Acta Math. Univ. Comenianae
Vol. LXXI, 2(2002), pp. 121–138

THE DIOPHANTINE EQUATION $AX^2 - BY^2 = C$ SOLVED VIA CONTINUED FRACTIONS

R. A. MOLLIN, K. CHENG AND B. GODDARD

ABSTRACT. The purpose of this article is to provide criteria for the solvability of the Diophantine equation $a^2X^2 - bY^2 = c$ in terms of the simple continued fraction expansion of $\sqrt{a^2b}$, and to explore criteria for the solvability of $AX^2 - BY^2 = C$ for given $A, B, C \in \mathbb{N}$ in the general case. This continues work in [**9**]–[**11**].

1. INTRODUCTION

The equation $ax^2 - by^2 = c$ has been a topic of interest for some time. For instance, Gauss provided criteria for the solvability of $|ax^2 - by^2| = 4$ in terms of the fundamental unit of the underlying real quadratic field $\mathbb{Q}(\sqrt{ab})$ (see Corollary 3.5 below). Also, Eisenstein looked at the solvability of that equation in similar terms (see [**6**, Exercise 2.1.15, p. 60] and Remark 3.2 below). In [**15**], H. C. Williams gives criteria for the solvability of $|x^2 - \Delta y^2| = 4$ with $\gcd(x, y) = 1$ in terms of the simple continued fraction expansion of the quadratic irrational $(1 + \sqrt{\Delta})/2$ where $\Delta \equiv 5 \pmod 8$ is a fundamental discriminant. Similarly, in [**3**], P. Kaplan and K. S. Williams gave criteria for the solvability of $x^2 - Dy^2 = -4$ for $\gcd(x, y) = 1$ in terms of the simple continued fraction expansion of $\sqrt{D}$ when D is not a perfect square (also see [**6**, Exercise 2.1.14, pp. 59–60]). It is in this vein that we are focused, namely toward a criterion for the solution of $|a^2X^2 - bY^2| = c$ in terms of the simple continued fraction expansion related to the radicand $D = a^2b$.

2. NOTATION AND PRELIMINARIES

We will be studying solutions of quadratic Diophantine equations of the general shape

$$AX^2 - BY^2 = C \quad (A, B \in \mathbb{N},\ C \in \mathbb{Z}), \tag{2.1}$$

where not both of A and B are squares. If $x, y \in \mathbb{Z}$ is a solution of (2.1), then it is called *positive* if $x, y \in \mathbb{N}$ and it is called *primitive* if it is positive and $\gcd(x, y) = 1$. It is easily verified that, given two positive solutions $x\sqrt{A}+y\sqrt{B}$ and $u\sqrt{A}+v\sqrt{B}$

Received September 3, 2001.
2000 *Mathematics Subject Classification.* Primary 11A55, 11R11, 11D09.
Key words and phrases. continued fractions, diophantine equations, fundamental units.

of (2.1), the following are equivalent:

$$(1)\ x < u, \quad (2)\ y < v, \quad \text{and} \quad (3)\ x\sqrt{A} + y\sqrt{B} < u\sqrt{A} + v\sqrt{B}.$$

Hence, among the primitive solutions of (2.1), if such solutions exists, there is one in which both x and y have their least values. Such a solution is called the *fundamental solution.* We will use the notation

$$\alpha = x\sqrt{A} + y\sqrt{B}$$

to denote a positive solution of (2.1), and we let

$$N(\alpha) = Ax^2 - By^2$$

denote the *norm* of α. We will be linking such solutions to simple continued fraction expansions that we now define.

Recall that a *quadratic irrational* is a number of the form

$$(P + \sqrt{D})/Q$$

where $P, Q, D \in \mathbb{Z}$ with $D > 1$ not a perfect square, $P^2 \equiv D \pmod{Q}$, and $Q \neq 0$. Now we set:

$$P_0 = P,\ Q_0 = Q, \text{ and recursively for } j \geq 0,$$

$$q_j = \left\lfloor \frac{P_j + \sqrt{D}}{Q_j} \right\rfloor, \tag{2.2}$$

$$P_{j+1} = q_j Q_j - P_j, \tag{2.3}$$

and

$$D = P_{j+1}^2 + Q_j Q_{j+1}. \tag{2.4}$$

Hence, we have the simple continued fraction expansion:

$$\alpha = \frac{P + \sqrt{D}}{Q} = \frac{P_0 + \sqrt{D}}{Q_0} = \langle q_0; q_1, \ldots, q_j, \ldots \rangle,$$

where the q_j for $j \geq 0$ are called the *partial quotients* of α.

To further develop the link with continued fractions, we first note that it is well-known that a real number has a periodic continued fraction expansion if and only if it is a quadratic irrational (see [**7**, Theorem 5.3.1, p. 240]). Furthermore a quadratic irrational *may* have a *purely* periodic continued fraction expansion which we denote by

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

meaning that $q_n = q_{n+\ell}$ for all $n \geq 0$, where $\ell = \ell(\alpha)$ is the period length of the simple continued fraction expansion. It is known that a quadratic irrational α *has* such a purely periodic expansion if and only if $\alpha > 1$ and $-1 < \alpha' < 0$. Any quadratic irrational which satisfies these two conditions is called *reduced* (see [**7**, Theorem 5.3.2, p. 241]). If α *is* a reduced quadratic irrational, then for all $j \geq 0$,

$$0 < Q_j < 2\sqrt{D}, \quad 0 < P_j < \sqrt{D}, \text{ and} \quad q_j \leq \lfloor \sqrt{D} \rfloor \tag{2.5}$$

Finally, we need an important result which links the solutions of quadratic Diophantine equations with the Q_j defined above. We first need the following notation.

Let $D_0 > 1$ be a square-free positive integer and set:

$$\sigma_0 = \begin{cases} 2 & \text{if } D_0 \equiv 1 \pmod 4, \\ 1 & \text{otherwise.} \end{cases}$$

Define:

$$\omega_0 = (\sigma_0 - 1 + \sqrt{D_0})/\sigma_0, \text{ and } \Delta_0 = (\omega_0 - \omega_0')^2 = 4D_0/\sigma_0^2,$$

where ω_0' is the *algebraic conjugate* of ω_0, namely

$$\omega_0' = (\sigma_0 - 1 - \sqrt{D_0})/\sigma_0.$$

The value Δ_0 is called a *fundamental discriminant* or *field discriminant* with associated *radicand* D_0, and ω_0 is called the *principal fundamental surd associated with* Δ_0. Let $\Delta = f_\Delta^2 \Delta_0$ for some $f_\Delta \in \mathbb{N}$. If we set

$$g = \gcd(f_\Delta, \sigma_0), \sigma = \sigma_0/g, D = (f_\Delta/g)^2 D_0, \text{ and } \Delta = 4D/\sigma^2,$$

then Δ is called a *discriminant* with associated *radicand* D. Furthermore, if we let

$$\omega_\Delta = (\sigma - 1 + \sqrt{D})/\sigma = f_\Delta \omega_0 + h$$

for some $h \in \mathbb{Z}$, then ω_Δ is called the *principal surd* associated with the discriminant

$$\Delta = (\omega_\Delta - \omega_\Delta')^2.$$

This will provide the canonical basis element for certain rings that we now define.

Let $[\alpha, \beta] = \alpha\mathbb{Z} + \beta\mathbb{Z}$ be a $\mathbb{Z}$-module. Then $\mathcal{O}_\Delta = [1, \omega_\Delta]$, is an *order* in $K = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{D_0})$ with conductor f_Δ. If $f_\Delta = 1$, then $\mathcal{O}_\Delta$ is called the *maximal order in* K. The units of $\mathcal{O}_\Delta$ form a group which we denote by U_Δ. The positive units in U_Δ have a generator which is the smallest unit that exceeds 1. This selection is unique and is called the *fundamental unit of* K, denoted by ε_Δ.

