

A Continued Fraction Approach to the Diophantine Equation $ax^2 - by^2 = \pm 1$ *

R.A. Mollin

Abstract

We revisit the Diophantine equation of the title, and related equations, from new perspectives that add connections to continued fractions, fundamental units of real quadratic fields, Jacobi symbol equations, and ideal theory. We also develop an analogous theory for the related equation $ax^2 - by^2 = \pm 4$ with $\gcd(x, y) = 1$. Included in both cases is a means for finding the fundamental unit of the underlying quadratic order "halfway" along the period of the simple continued fraction expansion of $(\sigma - 1 + \sqrt{ab})/\sigma$ where $\sigma = 1, 2$. We show, as well, how the fundamental units of these two orders may be linked explicitly in the two simple continued fraction expansions. In addition, we explore the links with the solvability of the norm form equation $x^2 - aby^2 = c \in \mathbb{Z}$. Moreover, we give explicit necessary and sufficient conditions for the parity of the period length of the simple continued fraction expansion of \sqrt{D} to be even in terms of the solvability of the title equation plus a related such equation, and an analogue for $(1 + \sqrt{D})/2$. Also, we give a criterion for the period length to be odd in terms of ambiguous ideal classes.

1 Introduction

The Diophantine equations $ax^2 - by^2 = \pm 1, \pm 4$ for $1 < a < b$ go back at least to Gauss (see Remark 3 below), and there are numerous authors who

*Mathematics Subject Classification 2000: 11A55, 11D09, 11R11. Key words and phrases: quadratic Diophantine equations, continued fractions, norm form equations, fundamental units.

have studied related equations (see the list of references for this paper). Some papers such as [9] and [11] have a non-trivial intersection with the results herein, but our approach is more elementary, more far-reaching, and more accessible. Of course, the study of the classical Pell equation $X^2 - DY^2 = \pm 1$ goes back to Archimedes, and we will link the study of the former to the latter via fundamental units of the underlying quadratic orders, including an interplay between various orders described below.

A seminal paper by Walker [39] in 1967 provided insights into the solvability of $ax^2 - by^2 = \pm 1$ for $a \neq 1 \neq b$. However, there is no connection made with continued fractions therein. We remedy this by extrapolating what was done in [39] and adding the continued fraction connections which yield informative data for the fundamental units of the quadratic order $\mathbb{Z}[\sqrt{ab}]$ when ab is not a perfect square. We link these results with the solvability of the Diophantine equation $aX^2 - bY^2 = \pm 4$ where $\gcd(X, Y) = 1$ and the underlying quadratic order $\mathbb{Z}[(1 + \sqrt{ab})/2]$, when ab is not a perfect square. This provides an analogue of results (not given in [39]) and allows us to provide an explicit formula linking the fundamental units of the aforementioned two orders via continued fraction expansions (see Theorem 4 below). Next, we examine the Diophantine equation $ax^2 - by^2 = \pm 2$ for $1 \leq a < b$ and provide criteria for its solvability. Consequences of these results include a criterion for the period length of the simple continued fraction expansion of \sqrt{ab} to be even in terms of the solvability of $ax^2 - by^2 = \pm 1, \pm 2$. This generalizes and refines results in [36] (see Theorem 6 below, consequences of which include conditions for $Q_{\ell/2}$, the “central norm”, to be 4 — see Equation (11) and Corollary 6 below). For a complete discussion on parity, we provide a criterion for the period length of the simple continued fraction expansion of $(1 + \sqrt{ab})/2$ to be even in terms of the solvability of $aX^2 - bY^2 = \pm 4$ with $\gcd(X, Y) = 1$. Moreover, we provide a criterion for the parity of the period lengths to be odd in terms of ambiguous ideal classes and sums of squares.

At the end of the paper, we generalize results in the literature involving the aforementioned Diophantine equations and certain Jacobi symbol identities involving period lengths discussed above. Lastly, we look at the related Diophantine equations $aX^4 - bY^2 = \pm 1$ and recent results in the literature, culminating with a conjecture related to them in terms of simple continued fractions.

2 Notation and Preliminaries

Herein, we will be concerned with the simple continued fraction expansions of quadratic irrationals $\alpha = (P + \sqrt{D})/Q$ where $D \in \mathbb{N}$ (the natural numbers), D is not a perfect square, and $P^2 \equiv D \pmod{Q}$ with $P, Q \in \mathbb{Z}$ (the integers) and $Q \neq 0$. We denote this expansion by,

$$\alpha = \langle q_0; \overline{q_1, q_2, \dots, q_{\ell-1}, q_{\ell}} \rangle,$$

where $\ell = \ell(\alpha)$ is the period length, $q_0 = \lfloor \alpha \rfloor$ (the *floor* of α). The *norm* of α is given by $N(\alpha) = (P^2 - D)/Q^2$.

The j th *convergent* of α for $j \geq 0$ are given by,

$$\frac{A_j}{B_j} = \langle q_0; q_1, q_2, \dots, q_j \rangle = \frac{q_j A_{j-1} + A_{j-2}}{q_j B_{j-1} + B_{j-2}}. \quad (1)$$

The *complete quotients* are given by, $(P_j + \sqrt{D})/Q_j$, where $P_0 = P$, $Q_0 = Q$, and for $j \geq 1$,

$$P_{j+1} = q_j Q_j - P_j, \quad (2)$$

$$q_j = \left\lfloor \frac{P_j + \sqrt{D}}{Q_j} \right\rfloor, \quad (3)$$

and

$$D = P_{j+1}^2 + Q_j Q_{j+1}. \quad (4)$$

We will also need the following facts (which can be found in most introductory texts in number theory, such as [22], or see [21] for a more advanced exposition).

$$A_j B_{j-1} - A_{j-1} B_j = (-1)^{j-1}. \quad (5)$$

Also, if we define for any $j \in \mathbb{N}$,

$$G_{j-1} = Q_0 A_{j-1} - P_0 B_{j-1}, \quad (6)$$

then

$$G_{j-1} = P_j B_{j-1} + Q_j B_{j-2}, \quad (7)$$

and

$$G_{j-1}^2 - B_{j-1}^2 D = (-1)^j Q_j Q_0. \quad (8)$$

In particular,

$$G_{\ell-1}^2 - B_{\ell-1}^2 D = (-1)^\ell Q_0^2. \quad (9)$$

In what follows, for a general discriminant Δ , with associated radicand D , and conductor f_Δ , the value σ is defined by

$$\sigma = \begin{cases} 2 & \text{if } D \equiv 1 \pmod{4}, \text{ and } f_\Delta \text{ is odd} \\ 1 & \text{otherwise.} \end{cases} \quad (10)$$

(The reader unfamiliar with the notions of a general discriminant and radicand may consult [21, Section 1.5, pp. 23–24], for instance.)

If $\alpha = (\sigma - 1 + \sqrt{D})/\sigma$, then $G_{\ell-1} + B_{\ell-1}\sqrt{D}$ is the fundamental solution of the Pell equation (9). By “fundamental solution” $X + Y\sqrt{D}$, to a norm-form equation $X^2 - DY^2 = c$, we mean that X, Y have the least positive values possible. When $c \neq \pm 1, \pm 4$ this may involve several “classes” of such solutions, so in that case, we mean the fundamental solution in its class (see [22, pp. 298–301] for instance). In general, a *positive* solution is one for which both X and Y are positive values. Similarly, for equations of the form $aX^2 - bY^2 = c$, there are classes of solutions. However, it is easy to show that if $X\sqrt{a} + Y\sqrt{b}$ and $W\sqrt{a} + Z\sqrt{b}$ are both positive solutions of the latter, then the following are equivalent: (1) $X < W$, (2) $Y < Z$, (3) $X\sqrt{a} + Y\sqrt{b} < W\sqrt{a} + Z\sqrt{b}$. Hence, there is a solution with X and Y of least positive value. We will call this the *fundamental solution* of the equation. Furthermore, the *norm* of $\alpha = X\sqrt{a} + Y\sqrt{b}$ is given by $N(\alpha) = aX^2 - bY^2$. This corresponds to the usual norm for elements of the form $\beta = x + y\sqrt{D}$, namely, $N(\beta) = x^2 - Dy^2$.

When ℓ is even, $P_{\ell/2} = P_{\ell/2+1}$, so by Equation (2),

$$Q_{\ell/2} \mid 2P_{\ell/2}, \quad (11)$$

where $Q_{\ell/2}$ is called the *central norm*, (via Equation (8)), and

$$q_{\ell/2} = 2P_{\ell/2}/Q_{\ell/2}. \quad (12)$$

We will utilize the following in the next section.

Theorem 1 *Suppose that $\Delta = 4D/\sigma^2$ is a discriminant and*

$$\ell = \ell((\sigma - 1 + \sqrt{D})/\sigma)$$

with Q_j defined for the simple continued fraction expansion of the principal surd,

$$\omega_\Delta = (\sigma - 1 + \sqrt{D})/\sigma. \quad (13)$$

Then

1. If Q_j/σ is a squarefree divisor of $2D$ for some $j \in \mathbb{N}$ with $j < \ell$, then $j = \ell/2$.
2. If ℓ is even, then $Q_{\ell/2}/\sigma \mid 2D$, where $Q_{\ell/2}/\sigma$ is not necessarily square-free.
3. If $c < \sqrt{\Delta}/2$, then

$$x^2 - Dy^2 = \pm\sigma^2c$$

has a primitive solution if and only if $c = Q_j/\sigma$ for some $j \geq 0$ in the simple continued fraction expansion of ω_Δ .

Proof. See [28, Theorem 2.3, pp. 63–65] and [22, Theorem 5.5.2, p. 261]. \square

Lastly, in [26, Lemma 3.3, p. 323], we established results for \sqrt{D} , which generalize in a similar fashion to the proofs given therein to yield the following two formulas. If ℓ is even, and $\alpha = \omega_\Delta$, then for any odd $j \in \mathbb{N}$,

$$Q_{\ell/2}G_{j\ell-1} = G_{j\ell/2-1}^2 + B_{j\ell/2-1}^2D, \quad (14)$$

and

$$Q_{\ell/2}B_{j\ell-1} = 2G_{j\ell/2-1}B_{j\ell/2-1}. \quad (15)$$

3 Connections with Continued Fractions

Let $D \in \mathbb{N}$ where D is not a perfect square and let $T + U\sqrt{D}$ denote the fundamental solution of the Pell equation

$$x^2 - Dy^2 = \sigma^2 \text{ with } \gcd(x, y) = 1, \quad (16)$$

where σ is defined by Equation (10). In the following, we will use the fact that if $X + Y\sqrt{D}$ is a positive solution of Equation (16), then $(X + Y\sqrt{D})/\sigma = ((T + U\sqrt{D})/\sigma)^j$ for some $j \in \mathbb{N}$.

Theorem 2 *Let $D = ab \in \mathbb{N}$ where $a > 1$, $b > 1$ and D is not a perfect square. Then if the The Diophantine equation*

$$aX^2 - bY^2 = \pm\sigma^2 \text{ with } \gcd(X, Y) = 1 \quad (17)$$

has a solution $(X, Y) = (r, s) \in \mathbb{N}^2$, and Equation (16) has fundamental solution $T + U\sqrt{ab}$, then

$$\left(\frac{r\sqrt{a} + s\sqrt{b}}{\sigma}\right)^2 = \left(\frac{T + U\sqrt{ab}}{\sigma}\right)^{2i+1}$$

for some $i \geq 0$. In particular, $r\sqrt{a} + s\sqrt{b}$ is the fundamental solution of equation (17) if and only if $i = 0$, and all solutions of Equation (17) are given by

$$\frac{(r\sqrt{a} + s\sqrt{b})^{2j+1}}{\sigma^{2j}} \quad \text{for} \quad j \geq 0,$$

where $j \not\equiv 1 \pmod{3}$ if $\sigma = 2$.

Proof. Walker [39] proved this for the $\sigma = 1$ case. We now provide a proof for the $\sigma = 2$ case.

If $\alpha = ((r\sqrt{a} + s\sqrt{b})/2)^2 = (r^2a + s^2b + 2rs\sqrt{ab})/4$, then $N(\alpha) = 1$. Thus, $\alpha = ((T + U\sqrt{ab})/2)^j$ for some $j \in \mathbb{N}$. If $j = 2i$ then

$$r^2a + s^2b + 2rs\sqrt{ab} = T_i^2 + U_i^2ab + 2T_iU_i\sqrt{ab},$$

where

$$\left(\frac{T_i + U_i\sqrt{ab}}{2}\right) = \left(\frac{T + U\sqrt{ab}}{2}\right)^i.$$

Therefore, $r^2a + s^2b = T_i^2 + U_i^2ab$, so by Equations (16)–(17),

$$2s^2b \pm 4 = 2S_i^2ab + 4,$$

so if the plus sign holds on the left, then $a \mid s^2$, forcing $a \mid 4$ by Equation (17), a contradiction since $a > 1$ is odd since $\sigma = 2$. If the minus sign holds on the left, then $b \mid 4$, contradicting that $b > 1$ is odd. We have shown that $j = 2i + 1$ for some $i \geq 0$. Therefore,

$$\left(\frac{r\sqrt{a} + s\sqrt{b}}{2}\right)^2 = \left(\frac{T + U\sqrt{ab}}{2}\right) \left(\frac{T_i + U_i\sqrt{ab}}{2}\right)^2,$$

so

$$\left(\frac{r\sqrt{a} + s\sqrt{b}}{2}\right)^2 \left(\frac{T_i - U_i\sqrt{ab}}{2}\right)^2 = \left(\frac{T + U\sqrt{ab}}{2}\right)^2.$$

Also, the quantity on the left is of the form $((R\sqrt{a} + S\sqrt{b})/2)^2$ where $R\sqrt{a} + S\sqrt{b}$ is a solution of Equation (17), so if $r\sqrt{a} + s\sqrt{b}$ is the fundamental solution of Equation (17), then

$$\left(\frac{r\sqrt{a} + s\sqrt{b}}{2}\right)^2 = \left(\frac{T + U\sqrt{ab}}{2}\right)^{2i+1} = \left(\left(\frac{R\sqrt{a} + S\sqrt{b}}{2}\right)^{2i+1}\right)^2,$$

and for $i > 0$, this contradicts the minimality of $r\sqrt{a} + s\sqrt{b}$. Conversely, if $i = 0$, then $r\sqrt{a} + s\sqrt{b}$ must be the fundamental solution of Equation (17) by the minimality of $T + U\sqrt{ab}$.

