Quadratic Diophantine Equations $x^2 - Dy^2 = c^n$

RICHARD A. MOLLIN

Abstract. We consider the Diophantine equation $x^2-Dy^2=c^n$ for non-square positive integers D and natural numbers n for a given nonzero integer c. We provide continued fraction solutions to the case where $n=1$ in terms of the central norm (as defined by the underlying infrastructure of the quadratic field $\mathbb{Q}(\sqrt{D})$). This allows a formulation of matrix equations to build such solutions for arbitrary n, which generalizes recent results in the literature, where only the case $c=2$ was considered.

1. Introduction

The equation $x^2 - Dy^2 = C \in \mathbb{Z}$, called a quadratic norm-form equation, has a long and distinguished history, a nice rendering of which may be found in the perennial favourite, Dickson's volume [1] on Diophantine analysis. Of course, study of the Pell equation (the case $C = \pm 1$) goes back to Archimedes (see [7], for instance). More recently, for our area of interest in this paper, in the middle of the last century, pioneering work was done by Stolt in [11]–[13] on $x^2 - Dy^2 = \pm 4N$. Also, in the latter part of the last century, work was done on a form of the title equation with $c = 2$ by Tzanakis [15], among many others. Also, work by this author and coauthors has been accomplished in the latter part of the last century and the beginning of this one in [2], [5]–[9], to mention a few. Also, quite recently there is a paper by Tekcan [14], published in this journal, for the case $c = 2$. In this paper, we generalize some of the above by linking solutions of norm-form equations of the title to continued fraction expansions of $\sqrt{D}$ and central norms arising from the infrastructure of the underlying real quadratic field (see equation (2.10) below).

2000 *Mathematics Subject Classification.* 11A55, 11R11, 11D09, 11D61.
Key words and phrases. Continued fractions, Pell's equation, central norms.

2. Preliminaries

Herein, we will be concerned with the simple continued fraction expansions of $\sqrt{D}$, where D is an integer that is not a perfect square. We denote this expansion by,

$$\sqrt{D} = \langle q_0; \overline{q_1, q_2, \ldots, q_{\ell-1}, 2q_0}\rangle,$$

where $\ell = \ell(\sqrt{D})$ is the period length, $q_0 = \lfloor\sqrt{D}\rfloor$ (the *floor* of $\sqrt{D}$), and $q_1, q_2, \ldots, q_{\ell-1}$ is a palindrome.

The kth *convergent* of α for $k \geq 0$ is given by,

$$\frac{A_k}{B_k} = \langle q_0; q_1, q_2, \ldots, q_k\rangle,$$

where

$$A_k = q_k A_{k-1} + A_{k-2}, \tag{2.1}$$

$$B_k = q_k B_{k-1} + B_{k-2}, \tag{2.2}$$

with $A_{-2} = 0$, $A_{-1} = 1$, $B_{-2} = 1$, $B_{-1} = 0$. The *complete quotients* are given by, $(P_k + \sqrt{D})/Q_k$, where $P_0 = 0$, $Q_0 = 1$, and for $k \geq 1$,

$$P_{k+1} = q_k Q_k - P_k, \tag{2.3}$$

$$q_k = \left\lfloor \frac{P_k + \sqrt{D}}{Q_k} \right\rfloor,$$

and

$$D = P_{k+1}^2 + Q_k Q_{k+1}.$$

We will also need the following facts (which can be found in most introductory texts in number theory, such as [4]. Also, see [3] for a more advanced exposition).

$$A_k B_{k-1} - A_{k-1} B_k = (-1)^{k-1}. \tag{2.4}$$

Also,

$$A_{k-1} = P_k B_{k-1} + Q_k B_{k-2}, \tag{2.5}$$

$$DB_{k-1} = P_k A_{k-1} + Q_k A_{k-2}, \tag{2.6}$$

and

$$A_{k-1}^2 - B_{k-1}^2 D = (-1)^k Q_k. \tag{2.7}$$

In particular, for any $k \in \mathbb{N}$,

$$A_{k\ell-1}^2 - B_{k\ell-1}^2 D = (-1)^{k\ell}, \tag{2.8}$$

namely, if

$$N(A_{\ell-1} + B_{\ell-1}\sqrt{D})^k) = N(A_{k\ell-1} + B_{k\ell-1}\sqrt{D})$$
$$= A_{k\ell-1}^2 - B_{k\ell-1}^2 D = (-1)^{k\ell},$$

where N is the norm from $\mathbb{Q}(\sqrt{D})$ to $\mathbb{Q}$.