It may be shown that any $\mathbb{Z}$-module $I \neq (0)$ of $\mathcal{O}_\Delta$ has a representation of the form $[a, b + c\omega_\Delta]$, where $a, c \in \mathbb{N}$ with $0 \leq b < a$. We will be concerned only with *primitive* ones, namely those for which $c = 1$. In other words, I is a primitive $\mathbb{Z}$-submodule of $\mathcal{O}_\Delta$ if whenever $I = (z)J$ for some $z \in \mathbb{Z}$ and some $\mathbb{Z}$-submodule J of $\mathcal{O}_\Delta$, then $|z| = 1$. Thus, a canonical representation of a primitive $\mathbb{Z}$-submodule of $\mathcal{O}_\Delta$ is obtained by setting:

$$\sigma a = Q \text{ and } b = (P-1)/2 \text{ if } \sigma = 2, \text{ while } b = P \text{ if } \sigma = 1 \text{ for } P, Q \in \mathbb{Z},$$

namely

$$I = [Q/\sigma, (P + \sqrt{D})/\sigma]. \tag{2.6}$$

Now we set the stage for linking ideal theory with continued fractions by giving a criterion for a primitive $\mathbb{Z}$-module to be a primitive ideal in $\mathcal{O}_\Delta$. A nonzero $\mathbb{Z}$-module I as given in (2.6) is called a primitive $\mathcal{O}_\Delta$-ideal if and only if $P^2 \equiv D \pmod Q$ (see [**7**, Theorem 3.5.1, p. 173]). *Henceforth, when we refer to* *an $\mathcal{O}_\Delta$-ideal it will be understood that we mean a* primitive *$\mathcal{O}_\Delta$-ideal.* Also, the value Q/σ is called the *norm of I*, denoted by $N(I)$. Hence, we see that

$$I \text{ is an } \mathcal{O}_\Delta\text{-ideal if and only if } \alpha = (P + \sqrt{D})/Q \text{ is a quadratic irrational.}$$

When referring to an ideal I of $\mathcal{O}_\Delta$, we call I a *reduced $\mathcal{O}_\Delta$-ideal* if it contains an element $\beta = (P + \sqrt{D})/\sigma$ such that $I = [N(I), \beta]$, where $\beta > N(I)$ and $-N(I) < \beta' < 0$. In fact, the following holds.

Theorem 2.1. *Let Δ be a discriminant with associated radicand D. Then $I = [Q/\sigma, b + \omega_\Delta]$ is a reduced $\mathcal{O}_\Delta$-ideal if $Q/\sigma < \sqrt{\Delta}/2$. Conversely, if I is reduced, then $Q/\sigma < \sqrt{\Delta}$. Furthermore, if $0 \leq b < Q/\sigma$ and $Q > \sqrt{\Delta}/2$, then I is reduced if and only if $Q/\sigma - \omega_\Delta < b < -\omega'_\Delta$.*

Proof. See [**6**, Corollaries 1.4.2–1.4.4, p. 19; pp. 23–28]. □

Now the stage is set for the appearance of the result that formally merges ideals and continued fractions. We only need the notion of the equivalence of two $\mathcal{O}_\Delta$-ideals I and J, denoted by $I \sim J$ to proceed. We write $I \sim J$ to denote the fact that there exist nonzero integers $\alpha, \beta \in \mathcal{O}_\Delta$ such that $(\alpha)I = (\beta)J$, where (x) denotes the principal $\mathcal{O}_\Delta$-ideal generated by $x \in \mathcal{O}_\Delta$. For a given discriminant Δ, the *class group* of $\mathcal{O}_\Delta$ determined by these equivalence classes, denoted by $\mathfrak{C}_\Delta$, is of finite order, denoted by h_Δ, called the *class number* of $\mathcal{O}_\Delta$. Now we may present the *Continued Fraction Algorithm.*

Theorem 2.2. *Suppose that $\Delta \in \mathbb{N}$ is a discriminant, P_j, Q_j are given by* (2.2)–(2.4)*, and*

$$I_j = [Q_{j-1}/\sigma, (P_{j-1} + \sqrt{D})/\sigma]$$

for nonnegative $j \in \mathbb{Z}$. Then $I_1 \sim I_j$ for all $j \in \mathbb{N}$. Furthermore, there exists a least *natural number n such that I_{n+j} is reduced for all $j \geq 0$, and these I_{n+j} are* all *of the reduced ideals equivalent to I_1. If $\ell \in \mathbb{N}$ is the least value such that $I_n = I_{\ell+n}$, then for $j \geq n-1$,*

$$\alpha_j = (P_j + \sqrt{D})/Q_j$$

all have the same period length $\ell = \ell(\alpha_j) = \ell(\alpha_{n-1})$

Proof. See [**7**, Theorem 5.5.2, pp. 261–266]. □

Remark 2.1. From the Continued Fraction Algorithm, we see that if

$$I = [Q/\sigma, (P + \sqrt{D})/\sigma]$$

is a reduced $\mathcal{O}_\Delta$-ideal, then the set

$$\{Q_1/\sigma, Q_2/\sigma, \ldots, Q_\ell/\sigma\}$$

represents the *norms of all reduced ideals equivalent to I.* This is achieved via the simple continued fraction expansion of $\alpha = (P + \sqrt{D})/Q$.

A immediate consequence of the Continued Fraction Algorithm is the following application.

Corollary 2.1. *Let Δ be a discriminant with radicand D and let $c \in \mathbb{N}$ with $c < \sqrt{\Delta}/2$. Then*

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

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.

Also, the following consequence of the Continued Fraction Algorithm is of use in the next section.

Corollary 2.2. *If Δ is a discriminant, and $Q_j/\sigma \neq 1$, in the simple continued fraction expansion of ω_Δ. If Q_j/σ is a squarefree divisor of Δ, then $\ell = \ell(\omega_\Delta = = 2j$. Conversely, if ℓ is even, then $Q_{\ell/2}/\sigma|\Delta$ (where $Q_{\ell/2}/\sigma$ is not necessarily squarefree).*

Proof. See [**5**, Lemma 3.5, p. 831]. □

The following result will be useful in proving the main result in the next section.

Theorem 2.3. *If $D \in \mathbb{N}$ is not a perfect square and $n \in \mathbb{Z}$ such that the Diophantine equation $x^2 - Dy^2 = n$ has a primitive solution $X_0 + Y_0\sqrt{D}$, then there exists a unique element $P_1 \in \mathbb{Z}$ with $-|c|/2 < P_1 \leq |c|/2$ such that*

$$P_1 + \sqrt{D} = (X_0 - Y_0\sqrt{D})(x + y\sqrt{D})$$

for some $x, y \in \mathbb{Z}$ given by

$$x = \frac{X_0P_1 - Y_0D}{n} \quad \text{and} \quad y = \frac{Y_0P_1 - X_0}{n}.$$

Proof. See [**7**, Theorem 6.2.7, pp. 302–303]. □

In the next section we require results on the following well-known sequences. For a quadratic irrational

$$\alpha = \frac{P + \sqrt{D}}{Q} = \langle q_0; q_1, \ldots \rangle,$$

define two sequences of integers $\{A_j\}$ and $\{B_j\}$ inductively by:

$$A_{-2} = 0, A_{-1} = 1, A_j = q_jA_{j-1} + A_{j-2} \quad (\text{for } j \geq 0), \tag{2.7}$$

$$B_{-2} = 1, B_{-1} = 0, B_j = q_jB_{j-1} + B_{j-2} \quad (\text{for } j \geq 0). \tag{2.8}$$

By [**7**, Theorem 5.3.4, p. 246],

$$A_{j-1}^2 - B_{j-1}^2 D = (-1)^j Q_j Q_0 \quad (\text{for } j \geq 1), \tag{2.9}$$

There is also a pretty relationship between these sequences and the fundamental unit given as follows.