Now we show that all solutions of Equation (17) are of the prescribed form. Set

$$\alpha = \frac{(r\sqrt{a} + s\sqrt{b})^{2j+1}}{2^{2j}}. \quad (18)$$

By the above,

$$\alpha = \left(\left(\frac{r\sqrt{a} + s\sqrt{b}}{2}\right)^2\right)^j (r\sqrt{a} + s\sqrt{b}) = \left(\frac{T + U\sqrt{ab}}{2}\right)^j (r\sqrt{a} + s\sqrt{b}).$$

First we show that we cannot have $j \equiv 1 \pmod{3}$. If $j = 1 + 3k$, then since $((T + U\sqrt{ab})/2)^3 \in \mathbb{Z}[\sqrt{ab}]$, we must have,

$$\alpha = \left(\frac{T + U\sqrt{ab}}{2}\right)^{3k} \left(\frac{T + U\sqrt{ab}}{2}\right) (r\sqrt{a} + s\sqrt{b}) =$$

$$(R + S\sqrt{ab})(r\sqrt{a} + s\sqrt{b})^3 = (R + S\sqrt{ab})(A\sqrt{a} + B\sqrt{b}),$$

where R and S are of different parity and $A \equiv B \equiv 0 \pmod{8}$. Hence, $\alpha = E\sqrt{a} + F\sqrt{b}$, where both E and F are even. Hence, α is not a solution to Equation (17). Now we show that all solutions are given by α for $j \equiv 0, 2 \pmod{3}$.

If $j = 3k$, then

$$\alpha = \left(\left(\frac{T + U\sqrt{ab}}{2}\right)^3\right)^k (r\sqrt{a} + s\sqrt{b}) =$$

$$(R + S\sqrt{ab})(r\sqrt{a} + s\sqrt{b}),$$

where R and S are of different parity and both r and s are odd. Thus, $\alpha = E\sqrt{a} + F\sqrt{b}$ where E and F are both odd. Since $N(\alpha) = \pm 4$, then α is a solution to Equation (17). If $j = 3k + 2$, then

$$\begin{aligned} \alpha &= \left(\left(\frac{T + U\sqrt{ab}}{2} \right)^{3k} \right) \left(\frac{T + U\sqrt{ab}}{2} \right)^2 (r\sqrt{a} + s\sqrt{b}) = \\ & \left(\frac{T + U\sqrt{ab}}{2} \right)^{3(k+1)} \left(\frac{T - U\sqrt{ab}}{2} \right) (r\sqrt{a} + s\sqrt{b}) = \\ & (R + S\sqrt{ab}) \left(\frac{r\sqrt{a} - s\sqrt{b}}{2} \right)^2 (r\sqrt{a} + s\sqrt{b}) = \\ & (R + S\sqrt{ab})(r\sqrt{a} + s\sqrt{b}). \end{aligned}$$

Where we conclude as in the previous case that α is a solution to Equation (17).

We have shown that all α of the form given in Equation (18) are solutions of Equation (17) for $j \not\equiv 1 \pmod{3}$. It remains to verify that there are no other solutions than these. Suppose that $A\sqrt{a} + B\sqrt{b}$, ($A, B \in \mathbb{N}$) is a solution of Equation (17) that is not of the prescribed form for α . Then for some $j \geq 0$,

$$\frac{(r\sqrt{a} + s\sqrt{b})^{2j+1}}{2^{2j}} < A\sqrt{a} + B\sqrt{b} < \frac{(r\sqrt{a} + s\sqrt{b})^{2j+3}}{2^{2j+2}}$$

We will assume that $r^2a - s^2b = 4$ since the other case is similar. Thus, $r\sqrt{a} - s\sqrt{b} = 4/(r\sqrt{a} + s\sqrt{b}) > 0$, and since

$$(r^2a - s^2b)^{2j+1} = (r\sqrt{a} + s\sqrt{b})^{2j+1}(r\sqrt{a} - s\sqrt{b})^{2j+1} = 4^{2j+1},$$

then

$$1 < \frac{(A\sqrt{a} + B\sqrt{b})(r\sqrt{a} - s\sqrt{b})^{2j+1}}{4 \cdot 2^{2j}} < \frac{(r\sqrt{a} + s\sqrt{b})^2}{4}.$$

Therefore,

$$1 < \frac{(A\sqrt{a} + B\sqrt{b})(X\sqrt{a} - Y\sqrt{b})}{4} < \frac{T + U\sqrt{ab}}{2},$$

where $A, B, X, Y \in \mathbb{N}$ are odd. Thus,

$$1 < \frac{AXa - BYb + (BX - AY)\sqrt{ab}}{4} < \frac{T + U\sqrt{ab}}{2},$$

where the quantity in the middle is a solution of $x^2 - aby^2 = 1$, contradicting the minimality of $(T + U\sqrt{ab})/2$ if both $R = AXa - BYb > 0$ and $S = BX - AY > 0$. Therefore, it remains in the proof to show that R and S are positive. However, we know that

$$(R + S\sqrt{ab})/4 > 1 \text{ and } 0 < R - S\sqrt{ab} = 4/(R + S\sqrt{ab}) < 1,$$

whence $R > 0$ and $S > 0$. (The proof that $R, S > 0$ follows the line of reasoning, adapted for our case where $\sigma = 2$, that Walker used in his proof for the case $\sigma = 1$.) \square

Remark 1 In [39], Walker uses an overriding hypothesis that neither a nor b , in Theorem 2, is a perfect square. However, he does not use this hypothesis to prove the above. All that is required is that $D = ab$ is not a perfect square and $a > 1, b > 1$. The following illustrates the case where a is a square and $\sigma = 1$.

Example 1 Let $D = 2340 = 9 \cdot 260 = a \cdot b$, and $\sigma = 1$. Then

$$T + U\sqrt{D} = 33281 + 688\sqrt{D} = (43\sqrt{9} + 8\sqrt{260})^2 = (r\sqrt{a} + s\sqrt{b})^2,$$

where

$$43\sqrt{9} + 8\sqrt{260} = 129 + 16\sqrt{65}$$

is the fundamental solution of

$$9r^2 - 260s^2 = 1.$$

Notice that, in turn, $129 + 16\sqrt{65} = (8 + \sqrt{65})^2$, where $8 + \sqrt{65}$ is the fundamental unit of $\mathbb{Q}(\sqrt{65})$. It is also noteworthy to observe that in the simple continued fraction expansion of \sqrt{D} we have $\ell(\sqrt{D}) = 8$ and $Q_1 = 36$, which divides D . This provides a counterexample to [23, Theorem 1.3, p. 334], wherein the hypothesis, for the sufficiency, should include that the Q_j are squarefree. This leaves a gap in the proof of [23, Theorem 2.3, p. 340]. However that theorem is correct. In fact, the Theorem 3 below generalizes that result and provides a link to continued fractions not given in [39]. We will exhibit numerous ramifications of this result in the latter part of the paper.

The following illustrates the case $\sigma = 2$.

Example 2 *If $a = 3$ and $b = 7$, then for all $i \geq 0$ with $i \not\equiv 1 \pmod{3}$, $\alpha_i = (\sqrt{3} + \sqrt{7})^{2i+1}/2^{2i}$ are all of the solutions of $3x^2 - 7y^2 = -4$, with $\gcd(x, y) = 1$. For instance, for $i = 2$, $\alpha_i = 29\sqrt{3} + 19\sqrt{7}$ is such a solution. If $i = 13$, then $\alpha_i = 15289\sqrt{3} + 10009\sqrt{7}$ is such a solution. However, if $i = 3$, then $\alpha_i = 6\sqrt{3} + 4\sqrt{7}$ is not such a solution.*

Remark 2 *Note that Theorem 3 tells us, when $\sigma = 2$, that if Equation (17) is solvable, then Equation (16) is solvable since $rs = B_{\ell-1}$ so $B_{\ell-1}$ cannot be even (see Equation (9)). However, the converse does not hold (for $\sigma = 1, 2$). When $\sigma = 1$, Equation (16) is always solvable, but Equation (17) is not. For instance, $D = 1891$ is such an instance (see Example 12 below). For $\sigma = 2$, with $D = 365 = 5 \cdot 73$, $\ell((1 + \sqrt{365})/2) = 1$, and $5x^2 - 53y^2 = \pm 4$ is not solvable for any integers x, y (since odd xy implies $5x^2 - 53y^2 \equiv 0 \pmod{8}$). Yet, $363^2 - 19^2 \cdot 365 = 4$.*

This is related to a result of Gauss [8, Article 187, p. 156] (rediscovered by Trotter [38]), which says that when D is a positive fundamental radicand divisible by only primes congruent to 1 modulo 4, then the Pell equation

$$X^2 - DY^2 = X^2 - abY^2 = -1 \quad (19)$$

is solvable if and only if $|ax^2 - by^2| = 4$ has no solutions with $D = ab$ unless $|a| = 1$ or $|b| = 1$. Also, it is easily seen that if $\sigma = 2$ and Equation (16) is solvable, then the fundamental unit of the order $\mathbb{Z}[(1 + \sqrt{D})/2]$ is not in the order $\mathbb{Z}[\sqrt{D}]$. This fact will also be used in what follows. Note as well that the latter result is related to a problem of Eisenstein as follows. When $D \equiv 5 \pmod{8}$, then the equation

$$x^2 - Dy^2 = \pm 4 \text{ with } \gcd(x, y) = 1 \quad (20)$$

has a solution if and only if the fundamental unit of $\mathbb{Z}[(1 + \sqrt{D})/2]$ is not in $\mathbb{Z}[\sqrt{D}]$. In general, if $D \equiv 1 \pmod{4}$, then Equation (20) has a solution if and only if $Q_j = 4$ for some $j \in \mathbb{N}$ in the simple continued fraction expansion of \sqrt{D} (see [33, Theorem 2.3, p. 222]). (Note that $Q_1 = 4$ in the simple continued fraction expansion of $\sqrt{365}$ and $19^2 - 365 = -4$.) The results of this paper correct errors in ([33]) and generalize results therein.

Theorems 6 and 9 below resolve the issues discussed in this remark by providing necessary and sufficient conditions for the parity of $\ell(\omega_\Delta)$ in terms of the Diophantine equations $ax^2 - by^2 = \pm 1, \pm 2$.

As a precursor to our next result, we provide the following useful and ostensibly not so well known result that underlies Theorem 2.

Lemma 1 *Suppose that $\ell = \ell(\omega_\Delta)$ where Δ is a discriminant with associated radicand D . If ℓ is even, then in the simple continued fraction expansion of ω_Δ , for any odd $j \geq 1$,*

$$\left(\frac{T + U\sqrt{D}}{\sigma}\right)^j = \frac{T_j + U_j\sqrt{D}}{\sigma} = \frac{G_{j\ell-1} + B_{j\ell-1}\sqrt{D}}{\sigma} = \frac{(G_{j\ell/2-1} + B_{j\ell/2-1}\sqrt{D})^2}{\sigma Q_{\ell/2}}.$$

Proof. From Equations (14)–(15),

$$G_{j\ell-1} = \frac{G_{j\ell/2-1}^2 + B_{j\ell/2-1}^2 D}{Q_{\ell/2}}$$

and

$$B_{j\ell-1} = \frac{2G_{j\ell/2-1}B_{j\ell/2-1}}{Q_{\ell/2}},$$

from which the result follows. \square

Remark 3 *In [39], Walker does use his squarefreeness hypothesis on a, b (see Remark 1), to prove that (a) of Theorem 2 never holds if $\sigma = 1$ and if Equation (19) does hold holds for some $X, Y \in \mathbb{N}$. However, his assumption is unnecessary. Here is a proof, for the general case, that relies only upon $D = ab$ with $a > 1$, $b > 1$, and D not a perfect square. Suppose that $A + B\sqrt{ab}$ is the fundamental solution of the Equation*

$$X^2 - DY^2 = X^2 - abY^2 = -\sigma^2. \quad (21)$$

Then

$$\frac{T + U\sqrt{ab}}{\sigma} = \left(\frac{A + B\sqrt{ab}}{\sigma}\right)^2.$$

Since Theorem 2 tells us that when Equation (17) holds, then

$$\frac{T + U\sqrt{ab}}{\sigma} = \left(\frac{r\sqrt{a} + s\sqrt{b}}{\sigma}\right)^2,$$

then in order that Equation (21) hold, we must have

$$\left(\frac{A + B\sqrt{ab}}{\sigma}\right)^2 = \frac{T + U\sqrt{ab}}{\sigma} = \left(\frac{r\sqrt{a} + s\sqrt{b}}{\sigma}\right)^2.$$

Hence, $r\sqrt{a} + s\sqrt{b} = \pm(A + B\sqrt{ab})$, so $a = 1$ or $b = 1$, a contradiction. We will use this fact in the following result.

