 \in \mathcal{Z}, b = a_1^2 + 2l, l \in \mathcal{Z}, c = 2c_1, c_1 = a_1l \pm 1, d = l^2 + 2t, t \in \mathcal{Z}$, and $l = t(\pm a_1 - t)$.
- (4) $W_0 = 2(x^2 + a_1x + l)^2 + 1 + 2(x^2 + a_1x + l)\sqrt{D}$, where $a = 2a_1, a_1 \in \mathcal{Z}, b = a_1^2 + 2l, l \in \mathcal{Z}, c = 2a_1l$, and $d = l^2 + 1$.
- (5) $W_0 = 2(x + (a_1 \mp t))^2(x \pm t) \pm 1 + 2(x + a_1 \mp t)\sqrt{D}$, where $a = 2a_1, a_1 \in \mathcal{Z}, b = a_1^2 + 2l, l \in \mathcal{Z}, c = 2a_1l \pm 1, d = l^2 + t, t \in \mathcal{Z}$, and $l = \pm t(a_1 \mp t)$.

Before proving this, we note that by letting $a = b = c = 0$ and $X = x^2$, we can obtain Nathanson’s result. Also, by letting $a = c = 0$ and $X = x^2$, we have the complete characterization of all quadratic polynomials for which Pell’s equation (1) with $D = X^2 + bX + d$ is solvable over $\mathcal{Z}[x]$.

Proof. Write $D = A^2 + 2C$, where

$$A = x^2 + \frac{a}{2}x + \frac{4b - a^2}{8}, \quad 2C = \frac{8c - 4ab + a^3}{8}x + \frac{64d - (4b - a^2)^2}{64}.$$

Then by Theorems 1 and 2, we have

- (1) $W_0 = A + \sqrt{D}$ if and only if $A \in \mathcal{Z}[x], 2C = -1$. This occurs if and only if $\frac{a}{2} \in \mathcal{Z}, \frac{4b - a^2}{8} \in \mathcal{Z}, 8c - 4ab + a^3 = 0$, and $64d - (4b - a^2)^2 = -64$, which in turn is equivalent to $a = 2a_1, a_1 \in \mathcal{Z}, b - a_1^2 = 2l, l \in \mathcal{Z}, c = \frac{4ab - a^3}{8} = \frac{8a_1(a_1^2 + 2l) - 8a_1^3}{8} = 2a_1l$, and $d = \frac{(4b - a^2)^2 - 64}{64} = l^2 - 1$. Thus $W_0 = x^2 + a_1x + l + \sqrt{D}$ if and only if $a = 2a_1, a_1 \in \mathcal{Z}, b = a_1^2 + 2l, l \in \mathcal{Z}, c = 2a_1l$, and $d = l^2 - 1$.

- (2) $W_0 = 2A + 2\sqrt{D}$ if and only if $A \notin \mathcal{Z}[x]$, $2A \in \mathcal{Z}[x]$, and $2C = -\frac{1}{4}$. This occurs if and only if $\frac{a}{2} \in \mathcal{Z}$, $\frac{4b-a^2}{4} \in \mathcal{Z}$, $\frac{4b-a^2}{8} \notin \mathcal{Z}$, $8c - 4ab + a^3 = 0$, and $64d - (4b - a^2)^2 = -16$, which in turn is equivalent to $a = 2a_1, a_1 \in \mathcal{Z}$, $b - a_1^2 = 2l + 1, l \in \mathcal{Z}$, $c = \frac{4ab-a^3}{8} = 2a_1l + a_1$, and $d = \frac{(4b-a^2)^2-16}{64} = l^2 + l$. Thus $W_0 = 2(x^2 + a_1x + l + \frac{1}{2}) + 2\sqrt{D}$ if and only if $a = 2a_1, a_1 \in \mathcal{Z}, b = a_1^2 + 2l + 1, l \in \mathcal{Z}, c = 2a_1l + a_1$, and $d = l^2 + l$.
- (3) $W_0 = \sigma(C)(B^2C + 1 + B\sqrt{D})$ if and only if $A, B = A/C, C \in \mathcal{Z}[x]$ which is equivalent to $a = 2a_1, a_1 \in \mathcal{Z}, b - a_1^2 = 2l, l \in \mathcal{Z}, \frac{8c-4ab+a^3}{16} = \frac{8c-16a_1l}{16} = \frac{c-2a_1l}{2} \in \mathcal{Z}, \frac{64d-(4b-a^2)^2}{128} = \frac{64(d-l^2)}{128} \in \mathcal{Z}$, and $B = A/C \in \mathcal{Z}[x]$. Note that $\frac{c-2a_1l}{2} \in \mathcal{Z}$ if and only if $c = 2c_1, c_1 \in \mathcal{Z}, \frac{64(d-l^2)}{128} \in \mathcal{Z}$ if and only if $d - l^2 = 2t, t \in \mathcal{Z}$. Also, $B = A/C \in \mathcal{Z}[x]$ if and only if