Theorem 2.4. *Let $\Delta > 0$ be a discriminant,*

$$I = [Q/\sigma, (P + \sqrt{D})/\sigma]$$

a reduced ideal in $\mathcal{O}_\Delta$, and

$$\alpha = (P + \sqrt{D})/Q.$$

If P_j and Q_j for $j = 1, 2, \ldots, \ell(\alpha) = \ell$ are defined by Equations (2.2)–(2.4) *in the simple continued fraction expansion of α, then*

$$\varepsilon_\Delta = \prod_{i=1}^{\ell} (P_i + \sqrt{D})/Q_i$$

and

$$N(\varepsilon_\Delta) = (-1)^\ell.$$

Also, either

$$\varepsilon_\Delta = A_{\ell-1} + B_{\ell-1}\sqrt{D},$$

or

$$\varepsilon_\Delta^3 = A_{\ell-1} + B_{\ell-1}\sqrt{D}.$$

Proof. See [**6**, Theorems 2.1.3–2.1.4, pp. 51–53]. □

3. Results

In what follows, we will employ the following notation. Given $b \in \mathbb{N}$ not a perfect square, let $T_{1,b} + U_{1,b}\sqrt{b}$ be the fundamental solution of the Pell equation

$$x^2 - by^2 = 1. \tag{3.10}$$

Then the integers $T_{k,b}$ and $U_{k,b}$ are defined by

$$(T_{1,b} + U_{1,b}\sqrt{b})^k = T_{k,b} + U_{k,b}\sqrt{b}.$$

Note that any positive solution $x_0 + y_0\sqrt{b}$ of Equation (3.10) must be a positive power of the fundamental solution. In other words, $x_0 + y_0\sqrt{b} = T_{k,b} + U_{k,b}\sqrt{b}$ for some $k \in \mathbb{N}$ (see for instance [**7**]–[**8**]).

The following generalizes [**9**, Theorem 2.3, pp. 340-341] and [**11**, Theorem 2.1, p. 221].

Theorem 3.1. *Let $a, b, c \in \mathbb{N}$, b not a perfect square, such that the congruence $a^2 \equiv bP^2 \pmod{c}$ is solvable for some integer P, and let $|t| \in \mathbb{N}$ denote the smallest value satisfying $a^2 - bP^2 = ct$. Suppose that either,*

(a) *$a \mid T_{k,b}$ for some $k \in \mathbb{N}$ and $c < a\sqrt{b}$,*
or
(b) *$|t| < a\sqrt{b}$.*

Then the following are equivalent.

(c) *There exists a primitive solution to*

$$|a^2X^2 - bY^2| = c. \tag{3.11}$$

(d) *For some integer $j \geq 0$ in the simple continued fraction expansion of $\sqrt{a^2b}$, $c = Q_j$ when* (a) *holds or $|t| = Q_j$ when* (b) *holds.*

Proof. First assume that (c) holds, so Equation (3.11) has a primitive solution $\alpha = x_0a + y_0\sqrt{b}$. If (a) holds, then $a \mid T_{k,b}$ for some $k \in \mathbb{N}$, so there exist $u, v \in \mathbb{N}$ such that $a^2u^2 - bv^2 = 1$. Therefore, for $D = a^2b$,

$$\pm c = (a^2u^2 - bv^2)(a^2x_0^2 - by_0^2) = (a^2x_0u + bvy_0)^2 - (x_0v + y_0u)^2D.$$

We now show that $X = a^2x_0u + bvy_0$ and $Y = x_0v + y_0u$ provide a primitive solution of $X^2 - DY^2 = \pm c$. Clearly $X, Y \in \mathbb{N}$. If p is a prime dividing both X and Y, then

$$a^2x_0u + bvy_0 = pr, \tag{3.12}$$

and

$$x_0v + y_0u = ps, \tag{3.13}$$

where $r, s \in \mathbb{Z}$. Multiplying a^2u times Equation (3.13) and subtracting v times Equation (3.12), we get,

$$y_0(u^2a^2 - bv^2) = p(sa^2u - rv),$$

but $a^2u^2 - bv^2 = 1$, so $y_0 = p(sa^2u - rv)$. We have shown that $p \mid y_0$. Similarly, by eliminating the y_0 term from both Equations (3.12)–(3.13), it can be shown that $p \mid x_0$, a contradiction to the primitivity of $ax_0 + y_0\sqrt{b}$. Hence, (X, Y) provides a primitive solution of $X^2 - DY^2 = \pm c$. We may therefore invoke Corollary 2.1. Since $c < \sqrt{D}$, then there exists a nonnegative integer j such that $c = Q_j$ in the simple continued fraction expansion of $\sqrt{D}$.

Now assume that (b) holds. Since $a^2x_0^2 - by_0^2 = \pm c$, then for $X_0 = by_0$, $Y_0 = x_0$ and $n = \mp bc$,

$$X_0^2 - DY_0^2 = b^2y_0^2 - ba^2x_0^2 = \mp bc = n,$$

so by invoking Theorem 2.3, we get that there is a unique $P_1 \in \mathbb{Z}$ such that $P_1 + \sqrt{D} = (X_0 - Y_0\sqrt{D})(x + y\sqrt{D})$ where $bP = P_1$ by the minimal choice of P and $|t|$, and

$$x = \frac{X_0P_1 - Y_0D}{n} = \frac{by_0P_1 - x_0a^2b}{\mp bc} = \frac{y_0P_1 - x_0a^2}{\mp c} = \frac{y_0bP - x_0a^2}{\mp c} \in \mathbb{Z},$$

and

$$y = \frac{Y_0P_1 - X_0}{n} = \frac{x_0P_1 - by_0}{\mp bc} = \frac{x_0P_1/b - y_0}{\mp c} = \frac{x_0P - y_0}{\mp c} \in \mathbb{Z}.$$

If $y = 0$, then $x_0P = y_0$ so, since $\gcd(x_0, y_0) = 1$, we must have that $x_0 = 1$ and $y_0 = P$. Therefore, $by_0^2 + ct = a^2$. However, since $a + y_0\sqrt{b}$ is a solution of Equation (3.11) then $a^2 - by_0^2 = \pm c$. Thus, $t = \pm 1$. so $|t| = 1 = Q_0$ in the simple continued fraction expansion of $\sqrt{a^2b}$. Therefore, we may assume that $y \neq 0$.

Since $P_1^2 - D = b^2P^2 - ba^2 = -bct$, then $x^2 - Dy^2 = \pm t$. Now we show that this solution is primitive. If $x = 0$, then $-y^2D = t$, so for $y \neq 0$, this means that $|t| > D$, contradicting that $|t| < \sqrt{D}$. Thus, $x = 0$ implies $y = 0$, a contradiction. Hence, $x \neq 0$. Thus, $|x|, |y| \in \mathbb{N}$. If p is a prime dividing both x and y, then we deduce that both

$$y_0bP - x_0a^2 = cpr, \tag{3.14}$$

for some $r \in \mathbb{Z}$ and

$$x_0P - y_0 = cps, \tag{3.15}$$

for some $s \in \mathbb{Z}$. Multiplying Equation (3.14) by $-x_0$ and adding it to $y_0 b$ times Equation (3.15), we achieve,

$$x_0^2 a^2 - y_0^2 b = cp(sy_0 b - rx_0),$$

but since $x_0^2 a^2 - y_0^2 b = \pm c$, then $p(sy_0 b - rx_0) = \pm 1$, thereby forcing $p \mid 1$, a contradiction. We have shown that $|x| + |y|\sqrt{D}$ is a primitive solution of equation (3.11), so we may invoke Theorem 2.2. Since $|t| < \sqrt{D}$, then there exists a j such that $Q_j = |t|$ in the simple continued fraction expansion of $\sqrt{D}$.

Now we assume the converse, namely that (d) holds. We first dispense with the case where $c = a^2$. In this case, let $U + V\sqrt{D}$ be the fundamental solution of $x^2 - Dy^2 = 1$. Thus, by setting $X = U$ and $Y = Va^2$ we get $aX + Y\sqrt{b}$ is a primitive solution of Equation (3.11). Note that when $c = a^2$, then $P = 0$ and $t = 1$. We may now assume that $c \neq a^2$.