Theorem 3 *Let Δ be a discriminant with associated radicand D , and suppose that $D = ab$ with $1 < a < b$. Then if $T + U\sqrt{ab}$ is the fundamental solution of Equation (16), and if $r\sqrt{a} + s\sqrt{b}$ is the fundamental solution of Equation (17), then each of the following holds.*

- (a) $\ell = \ell(\omega_\Delta)$ is even.
- (b) $Q_{\ell/2} = \sigma a$ in the simple continued fraction expansion of ω_Δ .
- (c) $G_{\ell/2-1} = ra$ and $B_{\ell/2-1} = s$.
- (d) $\frac{T+U\sqrt{ab}}{\sigma} = \frac{G_{\ell-1}+B_{\ell-1}\sqrt{ab}}{\sigma} = \left(\frac{\frac{G_{\ell/2-1}}{a}\sqrt{a}+B_{\ell/2-1}\sqrt{b}}{\sigma}\right)^2$.
- (e) $r^2a - s^2b = (-1)^{\ell/2}\sigma^2 = \left(\frac{G_{\ell/2-1}}{a}\right)^2 a - (B_{\ell/2-1})^2 b$.
- (f) For any odd $j \in \mathbb{N}$,

$$\begin{aligned} \left(\frac{r\sqrt{a} + s\sqrt{b}}{\sigma}\right)^{2j} &= \frac{G_{j\ell-1} + B_{j\ell-1}\sqrt{ab}}{\sigma} = \\ &\left(\frac{\frac{G_{j\ell/2-1}}{a}\sqrt{a} + B_{j\ell/2-1}\sqrt{b}}{\sigma}\right)^2 \end{aligned}$$

Proof. By Remark 3 and Equation (9), ℓ is even, which is (a). Also, by Theorem 2, Equations (9), and (15),

$$Q_{\ell/2}rs = \sigma G_{\ell/2-1}B_{\ell/2-1}. \quad (22)$$

Also, since $T + U\sqrt{ab} = G_{\ell-1} + B_{\ell-1}\sqrt{ab}$, by Equation (9), and

$$\frac{T + U\sqrt{ab}}{\sigma} = \left(\frac{r\sqrt{a} + s\sqrt{b}}{\sigma} \right)^2$$

by Theorem 2, then from Equations (8) and (14),

$$Q_{\ell/2}(r^2a + s^2b) = \sigma(G_{\ell/2-1}^2 + B_{\ell/2-1}^2ab) = 2\sigma G_{\ell/2-1}^2 - \sigma^2(-1)^{\ell/2}Q_{\ell/2}. \quad (23)$$

We now consider four cases.

Case 1: $ar^2 - bs^2 = -\sigma^2$ and $\ell/2$ is odd.

By Equation (23),

$$Q_{\ell/2}(2ar^2 + \sigma^2) = 2\sigma G_{\ell/2-1}^2 + \sigma^2 Q_{\ell/2},$$

so $Q_{\ell/2}ar^2 = \sigma G_{\ell/2-1}^2$. Thus, by Equation (22)

$$\frac{\sigma G_{\ell/2-1} B_{\ell/2-1} ar^2}{rs} = \sigma G_{\ell/2-1}^2,$$

so

$$arB_{\ell/2-1} = sG_{\ell/2-1}^2.$$

However, from Equations (5) and (6), $g = \gcd(G_{\ell/2-1}, B_{\ell/2-1}) \mid \sigma$. However, by Lemma 1 and Remark 3, we cannot have $g = \sigma = 2$, so $g = 1$. Thus,

$$A_{\ell/2-1} = ra \quad \text{and} \quad B_{\ell/2-1} = s,$$

as required. Moreover, by Equation (22),

$$Q_{\ell/2} = \frac{\sigma ras}{rs} = \sigma a.$$

This completes Case (1).

Case (2): $\ell/2$ is even and

$$ar^2 - bs^2 = -\sigma^2. \quad (24)$$

By Equation (23), $Q_{\ell/2}(2bs^2 - \sigma^2) = 2\sigma G_{\ell/2-1}^2 - \sigma^2 Q_{\ell/2}$, so $Q_{\ell/2}bs^2 = \sigma G_{\ell/2-1}^2$. Thus, by Equation (22),

$$\frac{\sigma G_{\ell/2-1} B_{\ell/2-1} bs^2}{rs} = \sigma G_{\ell/2-1}^2,$$

so by similar reasoning to that given in Case (1),

$$G_{\ell/2-1} = bs, \quad B_{\ell/2-1} = r, \quad \text{and} \quad Q_{\ell/2} = \sigma b.$$

However, by Equation (11), $2P_{\ell/2} = Q_{\ell/2}t = bt$ for some $t \in \mathbb{N}$, and by Equation (4),

$$ab = D = P_{\ell/2}^2 + Q_{\ell/2}Q_{\ell/2-1} = (\sigma bt/2)^2 + \sigma bQ_{\ell/2-1}.$$

Since $b > a$, then it follows that,

$$b > b(\sigma t/2)^2 + \sigma Q_{\ell/2-1},$$

whence, $t = 1 = \sigma$, b is even, and $P_{\ell/2} = b/2$.

Now, by Equation (7),

$$sb = G_{\ell/2-1} = P_{\ell/2}B_{\ell/2-1} + Q_{\ell/2}B_{\ell/2-2} = br/2 + bB_{\ell/2-2}.$$

Therefore, $2s = r + 2B_{\ell/2-2}$ forcing r to be even. Yet $\gcd(b, r) = 1$ by Equation (24), a contradiction, so Case (2) cannot occur.

Case (3): $ar^2 - bs^2 = \sigma^2$ and $\ell/2$ is odd.

Equation (23) tells us that,

$$Q_{\ell/2}(2bs^2 + \sigma^2) = 2\sigma A_{\ell/2-1}^2 + \sigma^2 Q_{\ell/2},$$

so we proceed as in Case (2) to get $G_{\ell/2-1} = bs$ and $B_{\ell/2-1} = r$. Then a contradiction is reached in the same fashion as in Case (2). In other words, Case (3) cannot occur.

Case (4): $ar^2 - bs^2 = \sigma^2$ and $\ell/2$ is even.

From Equation (23),

$$Q_{\ell/2}(2ar^2 - \sigma^2) = 2\sigma G_{\ell/2-1}^2 - \sigma^2 Q_{\ell/2},$$

and proceeding as in Case (1), we get that $G_{\ell/2-1} = ar$, $B_{\ell/2-1} = s$, and $Q_{\ell/2} = \sigma a$. This concludes case (4).

We have shown that (a)–(c) hold. Since (a) holds, then (d) holds by Lemma 1. Hence, (e)–(f) follow. \square

Remark 4 *Theorem 3, via Lemma 1, provides a palatable method for finding the fundamental unit of $\mathbb{Z}[\omega_\Delta]$ by going to less than half the period in the simple continued fraction expansion of ω_Δ , rather than the full period as mandated by Equation (9). Furthermore, $(G_{\ell/2-1}/a, B_{\ell/2-1}) = (r, s)$ provides the fundamental solution of Equation (17).*

Example 3 *Looking back to Example 1, we see that in the simple continued fraction expansion of $\sqrt{D} = \sqrt{2340}$, $Q_{\ell/2} = Q_4 = 9 = a$ where $2340 = 9 \cdot 260 = ab$ and $A_{\ell/2-1} = A_3 = 387 = 9 \cdot 43$, $B_{\ell/2-1} = B_3 = 8$, with*

$$\left(\frac{A_{\ell/2-1}}{a}\sqrt{a} + B_{\ell/2-1}\sqrt{b}\right)^2 = (r\sqrt{a} + s\sqrt{b})^2 = (43\sqrt{9} + 8\sqrt{260})^2 =$$

$$33281 + 688\sqrt{2340} = A_{\ell-1} + B_{\ell-1}\sqrt{D}.$$

Also,

$$ar^2 - bs^2 = 9 \cdot 43^2 - 260 \cdot 8^2 = (-1)^{\ell/2} = 1.$$

The above example demonstrates the case where $\ell/2$ is even. The following illustrates the case where $\ell/2$ is odd.

Example 4 *Let $D = 1274 = 26 \cdot 49 = ab$. Then $\ell(\sqrt{D}) = 18$, $Q_{\ell/2} = Q_9 = 26 = a$, and*

$$ar^2 - bs^2 = a \left(\frac{A_{\ell/2-1}}{a}\right)^2 - bB_{\ell/2-1}^2 = 26 \cdot 1020^2 - 49 \cdot 743^2 = (-1)^{\ell/2} = -1.$$

Moreover,

$$A_{\ell-1} + B_{\ell-1}\sqrt{ab} = 5400801 + 1515720\sqrt{1274} = (1020\sqrt{26} + 743\sqrt{49})^2 =$$

$$\left(\frac{A_{\ell/2-1}}{a}\sqrt{a} + B_{\ell/2-1}\sqrt{b}\right)^2 = (r\sqrt{a} + s\sqrt{b})^2.$$

It is possible that $Q_{\ell/2} = b > a$. However, Theorem 3 tells us that Equation (17) cannot hold in that case.

Example 5 Let $D = 19,360 = 121 \cdot 160 = ab$. Then $\ell(\sqrt{D}) = 18$, $Q_{\ell/2} = Q_9 = 160 = b = 2P_{\ell/2}$. However, $|r^2a - s^2b| = |121r^2 - 160s^2| = 1$ is not solvable for any $r, s \in \mathbb{N}$. The reason is that there do not exist any $r, s \in \mathbb{N}$ such that $A_{\ell-1} + B_{\ell-1}\sqrt{ab} = (r\sqrt{a} + s\sqrt{b})^2$, as the reader may verify by assuming the contrary. It turns out that $Q_4 = 121 = a$, but since $Q_{\ell/2} = b > a$, part (c) of Theorem 3 fails to hold.

In each of the above examples, D is even and not a fundamental radicand, namely D is squarefree. The following illustrates the odd case of a fundamental radicand.

Example 6 If $D = 55 = 5 \cdot 11 = ab$, $\sigma = 1$, then $\ell(\sqrt{55}) = 4$, $Q_{\ell/2} = Q_2 = 5$ and

$$A_{\ell-1} + B_{\ell-1}\sqrt{D} = 89 + 12\sqrt{55} = (3\sqrt{5} + 2\sqrt{11})^2 = \left(\frac{A_{\ell/2-1}}{a}\sqrt{a} + B_{\ell/2-1}\sqrt{b} \right)^2.$$

Example 7 If $D = 21 = 3 \cdot 7 = ab$, $\sigma = 2$, then $r^2a - s^2b = 3 - 7 = -4 = (-1)^{\ell/2}4$ with $\ell = \ell((1 + \sqrt{D})/2) = 2$, with $Q_{\ell/2} = Q_1 = 2a = 6$, while

$$\begin{aligned} \frac{R + S\sqrt{ab}}{2} &= \frac{G_{\ell-1} + B_{\ell-1}\sqrt{ab}}{2} = \frac{5 + \sqrt{21}}{2} = \left(\frac{\sqrt{3} + \sqrt{7}}{2} \right)^2 = \\ &= \left(\frac{\frac{G_{\ell/2-1}}{a}\sqrt{a} + B_{\ell/2-1}\sqrt{b}}{2} \right)^2. \end{aligned}$$

There is a means of linking Theorem 3 for both cases $\sigma = 1, 2$ that is informative in terms of Equation (17). In what follows, we use the fact that

$$\left(\frac{R + S\sqrt{D}}{2} \right)^3 = T + U\sqrt{D},$$

where $(R + S\sqrt{D})/2$ is the fundamental unit of $\mathbb{Z}[(1 + \sqrt{D})/2]$ and $T + U\sqrt{D}$ is the fundamental unit of $\mathbb{Z}[\sqrt{D}]$, in the case that $R + S\sqrt{D}$ is a solution of Equation (17) when $\sigma = 2$.

Theorem 4 *If $ab \equiv 1 \pmod{4}$, with $1 < a < b$, and $r\sqrt{a} + s\sqrt{b}$ is the fundamental solution of Equation (17) with $\sigma = 2$, then*

$$(X, Y) = \left(\frac{(ar^2 \mp 3)r}{2}, \frac{(ar^2 \mp 1)s}{2} \right)$$

is the fundamental solution of Equation (17) with $\sigma = 1$.

Proof. By [33, Theorem 2.3, p. 222], (X, Y) is indeed a positive solution of Equation (17) with $\sigma = 1$. We need only show that it is the fundamental solution. Since $((R + S\sqrt{D})/2)^3$ is the fundamental unit of $\mathbb{Z}[\sqrt{D}]$, we deduce from Theorem 3 that $((r\sqrt{a} + s\sqrt{b})/2)^3$ is the fundamental solution of Equation (17) with $\sigma = 1$. However,

$$\left(\frac{r\sqrt{a} + \sqrt{b}}{2} \right)^3 = \frac{(r^3a + 3rs^2b)\sqrt{a} + (3r^2as + s^3b)\sqrt{b}}{8},$$

which a simple manipulation using Equation (17) with $\sigma = 2$ shows to be equal to

$$\frac{r(r^2a \mp 3)\sqrt{a} + s(ar^2 \mp 1)\sqrt{b}}{2},$$

as required. □

Remark 5 *Theorem 4 gives us relationships between the simple continued fraction expansions of the two quadratic orders. To avoid confusing the notation for the two continued fraction expansions, we let the A_j and B_j refer to the values in Equation (1) for the simple continued fraction expansion of \sqrt{D} with $\ell = \ell(\sqrt{D})$, while \bar{G}_j and \bar{B}_j refer to the values in Equation (6) in the simple continued fraction expansion of $(1 + \sqrt{D})/2$ with $\bar{\ell} = \ell((1 + \sqrt{D})/2)$, then we have the following relationships immediate from the above.*

$$A_{\ell/2-1} = \frac{(\bar{G}_{\bar{\ell}/2-1}^2 \mp 3a)\bar{G}_{\bar{\ell}/2-1}}{2a},$$

and

$$B_{\ell/2-1} = \frac{(\bar{G}_{\bar{\ell}/2-1}^2 \mp a)\bar{B}_{\bar{\ell}/2-1}}{2a}.$$

The solution of Equation (17) for $\sigma = 1$ does not imply the solution of Equation (17) for $\sigma = 2$ (see the discussion after Theorem 9). Thus, a general converse of Theorem 4 is not possible. We must assume that a solution of Equation (17) holds for both $\sigma = 1, 2$, in which case, if $R^2a - S^2b = \pm 1$ is a solution for $\sigma = 1$ and $r^2a - s^2b = \pm 4$ is a solution for $\sigma = 2$, then by Lemma 1,

$$r = \frac{2R}{\overline{G}_{\ell-1} \mp 1} \quad \text{and} \quad s = \frac{2S}{\overline{G}_{\ell-1} \pm 1}.$$

Moreover, more can be said as follows, which is immediate from the above results.