Also, we will need the elementary facts that for any $k \geq 1$,

$$Q_{\ell+k} = Q_k, \qquad P_{\ell+k} = P_k, \qquad \text{and} \qquad q_{\ell+k} = q_k. \tag{2.9}$$

When ℓ is even,

$$P_{\ell/2} = P_{\ell/2+1} = P_{(2k-1)\ell/2+1} = P_{(2k-1)\ell/2}.$$

Also $Q_{\ell/2} = Q_{(2k-1)\ell/2}$, so by Equation (2.3),

$$Q_{(2k-1)\ell/2} \mid 2P_{(2k-1)\ell/2},$$

where $Q_{\ell/2}$ is called the *central norm*, (via Equation (2.7)). Furthermore,

$$Q_{(2k-1)\ell/2} \mid 2D, \tag{2.10}$$

and

$$q_{(2k-1)\ell/2} = 2P_{(2k-1)\ell/2}/Q_{(2k-1)\ell/2}. \tag{2.11}$$

In the next section, we will be considering what are typically called the standard Pell equations (2.12)–(2.13), given below. The *fundamental solution* of such an equation means the (unique) least positive integers $(x, y) = (x_0, y_0)$ satisfying it. The following result shows how all solutions of the Pell equations are determined from continued fractions.

Theorem 2.1. *Suppose that $\ell = \ell(\sqrt{D})$ and k is any positive integer. Then if ℓ is even, all positive solutions of*

$$x^2 - y^2 D = 1 \tag{2.12}$$

are given by

$$x = A_{k\ell-1} \text{ and } y = B_{kl-1},$$

whereas there are no solutions to

$$x^2 - y^2 D = -1. \tag{2.13}$$

If ℓ is odd, then all positive solutions of Equation (2.12) *are given by*

$$x = A_{2k\ell-1} \text{ and } y = B_{2k\ell-1},$$

whereas all positive solutions of Equation (2.13) *are given by*

$$x = A_{(2k-1)\ell-1} \text{ and } y = B_{(2k-1)\ell-1}.$$

Proof. This appears in many introductory number theory texts possessing an in-depth section on continued fractions. For instance, see [4, Corollary 5.3.3, p. 249]. □

From the above we see that all solutions of the Pell equations $x^2-Dy^2=\pm1$, arise from a single *class* in the sense that all solutions arise as powers of the *fundamental* unit $A_{\ell-1}+B_{\ell-1}\sqrt{D}$. For more general Pell-type equations such as the following, this is not always the case.

$$x^2-Dy^2=c. \tag{2.14}$$

We need more concepts to derive all solutions of such equations in general.

Definition 2.2. If $\alpha=x+y\sqrt{D}$ is a solution of Equation (2.14) with $\gcd(x,y)=1$, then so are certain of its **associates**, namely those $\beta\in\mathbb{Z}[\sqrt{D}]$. for which there is a unit $u\in\mathbb{Z}[\sqrt{D}]$, $u\neq1$ with such that $\beta=u\alpha$. Thus, α and β are called a **associated solutions** of Equation (2.14). These associated solutions form a class of solutions. For each such class we have an $\alpha_0=x_0+y_0\sqrt{D}$ with $y_0>0$ being the smallest value possible in its class. If $-x_0+y_0\sqrt{D}$ is also in the class, then the class is called **ambiguous**, and so in order to ensure a unique choice of α_0, we assume that $x_0>0$ in this case. We call such a solution the **fundamental solution of its class**. Hence, all solutions of Equation (2.14) are given by certain associates of the fundamental solutions in these (finitely many) classes.

Remark 2.3. An easy exercise shows that two solutions of Equation (2.14), $\alpha=x+y\sqrt{D}$ and $\alpha_1=x_1+y_1\sqrt{D}$, are in the same class if and only if both $(x_1x-y_1yD)/c\in\mathbb{Z}$ and $(yx_1-xy_1)/c\in\mathbb{Z}$. With the above being said, we are going to be concerned with certain Diophantine equations of the type (2.14) where there **is only one class of solutions**. The following will be critical in the next section.