First assume that (a) holds and $Q_j = c$ in the simple continued fraction expansion of $\sqrt{D}$. Since $Q_j = c$, we may use Corollary 2.1 to conclude that there is a primitive solution $x_0 + y_0\sqrt{D}$ to the Diophantine equation $x^2 - Dy^2 = \pm c$. As above $a^2u^2 - v^2 b = 1$ for some $u, v \in \mathbb{N}$, so

$$\pm c = \left(a^2u^2 - v^2 b\right)\left(x_0^2 - Dy_0^2\right) = a^2\left(x_0 u - by_0 v\right)^2 - b\left(vx_0 - a^2 y_0 u\right)^2,$$

which yields a solution $aX + Y\sqrt{b}$ to Equation (3.11) where

$$(X, Y) = (ux_0 - bvy_0, vx_0 - a^2 y_0 u).$$

We must show that it is primitive. If $X = 0$, then $u = bvy_0/x_0$, so

$$1 = a^2u^2 - v^2 b = a^2 b^2 v^2 y_0^2 / x_0^2 - v^2 b,$$

which forces, $(bvy_0/x_0) \mid 1$. Thus, $x_0 = bvy_0$, forcing $y_0 = 1$ and $x_0 = bv$, so $u = 1$. Since $1 = a^2 - v^2 b$ and $b^2v^2 - a^2 b = \pm c$, then $b^2v^2 - (1 + v^2 b) = \pm c$, so $b = c$. However, $bP^2 + ct = a^2$, so $b \mid a^2$. Since $a^2 = 1 + v^2 b$, then this means that $b \mid 1$, a contradiction. We have shown that $X \neq 0$. If $Y = 0$, then $v = a^2 y_0 u / x_0$, so $1 = a^2u^2 - a^4 y_0^2 u^2 b / x_0^2$ forcing $(a^2 u/x_0) \mid 1$. Thus, $x_0 = a^2 u$ and $v = y_0$. Therefore,

$$c = a^2 X^2 = a^2(ux_0 - bvy_0)^2 = a^2(a^2u^2 - bv^2)^2 = a^2,$$

so $c = a^2$, a contradiction. We have shown that $|X|, |Y| \in \mathbb{N}$. It remains to show that $\gcd(X, Y) = 1$. If p is a prime dividing both X and Y, then there are integers r, s such that

$$ux_0 - bvy_0 = pr, \tag{3.16}$$

and

$$vx_0 - a^2 y_0 u = ps. \tag{3.17}$$

multiplying v times Equation (3.16) and subtracting u times Equation (3.17), we get $y_0 = y_0(a^2u^2 - bv^2) = p(rv - su)$, from which we get that $p \mid y_0$. Similarly, we eliminate the y_0 term from both Equations (3.16)–(3.17) and we get that $p \mid x_0$, contradicting the primitivity of $x_0 + y_0\sqrt{D}$.

Now assume that (b) holds and $|t| = Q_j$ in the simple continued fraction expansion of $\sqrt{D}$. Thus, by Corollary 2.1, there is a primitive solution $x_0 + y_0\sqrt{D}$ to the Diophantine equation $X^2 - DY^2 = \pm t$. By Theorem 2.3 there is a unique $P_1 \in \mathbb{Z}$ such that $P_1 + \sqrt{D} = (x_0 - y_0\sqrt{D})(x + y\sqrt{D})$ where $P_1 = Pb$ by the minimal choice of $|t|$,

$$x = \frac{x_0 P_1 - y_0 D}{\pm t} = \frac{x_0 Pb - y_0 D}{\pm t} \in \mathbb{Z},$$

and

$$y = \frac{y_0 P_1 - x_0}{\pm t} = \frac{y_0 Pb - x_0}{\pm t} \in \mathbb{Z}.$$

Since $P_1^2 - D = -bct$, then $x^2 - Dy^2 = \pm bc$. Hence,

$$b(x/b)^2 - y^2a^2 = \pm c, \tag{3.18}$$

which yields a solution to Equation (3.11). It remains to show that this is a primitive solution. If $y = 0$, then $y_0 bP = x_0$, so by the relative primality of x_0 and y_0, this means that $y_0 = 1$ and $x_0 = bP$. Therefore, since $a^2b = b^2P^2 + bct$ by hypothesis,

$$\pm t = x_0^2 - a^2b = b^2P^2 - b^2P^2 - bct = -bct,$$

so $b = 1$, a contradiction to the fact that b is not a perfect square. Thus, $y \neq 0$. If $x = 0$, then by Equation (3.18), $a^2y^2 = c$. However, $x = 0$ also means that $y_0 = x_0P/a^2$ from the definition of x, so

$$\pm t = x_0^2 - Dy_0^2 = x_0^2 - bx_0^2P^2/a^2 = x_0^2(1 - bP^2/a^2) = x_0^2ct/a^2.$$

Thus, $x_0^2c = a^2$. Since $a^2y^2 = c$, this means that $x_0^2a^2y^2 = a^2$, so $x_0 = |y| = 1$ and $c = a^2$, a contradiction. We have shown that $|x|, |y| \in \mathbb{N}$. It remains only to prove that x and y are relatively prime. If p is a prime dividing both x and y, then there exist $r, s \in \mathbb{Z}$ such that

$$x_0 bP - y_0 a^2 b = tpr, \tag{3.19}$$

and

$$y_0 bP - x_0 = tps. \tag{3.20}$$

Multiplying Equation (3.19) by y_0 and subtracting x_0 times Equation (3.20), we get

$$\pm t = x_0^2 - y_0^2 D = t(ry_0 - sx_0)p,$$

from which it follows that $p \mid 1$, a contradiction that secures the result. □

When $a = c = 1$, we always have a solution of the Pell Equation (3.11) since $c = 1 = Q_0$ in the simple continued fraction expansion of $\sqrt{b}$. However, when $c = 1 \neq a$, then a little more can be said.

Corollary 3.1. *If $a, b \in \mathbb{N}$ with b not a perfect square, then*

$$a^2X^2 - bY^2 = 1 \tag{3.21}$$

has a solution if and only if $a \mid T_{k,b}$ for some $k \in \mathbb{N}$.

Proof. If $a \mid T_{k.b}$ for some $k \in \mathbb{N}$, then by Theorem 3.1, Equation (3.21) has a solution. Conversely, if $ax_0 + y_0\sqrt{b}$ is a solution of the equation, then by the discussion preceding the theorem, $ax_0 + y_0\sqrt{b} = T_{k,b} + U_{k,b}\sqrt{b}$ for some $k \in \mathbb{N}$. Hence, $a \mid T_{k,b}$. □

Remark 3.1. Corollary 3.1 is a well-known result (see [**13**] for example). In fact, it can be shown that if $ax_0 + y_0\sqrt{b}$ is the fundamental solution of Equation (3.21), then all positive solutions of (3.21) are given by $(ax_0 + y_0\sqrt{b})^{2k-1}$ for all $k \in \mathbb{N}$. In general, if $A > 1$, $B > 1$, and $\sqrt{A}x + \sqrt{B}y$ is a primitive solution of $Ax^2 - By^2 = 1$, then there exists a $j \geq 0$ such that

$$\sqrt{A}x + \sqrt{B}y = (T_{1,AB} + U_{1,AB}\sqrt{AB})^{2j+1},$$

(see [**13**, Theorem 4, p. 506]).

The following immediate consequence of Theorem 3.1 is an extension of the ideas expressed in Corollary 2.1.

Corollary 3.2. *Suppose that D is a radicand, $c \in \mathbb{N}$ with $DP^2 \equiv 1 \pmod{c}$ solvable for some integer P with $|t| \in \mathbb{N}$ the smallest value such that $1 - DP^2 = ct$ with $c|t| < D$. Then $|X^2 - DY^2| = c$ has a primitive solution if and only if either c or $|t|$ is equal to Q_j for some $j \geq 0$ in the simple continued fraction expansion of $\sqrt{D}$.*

Example 3.1. Let $D = 45$ and $c = 11$, then $P = 1$ and $t = -4$. Then

$$|X^2 - 45Y^2| = 11$$

has a primitive solution since $|t| < \sqrt{D} = \sqrt{45}$ and $|t| = 4 = Q_2$ in the simple continued fraction expansion of $\sqrt{45}$. One such solution is given by $67^2 - 45 \cdot 10^2 = = -11$.

