



CENTRAL NORMS: APPLICATIONS TO PELL'S EQUATION

R. A. MOLLIN and A. SRINIVASAN

Department of Mathematics and Statistics

University of Calgary

Canada

email: ramollin@math.ucalgary.ca

Department of Mathematics

Siddhartha College (Affiliated with Mumbai University)

India

email: rsrinivasan.anitha@gmail.com

Abstract

In this work, we explore the central norm in the simple continued fraction expansion of \sqrt{D} when $D > 1$ is a non-square integer. We use the results to extend what is known in the literature as well as to show how some classical results can be derived from them. We also address the solvability of the Pell's equation $x^2 - Dy^2 = -1$ employing our results.

1. Introduction

The central norm (see (2.12) below) in the simple continued fraction expansion of \sqrt{D} for a non-square positive integer D is linked to solvability of the Pell's equation in ways not obvious at first glance. For instance, Lagrange proved a result generalized by the first author in [15] that links central norms in this fashion. To see this, let $x_0 + y_0\sqrt{D}$ be the smallest positive (fundamental) solution of the *positive* Pell's equation $x^2 - Dy^2 = 1$ and let $\ell = \ell(\sqrt{D})$ be the period length of the simple

2010 Mathematics Subject Classification: Primary 11D09, 11A55; Secondary 11R11, 11R29.

Keywords and phrases: Pell's equation, continued fractions, central norms.

Received October 24, 2009

continued fraction expansion of \sqrt{D} . The principal result from [15] is that $x_0 \equiv \pm 1 \pmod{D}$ if and only if $Q_{\ell/2} = 2$ – see Corollary 3.4 below. Lagrange’s result is that if $D = p$ is a prime, then $x_0 \equiv 1 \pmod{p}$ if and only if $p \equiv 7 \pmod{8}$. The congruence conditions on x_0 from the positive Pell’s equation also have a striking relationship with the solution of the negative Pell’s equation $x^2 - Dy^2 = -1$, namely when $\ell(\sqrt{D})$ is odd. The authors of this paper prove in [23] that the *negative* Pell’s equation has a solution if and only if $x_0 \equiv -1 \pmod{2D}$. Thus, this criterion can be exploited to investigate parity issues with $\ell(\sqrt{D})$. We generalize numerous results in the literature including that of the first author in [17] from 2005, and show how to employ our new results to achieve classical results such as those of Perrot [24] from 1888, Rédei [26] from 1935, Jensen [5] from 1962, and include numerous other illustrations of this continued fraction approach.

2. Notation and Preliminaries

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

$$\sqrt{D} = \langle q_0; \overline{q_1, q_2, \dots, q_{\ell-1}, 2q_0} \rangle, \quad (2.1)$$

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

The k th convergent of α for $k \geq 0$ is given by

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

where

$$A_k = q_k A_{k-1} + A_{k-2}, \quad (2.2)$$

$$B_k = q_k B_{k-1} + B_{k-2}, \quad (2.3)$$

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 $k \geq 1$,

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

$$q_k = \left\lfloor \frac{P_k + \sqrt{D}}{Q_k} \right\rfloor \quad (2.4)$$

and

$$D = P_{k+1}^2 + Q_k Q_{k+1}. \quad (2.5)$$

We will also need the following facts (which can be found in most introductory texts in number theory, such as [18]. Also, see [11], for a more advanced exposition.),

$$A_k B_{k-1} - A_{k-1} B_k = (-1)^{k-1}. \quad (2.6)$$

Also,

$$A_{k-1} = P_k B_{k-1} + Q_k B_{k-2}, \quad (2.7)$$

$$DB_{k-1} = P_k A_{k-1} + Q_k A_{k-2} \quad (2.8)$$

and

$$A_{k-1}^2 - B_{k-1}^2 D = (-1)^k Q_k. \quad (2.9)$$

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

$$A_{k\ell-1}^2 - B_{k\ell-1}^2 D = (-1)^{k\ell}. \quad (2.10)$$

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

$$Q_{\ell+k} = Q_k, \quad P_{\ell+k} = P_k \quad \text{and} \quad q_{\ell+k} = q_k. \quad (2.11)$$

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 (2.4),

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

where

$$Q_{\ell/2} \text{ is called the } \textit{central norm}, \quad (2.12)$$

(via equation (2.9)).