Theorem 2.4. *Suppose that $D>1$ is not a perfect square, and $D>c^2>1$ where $|c|$ is either square-free divisor of D or is a prime divisor of $2D$. Then equation (2.14) has a solution if and only if $\ell=\ell(\sqrt{D})$ is even, and $c=(-1)^{\ell/2}Q_{\ell/2}$ in the simple continued fraction expansion of $\sqrt{D}$, in which case the fundamental solution of equation (2.14) is given by*

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

Proof. This is a consequence of both [7, Corollary 2, p. 180] and [8, Theorem 2, p. 275]. The only fact not made explicit in either [7] or [8] is the fact that there indeed *is* a *fundamental solution* of (2.14) in the sense that there is only one class. We use Remark 2.3 to verify that here.

We need only show that

$$A_{\ell/2-1} + B_{\ell/2-1}\sqrt{D}$$

and

$$\begin{aligned}(A_{k\ell-1} + B_{k\ell-1}\sqrt{D})(A_{\ell/2-1} + B_{\ell/2-1}\sqrt{D}) \\ = A_{k\ell-1}A_{\ell/2-1} + B_{k\ell-1}B_{\ell/2-1}D \\ +(A_{k\ell-1}B_{\ell/2-1} + B_{k\ell-1}A_{\ell/2-1})\sqrt{D}\end{aligned}$$

are in the same class for any $k \geq 1$. Since,

$$\begin{aligned}&\frac{A_{\ell/2-1}(A_{k\ell-1}A_{\ell/2-1} + B_{k\ell-1}B_{\ell/2-1}D)}{Q_{\ell/2}(-1)^{\ell/2}} \\ &- \frac{B_{\ell/2-1}D(A_{k\ell-1}B_{\ell/2-1} + B_{k\ell-1}A_{\ell/2-1})}{Q_{\ell/2}(-1)^{\ell/2}} \\ &= \frac{A^2_{\ell/2-1}A_{k\ell-1} - A_{k\ell-1}B^2_{\ell/2-1}D}{Q_{\ell/2}(-1)^{\ell/2}} \\ &= \frac{A_{k\ell-1}(A^2_{\ell/2-1} - B^2_{\ell/2-1}D)}{Q_{\ell/2}(-1)^{\ell/2}} = A_{k\ell-1},\end{aligned}$$

given that $A^2_{\ell/2-1} - B^2_{\ell/2-1}D = Q_{\ell/2}(-1)^{\ell/2}$.
Similarly, one may verify that

$$\begin{aligned}&\frac{A_{\ell/2-1}(A_{k\ell-1}B_{\ell/2-1} + B_{k\ell-1}A_{\ell/2-1})}{Q_{\ell/2}(-1)^{\ell/2}} \\ &- \frac{B_{\ell/2-1}(A_{k\ell-1}A_{\ell/2-1} + B_{k\ell-1}B_{\ell/2-1}D)}{Q_{\ell/2}(-1)^{\ell/2}} \\ &= B_{k\ell-1}.\end{aligned}$$

Hence, by Remark 2.3, there is only one class of solutions for equation 2.14, so the term *fundamental*, applied to

$$A_{\ell/2-1} + B_{\ell/2-1}\sqrt{D}$$

is well-defined. □

Lastly, we need the following result in the next section, the first result of which yields a matrix-theoretic solution of equation (2.14).

Theorem 2.5. *If $D \in \mathbb{N}$ is not a perfect square and $\ell = \ell(\sqrt{D})$ is even, then in the simple continued fraction expansion of $\sqrt{D}$, the following both hold for all integers $k \geq 0$.*

(1) $Q_{\ell/2}A_{(2k+1)\ell-1} = A^2_{(2k+1)\ell/2-1} + B^2_{(2k+1)\ell/2-1}D$.
(2) $Q_{\ell/2}B_{(2k+1)\ell-1} = 2A_{(2k+1)\ell/2-1}B_{(2k+1)\ell/2-1}$.

Proof. This is [7, Equations (14)–(15), p. 164]. $\square$

3. Main Results

In what follows the A_i, B_i, ℓ and any other continued fraction notation from Section 1, refer to the simple continued fraction expansion of $\sqrt{D}$, where $D > 1$ is a non-square integer.