The following consequence of Theorem 3.1 has some connections to well-known problems (see Remark 3.2 below).

Corollary 3.3. *If $D \equiv 1 \pmod{4}$ is a radicand, then*

$$|X^2 - DY^2| = 4$$

has a primitive solution if and only if $4 = Q_j$ for some $j > 0$ in the simple continued fraction expansion of $\sqrt{D}$.

Proof. If $D \geq 17$, then $c = 4 < \sqrt{D}$ and $a = 1 \mid T_{1,D}$, so Theorem 3.1 applies and we are done. If $D < 17$, then $(D - 1)/4 = t < \sqrt{D}$ and $P = 1$ in Theorem 3.1. When $D = 5$, $t = 1 = Q_0$ in the simple continued fraction expansion of $\sqrt{5}$ and when $D = 13$, $t = 3 = Q_2$ in the simple continued fraction expansion of $\sqrt{13}$, so by Theorem 3.1, we have secured the proof. □

Remark 3.2. There is an underlying interplay between quadratic orders that we have not yet addressed. In the above, we have been tacitly assuming that we are working in the order $\mathbb{Z}[\sqrt{a^2b}]$, which means that the underlying discriminant is $\Delta = 4a^2b$. For instance, if $a = 1$, $b = 65$, $c = 4$, $t = -16$, and $P = 1$, then by Theorem 3.1

$$X^2 - 65Y^2 = \pm 4$$

has no primitive solutions, since $c < \sqrt{a^2b} = \sqrt{65}$, but $c \neq Q_j$ in the simple continued fraction expansion of $\sqrt{65}$. In fact, since $\ell(\sqrt{65}) = 1$, then the only such Q_j is $Q_0 = Q_1 = 1$. Thus, by Theorem 2.2, there can be no primitive, principal ideal of norm 4 in $\mathbb{Z}[\sqrt{65}]$. On the other hand, by Theorem 2.2, in the maximal order $\mathbb{Z}\left[(1+\sqrt{65})/2\right]$ we have a primitive ideal of norm 4 since $4 = Q_1/2$ in the simple continued fraction expansion of $(1+\sqrt{65})/2$. By Corollary 2.1, this means that $X^2 - 65Y^2 = \pm 16$ has a primitive solution. In fact, $X = 7$, $Y = 1$ yields $X^2 - 65Y^2 = -16$. Note that $[4, (7+\sqrt{65})/2]$ is a principal ideal of norm 4 in $\mathbb{Z}\left[(1+\sqrt{65})/2\right]$.

By Corollary 3.3, if $D \equiv 1 \pmod 4$ is a radicand, then

$$|X^2 - DY^2| = 4 \tag{3.22}$$

has a primitive solution if and only if $Q_j = 4$ for some $j > 0$ in the simple continued fraction expansion of $\sqrt{D}$, and this in turn is tantamount to saying that $[4, 1+\sqrt{D}]$ is a principal ideal in $\mathbb{Z}[\sqrt{D}]$, by Theorem 2.2. Observe that in the above illustration, $[4, 1+\sqrt{65}]$ is *not* principal in $\mathbb{Z}[\sqrt{65}]$.

When $D \equiv 5 \pmod 8$ is a radicand, then Equation (3.22) has a primitive solution if and only if the fundamental unit ε_D of $\mathbb{Z}[(1+\sqrt{D})/2]$ is *not* in $\mathbb{Z}[\sqrt{D}]$. This is related to a problem of Eisenstein, also investigated by Gauss (see [**6**, pp. 59–61] for details). In general, if $D \equiv 1 \pmod 4$, if the (more specific) equation $X^2 - DY^2 = -4$ has a primitive solution, then ε_D is not in $\mathbb{Z}[\sqrt{D}]$, but the converse fails. For instance, if $D = 21$, then $\varepsilon_{21} = (5+\sqrt{21})/2 \notin \mathbb{Z}[\sqrt{21}]$, but $X^2 - 21Y^2 = -4$ has *no* primitive solution. However, it is clear that for $D \equiv 1 \pmod 4$, $x^2 - Dy^2 = -4$ has a primitive solution if and only if $\varepsilon_D \notin \mathbb{Z}[\sqrt{D}]$ and $N(\varepsilon_D) = -1$.

Example 3.2. Let $a = 3$, $b = 85$, $c = 4$, $t = -19$, and $P = 1$. Then $|t| = 19 = Q_2$ in the simple continued fraction expansion of $\sqrt{765} = \sqrt{a^2b}$. Thus, by Theorem 3.1, $9X^2 - 85Y^2 = \pm 4$ has a primitive solution. In fact, $X = 3$, $Y = 1$ provides a primitive solution to $9X^2 - 85Y^2 = -4$. Notice that, although $c = Q_4 = 4$ in $\sqrt{765}$, $a = 3$ does not divide $T_{k,85}$ for any $k \in \mathbb{N}$. The reason is that

$$T_{1,85} + U_{1,85}\sqrt{85} = 285769 + 30996\sqrt{85},$$

so $3 \mid U_{1,85}$. Thus, $3 \nmid T_k$ for all $k \in \mathbb{N}$ since $U_{1,85} \mid U_{k,85}$ for all $k \in \mathbb{N}$ (see [**7**, Exercise 6.5.13, p. 355]). Hence (a) of Theorem 3.1 fails, which is the reason for invoking the theorem via (b) above.

With reference to the problems discussed in Remark 3.2, notice that $D = a^2b = 765 \equiv 5 \pmod 8$ and $\varepsilon_{765} = (83 + 3\sqrt{765})/2 \notin \mathbb{Z}[\sqrt{765}]$.

Example 3.3. Let $a = 3$, $b = 19$, $c = 5$, $t = -2$, and $P = 1$. Since $3 \nmid T_{k,19}$ for any $k \in \mathbb{N}$, given that $\varepsilon_{19} = 170 + 39\sqrt{19}$ with $3 \mid U_{1,19}$ (see the argument in Example 3.2), and $|t| = 2 = Q_1$ in the simple continued fraction expansion

expansion of $\sqrt{171} = \sqrt{a^2 b}$, then we invoke Theorem 3.1 via (b) to get that $9X^2 - 19Y^2 = \pm 5$ has a primitive solution. In fact, $X = 3$, $Y = 2$ provides a primitive solution of $9X^2 - 19Y^2 = 5$.

The following shows that conditions (a)–(b) in Theorem 3.1 are essential for the equivalence of (c)–(d). In other words, the equivalence of (c)–(d) *fails* in the absence of one of (a) or (b) holding, so that we *cannot* dispense with conditions (a)–(b) in the hypothesis.

Example 3.4. Let $a = 3$, $b = 19$ and $c = 17$. Then $P = 8$ and $t = -71$. Since $a = 3 \mid U_{1,19} = 39$, then 3 cannot divide $T_{k,19}$ for any $k \geq 0$ since (see the argument in Example 3.2). Thus, (a) of Theorem 3.1 fails to hold. Also, $|t| > a\sqrt{b} = 3\sqrt{19}$, so (b) of Theorem 3.1 fails to hold as well. Yet,

$$a^2X^2 - bY^2 = 9X^2 - 19Y^2 = 17 = c,$$

has the primitive solution $X = 2$, $Y = 1$ and there does not exist any $j \geq 0$ such that either c or $|t|$ equals any Q_j in the simple continued fraction expansion of $\sqrt{D} = a\sqrt{b} = \sqrt{171}$. In fact, the only such Q_j are $Q_0 = Q_2 = 1$ and $Q_1 = 5$ since $\ell(\sqrt{171}) = 2$.