Corollary 1 *If $r\sqrt{a} + s\sqrt{b}$ is the fundamental solution of Equation (17) with $\sigma = 2$, then the fundamental unit of $\mathbb{Z}[\sqrt{ab}] = \mathbb{Z}[\sqrt{D}]$ is given by*

$$A_{\ell-1} + B_{\ell-1}\sqrt{D} = \left(\frac{(ar^2 \mp 3)r}{2}\sqrt{a} + \frac{(ar^2 \mp 1)s}{2}\sqrt{b} \right)^2.$$

Example 8 *Let $D = 805 = 5 \cdot 161 = a \cdot b$. Then the fundamental solution of*

$$5r^2 - 161s^2 = -4$$

is $(r, s) = (17, 3)$. In this case, we have $A_{\ell/2-1} = 61540$, $B_{\ell/2-1} = 2169$, $A_{\ell-1} = 1514868641$, $B_{\ell-1} = 53392104$, and

$$\begin{aligned} 1514868641 + 53392104\sqrt{805} &= A_{\ell-1} + B_{\ell-1}\sqrt{D} = \\ &= \left(\frac{(ar^2 + 3)r}{2}\sqrt{a} + \frac{(ar^2 + 1)s}{2}\sqrt{b} \right)^2 = (12308\sqrt{5} + 2169\sqrt{161})^2, \end{aligned}$$

where $12308\sqrt{5} + 2169\sqrt{161}$ is the fundamental solution of

$$5X^2 - 161Y^2 = -1.$$

Moreover, in the notation of Remark 5, $\overline{G}_{\ell/2-1} = 85$, $\overline{B}_{\ell/2-1} = 3$,

$$A_{\ell/2-1} = \frac{(\overline{G}_{\ell/2-1}^2 + 3a)\overline{G}_{\ell/2-1}}{2a},$$

and

$$B_{\ell/2-1} = \frac{(\overline{G}_{\ell/2-1}^2 + a)\overline{B}_{\ell/2-1}}{2a}.$$

Corollary 1 generalizes [33, Theorem 2.3, p. 222] and explains a phenomenon that was only touched upon therein, namely, the finding of the fundamental unit halfway into the period. Moreover, this links the simple continued fractions of the two orders, a phenomenon not suspected in earlier work such as [33]. The following generalizes results in [34] for the case where $c = -3$. Furthermore, it answers the natural question as to which other values of c than $c = \pm 1, \pm 4$ satisfy

$$c = ax^2 - by^2 \text{ with } \gcd(x, y) = 1 \quad (25)$$

with the connections to continued fractions. In [30], we proved that any squarefree value of c dividing b where $D = ab$ and b is bounded above by $\sqrt{4D/\sigma^2}$ while a is a perfect square satisfying certain restrictive divisibility conditions, then (25) has a solution if and only if $c = Q_{\ell/2}/\sigma$ in the simple continued fraction expansion of $(\sigma - 1 + \sqrt{D})/\sigma$. The following generalizes this result as well.

Corollary 2 *Suppose that $c \in \mathbb{Z}$ is squarefree, $|c| \mid D > 1$, which is not a perfect square, and $1 < |c| < D/|c|$. Then if*

$$x^2 - Dy^2 = \sigma^2 c \text{ with } \gcd(x, y) = 1, \quad (26)$$

each of the following holds.

- (a) $\ell = \ell((\sigma - 1 + \sqrt{D})/\sigma)$ is even.
- (b) $c = (-1)^{\ell/2} Q_{\ell/2}$ in the simple continued fraction expansion of the principal surd, $(\sigma - 1 + \sqrt{D})/\sigma$.
- (c) The fundamental solution of Equation (26) is given by

$$x + y\sqrt{D} = G_{\ell/2-1} + B_{\ell/2-1}\sqrt{D} = ra + s\sqrt{D}.$$

Proof. Since Equation (26) has a solution then $aX^2 - bY^2 = \pm\sigma^2$, where $a = |c|$, $X = x/|c|$, $b = D/|c|$, and $Y = y$. Observe that $|c| \mid x$ since c is squarefree and that $\gcd(X, Y) = 1$ since $\gcd(x, y) = 1$. Hence, the result follows from Theorem 3. \square

Remark 6 *Corollary 2 fails if the squarefreeness condition on c is dropped. For instance, take $D = 75$, $c = 25$, then $10^2 - D = c$, but $Q_{\ell/2} = Q_2 = 6 \neq (-1)^{\ell/2}c = 25$. The reason is that 25 does not divide $x = 10$, so $10^2/c - D/c = 2^2 - 3 = 1$ where $a = 1$ and $b = 3$, so Theorem 3 does not apply. In the following, we illustrate a situation where it does apply.*

Example 9 *Let $D = 1729 = 7 \cdot 13 \cdot 19$, and $c = -13$, then $\ell = 30$ and*

$$-13 = c = (-1)^{\ell/2}Q_{\ell/2} = A_{\ell/2-1}^2 - B_{\ell/2-1}^2 D = 17028726^2 - 409529^2 \cdot 1729.$$

Example 10 *Let $D = 38 = 2 \cdot 19 = a \cdot b$ and $c = -2$. Then $\ell = 2$, $Q_{\ell/2} = Q_1 = 2$,*

$$A_{\ell/2-1} + B_{\ell/2-1}\sqrt{D} = 6 + \sqrt{38},$$

and

$$\begin{aligned} \left(\frac{A_{\ell/2-1}\sqrt{a}}{a} + B_{\ell/2-1}\sqrt{b} \right)^2 &= (3\sqrt{2} + \sqrt{19})^2 = 37 + 6\sqrt{38} = \\ &= A_1 + B_1\sqrt{D} = A_{\ell-1} + B_{\ell-1}\sqrt{D}, \end{aligned}$$

which is the fundamental unit of $\mathbb{Z}[\sqrt{38}]$.

Another natural question to ask is for a criterion in terms of simple continued fractions for Equation (26) to hold when c does not divide D . For instance, for the case $c = -3$, we explored this question in [34] and developed a criterion. In [24], this author found explicit methods in terms of continued fractions for the solution of any equation of type (26) with no restrictions on the nonzero integer c whatsoever.

Example 11 *Let $D = 119 = 7 \cdot 17$. Then $11^2 - 119 = 2$ and $\ell = 4$ with $Q_{\ell/2} = Q_2 = 2$ and $A_{\ell/2-1} + B_{\ell/2-1}\sqrt{D} = 11 + \sqrt{119}$.*

Unfortunately, the criterion that is suggested by Corollary 2 fails in general. In other words, the solvability of $x^2 - Dy^2 = c < \sqrt{D}$ with $\gcd(x, y) = 1$ does not imply that $Q_{\ell/2} = |c|$ even for small values as the following illustrates.

Example 12 Let $D = 1891 = 31 \cdot 61$. Then $x^2 - Dy^2 = -3$ has solutions. For instance, $(x, y) = (34798636, 800233)$. However, in the simple continued fraction expansion of \sqrt{D} , $Q_{\ell/2} = Q_{18} = 62 = 2 \cdot 31$. Moreover, $ax^2 - by^2 = 2$ has solutions for $a = 31$ and $b = 61$ such as $x = 162553839$ and $y = 115881247$, but it does not have solutions for $ax^2 - by^2 = \pm 1$ when $a > 1$.

Example 12 motivates the following, which provides more information than that given by the authors of [36], who provided a parity criterion (see Theorem 6 below).

Theorem 5 Let $D = ab > 2$, not a perfect square, with $1 \leq a < b$. Suppose that

$$ax^2 - by^2 = \pm 2 \quad (27)$$

has a solution $(x, y) = (r, s) \in \mathbb{N}^2$ where xy is odd. Then each of the following holds.

1. $\ell = \ell(\sqrt{D})$ is even.
2. If $r\sqrt{a} + s\sqrt{b}$ is the fundamental solution of Equation (27), then for any odd integer $j \geq 1$,

$$\frac{(r\sqrt{a} + s\sqrt{b})^{2j}}{2^j} = A_{j\ell-1} + B_{j\ell-1}\sqrt{D}.$$

3. $A_{\ell/2-1} = ar$, $B_{\ell/2-1} = s$, and $Q_{\ell/2} = 2a$.
4. $r^2a - s^2b = 2(-1)^{\ell/2}$.

Proof. Suppose that $r\sqrt{a} + s\sqrt{b}$ is the fundamental solution of Equation (27) and that $T + U\sqrt{ab}$ is the fundamental solution of $X^2 - abY^2 = -1$. Since

$$N((r\sqrt{a} + s\sqrt{b})^2/2) = 1,$$

there is a $j \in \mathbb{N}$ such that $(r\sqrt{a} + s\sqrt{b})^2/2 = (T + U\sqrt{ab})^{2i} = (T_j + U_j\sqrt{ab})^2$. Thus,

$$r^2a + s^2b = 2(T_i^2 + U_i^2ab), \quad (28)$$

so $r^2a \pm 1 = 2U_i^2ab \pm 1$. If the signs agree on both sides of the last equation, then $r^2 = 2U_i^2b$, so $b \mid r^2$ forcing $b \mid 2$ since

$$r^2a - s^2b = \pm 2. \quad (29)$$

However, $b \neq 2$, so $b = 1$, a contradiction since $1 \leq a < b$. Hence, the signs do not agree and we must have $r^2a = 2(U_i^2ab \pm 1)$. Therefore, $a \mid 2$. If $a = 2$, then since $r^2 = 2U_i^2b \pm 1$ and $r^2 = s^2b/2 \pm 1$, we deduce that $s^2 = 4U_i^2$, forcing s to be even, a contradiction. Thus, $a = 1$. Hence, $2 \mid r^2$, also a contradiction. Hence, $X^2 - DY^2 = -1$ has no solution. Equation (9) now tells us that ℓ must be even, which is part 1.

To establish part 2, we need only show that it holds for $j = 1$ since the rest follows for any odd j . Since $(r\sqrt{a} + s\sqrt{b})^2/2 = (T + U\sqrt{ab})^{2i+1}$ for some $i \geq 0$, we need only show that $i = 0$. We have

$$\frac{(r\sqrt{a} + s\sqrt{b})^2}{2}(T_i - U_i\sqrt{ab})^2 = T + U\sqrt{ab},$$

where the left-hand side is of the form $(U\sqrt{a} + V\sqrt{b})^2/2$ with $U\sqrt{a} + V\sqrt{b}$ being a solution of Equation (27). Therefore,

$$(r\sqrt{a} + s\sqrt{b})^2/2 = ((U\sqrt{a} + V\sqrt{b})^2/2)^{2i+1},$$

which is a contradiction to the minimality of $r\sqrt{a} + s\sqrt{b}$ for any $i > 0$. This establishes part 2.

For part 3, we have from part 2 and Lemma 1 that

$$\frac{(r\sqrt{a} + s\sqrt{b})^2}{2} = A_{\ell-1} + B_{\ell-1}\sqrt{ab} = \frac{(A_{\ell/2} + B_{\ell/2-1}\sqrt{ab})^2}{Q_{\ell/2}}.$$

Therefore,

$$Q_{\ell/2}(r^2a + s^2b) = 2(A_{\ell/2}^2 + B_{\ell/2-1}^2ab), \quad (30)$$

and

$$rsQ_{\ell/2} = 2A_{\ell/2-1}B_{\ell/2-1}. \quad (31)$$

We now consider four cases.

Case 1: $ar^2 - bs^2 = -2$ and $\ell/2$ is odd.

From Equations (16), (27), and (30), we have $Q_{\ell/2}ar^2 = 2A_{\ell/2-1}^2$. Thus, from Equation (31), $B_{\ell/2-1}ar = A_{\ell/2-1}s$. From the relative primality of $A_{\ell/2-1}$ and $B_{\ell/2-1}$ via Equation (5), we get that $A_{\ell/2-1} = ar$ and $B_{\ell/2-1} = s$. Plugging these values into Equation (31), we get $Q_{\ell/2} = 2a$, as required.

Case 2: $ar^2 - bs^2 = 2$ and $\ell/2$ is odd.

From Equations (16), (27), and (30), $Q_{\ell/2}bs^2 = 2A_{\ell/2-1}^2$, so we deduce from Equation (31) that $B_{\ell/2-1}bs = A_{\ell/2-1}r$. By relative primality as in

Case 1, $A_{\ell/2-1} = bs$ and $B_{\ell/2-1} = r$, so $Q_{\ell/2} = 2b$. However, by Equation (11), there exists a $t \in \mathbb{N}$ such that $P_{\ell/2} = tQ_{\ell/2} = bt$. Therefore, by Equation (4),

$$ab = P_{\ell/2}^2 + Q_{\ell/2}Q_{\ell/2-1} = b^2t^2 + 2bQ_{\ell/2-1}.$$

Since $b > a$, this implies that $b > bt + 2Q_{\ell/2-1}$, a contradiction. Hence, Case 2 cannot occur.

Case 3: $ar^2 - bs^2 = -2$ and $\ell/2$ is even.

As in Cases, 1-2, we can use Equations (16), (27), (30), and (31) to deduce that $A_{\ell/2-1}r = B_{\ell/2-1}bs$, from which we deduce that $A_{\ell/2-1} = bs$, $B_{\ell/2-1} = r$, and $Q_{\ell/2} = 2b$, which leads to a contradiction as in Case 3.

Case 4: $ar^2 - bs^2 = 2$ and $\ell/2$ is even.

We deduce as in Case 1 that $A_{\ell/2-1} = ar$, $B_{\ell/2-1} = s$, and $Q_{\ell/2} = 2a$, as required.

We have proved part 3 from which part 4 follows via Equation (8). \square

The following isolates the case where $a = 1$ in Theorem 5.

Corollary 3 *Suppose that $D > 2$ is not a perfect square. If*

$$x^2 - Dy^2 = \pm 2, \tag{32}$$

has a solution $x, y \in \mathbb{N}$, then $\ell = \ell(\sqrt{D})$ is even, $\pm 2 = (-1)^{\ell/2}Q_{\ell/2}$, and $A_{\ell/2-1} + B_{\ell/2-1}\sqrt{D}$ is the smallest positive solution of Equation (32). Also,

$$A_{\ell-1} + B_{\ell-1}\sqrt{D} = \frac{(A_{\ell/2-1} + B_{\ell/2-1}\sqrt{D})^2}{2}.$$

As the following consequence of Corollary 3 shows, there are classes of radicands with guaranteed solvability of Equation (32).