$$\begin{aligned} B &= \frac{x^2 + a_1x + l}{(c_1 - a_1l)x + t} \\ &= \frac{1}{c_1 - a_1l}x + \frac{a_1c_1 - a_1^2l - t}{(c_1 - a_1l)^2} \in \mathcal{Z}[x] \end{aligned}$$

and the remainder term satisfies

$$l(c_1 - a_1l)^2 - t(a_1c_1 - a_1^2l - t) = 0.$$

Now $c_1 - a_1l \in \mathcal{Z}$ and $\frac{1}{c_1 - a_1l} \in \mathcal{Z}$ if and only if $c_1 - a_1l = \pm 1$. Thus $W_0 = (x + a_1 \mp t)^2(x \pm t) \pm 1 + (x + a_1 \mp t)\sqrt{D}$ if and only if $a = 2a_1, a_1 \in \mathcal{Z}, b = a_1^2 + 2l, l \in \mathcal{Z}, c = 2c_1, c_1 = a_1l \pm 1, d = l^2 + 2t, t \in \mathcal{Z}$, and $l = t(\pm a_1 - t)$.

- (4) $W_0 = 2A^2 + 1 + 2A\sqrt{D}$ if and only if $A \in \mathcal{Z}[x]$, $2C = 1$. This occurs if and only if $\frac{a}{2}, \frac{4b-a^2}{8} \in \mathcal{Z}, 8c - 4ab + a^3 = 0$, and $64d - (4b - a^2)^2 = 64$, which in turn is equivalent to $a = 2a_1, a_1 \in \mathcal{Z}, b - a_1^2 = 2l, l \in \mathcal{Z}, c = \frac{4ab-a^3}{8} = \frac{8a_1(a_1^2+2l)-8a_1^3}{8} = 2a_1l$, and $d = \frac{(4b-a^2)^2+64}{64} = l^2 + 1$. Thus $W_0 = 2(x^2 + a_1x + l)^2 + 1 + 2(x^2 + a_1x + l)\sqrt{D}$ if and only if $a = 2a_1, a_1 \in \mathcal{Z}, b = a_1^2 + 2l, l \in \mathcal{Z}, c = 2a_1l$, and $d = l^2 + 1$.
- (5) $W_0 = \sigma(C)(B^2C + 1 + B\sqrt{D})$ if and only if $A \in \mathcal{Z}, B = 2B_1, B_1 \in \mathcal{Z}[x]$, $\text{sgn } C = \pm \frac{1}{2}, 2C \in \mathcal{Z}[x], \text{deg } C > 0$. This occurs if and only if $a = 2a_1, a_1 \in \mathcal{Z}, b - a_1^2 = 2l, l \in \mathcal{Z}, \frac{8c-4ab+a^3}{16} = \frac{8c-16a_1l}{16} = \frac{c-2a_1l}{2} = \pm \frac{1}{2}, \frac{64d-(4b-a^2)^2}{64} = \frac{64(d-l^2)}{64} \in \mathcal{Z}$, and $B = A/C \in \mathcal{Q}[x]$. Note that $\frac{c-2a_1l}{2} = \pm \frac{1}{2}$ if and only if $c = 2a_1l \pm 1, \frac{64(d-l^2)}{64} \in \mathcal{Z}$ if and only if $d - l^2 = t \in \mathcal{Z}$, and $B = A/C \in \mathcal{Q}[x]$ if and only if