Furthermore,

$$Q_{(2k-1)\ell/2} | 2D \quad (2.13)$$

and

$$q_{(2k-1)\ell/2} = 2P_{(2k-1)\ell/2} / Q_{(2k-1)\ell/2}. \quad (2.14)$$

In the next section, we will be considering what are typically called the *standard Pell's equations* (2.15)-(2.16), given below. The *fundamental solution* of such an equation means the (unique) least positive integers (x, y) satisfying it. The following result shows how all solutions of the Pell's 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*

$$x^2 - y^2D = 1 \quad (2.15)$$

are given by

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

whereas there are no solutions to

$$x^2 - y^2D = -1. \quad (2.16)$$

If ℓ is odd, then all positive solutions of equation (2.15) are given by

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

whereas all positive solutions of equation (2.16) are given by

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

Proof. This appears in many introductory number theory texts possessing an in-depth section on continued fractions. For instance, see [18, Corollary 5.7, p. 236]. \square

We highlight the following fact which will be used throughout.

Remark 2.1. The *fundamental solution* of $x^2 - Dy^2 = (-1)^\ell$ is given by $A_{\ell-1} + B_{\ell-1}\sqrt{D}$. This is the solution with least positive x, y . Moreover, as stated in

Theorem 2.1, all solutions of (2.15) are powers of $A_{\ell-1} + B_{\ell-1}\sqrt{D}$ and all solutions of (2.16) are *odd powers* of $A_{\ell-1} + B_{\ell-1}\sqrt{D}$. Thus, (2.16), called the *negative Pell's equation*, is solvable if and only if $\ell = \ell(\sqrt{D})$ is odd, whereas (2.15), called the *positive Pell's equation*, is always solvable with its fundamental solution being $A_{\ell-1} + B_{\ell-1}\sqrt{D}$ when ℓ is even and $A_{2\ell-1} + B_{2\ell-1}\sqrt{D}$ when ℓ is odd.

We also need the following.

Theorem 2.2. *Let D be a positive integer that is not a perfect square. Then $\ell = \ell(\sqrt{D})$ is even if and only if one of the following two conditions occurs:*

1. *There exists a factorization $D = ab$ with $1 < a < b$ such that the following equation has an integral solution (x, y) :*

$$ax^2 - by^2 = \pm 1. \quad (2.17)$$

Furthermore, in this case, each of the following holds, where $(x, y) = (r, s)$ is the fundamental solution of equation (2.17):

- (a) $Q_{\ell/2} = a$.
- (b) $A_{\ell/2-1} = ra$ and $B_{\ell/2-1} = s$.
- (c) $A_{\ell-1} = r^2a + s^2b = x_0$, where

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

and $B_{\ell-1} = 2rs = y_0$, where

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

since

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

- (d) $r^2a - s^2b = (-1)^{\ell/2}$.

2. There exists a factorization $D = ab$ with $1 \leq a < b$ such that the following equation has an integral solution (x, y) with xy odd:

$$ax^2 - by^2 = \pm 2. \quad (2.18)$$

Moreover, in this case, each of the following holds, where $(x, y) = (r, s)$ is the fundamental solution of equation (2.18):

(a) $Q_{\ell/2} = 2a$.

(b) $A_{\ell/2-1} = ra$ and $B_{\ell/2-1} = s$.

(c) $2A_{\ell-1} = r^2a + s^2b = 2x_0$, where

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

and $B_{\ell-1} = rs = y_0$, where

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

since

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

(d) $r^2a - s^2b = 2(-1)^{\ell/2}$.

Proof. All this is proved in [14]. □

It is worth noting that the above leads to the following classical result, where $(*/p)_4$ is the quartic residue symbol – see [12, Chapter 5] for instance.