Corollary 4 *Suppose that $D = 2^a \cdot p^{2i+1} > 2$ where $a \in \{0, 1\}$, $p \equiv 3 \pmod{4}$ is a prime and $i \geq 0$. Then Equation (32) is solvable, with smallest solution $A_{\ell/2-1} + B_{\ell/2-1}\sqrt{D}$, $Q_{\ell/2} = 2$, and*

$$A_{\ell-1} + B_{\ell-1}\sqrt{D} = \frac{(A_{\ell/2-1} + B_{\ell/2-1}\sqrt{D})^2}{2}.$$

Furthermore,

$$A_{\ell-1}^2 - B_{\ell-1}^2 D = \pm 2 = (-1)^{\ell/2}Q_{\ell/2},$$

where $\ell/2$ is odd when $p \equiv 3 \pmod{8}$ and $\ell/2$ is even when $p \equiv 7 \pmod{8}$.

Proof. For $D = 3$ the result is clear, so we assume now that $D > 5$. By [25, Theorem 3.70, p. 162] and [21, Footnote (1.5.9), pp. 25–26], the class number of the order $\mathcal{O}_\Delta = \mathbb{Z}[\sqrt{D}]$ is odd, where $\Delta = 4D$. Since $2 \mid \Delta$, then 2 is ramified in the order, so the \mathcal{O}_Δ -prime over 2 is principle (see [25, Exercise 3.77, p. 167]). Therefore, $x^2 - Dy^2 = \pm 2$ has a solution, so by Theorem 1, ℓ is even, and $2 = Q_{\ell/2}$ since $D > 5$. Moreover,

$$A_{\ell/2-1}^2 - B_{\ell/2-1}^2 D = (-1)^{\ell/2} Q_{\ell/2} = (-1)^{\ell/2} 2.$$

If $\ell/2$ is even then the Legendre symbol equality

$$\left(\frac{2}{p}\right) = 1$$

holds, so $p \equiv 7 \pmod{8}$, and if $\ell/2$ is odd, then

$$\left(\frac{2}{p}\right) = -1,$$

so $p \equiv 3 \pmod{8}$ (see [25, Theorem 4.1.6], for instance). \square

Remark 7 *From Corollary 3, we may deduce that when $D > 2$ is not a perfect square and $\ell = \ell(\sqrt{D})$ is even, then $Q_{\ell/2} = 2$ in the simple continued fraction expansion of \sqrt{D} if and only if there is a solution to Equation (32). Also, when this occurs, one of the following must hold: (1) $D \equiv 3 \pmod{8}$ and $\ell/2$ is odd (eg. $D = 3$); (2) $D \equiv 7 \pmod{8}$ and $\ell/2$ is even (eg. $D = 7$); (3) $D \equiv 2 \pmod{8}$, $D/2 \equiv 1 \pmod{8}$, $A_{\ell/2-1} \equiv 0 \pmod{4}$, and $\ell/2$ is odd (eg. $D = 18$); (4) $D \equiv 2 \pmod{8}$, $D/2 \equiv 1 \pmod{8}$, $A_{\ell/2-1} \equiv 2 \pmod{4}$, and $\ell/2$ is even (eg. $D = 34$); (5) $D \equiv 6 \pmod{8}$, $D/2 \equiv 3 \pmod{8}$, and $\ell/2$ is odd (eg. $D = 6$); (6) $D \equiv 6 \pmod{8}$, $D/2 \equiv 7 \pmod{8}$, and $\ell/2$ is even (eg. $D = 14$).*

Notice that the solution of Equation (32) implies that Equation (27) is solvable only for $a = 1$. Moreover, the solution of Equation (27) with $a > 1$ ensures that 2 is not principal in $\mathbb{Z}[\sqrt{ab}]$, for $ab > 5$, since, if it were, then by Theorem 1, $Q_{\ell/2} = 2$, and by Theorem 5, $Q_{\ell/2} = 2a$. For instance, if $D = 91$, then $Q_{\ell/2} = Q_4 = 14$ and $7 \cdot 15^2 - 13 \cdot 11^2 = 2$, whereas if $D = 119$, then $Q_{\ell/2} = 2$, and $11^2 - 119 = 2$.

Corollary 4 tells us that if there exists a solution to $x^2 - 2^a p y^2 = \pm 2$ then there exists a solution to $X^2 - 2^a p^{2i+1} = \pm 2$ for any $i \geq 0$, whenever $a \in \{0, 1\}$ and $p \equiv 3 \pmod{4}$ is prime. The following examples illustrate.

Example 13 Let $D = 2 \cdot 3^7$. Then $Q_{\ell/2} = Q_5 = 2$, $A_{\ell/2-1} = 21362$, $B_{\ell/2-1} = 323$, and

$$\frac{(A_{\ell/2-1} + B_{\ell/2-1}\sqrt{D})^2}{2} = 456335045 + 6899926\sqrt{D} = A_{\ell-1} + B_{\ell-1}\sqrt{D}.$$

Example 14 Let $D = 2 \cdot 7^3$. Then $Q_{\ell/2} = Q_8 = 2$, and

$$\begin{aligned} \frac{(A_{\ell/2-1} + B_{\ell/2-1}\sqrt{D})^2}{2} &= \frac{(104164 + 3977\sqrt{D})^2}{2} = \\ &10850138895 + 414260228\sqrt{D} = A_{\ell-1} + B_{\ell-1}\sqrt{D}. \end{aligned}$$

Example 15 Let $D = 7^3$. Then $Q_{\ell/2} = Q_8 = 2$, and

$$\frac{(A_{\ell/2-1} + B_{\ell/2-1}\sqrt{D})^2}{2} = \frac{(11427 + 617\sqrt{D})^2}{2} = A_{\ell-1} + B_{\ell-1}\sqrt{D}.$$

Remark 8 It follows from the above that when Equation (32) has a solution, then there is no solution to $ax^2 - by^2 = \pm 1$ with $D = ab$ unless one of $|a| = 1$ or $|b| = 1$. Note, as well, that there does not exist an analogue of Theorem 5 for $\sigma = 2$ since if

$$aX^2 - bY^2 = \pm 8 \text{ with } \gcd(X, Y) = 1 \quad (33)$$

is solvable, then Equation (17) with $\sigma = 2$ is not solvable since Equation (33) implies that $a \equiv b \pmod{8}$. For instance, if $D = 65$, $a = 5$, $b = 13$, then $\ell((1 + \sqrt{65})/2) = 3$, with $G_{\ell-1} = 16$, $B_{\ell-1} = 2$ in the simple continued fraction expansion of $(1 + \sqrt{65})/2$; and if $D = 713$, $a = 23$, $b = 31$, then $\ell((1 + \sqrt{713})/2) = 14$ with $G_{\ell-1} = 10572734$, and $B_{\ell-1} = 395952$ in the simple continued fraction expansion of $(1 + \sqrt{713})/2$.

Now we are in a position to provide more information than that given in [36], and with a much simpler proof. The following generalizes the result of Gauss cited in Remark 2.

Theorem 6 *Let $D > 2$, not a perfect square. Then $\ell = \ell(\sqrt{D})$ is even if and only if one of the following holds.*

1. *There exists a factorization $D = ab$ with $1 < a < b$ such that Equation (17) with $\sigma = 1$ has a solution.*
2. *There exists a factorization $D = ab$ with $1 \leq a < b$ such that Equation (27) has a solution (with xy odd).*

Proof. By Theorem 3, we need only prove one direction. Assume that ℓ is even. Then by Equations (7) and (11), $Q_{\ell/2} \mid 2A_{\ell/2-1}$ and by Theorem 1, $Q_{\ell/2} \mid 2D$. If $Q_{\ell/2} \mid D$, and $Q_{\ell/2} \mid A_{\ell/2-1}$, then

$$ar^2 - bs^2 = (-1)^{\ell/2},$$

where $a = Q_{\ell/2}$, $r = A_{\ell/2-1}/a$, $b = D/a$, and $s = B_{\ell/2-1}$. Moreover $a \neq 1$ since only Q_0 and Q_ℓ take on the value 1 for any Q_j with $0 \leq j \leq \ell$ in the simple continued fraction expansion of \sqrt{D} . This is part 1.

Now we assume that part 1 does not hold. If either $Q_{\ell/2}$ does not divide D or $Q_{\ell/2}$ does not divide $A_{\ell/2-1}$, then

$$ar^2 - bs^2 = (-1)^{\ell/2}2,$$

where $a = Q_{\ell/2}/2$, $r = A_{\ell/2-1}/a$, $b = D/a$, and $s = B_{\ell/2-1}$. It remains to show that rs is odd. If r is even and s is odd, it can be shown that $Q_{\ell/2} \mid D$ and $Q_{\ell/2} \mid A_{\ell/2-1}$, contradicting the hypothesis. Thus, we may assume that s is even, so $A_{\ell/2-1}$ is also even. If 4 does not divide $Q_{\ell/2}$, then by Lemma 1, both $A_{\ell-1}$ and $B_{\ell-1}$ are even, a contradiction. Thus, $4 \mid Q_{\ell/2}$. Therefore,

$$AR^2 - BS^2 = (-1)^{\ell/2},$$

where $A = Q_{\ell/2}/4$, $R = 2A_{\ell/2-1}/Q_{\ell/2}$, $B = 4D/Q_{\ell/2}$, and $S = B_{\ell/2-1}/2$, contradicting that part 1 does not hold. This is part 2. \square

Some classical results follow from Theorem 6, such as the following, which is standard in any introductory algebraic number theory course.

Corollary 5 *If $D = p^j$ where $p \equiv 1 \pmod{4}$ is prime and $j \geq 1$ is odd, then $\ell(\sqrt{D})$ is odd and $\ell(\sqrt{4D})$ is even.*

Proof. If $\ell(\sqrt{D})$ were even, then by Theorem 6, there is a factorization $D = ab$ such that either $ax^2 - by^2 = \pm 1$ with $1 < a < b$, or $ax^2 - by^2 = \pm 2$ with xy odd. The first case is impossible since $p \mid a$ and $p \mid b$ when $a > 1$. Thus, the second case holds, and for the same reason, $a = 1$, namely $x^2 - p^j y^2 = \pm 2$, with xy odd. However,

$$\pm 2 \equiv x^2 - p^j y^2 \equiv 0 \pmod{4},$$

which is a contradiction. Thus, $\ell(\sqrt{D})$ is odd, so there exist $x, y \in \mathbb{N}$ such that $x^2 - Dy^2 = -1$. If x is even, then $4(x/2)^2 - Dy^2 = -1$, and Theorem 3 tells us that $\ell(\sqrt{4D})$ is even. By considerations modulo 8, y may be shown to be necessarily odd. \square

The following consequence of Theorem 6 is a generalization of recent work in [13] recently communicated to this author. One of the focuses of [13] is when $Q_{\ell/2} = 4$.

Corollary 6 *Let $D \neq 3$ be a positive nonsquare integer such either $D = p^j$ where p is an odd prime and j is an odd positive integer, or $D \equiv 1, 2 \pmod{4}$ and $\ell(\sqrt{D})$ is odd. Then $\ell = \ell(\sqrt{4D})$ is even and $Q_{\ell/2} = 4$ in the simple continued fraction expansion of $\sqrt{4D}$.*

Proof. First assume that $D \equiv 1, 2 \pmod{4}$ and $\ell(\sqrt{D})$ is odd. Then by [10], $\ell(\sqrt{4D})$ is even. Thus, by Theorem 6, there is a factorization $4D = ab$ with either $ax^2 - by^2 = \pm 1$ with $1 < a < b$, or $ax^2 - by^2 = \pm 2$ with xy odd. If the latter case holds, then both a and b must be even, so $(a/2)x^2 - (b/2)y^2 = \pm 1$. If $a \neq 2$, then by Theorem 6, $\ell(\sqrt{D})$ is even, a contradiction. Thus, $a = 2$, so by Corollary 3, $\ell(\sqrt{D})$ is even, a contradiction. Hence, the latter case cannot hold. In the former case, one of a or b must be odd. When b is odd, then $(a/4)(2x)^2 - by^2 = \pm 1$, with $\gcd(2x, y) = 1$. If $a > 4$, then by Theorem 3, $\ell(\sqrt{D})$ is even, a contradiction. Hence, $a = 4$, so by Theorem 3, $Q_{\ell/2} = 4$ in the simple continued fraction expansion of $\sqrt{4D}$. Similarly, if a is odd, then $ax^2 - (b/4)y^2 = \pm 1$. If $1 < a < b/4$, then by Theorem 3, $\ell(\sqrt{D})$ is even, a contradiction. Thus, $a \geq b/4$ and $(b/4)(2y)^2 - ax^2 = \mp 1$, with $\gcd(x, 2y) = 1$. If $b > 4$, then by Theorem 3, $\ell(\sqrt{D})$ is even, a contradiction, so $b = 4$. However, $1 < a < b$, so $a = 3$, contradicting the hypothesis.

The case $D = p^j > 3$ for p an odd prime and $j \geq 1$ odd, is covered in the above when $p \equiv 1 \pmod{4}$ by Corollary 5. Thus, we assume $p \equiv 3 \pmod{4}$. By Equation (9), $\ell(\sqrt{4D})$ is even, since -1 is not a square modulo p . By

Theorem 6, there is a factorization $4D = AB$ with either $AX^2 - BY^2 = \pm 1$ and $1 < A < B$, or $AX^2 - BY^2 = \pm 2$ with XY odd. In the former case, we must have $p^j \mid B$ since otherwise $p \mid A$ and $p \mid B$. Note that $B = 4$ and $A = 3$ is excluded by hypothesis. Hence, $A = 4$, so $Q_{\ell/2} = 4$ by Theorem 3. In the latter case, $p^j \mid B$ by similar reasoning, and $A = 2$ is forced. By Theorem 5, $Q_{\ell/2} = 4$. \square

Corollary 6 generalizes [13, Theorem 5.1], which is the case where $D = 4p^j$, and corrects the result since the case $p^j = 3$ was not excluded therein.