Theorem 3.1. *If $D > c^2$ is a non-square integer, where either $|c| > 1$ is a square-free divisor of D, or $|c|$ is a prime divisor of $2D$. Then equation (2.14) has a solution if and only if ℓ is even and $c = (-1)^{\ell/2}Q_{\ell/2}$, in which case the fundamental solution of it is given by $(A_{\ell/2-1}, B_{\ell/2-1})$, and all other solutions of the equation are given by the following for $k \geq 1$.*

$$\begin{pmatrix} A_{(2k+1)\ell/2-1} \\ B_{(2k+1)\ell/2-1} \end{pmatrix} = \begin{pmatrix} A_{\ell/2-1} & B_{\ell/2-1}D \\ B_{\ell/2-1} & A_{\ell/2-1} \end{pmatrix} \begin{pmatrix} A_{k\ell-1} \\ B_{k\ell-1} \end{pmatrix}. \tag{3.15}$$

Proof. First we show that the right-hand side of equation (3.15) is indeed a solution to equation (2.14) when $c = (-1)^{\ell/2}Q_{\ell/2}$ for even ℓ.

$$\begin{aligned}
&(A_{\ell/2-1}A_{k\ell-1} + B_{\ell/2-1}A_{k\ell-1}D)^2 \\
&\quad - (B_{\ell/2-1}A_{k\ell-1} + A_{\ell/2-1}B_{k\ell-1})^2 D \\
&= A^2_{\ell/2-1}A^2_{k\ell-1} + 2A_{\ell/2-1}A_{k\ell-1}B_{\ell/2-1}B_{k\ell-1}D \\
&\quad + B^2_{\ell/2-1}A^2_{k\ell-1}D^2 - B^2_{\ell/2-1}A^2_{k\ell-1}D \\
&\quad - 2A_{\ell/2-1}A_{k\ell-1}B_{\ell/2-1}B_{k\ell-1}D \\
&\quad - A^2_{\ell/2-1}B^2_{k\ell-1}D \\
&= A^2_{\ell/2-1}(A^2_{k\ell-1} - B^2_{k\ell-1}D) \\
&\quad - B^2_{\ell/2-1}D(A^2_{k\ell-1} - B^2_{k\ell-1}D)
\end{aligned}$$

$$= (A^2_{\ell/2-1} - B^2_{\ell/2-1}D)(A^2_{k\ell-1} - B^2_{k\ell-1}D)$$
$$= (-1)^{\ell/2}Q_{\ell/2} = c,$$

where the last equality follows from Theorem 2.4, and equation (2.8), as required. On the other hand, if (2.14) has a solution, then Theorem 2.4 tells us that the fundamental solution is what we assert.

Now, to see that the left side equals the right side of equation (3.15) consider the following, which follows from the results in Theorem 2.5.

$$\begin{aligned}
&(A_{(2k+1)\ell/2-1} + B_{(2k+1)\ell/2-1}\sqrt{D})^2 \\
&\qquad = Q_{\ell/2}(A_{(2k+1)\ell-1} + B_{(2k+1)\ell-1}\sqrt{D}) \\
&\qquad = Q_{\ell/2}(A_{k\ell-1} + B_{(2k-1)\ell-1}\sqrt{D})^2(A_{\ell-1} + B_{\ell-1}\sqrt{D}) \\
&\qquad = Q_{\ell/2}(A_{k\ell-1} + B_{(2k-1)\ell-1}\sqrt{D})^2 \times \\
&\qquad\qquad (A_{(2k-1)\ell/2-1} + B_{(2k-1)\ell/2-1}\sqrt{D})^2/Q_{\ell/2} \\
&\qquad = \big(A_{k\ell-1}A_{(2k-1)\ell/2-1} + B_{k\ell-1}B_{(2k-1)\ell/2-1}D \\
&\qquad\quad + (A_{(2k-1)\ell/2-1}B_{k\ell-1} + A_{k\ell-1}B_{(2k-1)\ell/2-1})\sqrt{D}\big)^2,
\end{aligned}$$

which, by comparing coefficients, yields that

$$A_{(2k+1)\ell/2-1} = A_{k\ell-1}A_{\ell/2-1} + B_{k\ell-1}B_{\ell/2-1}D,$$

and

$$B_{(2k+1)\ell/2-1} = A_{\ell/2-1}B_{k\ell-1} + A_{k\ell-1}B_{\ell/2-1},$$

as required. Since all the continued fraction expansion of $\sqrt{D}$ dictates, via Theorem 2.4, that all solutions of equation (2.14) are given by

$$A_{(2k+1)\ell/2-1} + B_{(2k+1)\ell/2-1}\sqrt{D}$$

for all $k \geq 0$, the proof is complete. □

Example 3.2. Let $D = 75$ and $c = 6$. Then $\ell(\sqrt{D}) = \ell = 4$, $A_{\ell/2-1} = A_1 = 9$, $B_{\ell/2-1} = B_1 = 1$, $A_{\ell-1} = A_3 = 26$, $B_{\ell-1} = B_3 = 3$, and $(-1)^{\ell/2}Q_{\ell/2} = 6$, so all solutions of

$$x^2 - 75y^2 = 6$$

are given, for $k \geq 1$, by

$$\begin{pmatrix} A_{4k+1} \\ B_{4k+1} \end{pmatrix} = \begin{pmatrix} 9 & 75 \\ 1 & 9 \end{pmatrix} \begin{pmatrix} A_{4k-1} \\ B_{4k-1} \end{pmatrix}.$$