Corollary 2.1 (Dirichlet [3]). *If p is a prime with $p \equiv 9 \pmod{16}$ and $(2/p)_4 = -1$, then $\ell(\sqrt{2p})$ is odd.*

Proof. By Theorem 2.2, $2r^2 - ps^2 = \pm 1$. If $2r^2 - ps^2 = 1$, then s is odd so the Jacobi symbol identities hold as follows: $(2/s) = ((2r^2 - ps^2)/s) = (1/s) = 1$, so

$s \equiv \pm 1 \pmod{8}$. Thus, $s^2 \equiv 1 \pmod{16}$, which implies that

$$1 = 2r^2 - ps^2 \equiv 2r^2 - p \pmod{16}$$

which in turn implies that $9 \equiv p \equiv 2r^2 - 1 \pmod{16}$, forcing $r^2 \equiv 5 \pmod{8}$, a contradiction.

Suppose that $2r^2 - ps^2 = -1$. Since the Jacobi symbol equality

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

holds,

$$\begin{aligned} 1 &= \left(\frac{1}{p}\right)_4 = \left(\frac{ps^2 - 2r^2}{p}\right)_4 = \left(\frac{-2r^2}{p}\right)_4 = \left(\frac{-1}{p}\right)_4 \left(\frac{2}{p}\right)_4 \left(\frac{r^2}{p}\right)_4 \\ &= \left(\frac{2}{p}\right)_4 \left(\frac{r}{p}\right)_4^2 = \left(\frac{2}{p}\right)_4 \left(\frac{r}{p}\right)_4 = \left(\frac{2}{p}\right)_4 = -1, \end{aligned}$$

a contradiction. □

Remark 2.2. Legendre knew in 1830 [9] that when the Pell's equation $x^2 - Dy^2 = 1$ is considered, then exactly one of the equations $ax^2 - by^2 = \pm 1, \pm 2$ is solvable for some factorization $D = ab$. However, the continued fraction formulation given in Theorem 3.4 was not known to him. Dirichlet was essentially applying Legendre's result to get Corollary 2.1. Later, we will develop more quartic residue symbol results to describe the relationship between parity of the continued fraction expansion of related quadratic orders.

The following was proved by Pumplün [25] in 1968, which generalized a result of Dirichlet, the case $n = 1$.

Corollary 2.2. *Let $D = \prod_{j=1}^{2n+1} p_j$, where $p_j \equiv 1 \pmod{4}$ are distinct primes. If there is no triple i, j, k such that the Legendre symbol equality $(p_i/p_j) = (p_j/p_k) = 1$, then $\ell = \ell(\sqrt{D})$ is odd.*

Proof. If ℓ is even, then by Theorem 2.2, there is a solution $ar^2 - bs^2 = \pm 1, \pm 2$ for some factorization $D = ab$. However, since $a \equiv b \equiv 1 \pmod{4}$ we cannot have the ± 2 case since rs is odd by part 2 of Theorem 2.2, and hence $ar^2 - bs^2 \equiv 0 \pmod{4}$. Thus, $ax^2 - by^2 = \pm 1$. Let $a = p_1 p_2 \cdots p_{2r}$ for some $r \in \mathbb{N}$ and $b = p_{2r+1} \cdots p_{2n+1}$. Since $(b/p_1) = 1$, there must be at least one $j = 2r+1, \dots, 2n+1$ with $(p_j/p_1) = 1$, and without loss of generality, say $(p_{2r+1}/p_1) = 1$. By hypothesis, $(p_{2r+1}/p_i) = -1$ for all $i = 2, 3, \dots, 2r$ and so $(p_{2r+1}/p_2 \cdots p_{2r}) = -1$ which gives $(a/p_{2r+1}) = -1$, a contradiction. \square

3. The Pell's Equation

The following criterion for solvability of the negative Pell's equation will be a useful tool.