Example 16 *Let $D = 2d$ where $d > 1$ is a perfect square divisible only by primes congruent to 5 modulo 8. Then $\ell(\sqrt{D})$ is odd. To see this, assume that $\ell(\sqrt{D})$ is even so by Theorem 6, there is a factorization $D = ab$ such that one of $ax^2 - by^2 = \pm 1$ with $1 < a < b$, or $ax^2 - by^2 = \pm 2$ with xy odd. However, the latter cannot occur since ax^2 and by^2 have different parities. If the former holds, then the following Legendre symbol equality holds (for example see [22, Theorem 4.1.6, p. 191]), where p is any prime dividing b and a is even,*

$$-1 = \left(\frac{\pm 2}{p} \right) = \left(\frac{ax^2 - by^2}{p} \right) = \left(\frac{\pm 1}{p} \right) = 1,$$

a contradiction. A similar contradiction is reached if p divides a and b is even. These are the only two cases possible since $1 < a < b$.

Remark 9 *The phenomenon in Corollary 6 gives criteria for $\ell(\sqrt{4D})$ to be even when $\ell(\sqrt{D})$ is odd. There is a more general related phenomenon worth highlighting. If $D > 1$ is not a perfect square and $\Delta = f^2D$, where $f \in \mathbb{N}$, with $\ell(\sqrt{D})$ even, then $\ell(\sqrt{\Delta})$ is even. This fact is immediate from Equation (9). Thus, Corollary 6 provides conditions under which the converse of this fact fails to hold (for $f = 2$).*

Remark 10 *It should be observed that both parts 1 and 2 of Theorem 6 cannot occur together. To see this, assume that there exist $a, b, a_1, b_1 \in \mathbb{N}$ such that $ar^2 - bs^2 = (-1)^{\ell/2}$, with $a > 1$, and $a_1r_1^2 - b_1s_1^2 = 2(-1)^{\ell/2}$, with r_1s_1 odd. Multiplying the first equation by 2 and equating, we deduce that $a = 2a_1$, $b = b_1/2$, $r = r_1/2$, and $s = s_1$. Hence, r_1 is even, a contradiction.*

Hence, $\ell = \ell(\sqrt{4D})$ is even and $Q_{\ell/2} = 4$. For instance, if $D = 2 \cdot 5^2 \cdot 13^2$, then $\ell(\sqrt{D}) = 13$, $\ell = \ell(\sqrt{4D}) = 26$, and $Q_{\ell/2} = 4$.

Also, notice that there cannot exist two distinct factorizations of the form $ar^2 - bs^2 = \pm 1$ with $1 < a < b$ since $a = Q_{\ell/2}$.

Example 17 Let $D = 296$ with $a = 2$ and $b = 148$, then $ar^2 - bs^2 = 2 \cdot 43^2 - 5^2 \cdot 148 = -2 = (-1)^{\ell/2} 2$ with $Q_{\ell/2} = 4 = Q_3$.

In [36] the authors prove that the $\ell(\sqrt{D})$ is even if and only if one of the Equations (17) or (27) has a solution. However, they do not mention the involvement of the central norm $Q_{\ell/2}$. They also mention that $d = 74$, for which $\ell = 5$, with $a = 2$, $b = 37$ shows that the hypothesis that xy is odd in part 2 of Theorem 6 cannot be removed since $2 \cdot 43^2 - 37 \cdot 10^2 = -2$. However, what our more informative Theorem 5 shows is that the case where $a = 2$ (and xy odd) forces $Q_{\ell/2} = 4$. Theorem 6 provides an insight into the even parity of $\ell(\sqrt{D})$ via the central norm $Q_{\ell/2}$ depending on the solvability of one of Equations (17) or (27).

From the above development, we also get the following new result which solves the problem of a criterion for the parity of the central quotient.

Theorem 7 Suppose that $D > 1$ is not a perfect square and $\ell = \ell(\sqrt{D})$ is even. Then the following are equivalent.

1. The central (partial) quotient $q_{\ell/2}$ in the simple continued fraction expansion of \sqrt{D} is even.
2. There exists a factorization $D = ab$ with $1 < a < b$ and $ar^2 - bs^2 = \pm 1$ for some $r, s \in \mathbb{N}$.
3. There does not exist a factorization $D = ab$ such that $1 \leq a < b$ and $ar^2 - bs^2 = \pm 2$ with rs odd.

Proof. The equivalence of parts 2–3 follows from Remark 10. We now show that part 1 is equivalent to part 2.

Suppose that part 2 holds. If D is odd, then by Equation (12), and Theorem 3, $q_{\ell/2} = 2P_{\ell/2}/Q_{\ell/2} = 2P_{\ell/2}/a$, where $a \mid P_{\ell/2}$ so $q_{\ell/2}$ is even. Now

assume that D is even. If $D \equiv 2 \pmod{4}$, then one of a or b is even. If a is even, then by Equation (4),

$$D = ab = P_{\ell/2}^2 + Q_{\ell/2}Q_{\ell/2-1} = P_{\ell/2}^2 + aQ_{\ell/2-1},$$

so $P_{\ell/2}$ is even. Thus, by Equation (12), $a \mid P_{\ell/2}$, whence $q_{\ell/2}$ is even.

Now suppose that $D \equiv 0 \pmod{4}$ and a is even. If $q_{\ell/2}$ is odd, then $a = Q_{\ell/2}$ does not divide $P_{\ell/2}$ by Equation (12). Therefore, $P_{\ell/2} = Q_{\ell/2}t/2 = at/2$ where t is odd by Equation (11). However, by Equation (7) and Theorem 3, $ra = ats/2 + aB_{\ell/2-2}$, so $r = ts/2 + B_{\ell/2-2}$, forcing s to be even, a contradiction, given that a is even and $ar^2 - bs^2 = \pm 1$. Hence, $q_{\ell/2}$ is even. If $D \equiv 0 \pmod{4}$ and a is odd, then $q_{\ell/2}$ is even by Equation (12). We have shown that part 2 implies part 1.

Now assume that $q_{\ell/2}$ is even. If $ar^2 - bs^2 = \pm 2$ where rs is odd, then $Q_{\ell/2} = 2a$ by Theorem 5. Thus, by Equation (12), $q_{\ell/2} = 2P_{\ell/2}/Q_{\ell/2} = P_{\ell/2}/a$, so $P_{\ell/2}/a$ is even. Set $P_{\ell/2} = at$ where t is even. By Equation (7) and Theorem 5,

$$ar = A_{\ell/2-1} = P_{\ell/2}B_{\ell/2-1} + Q_{\ell/2}B_{\ell/2-2} = ats + 2aB_{\ell/2-2},$$

so $r = ts + 2B_{\ell/2-2}$, forcing r to be even, a contradiction. Hence, part 2 must hold by the equivalence of parts 2 and 3. \square

The following is a classical consequence of Theorem 7 (see [27, Conjecture 2.1, p. 61]).

Corollary 7 *If $p \equiv 3 \pmod{4}$ is prime, then $\ell = \ell(\sqrt{p})$ is even and $q_{\ell/2}$ is odd.*

Proof. By Equation (9), ℓ is even and since there is no nontrivial factorization of p , then by Theorem 7, $q_{\ell/2}$ is odd. \square

More generally, we have the following consequence.

Corollary 8 *If $D = 4b$ is not a perfect square, b is odd and is divisible by a prime congruent to 3 modulo 4, then $\ell = \ell(\sqrt{D})$ is even and $q_{\ell/2}$ is even.*

Proof. As above, ℓ is even. Suppose that part 2 of Theorem 6 holds. Since rs is odd, then both a and b are even, so given that $ab \equiv 4 \pmod{8}$, we must

have that $ar^2 - bs^2 \equiv 0 \pmod{4}$, a contradiction. Thus, part 1 of Theorem 6 holds. By Theorem 7, $q_{\ell/2}$ is even. \square

The authors of [36] also provide a criterion for the oddness of $\ell(\sqrt{D})$ in terms of D being a sum of two squares and the solvability of another Diophantine equation. However, that result is strikingly similar to that given by Kaplan and Williams in [10]. However, in neither of these papers do the authors give the underlying reasons for the oddness of $\ell(\sqrt{D})$ in terms of underlying ideal theory. In [17, Theorem 8, p. 66], Louboutin gave the following criterion for *fundamental* discriminants, and in [21], this author generalized to *arbitrary* discriminants and provided a count on the number of ambiguous ideal classes without ambiguous ideals. This calls for some background explanation.

An ideal I in the $\mathbb{Z}[\sqrt{D}]$ is called *ambiguous* if $I = I'$, where I' is the conjugate ideal of I , and I is said to be in an *ambiguous* class in the class group \mathcal{O}_{4D} of $\mathbb{Z}[\sqrt{D}]$ if $I \sim I'$, where \sim denotes equivalence of ideals in \mathcal{O}_{4D} . It can occur that there is an ambiguous class of ideals having no ambiguous ideals (see [21] for an in-depth analysis of this phenomenon). The following is the criterion provided in [21] (without the count on the number of ambiguous classes without ambiguous ideals, for which the reader may consult [21, Theorem 6.1.3, p. 191]).

Theorem 8 *Suppose that $D > 1$ is not a perfect square, but is a sum of two integer squares. Then $\ell(\sqrt{D})$ is odd if and only if there do not exist any ambiguous classes of \mathcal{O}_{4D} -ideals without ambiguous ideals in them.*

Example 18 *$D = 34 = 3^2 + 5^2$ has $\ell(\sqrt{D}) = 4$ and the ideal $[5, 3 + \sqrt{34}] = 5\mathbb{Z} \oplus (3 + \sqrt{34})\mathbb{Z}$ is in an ambiguous ideal class without ambiguous ideals. In fact, any $D = p^2 + ((p^2 + 1)/2)^2$ where $p \geq 3$ is prime represents a radicand such that there are ambiguous classes without ambiguous ideals. Here $\ell(\sqrt{D}) = 4$. This example was discussed in [36], but there is no mention of the ideal theory underlying it.*

The notion of parity and ambiguous classes is also related to pure symmetry in the simple continued fraction expansion of \sqrt{D} (see [31] for details). Note, as well, that if $\ell = \ell(\sqrt{D})$ is odd then necessarily D is a sum of two

integer squares since, in that case, $D = P_{(\ell+1)/2}^2 + Q_{(\ell+1)/2}^2$ in the simple continued fraction expansion of \sqrt{D} . For instance, $D = 145 = 12^2 + 1^2$ and $\ell = 5$. It is also the case that D is a sum of two integer squares if and only if there exists an element $\beta \in \mathbb{Q}(\sqrt{D})$ with $N(\beta) = -1$. Of course, if ℓ is even, then $\beta \notin \mathcal{O}_{4D}$. Hence, if ℓ is even but -1 is a norm from $\mathbb{Q}(\sqrt{D})$, then each ambiguous class of \mathcal{O}_{4D} has two ideals corresponding to elements of norm -1 . For example, $I = [5, (11 + \sqrt{221})/2]$ and $I' = [5, (11 - \sqrt{221})/2]$ are two ideals that correspond to an element of norm -1 since $(11^2 - 221)/10^2 = -1$. Here $\ell = 6$.

The reader may wonder about an analogue of Theorem 6 for $(1 + \sqrt{D})/2$ when $D \equiv 1 \pmod{4}$. It is given as follows.

Theorem 9 *Let $D = ab \equiv 1 \pmod{4}$, not a perfect square, with $1 < a < b$, and assume that there is a solution to Equation (16) with $\sigma = 2$. Then $\ell = \ell((1 + \sqrt{D})/2)$ is even if and only if there exists a solution to Equation (17) with $\sigma = 2$ (in which case (b)–(f) of Theorem 3 hold.)*

Proof. In view of Theorem 3, we need only prove that ℓ being even implies a solution of Equation (17) with $\sigma = 2$. By Equation (11), if $4 \mid Q_{\ell/2}$, then $2 \mid P_{\ell/2}$. However, this is a contradiction via Equation (4) since D is not even. Thus, 2 properly divides $Q_{\ell/2}$. From Equation (8), we have that

$$G_{\ell/2-1}^2 - DB_{\ell/2-1}^2 = (-1)^{\ell/2} 2Q_{\ell/2}.$$

Therefore,

$$ar^2 - bs^2 = (-1)^{\ell/2} 4,$$

where $a = Q_{\ell/2}/2$, $r = 2G_{\ell/2-1}/Q_{\ell/2}$, $b = 2D/Q_{\ell/2}$, and $s = B_{\ell/2-1}$. Note that $Q_{\ell/2} \mid 2G_{\ell/2-1}$ by Equations (7) and (11). Also, $\gcd(r, s) = 1$ since Equation (16) with $\sigma = 2$. The reason is that from Lemma 1, $rs = B_{\ell-1}$ which is odd, and $\gcd(r, s) \mid 2$ by Equation (8). \square

Corollary 9 *If $D > 1$ is not a perfect square and $\sigma = 2$, then*

$$\ell(\sqrt{D}) \equiv \ell((1 + \sqrt{D})/2) \pmod{2}.$$

Proof. If D is prime, then it is a well-known fact that $\ell((1 + \sqrt{D})/2)$ is odd, and $\ell(\sqrt{D})$ is odd. If D is composite and $\ell((1 + \sqrt{D})/2)$ is even, then Equation (17) with $\sigma = 2$ has a solution by Theorem 9. Therefore,

by Theorem 4, Equation (17) with $\sigma = 1$ has a solution, so by Theorem 3, $\ell(\sqrt{D})$ is even. If $\ell((1 + \sqrt{D})/2)$ is odd, then $\varepsilon_D^3 \in \mathbb{Z}[\sqrt{D}]$, where ε_D is the fundamental unit of $\mathbb{Z}[(1 + \sqrt{D})/2]$, and since $N((\varepsilon_D^3)) = -1$, then $\ell(\sqrt{D})$ must be odd via Equation (9). \square

Note that we cannot remove the solvability of Equation (16) with $\sigma = 2$ from the hypothesis of Theorem 9. Consider $D = 57$, where $\ell((1 + \sqrt{D})/2) = 6$, but $\varepsilon_D \in \mathbb{Z}[\sqrt{D}]$ and the equation $3x^2 - 19y^2 = \pm 4$ with $\gcd(x, y) = 1$ is not solvable, since odd xy implies $3x^2 - 19y^2 \equiv 0 \pmod{8}$. (However, note that $3 \cdot 5^2 - 19 \cdot 2^2 = -1$.) Thus, both Equations (16)–(17) fail in this case. See Remark 2 for related data.