For instance, if $k = 3$, then

$$\begin{pmatrix} A_{13} \\ B_{13} \end{pmatrix} = \begin{pmatrix} 9 & 75 \\ 1 & 9 \end{pmatrix} \begin{pmatrix} A_{11} \\ B_{11} \end{pmatrix}$$

$$= \begin{pmatrix} 9 & 75 \\ 1 & 9 \end{pmatrix} \begin{pmatrix} 70226 \\ 8109 \end{pmatrix} = \begin{pmatrix} 1240209 \\ 143207 \end{pmatrix}.$$

Corollary 3.3. *The solutions of equation* (2.14) *satisfy the following recurrence relations for* $k \geq 1$,

$$\begin{pmatrix} A_{(2k+1)\ell/2-1} \\ B_{(2k+1)\ell/2-1} \end{pmatrix} = \begin{pmatrix} A_{\ell-1} & B_{\ell-1}D \\ B_{\ell-1} & A_{\ell-1} \end{pmatrix} \begin{pmatrix} A_{(2k-1)\ell/2-1} \\ B_{(2k-1)\ell/2-1} \end{pmatrix}$$

$$= \begin{pmatrix} A_{\ell-1}A_{(2k-1)\ell/2-1} + B_{\ell-1}B_{(2k-1)\ell/2-1}D \\ B_{\ell-1}A_{(2k-1)\ell/2-1} + A_{\ell-1}B_{(2k-1)\ell/2-1} \end{pmatrix}.$$

Proof. This is verified, in a similar fashion to the proof of Theorem 3.1, by observing that,

$$\begin{aligned}
&(A_{(2k+1)\ell/2-1} + B_{(2k+1)\ell/2-1}\sqrt{D})^2 \\
&\quad = Q_{\ell/2}(A_{(2k+1)\ell-1} + B_{(2k+1)\ell-1}\sqrt{D}) \\
&\quad = Q_{\ell/2}(A_{(2k-1)\ell-1} + B_{(2k-1)\ell-1}\sqrt{D})(A_{2\ell-1} + B_{2\ell-1}\sqrt{D}) \\
&\quad = (A_{(2k-1)\ell/2-1} + B_{(2k-1)\ell/2-1}\sqrt{D})^2(A_{\ell-1} + B_{\ell-1}\sqrt{D})^2 \\
&\quad = \big(A_{\ell-1}A_{(2k-1)\ell/2-1} + B_{\ell-1}B_{(2k-1)\ell/2-1}D \\
&\qquad\quad + (B_{\ell-1}A_{(2k-1)\ell/2-1} + A_{\ell-1}B_{(2k-1)\ell/2-1})\sqrt{D}\big)^2,
\end{aligned}$$

which, by comparing coefficients, yields the desired result. $\square$

Example 3.4. As an Illustration of Corollary 3.3, we look at Example 3.2 again with $k = 3$.

$$\begin{pmatrix} A_{13} \\ B_{13} \end{pmatrix} = \begin{pmatrix} A_{\ell-1} & B_{\ell-1}D \\ B_{\ell-1} & A_{\ell-1} \end{pmatrix} \begin{pmatrix} A_9 \\ B_9 \end{pmatrix}$$
$$= \begin{pmatrix} 26 & 225 \\ 3 & 26 \end{pmatrix} \begin{pmatrix} 23859 \\ 2755 \end{pmatrix} = \begin{pmatrix} 1240209 \\ 143207 \end{pmatrix}.$$

The following results are immediate from the above.

Corollary 3.5. (Tekcan [14, Theorem 2.3, p. 80]) *Suppose that* $(X_1, Y_1) = (k, m)$ *is the fundamental solution of* $x^2 - Dy^2 = 2$, *and* $x_1 + y_1\sqrt{D}$ *is the fundamental solution of* $x^2 - Dy^2 = 1$, *with* $x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$. *Then the other solutions of* $x^2 - Dy^2 = 2$ *are* (X_n, Y_n), *where*

$$\begin{pmatrix} X_n \\ Y_n \end{pmatrix} = \begin{pmatrix} k & mD \\ m & k \end{pmatrix} \begin{pmatrix} x_{n-1} \\ y_{n-1} \end{pmatrix},$$

for $n \geq 2$.