Theorem 3.1. *If $D \equiv 1, 2 \pmod{4}$ is a non-square integer, then there is a solution to $x^2 - Dy^2 = -1$ if and only if $x_0 \equiv -1 \pmod{2D}$, where (x_0, y_0) is the fundamental solution of $x^2 - Dy^2 = 1$.*

Proof. See [23]. \square

Remark 3.1. Note that if k is odd, and $(x_0 + y_0\sqrt{D})^k = x_k + y_k\sqrt{D}$, then $x_0 \equiv -1 \pmod{D}$ if and only if $x_k \equiv -1 \pmod{D}$. We will be using this fact in what follows.

Note that for $D \equiv 1 \pmod{4}$, in [10], Lenstra provides an algorithm for finding a solution of the positive Pell's equation in subexponential time. Here is an algorithm for determining the sign of the norm of the fundamental unit, $(-1)^\ell$, by combining Lenstra with Theorem 3.1.

1. Find a solution (x, y) employing Lenstra's method.
2. If $x \equiv 1 \pmod{D}$, find another solution.
3. If $x \equiv -1 \pmod{D}$, then ℓ is odd and if $x \not\equiv 1 \pmod{D}$, then ℓ is even.

Note that if $x \not\equiv 1 \pmod{D}$, then $x + y\sqrt{D}$ is an odd power of $x_0 + y_0\sqrt{D}$ and hence by Remark 3.1, we have $x_0 \equiv x \pmod{D}$. In [10, p. 11], Lenstra points out that we do not get x_0 and y_0 explicitly *but* we can indeed compute the value modulo any integer. Thus, the above steps can be done easily. There may be difficulty in answering the question as to whether we ever get to Step 3. However, if this is answered in the affirmative, then we have an improvement on all previous algorithms to decide whether the negative Pell's equation is solvable or not.

Corollary 3.1 (Jensen [5]). *Suppose that $c > 1$ is a non-square integer with ε_{4c} , the fundamental unit of $\mathbb{Z}[\sqrt{4c}]$, and $(c/p) = 1$ for an odd prime p such that $2^\alpha \parallel (p-1)$ for $\alpha \geq 2$, with $\ell(\sqrt{c})$ is odd. Then $\ell = \ell(\sqrt{cp^2}) = \ell(\sqrt{D})$ is odd if and only if*

$$\varepsilon_{4c}^{(p-1)/2^{\alpha-1}} \equiv -1 \pmod{p} \quad (\text{in } \mathbb{Z}[\sqrt{c}]). \quad (3.19)$$

Furthermore, if $n > 1$ is any integer, then $\ell(\sqrt{n^2c})$ is odd if and only if $\ell(\sqrt{p^2c})$ is odd for all prime divisors of n .

Proof. Let $x_0 + py_0\sqrt{c} = \varepsilon_{4c}^{2k}$ be the fundamental solution of the positive Pell's equation $x^2 - p^2cy^2 = 1$ and let $\varepsilon_{4c}^2 = x_1 + y_1\sqrt{c}$ be the fundamental solution of the positive Pell's equation $x^2 - cy^2 = 1$. Observe that y_1 is even as $\ell(\sqrt{c})$ is odd. Also, by Theorem 3.1, we have

$$x_1 \equiv -1 \pmod{2c}. \quad (3.20)$$

Now assume that (3.19) holds. If $p-1 = 2^\alpha f$, where f is odd, then $\varepsilon_{4c}^{2f} = A + pB\sqrt{c}$, where

$$A \equiv -1 \pmod{p}. \quad (3.21)$$

Note that $A^2 - p^2cB^2 = 1$ and hence by Remark 3.1, for some integer n ,

$$\varepsilon_{4c}^{2f} = A + pB\sqrt{c} = (x_0 + y_0p\sqrt{c})^n = \varepsilon_{4c}^{2kn} = (x_1 + y_1\sqrt{c})^{kn}. \quad (3.22)$$

It follows that $f = kn$, hence kn is odd. From the binomial expansion, using (3.21)-

(3.22) and noting that $x_0^2 \equiv 1 \pmod{p^2}$, we have

$$-1 \equiv A \equiv x_0^n \equiv x_0 \pmod{p^2}. \quad (3.23)$$

Similarly, from (3.20) and (3.22) and as y_1 is even, we have

$$A \equiv x_1^{kn} \equiv x_0^n \equiv x_1 \equiv x_0 - 1 \pmod{2c}. \quad (3.24)$$

From (3.23)-(3.24), we have $x_0 \equiv -1 \pmod{2p^2c}$ and hence from Theorem 3.1, ℓ is odd.