$$\begin{aligned} B &= \frac{x^2 + a_1x + l}{\pm \frac{1}{2}x + \frac{t}{2}} \\ &= \pm 2x \pm 2(a_1 \mp t) \end{aligned}$$

and the remainder term satisfies

$$l \mp t(a_1 \mp t) = 0.$$

Thus $W_0 = 2(x + (a_1 \mp t))^2(x \pm t) \pm 1 + 2(x + a_1 \mp t)\sqrt{D}$ if and only if $a = 2a_1, a_1 \in \mathcal{Z}, b = a_1^2 + 2l, l \in \mathcal{Z}, c = 2a_1l \pm 1, d = l^2 + t, t \in \mathcal{Z}$, and $l = \pm t(a_1 \mp t)$. \square

By the corollary above, we can list the complete types of monic quartic polynomials for which the polynomial Pell's equation (1) has a nontrivial solution in $\mathcal{Z}[x]$:

- (1) $D = x^4 + 2ux^3 + (u^2 + 2v)x^2 + 2uvx + v^2 - 1$,
- (2) $D = x^4 + 2ux^3 + (u^2 + 2v + 1)x^2 + (2uv + u)x + v^2 + v$,
- (3) $D = x^4 + 2ux^3 + (u^2 + 2(v(\pm u - v)))x^2 + 2(uv(\pm u - v) \pm 1)x + v^2(\pm u - v)^2 + v$,
- (4) $D = x^4 + 2ux^3 + (u^2 + 2v)x^2 + 2uvx + v^2 + 1$,
- (5) $D = x^4 + 2ux^3 + (u^2 + 2(\pm v(u \mp v)))x^2 + (2u(\pm v(u \mp v)) \pm 1)x + v^2(u \pm v)^2 + v$, where $u, v \in \mathcal{Z}$.

REFERENCES

1. N. H. Abel, *Sur l'intégration de la formule différentielle pdx/\sqrt{R} , R et ρ étant des fonctions entières*, in: *Oeuvres Complètes de Niels Henrik Abel* (L. Sylow and S. Lie, eds.). Christiania, t, **1** (1881), 104-144.
2. E. Artin, *Quadratische Körper im Gebiet der höheren Kongruenzen I, II*, in: *The Collected Papers of Emil Artin*, Addison-Wesley, 1965 (originally published in *Math. Z.* 19 (1924), 153-246). MR **31**:1159
3. L.E. Baum and M. M. Sweet, *Continued fractions of algebraic power series in characteristic 2*, *Ann. of Math.* **103** (1976), 593-610. MR **53**:13127
4. R.A. Mollin, *Polynomial solutions for Pell's equation revisited*, *Indian J. Pure Appl. Math.* **28**(4), (1997) 429-438. MR **98b**:11025
5. M. B. Nathanson, *Polynomial Pell's equations*, *Proc. of the AMS* **56** (1976), 89-92. MR **53**:5468
6. A.M.S. Ramasamy, *Polynomial solutions for the Pell's equation*, *Indian J. Pure Appl. Math.* **25** (1994), 577-581. MR **95j**:11023

DEPARTMENT OF MATHEMATICS, WASHINGTON STATE UNIVERSITY, PULLMAN, WASHINGTON 99164

E-mail address: webb@math.wsu.edu

DEPARTMENT OF MATHEMATICS, HIROSHIMA INSTITUTE OF TECHNOLOGY, 2-1-1 MIYAKE SAEKI-KU HIROSHIMA, JAPAN

E-mail address: hyokota@cc.it-hiroshima.ac.jp