Corollary 3.6. (Tekcan [14, Corollary 2.4, p. 80]) *The solutions* (X_n, Y_n) *of* $x^2 - Dy^2 = 2$ *satisfy the following relations*

$$\begin{pmatrix} X_{n+1} \\ Y_{n+1} \end{pmatrix} = \begin{pmatrix} x_1 & y_1 D \\ y_1 & x_1 \end{pmatrix} \begin{pmatrix} X_n \\ Y_n \end{pmatrix} = \begin{pmatrix} x_1 X_n + y_1 D Y_n \\ y_1 X_n + x_1 Y_n \end{pmatrix}.$$

Corollary 3.7. (Mollin [7, Corollary 3, p. 184]) *If* $D > 4$ *is not a perfect square, then* $x^2 - Dy^2 = \pm 2$ *has a solution if and only if* $\ell = \ell(\sqrt{D})$ *is even and* $(-1)^{\ell/2} Q_{\ell/2} = \pm 2$.

Remark 3.8. What is missing from [14], and similar recent papers in Diophantine analysis, is the connection with the continued fractions which theorem 3.1 exposes in terms of the role of the central norm. This is important since it displays the underlying nature of the infrastructure of the real quadratic field via continued fractions and the fundamental importance of that structure in achieving complete solutions of certain quadratic Diophantine equations. Furthermore, in [14], there is no mention of criteria for the solvability of $x^2 - Dy^2 = 2$. Rather solutions to it are assumed. Indeed, what underlies the solutions of this special case is when the central norm in the simple continued fraction expansion of $\sqrt{D}$ is 2. A result we achieved in earlier work that is related to a classical result of Lagrange speaks directly to this fact as follows.

Theorem 3.9. *If $D > 4$ is a non-square integer, and $\ell = \ell(\sqrt{D})$ then the following are equivalent*

(1) *The Diophantine equation*
$$x^2 - Dy^2 = \pm 2 \tag{3.16}$$
has a solution.

(2) *$\ell = \ell(\sqrt{D})$ is even, $\pm 2 = (-1)^{\ell/2} Q_{\ell/2}$, and*
$$A_{(2k-1)\ell/2-1} + B_{(2k-1)\ell/2-1}\sqrt{D}$$
is the fundamental solution of equation (3.16).

(3) *ℓ is even and $A_{\ell-1} \equiv (-1)^{\ell/2} \pmod{D}$.*

Proof. See [8, Corollary 1, p. 277] and [8, Theorem 2, p. 275]. $\square$

Remark 3.10. The classical result of Lagrange which Theorem 3.9 generalizes is that if p is an odd prime and (x_0, y_0) is the fundamental solution of
$$x^2 - py^2 = 1,$$
then $x_0 \equiv 1 \pmod{p}$ if and only if $p \equiv 7 \pmod{8}$. When $p \equiv 7 \pmod{8}$, $\ell(\sqrt{p}) = \ell$ is even and $Q_{\ell/2} = 2$. Moreover, when $x_0 \equiv 1 \pmod{p}$, then since $x_0 = A_{\ell-1}$, Legendre symbol consideration with 2 and p force $p \equiv 7 \pmod{8}$ and $A_{\ell/2-1}^2 - B_{\ell/2-1}^2 p = 2$. All of this fits quite nicely with what we have been discussing herein.

There is a fundamental result that yields the fundamental unit of a real quadratic order via matrices as follows. This generalizes the result by Tekcan [14, Theorem 2.5, p. 83] where an element of $SL_2(2, \mathbb{R})$ is used for his special case where $x^2 - Dy^2 = 2$. The following holds without restriction.