Conversely, if ℓ is odd, then by Theorem 3.1, $x_0 \equiv -1 \pmod{2p^2c}$. However, by Corollary 4.1, $\varepsilon_{4c}^k = A_{\ell-1} + B_{\ell-1}\sqrt{p^2c}$ for some odd integer k , and by Lucas-Lehmer theory – see [11, Exercises 3.1.5-3.1.6, pp. 73-75], we know that $k \mid (p-1)$ since $(c/p) = 1$. But $x_0 = A_{\ell-1}^2 + B_{\ell-1}^2 p^2 c$. Thus, by setting $f = (p-1)/(2^\alpha k)$, which is odd, we get

$$\begin{aligned} \varepsilon_{4c}^{(p-1)/2^{\alpha-1}} &\equiv \varepsilon_{4c}^{2kf} = (A_{\ell-1}^2 + B_{\ell-1}^2 p^2 c + 2A_{\ell-1}B_{\ell-1}p\sqrt{c})^f \\ &\equiv (-1 + 2A_{\ell-1}B_{\ell-1}p\sqrt{c})^f \equiv -1 \pmod{p} \end{aligned}$$

in $\mathbb{Z}[\sqrt{4c}]$.

Now if $n = \prod_{j=1}^r p_j^{a_j}$ is the canonical prime factorization of n , then for each j , there is an odd integer f_j such that $\varepsilon_c^{2f_j} \equiv -1 \pmod{p_j^{a_j}}$, so by the Chinese Remainder Theorem,

$$\varepsilon_{4c}^{2f} \equiv -1 \pmod{n}. \quad (3.25)$$

Conversely, it is clear that if (3.25) holds, then it holds for each prime factor. \square

Remark 3.2. It follows from Theorem 3.1 that $\ell(\sqrt{p^2c})$ is odd if and only if there is an odd integer such that $\varepsilon_{4c}^{2f} \equiv -1 \pmod{p}$ for an odd integer f , which is [5, Lemma 1, p. 72].

Corollary 3.2 (Stevenhagen [27]). *Suppose that $p \equiv 1 \pmod{4}$ is prime, $c \in \mathbb{N}$, not a perfect square, $(c/p) = 1$, and ε_{4c} is the fundamental unit of $\mathcal{O}_{4c}\mathbb{Z}[4\sqrt{c}]$ with \mathcal{P} an \mathcal{O}_{4c} -prime over p and $\ell(\sqrt{c})$ is odd. Then $\ell = \ell(\sqrt{cp^2})$ is odd if and only if ε_{4c} has order 4 modulo 8 in the multiplicative group of units $(\mathcal{O}_{4c}/\mathcal{P})^*$ of \mathcal{O}_{4c} modulo \mathcal{P} .*

Proof. By Corollary 3.1, ℓ is odd if and only if

$$\varepsilon_{4c}^{(p-1)/2^{\alpha-1}} \equiv -1 \pmod{p} \quad (\text{in } \mathbb{Z}[\sqrt{c}])$$

and this holds if and only if $\varepsilon_{4c}^{2f} \equiv 1 \pmod{p}$ for some odd f by Remark 3.2.