The following illustrates that Theorem 3.1 fails without the hypothesis on the solvability of the congruence $a^2 \equiv bP^2 \pmod{c}$. Note that, as shown in [**12**, pp. 164–169], the existence of a solution to the congruence is necessary and sufficient for the existence of a solution to $a^2x^2 - by^2 = ct$ for some integer t with $|t| < a\sqrt{b}$.

Example 3.5. If $a = 7$, $b = 3$, and $c = 5$, then

$$7^2X^2 - 3Y^2 = \pm 5$$

has no solutions since there is no integer P such that $3P^2 \equiv 49 \pmod{5}$, given that the Legendre symbol $(3/5) = -1$. Also, $c = 5 < 7\sqrt{3} = a\sqrt{b}$, and $a = 7 \mid T_{2,3} =$ $= 7 = T_{2,b}$, namely even in the presence of the satisfaction of (a) in Theorem 3.1, we do not have a solution of the displayed equation.

The following illustrates the case where (a) does not hold, but (b) does in Theorem 3.1.

Example 3.6. Let $a = 5$, $b = 3$, $c = 22$, $P = 1$, and $t = 1$. We have that $c = 22 > 5\sqrt{3}$, so (a) fails, but $t = 1 < a\sqrt{b}$ so (b) holds. Since $t = Q_0 = 1$ in the simple continued fraction expansion of $\sqrt{75} = a\sqrt{b}$, then by Theorem 3.1,

$$a^2X^2 - bY^2 = 25X^2 - 3Y^2 = 22 = c,$$

has a primitive solution, the smallest positive of which is given by $X = Y = 1$.

The following illustrates the case where (a) holds but (b) fails.

Example 3.7. Let $a = 13$, $b = 5719$, $c = 3$, $P = 1$, and $t = -1850$. Since $|t| = 1850 > 13\sqrt{3} = a\sqrt{b}$, then (b) of Theorem 3.1 fails. However, $c = 3 < a\sqrt{b}$ and $a = 13 \mid T_{3,5719}$ whose prime factorization is given by

$$T_{3,5719} = 13 \cdot 73 \cdot 3090595037619968783 \cdot 491670203565799 \cdot 329685203,$$

where, for interests sake,

$$T_{1,b} + U_{1,b}\sqrt{b} = 491670203565799 + 6501504110940\sqrt{5719},$$

with both $T_{1,b}$ and $T_{2,b}$ prime. Since $c = Q_{69} = 3$ in the simple continued fraction expansion of $a\sqrt{b} = \sqrt{966511}$ (where $\ell(\sqrt{966511}) = 156$), then by Theorem 3.1,

$$a^2X^2 - bY^2 = 169X^2 - 5719Y^2 = -3 = -c$$

has a primitive solution, one of which is given by $X = 104018$ and $Y = 17881$.

Example 3.7 is related to another problem involving continued fractions and solutions of Diophantine equations investigated by the first author, A. J. van der Poorten, and H. C. Williams (see [**6**, pp. 96–104], especially [**6**, Example 3.5.3, p. 101]).

The following is an instance where both (a) and (b) hold in Theorem 3.1.

Example 3.8. Let $a = 7$, $b = 13$, $c = 9$, $P = 1$, and $t = 4$. Here $c = 9 < 7\sqrt{13} = a\sqrt{b}$ and $7 \mid T_{2,13} = T_{2,b} = 842401 = 7 \cdot 17 \cdot 7079$, where $T_{1,13} + U_{1,13}\sqrt{13} = 649 + 180\sqrt{13}$, so (a) holds. Also, $t = 4 < a\sqrt{b}$, so (b) holds as well. Moreover, $c = 9 = Q_2$ and $t = 4 = Q_8$ in the simple continued fraction expansion of $a\sqrt{b} = \sqrt{637}$. Thus, by Theorem 3.1,

$$a^2X^2 - bY^2 = 49X^2 - 13Y^2 = 9,$$

has a primitive solution. One such solution is $X = 5363$ and $Y = 10412$.

In the examples thus far, we have had relative primality between a, b, and c. Now we illustrate an interesting case covered by Theorem 3.1, where the gcds are not 1.

Example 3.9. Let $a = 9$, $b = 5$, $c = 81$, so $t = 1$ and $P = 0$. Then,

$$a^2X^2 - bY^2 = 9^2X^2 - 5Y^2 = 81 = c = a^2$$

has the primitive solution $X = 161$, $Y = 648$. In this case, (b) of Theorem 3.1 holds since $|t| < a\sqrt{b} = 9\sqrt{5}$, and of course $t = Q_0 = 1$ in the simple continued fraction expansion of $\sqrt{D} = \sqrt{405} = \sqrt{a^2b}$.

Notice as well in this example that if t is not minimally chosen, for instance $t = -4$ and $P = 9$, then $|t| \neq Q_j$ for any $j \geq 0$ in the simple continued fraction expansion of $\sqrt{405}$ since $Q_0 = 1 = Q_2$ and $Q_1 = 5$ given that $\ell(\sqrt{405}) = 2$.

Of course, what underlies this example, when we divide through the displayed equation by 81, is that $161^2 - 72^2 \cdot 5 = 1$. Here $161 + 72\sqrt{5} = ((1+\sqrt{5}))/2)^2$ where $(1 + \sqrt{5})/2$ is the fundamental unit of $\mathbb{Z}[(1 + \sqrt{5})/2]$. Numerous similar examples may be depicted with underlying fundamental units. For instance, if $a = 7 \cdot 13$ and $b = c = 13$, then

$$7^2 \cdot 13^2 \cdot 56233877040^2 - 13 \cdot 1419278889601^2 = -13,$$

where
$$\left(\frac{14159 + 561\sqrt{7^2 \cdot 13}}{2}\right)^3 = 1419278889601 + 56233877040\sqrt{7^2 \cdot 13},$$

and $(14159 + 561\sqrt{7^2 \cdot 13})/2$ is the fundamental unit of $\mathbb{Z}[(1 + \sqrt{7^2 \cdot 13})/2]$.

Example 3.10. If $a = 3$, $b = 65$, $c = 8$, $t = -7$, and $P = 1$, then $c = 8 < < 3\sqrt{65} = a\sqrt{b}$, $3 \mid T_{2,65} = 129$, and $|t| = 7 < a\sqrt{b}$, so (a)–(b) of Theorem 3.1 are satisfied. However,

$$9X^2 - 65Y^2 = \pm 8$$

is not solvable since $8 = c \neq Q_j$ and $7 = |t| \neq Q_j$ for any $j \geq 0$ in the simple continued fraction expansion of $a\sqrt{b} = \sqrt{585}$. Note, however, that

$$9X^2 - 65Y^2 = -56 \tag{3.23}$$

is solvable since, in this case $c = 56$, $P = 1$, and $t = -1$, so $|t| = Q_0$ in the simple continued fraction expansion of $\sqrt{585}$, the smallest positive solution being $X = Y = 1$. Observe that the only Q_j in the simple continued fraction expansion of $\sqrt{585}$ are $Q_0 = 1$, $Q_1 = 9 = Q_4$, $Q_2 = 16$, and $Q_3 = 29$ since $\ell(\sqrt{585}) = 8$.

Remark 3.3. Notice in Example 3.10, the solution to Equation (3.23) given by $X = Y = 1$ is also a solution to $9X^4 - 65Y^2 = -56$. Recent developments in the related Diophantine equation

$$a^2X^4 - bY^2 = 1 \tag{3.24}$$

are given as follows. Bennet and Walsh [**1**] have shown that Equation (3.24) has at most one solution and if that solution exists, then the least value of $k \in \mathbb{N}$ such that $a \mid T_{k,b}$ must satisfy that $T_{k,b} = am^2$ for some $m \in \mathbb{N}$. Thus, for instance, $9X^4 - 65Y^2 = 1$ cannot have a solution since, as shown in Example 3.10, $T_{2,b} = T_{2,65} = 129 = 3 \cdot 43$. Similarly, the Diophantine equation

$$a^2X^2 - bY^4 = 1 \tag{3.25}$$

has been shown by Walsh [**14**], as an extension of work by Ljunggren [**4**], to have at most one solution $X, Y \in \mathbb{N}$ and if it exists, then given the positive solution $u\sqrt{a} + v\sqrt{b}$ of $aX^2 - bY^2 = 1$,

$$X\sqrt{a} + Y\sqrt{b} = (u\sqrt{a} + v\sqrt{b})^\ell,$$

where $v = k^2\ell$, with ℓ is odd and squarefree. For instance, in Example 3.10, $3u^2 - 65v^2 = 1$ can have no solution since $9X^2 - 65Y^4 = 1$ has no solution.