Theorem 3.11. (Fundamental Unit Theorem for Quadratic Orders) *Suppose that $D > 1$ is a non-square integer where*
$$\sqrt{D} = \langle q_0; \overline{q_1, \ldots, q_{\ell-1}, 2q_0} \rangle, \tag{3.17}$$
holds. Then
$$\prod_{j=0}^{\ell-1} \begin{pmatrix} q_j & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} DB_{\ell-1} & A_{\ell-1} \\ A_{\ell-1} & B_{\ell-1} \end{pmatrix}. \tag{3.18}$$

Proof. This is proved more generally in [10, Theorem 3, p. 44]. $\square$

Now we show how to use the solutions of equation (2.14) to find solutions of

$$u^2 - Dv^2 = c^n \tag{3.19}$$

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

Theorem 3.12. *Suppose that $D > c^2 > 1$ is a non-square integer where either $|c|$ is a square-free divisor of D or else is a prime divisor of $2D$, and equation (2.14) is solvable. Then for any fixed $n \in \mathbb{N}$, all solutions of equation (3.19) are given by (U_n, V_n), where*

$$\begin{pmatrix} U_n \\ V_n \end{pmatrix} = \begin{pmatrix} A_{\ell/2-1} & B_{\ell/2-1}D \\ B_{\ell/2-1} & A_{\ell/2-1} \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{3.20}$$

Proof. We use induction on n. If $n = 1$, then the result follows from Theorem 3.1. Assume the induction hypothesis:

$$U_{n-1}^2 - V_{n-1}^2 D = c^{n-1}.$$

Since

$$\begin{pmatrix} U_n \\ V_n \end{pmatrix} = \begin{pmatrix} A_{\ell/2-1} & B_{\ell/2-1}D \\ B_{\ell/2-1} & A_{\ell/2-1} \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\begin{aligned}\begin{pmatrix} U_n \\ V_n \end{pmatrix} &= \begin{pmatrix} A_{\ell/2-1} & B_{\ell/2-1}D \\ B_{\ell/2-1} & A_{\ell/2-1} \end{pmatrix} \begin{pmatrix} U_{n-1} \\ V_{n-1} \end{pmatrix} \\ &= \begin{pmatrix} A_{\ell/2-1}U_{n-1} + B_{\ell/2-1}V_{n-1}D \\ B_{\ell/2-1}U_{n-1} + A_{\ell/2-1}V_{n-1} \end{pmatrix},\end{aligned}$$

we have

$$\begin{aligned} U_n^2 - DV_n^2 &= (A_{\ell/2-1}U_{n-1} + B_{\ell/2-1}V_{n-1}D)^2 \\ &\qquad - (B_{\ell/2-1}U_{n-1} + A_{\ell/2-1}V_{n-1})^2 D \\ &= A_{\ell/2-1}^2 U_{n-1}^2 + 2A_{\ell/2-1}B_{\ell/2-1}U_{n-1}V_{n-1}D \\ &\qquad + B_{\ell/2-1}^2 V_{n-1}^2 D^2 - B_{\ell/2-1}^2 U_{n-1}^2 D \\ &\qquad - 2A_{\ell/2-1}B_{\ell/2-1}U_{n-1}V_{n-1}D \\ &\qquad - A_{\ell/2-1}^2 V_{n-1}^2 D \\ &= A_{\ell/2-1}^2 (U_{n-1}^2 - V_{n-1}^2 D) - B_{\ell/2-1}^2 D (U_{n-1}^2 - V_{n-1}^2 D) \\ &= (A_{\ell/2-1}^2 - B_{\ell/2-1}^2 D)(U_{n-1}^2 - V_{n-1}^2 D) = c \cdot c^{n-1} = c^n \end{aligned}$$

which secures the proof. □

Example 3.13. To illustrate Theorem 3.12, we go to Example 3.2 again. Take $n = 4$, then

$$\begin{pmatrix} U_4 \\ V_4 \end{pmatrix} = \begin{pmatrix} 9 & 75 \\ 1 & 9 \end{pmatrix}^4 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 48636 \\ 5616 \end{pmatrix},$$

and indeed, $U_4^2 - 75V_4^2 = 48636^2 - 75 \cdot 5616^2 = 1296 = 6^4$.

The following is immediate from the above and our proofs of the results from [14] are simpler and more revealing in general.

Corollary 3.14. (Tekcan [14, Theorem 2.7, p. 86]) *Suppose that* $(X_1, Y_1) = (k, m)$ *is the fundamental solution of* $x^2 - Dy^2 = 2$*, then all solutions of* $x^2 - Dy^2 = 2^n$ *for* $n \in \mathbb{N}$ *are given by* $(x, y) = (U_n, V_n)$*, where*

$$\begin{pmatrix} U_n \\ V_n \end{pmatrix} = \begin{pmatrix} k & mD \\ m & k \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Some special cases of the above are given as follows. Consider the Diophantine equations,

$$x^2 - Dy^2 = 1 \tag{3.21}$$

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

Theorem 3.15. *If* $D = a^2b^2 - 2a > 0$ *where* $a, b \in \mathbb{N}$*, where* a *is square-free and* $b > 1$ *then the fundamental solution of equation* (3.21) *is given by*

$$(x, y) = (a \cdot b^2 - 1, b) \tag{3.23}$$

and the fundamental solution of equation (3.22) *is given by* $(X, Y) = (ab, 1)$.