Now, there is a natural isomorphism as follows:

$$\iota : (\mathcal{O}_{4c}/p\mathcal{O}_{4c})^*/(\mathbb{Z}/p\mathbb{Z})^* \rightarrow (\mathcal{O}_{4c}/\mathcal{P})^*$$

given by

$$\iota(x \pmod{p\mathcal{O}_{4c}}) \mapsto \iota(x^2/N(x)).$$

Hence, for $x = \varepsilon_{4c}$, we have that x has odd order in $(\mathcal{O}_{4c}/p\mathcal{O}_{4c})^*/(\mathbb{Z}/p\mathbb{Z})^*$ if and only if $\iota(-\varepsilon_{4c}^2)$ has odd order in $(\mathcal{O}_{4c}/\mathcal{P})^*$, which it does by the above. Since $4 \mid |(\mathcal{O}_{4c}/\mathcal{P})^*|$, we have the result. \square

Remark 3.3. In [27], the above identifications are made in the proof to establish the result since, as noted therein, ℓ is odd if and only if $\ell(\sqrt{c})$ is odd and $\mathcal{O}^*/\mathbb{Z}[\sqrt{cp^2}]$ has odd order, observing that $\mathcal{O}^*/\mathbb{Z}[\sqrt{cp^2}] = \langle \varepsilon_{4c} \rangle$. However, the connection with Corollary 3.1 is not made as we have above.

Example 3.1. Let $D = 2 \cdot 137^2$ with $\ell(\sqrt{D}) = 9$, $\ell(\sqrt{c}) = 1$, $\varepsilon_{4c} = \varepsilon_8 = 1 + \sqrt{2}$, $c = 2$ and $p = 137 \equiv 9 \pmod{16}$. Here

$$\varepsilon_{4c}^{(p-1)/2^{\alpha-1}} = \varepsilon_8^{34} = \varepsilon_8^{2f} = 5168247530883 + 3654502875938\sqrt{2} \equiv -1 \pmod{p}$$

since

$$x_0 = A_{\ell-1}^2 + B_{\ell-1}^2 p^2 c = 5168247530883 \equiv -1 \pmod{p}$$

and

$$3654502875938 \equiv 0 \pmod{p}.$$

Some results on quartic residues will be needed – see [12] for background.

Theorem 3.2. *If $p = c^2 + 32d^2 \equiv 9 \pmod{16}$ is prime, then*

$$(1 + \sqrt{2})^{(p-1)/4} \equiv (-1)^{d+1} \pmod{p} \quad \text{in } \mathbb{Z}[\sqrt{2}]. \quad (3.26)$$

Proof. See [7, Theorem 1, p. 294]. □

Remark 3.4. We have stated Theorem 3.2 in a form that is tantamount to the quartic residue symbol being used. In other words, under the hypothesis of Theorem 3.2, $(\alpha/p)_4 = (-1)^{d+1}$, where the quartic residue symbol is equal to 1 if α is a fourth power modulo p and is equal to -1 otherwise. Note that Corollary 3.1 above is related to this discussion.

Note that without the hypothesis in Corollary 3.2, (3.26) does not hold. For instance, we have $73 \equiv 9 \pmod{16}$ but $73 \neq c^2 + 32d^2$. However, $((1 + \sqrt{2})/73)_4 = -1$ since $(1 + \sqrt{2})^{(p-1)/4} \equiv 6\sqrt{2} \pmod{73}$. By the Euler criterion, if

$$((1 + \sqrt{2})/73)_4 = 1,$$

then $(1 + \sqrt{2}) \equiv x^4 \pmod{p}$, so $(1 + \sqrt{2})^{(p-1)/4} \equiv x^{(p-1)} \equiv 1 \pmod{p}$, and this fails to hold. Yet $\ell(\sqrt{2} \cdot 13^2) = 30$.

We also need the following which uses the usual notion of the quartic and octic residue symbols as given in [12].

Theorem 3.3. *If $p = a^2 + 16b^2 = c^2 + 8d^2$ with $a \equiv c \equiv 1 \pmod{4}$, then*

$$\left(\frac{1 + \sqrt{2}}{p} \right) = (-1)^d = \left(\frac{-4}{p} \right)_8, \quad (3.27)$$

where the left-hand symbol is the Legendre symbol and the right-hand symbol is the octic residue symbol.

Proof. See [1]. □

The following classical result ensues from the above.

Corollary 3.3 (Perrot [24]). *Let $D = 2p^2$, where $p > 2$ is prime and set $\ell = \ell(\sqrt{D})$. Then each of the following holds:*

(a) *If*

$$p \equiv 9 \pmod{16} \quad \text{with} \quad p = u^2 + 2v^2 \quad \text{and} \quad 8|v, \quad (3.28)$$

then ℓ is odd.