We now take another look at Corollary 4. The proof of this corollary motivates a look at Legendre and related symbols in connection with our Diophantine equations. We will look into this matter now. The following generalizes [28, Theorems 3.2–3.3, pp. 71–73].

Theorem 10 *Suppose that $D = ab$, not a perfect square, where $1 < a < b$ with $a = 2^t a_1$ and $b = 2^u b_1$ for $t, u \geq 0$. If $|r^2 a - s^2 b| = \sigma^2$ has a solution $r, s \in \mathbb{N}$, with $\gcd(r, s) = 1$, then the following Jacobi symbol equalities hold, where $\ell = \ell((\sigma - 1 + \sqrt{ab})/\sigma)$ is even,*

$$\left(\frac{b}{a_1}\right) = \left(\frac{-1}{a_1}\right)^{\ell/2+1} \quad \text{and} \quad \left(\frac{a}{b_1}\right) = \left(\frac{-1}{b_1}\right)^{\ell/2}.$$

Proof. By Theorems 3,

$$\left(\frac{G_{\ell/2-1}}{a}\right)^2 a - B_{\ell/2-1}^2 b = (-1)^{\ell/2} \sigma^2.$$

Thus,

$$\left(\frac{b}{a_1}\right) = \left(\frac{(-1)^{\ell/2+1}}{a_1}\right) = \left(\frac{-1}{a_1}\right)^{\ell/2+1},$$

and

$$\left(\frac{a}{b_1}\right) = \left(\frac{(-1)^{\ell/2}}{b_1}\right) = \left(\frac{-1}{b_1}\right)^{\ell/2},$$

as required. \square

Note that the use of the Jacobi symbol in the above is justified since $\gcd(a_1, b_1) = 1$ given that Equation (17) holds. Similarly this is true for the next set of results.

Remark 11 We get Gauss's quadratic reciprocity law from Theorem 10 when $\ell = \ell(\sqrt{pq})$ is even where $2 < p < q$ are primes. For instance, in the case $p \equiv q \equiv 3 \pmod{4}$, ℓ is even as above, and part 1 of Theorem 6 must hold since part 2 clearly cannot. Thus, $pr^2 - qs^2 = \pm 1$ for some $r, s \in \mathbb{N}$. Hence,

$$\left(\frac{p}{q}\right) = \left(\frac{pr^2 - qs^2}{q}\right) = \left(\frac{\pm 1}{q}\right) = \pm 1,$$

and

$$\left(\frac{q}{p}\right) = \left(\frac{qs^2 - pr}{p}\right) = \left(\frac{\mp 1}{p}\right) = \mp 1,$$

so

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

The following generalizes and refines [23, Theorem 2.6, p. 348], which in turn generalized results in [7].

Corollary 10 If $D = d_1d_2 \in \mathbb{N}$ where $d_1 \equiv 3 \pmod{8}$ and $d_2 \equiv 7 \pmod{8}$, then $\ell = \ell(\sqrt{D})$ is even, $B_{\ell-1}$ is even in the simple continued fraction expansion of \sqrt{D} , and the Jacobi symbol identities hold as follows:

$$\left(\frac{d_1}{d_2}\right) = \begin{cases} (-1)^{U/2} & \text{if } Q_{\ell/2} = d_2 \\ (-1)^{U/2+1} & \text{if } Q_{\ell/2} = d_1, \end{cases}$$

where

$$T + U\sqrt{D} = A_{\ell-1} + B_{\ell-1}\sqrt{D}$$

is the fundamental unit of $\mathbb{Z}[\sqrt{D}]$. Moreover, $\ell/2$ is odd and $B_{\ell/2-1}$ is even.

Proof. Since there must be a prime p dividing D such that $p \equiv 3 \pmod{4}$, then by Equation (9), ℓ is even. Thus, by Theorem 6, either Equation (17) holds for some factorization $D = ab$ with $a \neq 1 = \sigma$, or Equation (27) holds for some such factorization with xy odd. However, if Equation (27) holds then under the assumption that one of $Q_{\ell/2} = a = d_1$ or $Q_{\ell/2} = a = d_2$,

$$0 \equiv x^2a - y^2b \equiv \pm 2 \pmod{4},$$

since $a \equiv b \pmod{4}$, a contradiction. Hence, Equation (17) holds with $\sigma = 1$.

We prove the result for the case where $a = Q_{\ell/2} = d_2$, since the other case is similar. By Theorem 10, we need to show that

$$B_{\ell-1} \equiv \ell + 2 \pmod{4}. \quad (34)$$

From Theorem 3, we know that

$$B_{\ell-1} = 2A_{\ell/2-1}B_{\ell/2-1}/a = 2rs, \quad (35)$$

with one of r or s even. Therefore, $B_{\ell-1} \equiv 0 \pmod{4}$, so we must show that $\ell \equiv 2 \pmod{4}$. First, we demonstrate that $B_{\ell/2-1} = s$ must be even. If not, then by Equation (8), $A_{\ell/2-1}$ is even. If $A_{\ell/2-1} \equiv 0 \pmod{4}$, then by Equation (8),

$$A_{\ell/2-1}^2 - B_{\ell/2-1}^2 ab \equiv -ab \equiv (-1)^{\ell/2} a \pmod{8},$$

so $b \equiv (-1)^{\ell/2+1} \pmod{8}$. Since $b = d_1$, then $3 \equiv (-1)^{\ell/2+1} \pmod{8}$, a contradiction. Thus, $A_{\ell/2-1} \equiv 2 \pmod{4}$. By Equation (35), $B_{\ell-1} \equiv 4 \pmod{8}$, so

$$A_{\ell-1}^2 - B_{\ell-1}^2 ab \equiv 1 - 4ab \equiv 1 \pmod{8},$$

a contradiction since ab is odd. We have shown that $B_{\ell/2-1} = s$ is even.

Since $r^2 a - s^2 b = (-1)^{\ell/2}$ with $a = d_2$, $b = d_1$, $r = A_{\ell/2-1}/a$, and $B_{\ell/2-1} = s$, then $r^2 \equiv (-1)^{\ell/2+1} \pmod{4}$, in which case $\ell/2$ is odd, which establishes Equation (34). \square

Example 19 If $D = 77$, with $d_1 = 11$ and $d_2 = 7$, then $Q_{\ell/2} = Q_3 = 7$ and

$$\left(\frac{d_1}{d_2}\right) = \left(\frac{11}{7}\right) = 1 = (-1)^{B_{\ell-1}/2},$$

where $A_{\ell-1} + B_{\ell-1}\sqrt{D} = 351 + 40\sqrt{77}$.

Example 20 Let $D = 21$ with $Q_{\ell/2} = d_1 = 3$ and $d_2 = 7$. Then

$$\left(\frac{d_1}{d_2}\right) = \left(\frac{3}{7}\right) = 1 = (-1)^{B_{\ell-1}/2+1},$$

where $\ell = 6$, and $A_{\ell-1} + B_{\ell-1}\sqrt{D} = 55 + 12\sqrt{77}$.

The following generalizes [7, Theorem 2.6, p. 340].

Corollary 11 *Suppose that $D = 2d_1d_2 \in \mathbb{N}$, $d_1 \equiv 3 \pmod{8}$, $d_2 \equiv 7 \pmod{8}$, and $Q_{\ell/2} = 2d_1$. Then $\ell = \ell(\sqrt{D})$ is even, $B_{\ell-1}$ is even and the following Jacobi symbol identity holds,*

$$\left(\frac{d_1}{d_2}\right) = (-1)^{B_{\ell-1}/2}.$$

Proof. As above ℓ is even and since Equation (27) clearly cannot hold with xy odd, then by Theorem 6, Equation (17) must hold with $\sigma = 1$. Thus, by Theorem 10, we need to show that $B_{\ell-1} \equiv \ell \pmod{4}$. By Theorem 3, $a = Q_{\ell/2} = 2d_1$, $B_{\ell-1} = 2rs$, and s is odd, and $(-1)^{\ell/2} \equiv 6r^2 + 1 \pmod{8}$. If r is odd, then $\ell/2$ is odd, and if r is even then $\ell/2$ is even. This shows that $B_{\ell-1} \equiv \ell \pmod{4}$, as required. \square

Example 21 *Let $D = 42$ with $d_1 = 3$ and $d_2 = 7$. Then*

$$\left(\frac{d_1}{d_2}\right) = \left(\frac{3}{7}\right) = -1 = (-1)^{B_{\ell-1}/2},$$

where $\ell = 2 = B_{\ell-1}$, and $Q_{\ell/2} = Q_1 = 6 = 2d_1$.

In Corollaries 10–11, it is shown that under those hypotheses, Equation (27) cannot hold since Theorem 10 assumes that Equation (17) holds with $\sigma = 1$, and Remark 10 tells us that both of them cannot hold together. The following result deals with the case where Equation (27) holds. Moreover, this is completely new in the sense that it is not a generalization or refinement of known results.

Theorem 11 *Suppose that $D = ab \in \mathbb{N}$ is not a perfect square, where $1 \leq a < b$, $a = 2^t a_1$, $b = 2^u b_1$, $t, u \geq 0$. Then if Equation (27) holds for xy odd, the following Jacobi symbol identity holds,*

$$\left(\frac{a}{b_1}\right) = \left(\frac{2}{b_1}\right) \left(\frac{-1}{b_1}\right)^{\ell/2} \quad \text{and} \quad \left(\frac{b}{a_1}\right) = \left(\frac{2}{a_1}\right) \left(\frac{-1}{a_1}\right)^{\ell/2+1},$$

where $\ell = \ell(\sqrt{D})$ is even.

Proof. By Theorems 5–6, ℓ is even, and by Remark 10, Equation (17) cannot hold. Thus, by Theorem 5, $Q_{\ell/2} = 2a$, $A_{\ell-1} = ar$, $B_{\ell-1} = s$, and

$$\left(\frac{A_{\ell/2-1}}{a}\right)^2 a - B_{\ell/2-1}^2 b = 2(-1)^{\ell/2},$$

so

$$\left(\frac{a}{b_1}\right) = \left(\frac{r^2 a - s^2 b}{b_1}\right) = \left(\frac{2(-1)^{\ell/2}}{b_1}\right) = \left(\frac{2}{b_1}\right) \left(\frac{-1}{b_1}\right)^{\ell/2},$$

and similarly,

$$\left(\frac{b}{a_1}\right) = \left(\frac{2}{a_1}\right) \left(\frac{-1}{a_1}\right)^{\ell/2+1},$$

as required. \square

The following provides an analogue of Corollary 11 which establishes a Jacobi symbol identity in terms of the constant term in the the fundamental unit in $\mathbb{Z}[\sqrt{D}]$, rather than the coefficient of \sqrt{D} and ties this to the solvability of Equation (27).

Corollary 12 *Let $D = d_1 d_2 \in \mathbb{N}$, not a perfect square, with $d_1 \equiv 1 \pmod{4}$, $d_2 \equiv 7 \pmod{8}$. Then if $Q_{\ell/2} = 2d_2$ in the simple continued fraction expansion of \sqrt{D} , the following Jacobi symbol identity holds,*

$$\left(\frac{d_1}{d_2}\right) = (-1)^{A_{\ell-1}/2},$$

where $A_{\ell-1} + B_{\ell-1}\sqrt{D}$ is the fundamental unit in $\mathbb{Z}[\sqrt{D}]$ arising from the simple continued fraction expansion of \sqrt{D} .

Proof. As above ℓ is even, and if Equation (17) holds with $\sigma = 1$, then by Theorem 3, $D = ab$ with $Q_{\ell/2} = a = 2d_2$, a contradiction since D is odd. Hence, Equation (27) holds with xy odd by Theorem 10. Thus, by Theorem 5, $Q_{\ell/2} = 2a = 2d_2$, $b = d_1$, and $A_{\ell/2-1} = ar$. By Theorem 11, we need to show that $A_{\ell-1} \equiv \ell + 2 \pmod{4}$ in order to complete our task. By Theorem 5, $A_{\ell-1} = (r^2 a + s^2 b)/2$. Therefore, $A_{\ell-1} \equiv 0 \pmod{8}$ if $b \equiv 1 \pmod{8}$, and $A_{\ell-1} \equiv 6 \pmod{8}$ if $b \equiv 5 \pmod{8}$. Hence,

$$A_{\ell-1} \equiv 0 \pmod{4} \text{ if } b \equiv 1 \pmod{8} \text{ and } A_{\ell-1} \equiv 2 \pmod{4} \text{ if } b \equiv 5 \pmod{8}.$$

Moreover, by Theorem 5, $2(-1)^{\ell/2} \equiv d_2 - d_1 \equiv 6 \pmod{8}$ if $b \equiv 1 \pmod{8}$ and $2(-1)^{\ell/2} \equiv 6 \pmod{8}$ when $b \equiv 5 \pmod{8}$, so $(-1)^{\ell/2} \equiv 3 \pmod{4}$ when $b \equiv 1 \pmod{8}$ and $(-1)^{\ell/2} \equiv 1 \pmod{4}$ if $b \equiv 5 \pmod{8}$. This establishes that $A_{\ell-1} \equiv \ell + 2 \pmod{4}$, securing the result. \square

Example 22 *Looking back to Example 12, with $a = 31 = d_2$, and $b = 61 = d_1$, we get,*

$$\left(\frac{d_1}{d_2}\right) = -1 = (-1)^{409568133891387775} = (-1)^{A_{\ell-1/2}}.$$

An equation related to the title equation is,

$$aX^4 - bY^2 = \sigma^2, \quad (36)$$

which has been studied by numerous authors, such as [2]–[5], [12]–[20], and [35]. In particular, in [12], it is shown that if Equation (36) has a solution, then the fundamental solution $r\sqrt{a} + s\sqrt{b}$ of $ax^2 - by^2 = 1$ satisfies $r = t^2$ for some $t \in \mathbb{N}$. Therefore, from Theorem 3, we get that $A_{\ell/2-1} = t^2a$ and $Q_{\ell/2} = a$ in the simple continued fraction expansion of $\sqrt{D} = \sqrt{ab}$. Thus, this provides an easy check that Equation (36) has a solution. For instance, in [1], Bumby proves that the only solutions of the Diophantine equation

$$3x^4 - 2y^2 = 1 \quad (37)$$

in positive integers are $(x, y) \in \{(1, 1), (3, 11)\}$. We observe that $A_{\ell/2-1} = A_0 = 2 = 2 \cdot 1^2 = a \cdot t^2 = Q_{\ell/2} = Q_1$, while $\sqrt{2} + \sqrt{3}$ and $(\sqrt{2} + \sqrt{3})^3 = 9\sqrt{3} + 11\sqrt{2}$ provide the two solutions of Equation (37). Also, $9 = B_{3\ell/2-1} = B_2$ and $11 = A_{3\ell/2-1}/a = A_2/2$ in the simple continued fraction expansion of $\sqrt{6}$. Since all solutions of $3X^2 - 2Y^2 = 1$ are given by $(\sqrt{2} + \sqrt{3})^{2j+1}$ for any $j \geq 0$ by Theorem 2, then Bumby's result tells us that there cannot be a coefficient of $\sqrt{3}$ that is a square for $j > 1$. This is essentially what Bumby proves.