Proof. Since D is of RD-type, the fundamental unit is well-known to be that given in (3.23) (for instance, see [3, Theorem 3.2.1 (d), p. 78]), where $A_{\ell-1} = a \cdot b^2 - 1$ and $B_{\ell-1} = b$ (since $b > 1$ puts us into case (d) of that result). Moreover, the fundamental solution to equation (3.22) is given by $(X, Y) = (ab, 1)$, since it is clearly a solution and the fact that $Y = 1$ makes it fundamental. $\square$

Example 3.16. Let $D = 3^2 \cdot 7^2 - 2 \cdot 7 = 427 = a^2b^2 - 2a$. Then the fundamental solution of $x^2 - 427y^2 = 1$ is $(A_{\ell-1}, B_{\ell-1}) = (A_3, B_3) = (62, 3) = (a \cdot b^2 - 1, b)$ and the fundamental solution of $x^2 - 427y^2 = 14$ is $(ab, 1) = (21, 1)$.

Immediate from the above is the following recent result in the literature.

Corollary 3.17. [Tekcan [14, Theorem 2.2, p. 79]] *If* $D = b^2 - 2$, $b \geq 2$, *then the fundamental solution of equation* (3.21) *is* $(x, y) = (b^2-1, b)$ *and the fundamental solution of equation* (3.22) *is* $(X, Y) = (b, 1)$.

Some considerations for future work would be to replace the values D in this paper with polynomials of the type we considered in [6] for instance, which would generalize all of this to a higher level.

REFERENCES

[1] L. E. Dickson, *History of the Theory of Numbers*, Volume II, Diophantine Analysis, Chelsea, New York 1966.

[2] S. Louboutin and R. A. Mollin, *Solutions to* $x^2 - Dy^2 = Q$, in: *CRM Proc. and Lecture Notes* **18** (1998), 355–368.

[3] R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, New York, London, Tokyo 1996.

[4] R. A. Mollin, *Fundamental Number Theory with Applications*, CRC Press, Boca Raton, New York, London, Tokyo 1998.

[5] R. A. Mollin, *All solutions of the Diophantine equation* $x^2 - Dy^2 = n$, Far East J. Math., Special Volume Part III (1998), 257–293.

[6] R. A. Mollin, *Polynomials of Pellian type and continued fractions*, Serdica Math. J., Bulgarian Academy of Sciences **27** (2001), 317–342.

[7] R. A. Mollin, *A continued fraction approach to the Diophantine equation* $ax^2 - by^2 = \pm 1$, JP Journal of Algebra, Number Theory, and Apps. **4** (2004), 159–207.

[8] R. A. Mollin, *Norm form equations and continued fractions*, Acta Math. Univ. Comenianae **74** (2005), 273–278.

[9] R. A. Mollin, *Necessary and sufficient conditions for the central norm to equal* 2^h *in the simple continued fraction expansion of* $\sqrt{2^h c}$ *for any odd* $c > 1$, Canad. Math. Bull. **48** (2005),121–132.

[10] R. A. Mollin and K. Cheng, *Matrices and continued fractions*, Int. Math. J. **3** (2003), 41–58.

[11] B. Stolt, *On the Diophantine equation* $u^2 - Dv^2 = \pm 4N$, Arkiv för Matematik **2** (1951), 1–23.

[12] B. Stolt, *On the Diophantine equation* $u^2 - Dv^2 = \pm 4N$, *Part II*, Arkiv för Matematik **2** (1952), 251–268.

[13] B. Stolt, *On the Diophantine equation* $u^2 - Dv^2 = \pm 4N$, *Part III*, Arkiv för Matematik **3** (1954), 117–132.

[14] A. Tekcan, *Pell equation* $x^2 - Dy^2 = 2$, II, Irish Math. Soc. Bulletin **54** (2004), 79–89.

[15] N. Tzanakis, *On the Diophantine equation* $y^2 - D = 2^k$, J. Number Theory **17** (1983), 144–164.

Richard A. Mollin,
Department of Mathematics and Statistics,
University of Calgary,
Calgary, Alberta
Canada, T2N 1N4
ramollin@math.ucalgary.ca

Received on 26 January 2006 and in revised form on 17 November 2006.