It would be of great interest and value to extend this work to solutions of the more general equations $a^2X^4 - bY^2 = c$ and $a^2X^2 - bY^4 = c$ for given $c \in \mathbb{Z}$ in terms of continued fractions as we have for the case $a^2X^2 - bY^2 = c$ above.

In [**11**], we looked not only at the Diophantine equation studied above, but also the relationship between solutions of them in the following sense. The next result substantially generalizes [**11**, Theorem 2.3, p. 222].

Theorem 3.2. *Suppose that $D = ab$ is an odd radicand, $c \in \mathbb{N}$ is odd, and* $\gcd(a, c) = 1 = \gcd(b, c)$. *Then if the Diophantine equation*

$$ax^2 - by^2 = \pm 4c \tag{3.26}$$

has a primitive solution so does the Diophantine equation

$$aX^2 - bY^2 = \pm c^3. \tag{3.27}$$

Proof. If Equation (3.26) has a primitive solution $x\sqrt{a} + y\sqrt{b}$, then set

$$X = \frac{x(ax^2 \mp 3c)}{2} \qquad \text{and} \qquad Y = \frac{y(ax^2 \mp c)}{2}.$$

Since a, b, c are odd, then x cannot be even given that $x\sqrt{a} + y\sqrt{b}$ is a primitive solution of (3.26) and $\gcd(a, c) = \gcd(b, c) = 1$. Thus, $X, Y \in \mathbb{Z}$. We have,

$$(a^2x^2 - Dy^2)^3 = (ax(a^2x^2 + 3Dy^2))^2 - D(y(3a^2x^2 + Dy^2))^2 = \pm 64a^3c^3.$$

Moroever,

$$ax(a^2x^2 + 3Dy^2) = ax(4a^2x^2 - 3(a^2x^2 - Dy^2)) = ax(4a^2x^2 \mp 12ac) =$$
$$4a^2x(ax^2 \mp 3c) = 8a^2X,$$

and

$$y(3a^2x^2 + Dy^2) = y(4a^2x^2 - (a^2x^2 - Dy^2)) = y(4a^2x^2 \mp 4ac) =$$
$$4ay(ax^2 \mp c) = 8aY.$$

Hence,

$$\pm 64a^3c^3 = (8a^2X)^2 - D(8aY)^2,$$

so

$$\pm c^3 = aX^2 - bY^2. \tag{3.28}$$

It remains to show that $X\sqrt{a} + Y\sqrt{b}$ is a primitive solution. If a prime p divides both X and Y, then by (3.28), $p \mid c$. Since $p \mid X$ and $\gcd(a, c) = 1$, then $p \mid x$. By (3.26), $p \mid b$ or $p \mid y$, both of which are contradictions since $\gcd(b, c) = 1 = \gcd(x, y)$. $\square$

The following is immediate as the special case where $c = 1$.

Corollary 3.4. ([**11**, Theorem 2.3, p. 222]) *If $D = ab$ is an odd radicand and $ax^2 - by^2 = \pm 4$ has a solution, then $aX^2 - bY^2 = \pm 1$ has a (primitive) solution.*

Example 3.11. A primitive solution of $5x^2 - 161y^2 = -4$ is given by $(x, y) = (17, 3)$. By Corollary 3.4, there must be a solution to $5X^2 - 161Y^2 = \pm 1$. Indeed, $X = 12308$, and $Y = 2169$ provides a solution to $5X^2 - 161Y^2 = -1$.

Example 3.12. A primitive solution of $17x^2 - 5y^2 = -12$ is given by $(x, y) = (7, 13)$. By Theorem 3.2, there must be a primitive solution to $17X^2 - 5Y^2 = \pm 27$. Such a solution is given by $(X, Y) = (77, 142)$, which yields $17 \cdot 77^2 - 5 \cdot 142^2 = -27$.

The following consequence is the result of Gauss cited in the introduction.

Corollary 3.5. (Gauss [**2**, Article 187, p. 156])
Suppose that $\Delta = D$ is a fundamental discriminant. Then $N(\varepsilon_\Delta) = -1$ if and only if

$$|ax^2 - by^2| = 4 \tag{3.29}$$

has no primitive solution where $D = ab$ unless either $a = 1$ or $b = 1$.

Proof. Suppose that $N(\varepsilon_\Delta) = -1$ and Equation (3.29) has a primitive solution with $D = ab$. Thus, by Corollary 3.4, $ax^2 - by^2 = \pm 1$ has a solution, so $(ax)^2 - -Dy^2 = \pm a$, where we may assume without loss of generality that $a < \sqrt{D}$. Hence, by Theorems 2.1–2.2, $I = [a, \sqrt{D}]$ is a reduced principal ideal in $\mathbb{Z}[\sqrt{D}]$, and $a = Q_j$ for some $j \geq 0$ in the simple continued fraction expansion of $\sqrt{D}$. If $j > 0$, then by Corollary 2.2, $\ell(\sqrt{D}) = 2j$. Thus, by Theorem 2.4, $N(\varepsilon_\Delta) = (-1)^\ell = 1$, a contradiction, so $a = 1$. We have shown that if $N(\varepsilon_\Delta) = -1$, then Equation (3.29) has no primitive solution with $D = ab$ unless $a = 1$ or $b = 1$, since the latter will occur under the assumption that $b < \sqrt{D}$ in the above argument.

Conversely, assume that Equation (3.29) has no primitive solution with $D = ab$ unless $a = 1$ or $b = 1$. We need to show that $N(\varepsilon_\Delta) = -1$. Suppose that $N(\varepsilon_\Delta) = 1$. Then by Theorem 2.4, $\ell = \ell(\omega_\Delta)$ is even. Thus, by Corollary 2.2, $Q_{\ell/2}/2 \mid \Delta$. Hence, by Theorem 2.2 and Corollary 2.1, there exist $x, y \in \mathbb{Z}$ such that $x^2 - Dy^2 = \pm 4a$, where $a = Q_{\ell/2}/2$. Since $a \mid \Delta = D$, then $aX^2 - by^2 = \pm 4$ where $X = x/a$ and $b = D/a$. By hypothesis, $a = 1$ or $b = 1$. However, $a \neq 1$ since $a = Q_{\ell/2}/2$ is the *middle* of the period. Therefore, $b = 1$, so $D = a = Q_{\ell/2}/2$. However, by the inequalities in (2.5), $D = a < 2\sqrt{D}$, a contradiction. □

Example 3.13. Since $|13x^2 - 5y^2| = 4$ has no primitive solution, then, $N(\varepsilon_{65}) = -1$.

Remark 3.4. Theorem 3.2 dealt with the solvability of two related Diophantine equations. Another similar question that arises is the related solvability of the two Diophantine equations $a^2x^2 - by^2 = c \in \mathbb{N}$ and $a^2x^2 - by^2 = -c$. In [**10**, Corollary 4. p. 282], it is it incorrectly claimed that both of them cannot have primitive solutions when $\ell(\sqrt{b})$ is even. A counterexample is given by $1^2 - 34 = -33$ and $13^2 - 2^2 \cdot 34 = 33$, where $\ell(\sqrt{34})$ is even. However, the following does provide a situation where the parity of $\ell(\sqrt{D})$ is necessary and sufficient.