Theorem 3 provides a quick method for showing that Equation (36) does *not* have a solution merely by checking to see if $Q_{\ell/2} = a$ and $G_{\ell/2-1}/a = t^2$ for some $t \in \mathbb{N}$. For instance, from Example 1, $9x^2 - 260y^2 = 1$ has minimal solution $r\sqrt{a} + s\sqrt{b} = 43\sqrt{9} + 8\sqrt{260}$. Hence, $9X^4 - 260Y^2 = 1$ has no solution since $Q_{\ell/2} = Q_4 = a = 9$, and $A_{\ell/2-1} + A_3 = 9 \cdot 43 \neq 9 \cdot t^2$ for any $t \in \mathbb{N}$.

In [40], Walsh shows the following. Suppose that

$$(r\sqrt{a} + s\sqrt{b})^{2j+1} = v_{2j+1}\sqrt{a} + w_{2j+1}\sqrt{b},$$

where $r\sqrt{a} + s\sqrt{b}$ is the fundamental solution of $ax^2 - by^2 = 1$. If $r = t^2$ and we set $m = t^4a - 1$, then

$$(\sqrt{m+1} + \sqrt{m})^{2j+1} = V_{2j+1}\sqrt{m+1} + W_{2j+1}\sqrt{m},$$

then v_{2j+1} is a perfect square if and only if V_{2j+1} is a perfect square. Hence, in consideration of Equation (36) for $\sigma = 1$, it suffices to look equations of the form

$$(m+1)X^4 - mY^2 = 1. \quad (38)$$

for instance, the Bumby-type Equation (37) is of this form with $m = 2$.

In [41], Walsh shows that Equation (38) has the solution $(1, 1)$ and conjectures (for $m > 1$) that there are no others unless $m = t^2 + t$ for some $t \in \mathbb{N}$ in which case

$$(X, Y) = (2t + 1, 4t^2 + 4t + 3)$$

is the only other solution. The case $m = 1$ has been studied in various venues such as [6], where solvability of the Diophantine equation $p^m - 2q^n = \pm 1$, for primes p and q is shown to have no solutions unless with $m = n = 2$ or $m = 2, n = 4$. In the latter case the only solutions are $p = 239$ and $q = 13$ by [14]. The results of this paper can be used to achieve the latter. Similarly, in [37], the Diophantine equation $(x^2 - 2)^2 - 2 = 2y^2$ is considered, the solvability of which is shown to be equivalent to the solvability of $X^2 - 2Y^4 = -1$ and again by [14], we know what the solutions happen to be.

For the sister equation to that of Equation (38),

$$aX^2 - bY^4 = 1, \quad (39)$$

Ljunggren proved in [15] that when $r\sqrt{a} + s\sqrt{b}$ is the fundamental solution of $ax^2 - by^2 = 1$, then by setting $s = n^2w$ with w odd and squarefree, Equation (39) has at most one solution and it is given by

$$(r\sqrt{a} + s\sqrt{b})^w = u\sqrt{a} + v^2\sqrt{b}.$$

For $w \leq 5$, Walsh [41] shows that there are infinitely many a, b such that Equation (39) has a solution.

Example 23 For $a = 2$, $b = 19$, $r\sqrt{a} + s\sqrt{b} = 3\sqrt{2} + \sqrt{19}$ is the fundamental solution to $x^2a - y^2b = -1$. In the simple continued fraction expansion of $\sqrt{38}$, $Q_{\ell/2} = Q_1 = a = 2$. Also, $A_{3\ell/2-1} = A_2 = 450 = 2 \cdot 15^2$, $B_{3\ell/2-1} = B_2 = 73$, and

$$15^2\sqrt{2} + 73\sqrt{19} = (3\sqrt{2} + \sqrt{19})^3$$

is the solution to $19X^2 - 2Y^4 = 1$. Thus, Ljunggren's aforementioned result tells us that $(3\sqrt{2} + \sqrt{19})^{2j+1}$ has a square coefficient of $\sqrt{2}$ only for $j = 1$.

For $w \geq 7$, Walsh conjectured in [40] that Equation (39) has no solutions and proved this for $w = 7$. Thus, based upon our results in this paper, we pose the following.

Conjecture 1 If $1 < a < b$ and $r\sqrt{a} + s\sqrt{b}$ is the fundamental solution of

$$ax^2 - by^2 = 1,$$

with $s = n^2w$, where $w = 2j + 1 \geq 7$ is odd and squarefree, then

$$(r\sqrt{a} + s\sqrt{b})^w = (A_{j\ell-1}r + sbB_{j\ell-1})\sqrt{a} + (A_{j\ell-1}s + raB_{j\ell-1})\sqrt{b}$$

where $A_{j\ell-1}s + raB_{j\ell-1}$ is not a perfect square.

There is also a link to Theorems 3–4 via results of Ljunggren who proved in [16] that if the equation $ax^2 - by^2 = 4$ has a solution with $\gcd(x, y) = 1$, then the only solution to $aX^4 - bY^2 = 1$ is $r\sqrt{a} + s\sqrt{b}$, which is the smallest solution of $ax^2 - by^2 = 1$. Thus, via Theorem 4 we know how the solution relates to the order $\mathbb{Z}[(1 + \sqrt{ab})/2]$.

We conclude with the observation that results in [23] on alternating sums can also be generalized using the techniques of this paper.

Acknowledgements: The author's research is supported by NSERC Canada grant # A8484.

References

- [1] R.T. Bumby, *The Diophantine equation $3x^4 - 2y^2 = 1$* , Math. Scand. **21** (1967), 144–148.
- [2] J.H.E. Cohn, *On square Fibonacci numbers*, J. London Math. Soc. **39** (1964), 537–541.
- [3] J.H.E. Cohn, *Eight Diophantine equations*, Proc. London Math. Soc. (3) **16** (1966), 153–166. Addendum: *Eight Diophantine equations*, Proc. London Math. Soc. (3) **17** (1967), 381.
- [4] J.H.E. Cohn, *Five Diophantine equations*, Math. Scand. **21** (1967), 61–70.
- [5] J.H.E. Cohn, *Squares in some recurrent sequences*, Pacific J. Math. **41** (1972), 631–646. Addendum: *Waring’s problem in quadratic number fields* Acta Arith. **20** (1972), 1–16. Acta Arith. **23** (1973), 417–418.
- [6] P. Crescenzo, *A Diophantine equation which arises in the theory of finite groups*, Advances in Math. **17** (1975), 25–29.
- [7] C. Friesen, *Legendre symbols and continued fractions*, Acta Arith. **59** (1991), 365–379.
- [8] C.F. Gauss, **Disquisitiones Arithmeticae**, English Edition, Springer-Verlag, New York, Berlin, Heidelberg, Tokyo (1986).
- [9] P. Kaplan, *À propos des equation antipelliennes*, L’Ens. Math **29** (1983), 323–328.
- [10] P. Kaplan and K.S. Williams, *Pell’s equations $x^2 - my^2 = -1, -4$ and continued fractions*, J. Number Theory **23** (1986), 169–182.
- [11] F. Halter-Koch, *Über Pell’sche Gleichungen und Kettenbrüche*, Arch. Math **49** (1987), 29–37.
- [12] M.H. Le, *On the diophantine equation $D_1x^4 - D_2y^2 = 1$* , Acta Arith. **76** (1996), 1–9.
- [13] Q. Lin, *Central norm of an integer*, preprint.

- [14] W. Ljunggren, *Zur Theorie der Gleichung $x^2 + 1 = Dy^2$* , Avh. Norske Vid. Akad. Oslo I, no. (1942).
- [15] W. Ljunggren, Ein Satz über die Diophantische Gleichung $Ax^2 - By^2 = C$ ($C = 1, 4$), Tolfte Skand. Matemheikerkongressen, Lund, 1953, 188–194 (1954).
- [16] W. Ljunggren, *On the Diophantine equation $Ax^4 - By^2 = C$ ($C = 1, 4$)*, Math. Scand. **21** (1967), 149–158.
- [17] S. Louboutin, *Groupes des classes d'idéaux triviaux*, Acta Arith. **LIV** (1989), 61–74.
- [18] W.L. McDaniel and P. Ribenboim, *Squares and double squares in Lucas sequences*, C.R. Math. Rep. Acad. Sci. Canada **14** (1992), 104–108.
- [19] W.L. McDaniel and P. Ribenboim, *The square terms in Lucas sequences*, J. Number Theory **58** (1996), 104–123.
- [20] M. Mignotte and A. Pethö, *Sur les carrés dans certaines suites de Lucas*, J. Théorie Nombres Bordeaux **5** (1993), 333–341.
- [21] R.A. Mollin, **Quadratics**, CRC Press, Boca Raton, London, New York, Washington D.C. (1996).
- [22] R.A. Mollin **Fundamental Number Theory with Applications**, CRC Press, Boca Raton, London, New York, Washington D.C. (1998).
- [23] R. A. Mollin, *Jacobi symbols, ideals, and continued fractions*, Acta Arith. **LXXXV** (1998), 331–349.
- [24] R.A. Mollin, *All solutions of the Diophantine equation $x^2 - Dy^2 = n$* , Far East J. Math. Sci., Special Volume (1998), Part III, 257–293.
- [25] R.A. Mollin, **Algebraic Number Theory**, Chapman and Hall/CRC Press, Boca Raton, London, New York, Washington D.C. (1999).
- [26] R.A. Mollin, *Polynomials of Pellian type and continued fractions*, Serdica math. J. (2001), 317–342.
- [27] R.A. Mollin, *Proof of some conjectures by Kaplansky*, C. R. Math. Rep. Acad. Sci. Canada **23** (2001), 60–64.

- [28] R.A. Mollin, *Quadratic Diophantine equations determined by continued fractions*, JP Jour. Algebra, Number Theory and Appl. **1** (2001), 57–75.
- [29] R.A. Mollin, *A simple criterion for solvability of both $X^2 - DY^2 = c$ and $x^2 - Dy^2 = -c$* , New York J. Math. **7** (2001), 87–97.
- [30] R.A. Mollin, *The Diophantine equation $AX^2 - BY^2 = C$ and simple continued fractions*, Intern. Math. Journal, **2** (2002), 1–6.
- [31] R.A. Mollin and K. Cheng, *Palindromy and ambiguous ideals revisited*, J. Number Theory **74** (1999), 98–110.
- [32] R.A. Mollin, K. Cheng, and B. Goddard, *The Diophantine equation $AX^2 - BY^2 = C$ solved via continued fractions*, to appear Acta Math. Univ. Comenianae.
- [33] R.A. Mollin and A.J. van der Poorten, *continued fractions, Jacobi symbols, and quadratic Diophantine equations*, Canad. Math. Bull. **43** (2000), 218–225.
- [34] R.A. Mollin, A.J. van der Poorten, and H.C. Williams, *Halfway to a solution of $x^2 - Dy^2 = -3$* , Journal de Théorie des Nombres, Bordeaux **6** (1994), 421–459.
- [35] K. Nakamura and A. Pethö, *Squares in binary recurrence sequences in **Number Theory, Diophantine, Computational, and Algebraic Aspects***, Proceedings of a conference in Eger, Hungary, (Györy, Pethö, and Sós Eds.), Walter de Gruyter, Berlin (1998), 409–422.
- [36] P.J. Rippon and H. Taylor, *Even and odd periods in continued fractions of square roots*, preprint (2001).
- [37] R.J. Stroeker, *How to solve a Diophantine equation*, Amer. Math. Monthly **91**, (1984), 385–392.
- [38] H.F. Trotter, *On the norms of units in quadratic fields*, Proceed. Amer. Math. Soc. (1969), 198–201.
- [39] D.T. Walker, *On the Diophantine equation $mX^2 - nY^2 = \pm 1$* , Amer. Math. Monthly **74** (1967), 504–513.

- [40] P.G. Walsh, *A note on Ljunggren's theorem about the Diophantine equation $aX^2 - bY^2 = 1$* , C.R. Math. Rep. Acad. Sci. Canada **20**, (1998), 113–118.
- [41] P.G. Walsh, *Diophantine equations of the form $aX^4 - bY^2 = 1$* , in **Algebraic Number Theory and Diophantine analysis** (Graz 1998), de Gruyter, Berlin (2000), 532–554.

Department of Mathematics and Statistics

University of Calgary

Calgary, Alberta

Canada, T2N 1N4

URL: <http://www.math.ucalgary.ca/~ramollin/>

E-mail: ramollin@math.ucalgary.ca