Theorem 3.3. *Suppose that D is an integer, which is not a perfect square, and c is an integer such that $|c| = 1$ or $|c|$ is a prime not dividing D. If*

$$x^2 - Dy^2 = c \tag{3.30}$$

has a primitive solution, then

$$X^2 - DY^2 = -c \tag{3.31}$$

has a primitive solution if and only if $\ell(\sqrt{D})$ is odd.

Proof. If $\ell(\sqrt{D})$ is odd, then by Theorem 2.4, $N(\varepsilon_\Delta) = -1$ where $\Delta = 4D$. Thus, there exist integers u, v such that $u^2 - Dv^2 = -1$. Therefore, if $x_0 + y_0\sqrt{D}$ is a primitive solution of Equation (3.30), then

$$(x_0 + y_0\sqrt{D})(u + v\sqrt{D}) = (x_0u + y_0vD) + (uy_0 + vx_0)\sqrt{D}$$

is a primitive solution of Equation (3.31).

Conversely, suppose that both Equations (3.30)–(3.31) have primitive solutions, say $\alpha_0 = x_0 + y_0\sqrt{D}$ and $\beta_0 = X_0 + Y_0\sqrt{D}$ respectively. If $|c| = 1$, then by

Theorem 2.4, $\ell(\sqrt{D})$ is odd, so we may assume that $|c|$ is a prime p. In fact, we will assume that $c = p$ without loss of generality. Then $N(\alpha_0/\beta_0) = -1$, where

$$\frac{\alpha_0}{\beta_0} = \frac{x_0 + y_0\sqrt{D}}{X_0 + Y_0\sqrt{D}} = \frac{(x_0 + y_0\sqrt{D})(X_0 - Y_0\sqrt{D})}{X_0^2 - Y_0^2 D} =$$

$$\frac{(x_0X_0 - y_0Y_0D) + (y_0X_0 - x_0Y_0)\sqrt{D}}{-p}.$$

However, X_0^2 times $x_0^2 - y_0^2 D = p$ minus x_0^2 times $X_0^2 - Y_0^2 D = -p$ yields,

$$D(Y_0^2 x_0^2 - y_0^2 X_0^2) = p(X_0^2 + x_0^2),$$

so since $\gcd(p, D) = 1$, then either

$$p \mid (Y_0x_0 - y_0X_0) = Y_1 \text{ or } p \mid (y_0X_0 + Y_0x_0) = Y_2.$$

If $p \mid Y_1$, then $p \mid X_1$ where $X_1 = (x_0X_0 - y_0Y_0D)$ since,

$$N(X_1^2 - Y_1^2 D) = -p^2.$$

Therefore, $N((X_1/p)^2 - (Y_1/p)^2 D) = -1$. Hence, $N(\varepsilon_\Delta) = -1$, which implies by Theorem 2.4, that $\ell(\sqrt{D})$ is odd. Now we may assume that $p \mid Y_2$. Since $N(\alpha_0/\beta_0') = -1$, where

$$\frac{\alpha_0}{\beta_0'} = \frac{x_0 + y_0\sqrt{D}}{X_0 - Y_0\sqrt{D}} = \frac{(x_0 + y_0\sqrt{D})(X_0 + Y_0\sqrt{D})}{-p} =$$

$$\frac{(x_0X_0 + y_0Y_0D) + (x_0Y_0 + y_0X_0)\sqrt{D}}{-p} = \frac{(x_0X_0 + y_0Y_0D) + Y_2\sqrt{D}}{-p},$$

so, $p \mid (x_0X_0 + y_0Y_0D) = Y_3$. Thus,

$$-1 = N(\alpha_o/\beta_0') = N((Y_3/p) + (Y_2/p)\sqrt{D}),$$

so as above $N(\varepsilon_\Delta) = -1$ and $\ell(\sqrt{D})$ is odd. $\square$

Example 3.14. Let $D = 34$ and $c = 47$. Then $x^2 - 34y^2 = 47$ has the primitive solution given by $x = 9$ and $y = 1$. However, $x^2 - 34y^2 = -47$ has no solution since $\ell(\sqrt{34}) = 4$.

Example 3.15. Let $D = 65$ and $c = 29$. Then $x^2 - 65y^2 = -29$ has the primitive solution given by $x = 6$ and $y = 1$. Also, $x^2 - 65y^2 = 29$ has the primitive solution given by $x = 17$ and $y = 2$. Here $\ell(\sqrt{65}) = 1$.

Example 3.16. Let $D = 845$ and $p = 29$. Then $x^2 - 845y^2 = -29$ has the primitive solution given by $x = 436$ and $y = 15$. Also, $x^2 - 845y^2 = 29$ has the primitive solution given by $x = 407$ and $y = 14$. Here $\ell(\sqrt{845}) = 5$.

As seen by the counterexample in Remark 3.4, Theorem 3.3 is the best we can hope for in this regard since thecounterexample employs a value c with only two prime factors. It would of course be most valuable to find a general criterion for the mutual solvability of the two Diophantine equations $AX^2 - BY^2 = C$ and $Ax^2 - By^2 = -C$ for $A, B, C \in \mathbb{N}$.

Acknowledgment. The first author's research is supported by NSERC Canada grant # A8484, which also supports the second author, his graduate student. The third author wishes to express thanks to the University of Calgary for a pleasant working environment during his visit in the summer of 2001, when this research was carried out.

References

1. Bennett M. A. and Walsh G., *The Diophantine equation* $b^2X^4 - dY^2 = 1$, Proceed. Amer. Math. Soc. **127** (1999), 3481–3491.
2. Gauss C. F., *Disquisitiones Arithmeticae*, Springer-Verlag, (English edition) Berlin 1985.
3. Kaplan P. and Williams K. S., *Pell's equations* $x^2 - my^2 = -1, -4$ *and continued fractions*, J. Number Theory **23** (1986), 169–182.
4. Ljunggren W., *Ein Satz über die Diophantische Gleichung* $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$, Tolfte Skand. Matemheikerkongressen, Lund, 1953 (1954), 188–194.
5. Louboutin S., Mollin R. A., and Williams H. C., *Class numbers of real quadratic fields, continued fractions, reduced ideals, prime-producing quadratic polynomials, and quadratic residue covers*, Canad. J. Math., **44** (1992), 824–842.
6. Mollin R. A., *Quadratics*, CRC Press, Boca Raton, New York, London, Tokyo 1996.
7. Mollin R. A., *Fundamental Number Theory with Applications*, CRC Press, Boca Raton, New York, London, Tokyo 1998.
8. Mollin R. A., *Algebraic Number Theory*, Chapman and Hall/CRC, Boca Raton, New York, London, Tokyo 1999.
9. Mollin R. A., *Jacobi symbols, ambiguous ideals, and continued fractions*, Acta Arith. **LXXXV** (1998), 331–349.
10. Mollin R. A., *All solutions of the Diophantine equation* $x^2 - Dy^2 = n$, Far East J. Math. Sci., Special Volume (1998), Part III, 257–293.
11. Mollin R. A. and van der Poorten A. J., *Continued fractions, Jacobi symbols, and quadratic Diophantine equations*, Canad. Math. Bull. **43** (2000), 218–225.
12. Mordell L. J., *Diophantine Equations*, Academic Press, London and New York, (1969).
13. Walker D. T., *On the Diophantine equation* $mX^2 - nY^2 = \pm 1$, Amer. Math. Monthly **74** (1967), 504–513.
14. Walsh P. G., *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.
15. Williams H. C., *Eisenstein's problem and continued fractions*, Utilitas Math. **37** (1990), 145–158.

R. A. Mollin, Department of Mathematics and Statistics, University of Calgary, Calgary, Alberta, Canada, T2N 1N4, *e-mail*: `ramollin@math.ucalgary.ca`,
`http://www.math.ucalgary.ca/~ ramollin/`

K. Cheng, Department of Mathematics and Statistics, University of Calgary, Calgary, Alberta, Canada, T2N 1N4, *e-mail*: `khfcheng@math.ucalgary.ca`

B. Goddard, Mathematics Department, Concordia University at Austin, Austin, Texas 78705, U.S.A., *e-mail*: `goddardb@concordia.edu`