(b) *If*

$$p \equiv 1 \pmod{8} \quad \text{with} \quad p = u^2 + 2v^2 \quad \text{and} \quad \ell \text{ is odd}, \quad (3.29)$$

then $8|v$.

Proof. If (3.28) holds and ℓ is even, then by Corollary 3.1,

$$(1 + \sqrt{2})^{(p-1)/4} = \varepsilon_8^{(p-1)/4} \not\equiv -1 \pmod{p}$$

in $\mathbb{Z}[\sqrt{2}]$. However, by Theorem 3.2, this means that

$$p = c^2 + 32d^2 \quad (3.30)$$

with d odd, contradicting that $8|v$, since the representation (3.30) is unique.

Now assume that (3.29) holds. If $4|v$, then by (3.26) in Theorem 3.2 and Corollary 3.1,

$$\varepsilon_8^{(p-1)/4} \equiv (-1)^{-1+v/4} \equiv -1 \pmod{p},$$

making $v/4$ even, namely $8|v$. If $2||v$, then by (3.27) in Theorem 3.3,

$$\varepsilon_8^{(p-1)/2} \equiv -1 \pmod{p}. \quad (3.31)$$

If $p - 1 = 8f$ for odd f , then (3.31) implies

$$\varepsilon_8^{4f} \equiv -1 \pmod{p}.$$

However, since ℓ is odd, then by Corollary 3.1,

$$\varepsilon_8^{2f} = \varepsilon_8^{(p-1)/4} \equiv -1 \pmod{p},$$

so $\varepsilon_8^{2f} \equiv -1 \equiv \varepsilon_8^{4f} \pmod{p}$, a contradiction, so $8|v$. \square

Remark 3.5. Essentially Corollary 3.3 says that if $p = u^2 + 2v^2 \equiv 9 \pmod{16}$, then $\ell(\sqrt{2p^2})$ is odd if and only if $8|v$. Note, as well, that when $p \equiv 1 \pmod{8}$, then p always has a representation in the form $p = u^2 + 2v^2$ – see [18]-[19] for instance. Given that Perrot's proof of the quadratic non-residuacity of $\varepsilon_8^{(p-1)/4}$ takes the majority of his nearly forty page paper, and the paper is a tedious check involving primitive roots that is not easily read, it is worthy to have a proof such as that above.

Example 3.2. If $D = 2 \cdot 313^2$, then $\ell(\sqrt{D}) = 64$ and we note that $313 = 5^2 + 32 \cdot 3^2$ with

$$pB_{\ell-1} = 313 \cdot 811734725690917631699691070 = B'_{77} = B'_{2f-1}$$

but $p = 313$ does not divide B'_{f-1} . If $D = 2 \cdot 137^2$, then $\ell = 9$, and $pB_{\ell-1} = 137 \cdot 1607521 = B'_{16} = B'_{f-1}$.

Remark 3.6. Theorem 3.3 says that, in particular,

$$\left(\frac{1 + \sqrt{2}}{p} \right) = 1 \text{ if and only if } p = c^2 + 32d^2. \quad (3.32)$$

We also require the following, where (x_0, y_0) will denote the fundamental solution of $x^2 - Dy^2 = 1$ for the balance of this work.

Theorem 3.4. Suppose that $\Delta = 4\Delta$ is a discriminant with radicand $D = ab$, where $1/\alpha \leq a < b$, and $\alpha = 2$ if y_0 is odd and $\alpha = 1$ if y_0 is even. If $\ell = \ell(\sqrt{D})$ is even, then the following are equivalent:

(a) $Q_{\ell/2} = \alpha a$.

(b) *There exists a solution to the Diophantine equation*

$$ax^2 - by^2 = (-1)^{\ell/2} \alpha, \quad (3.33)$$

where $e\sqrt{a} + s\sqrt{b}$ is the fundamental one.

(c) *The following congruences hold:*

$$x_0 \equiv (-1)^{\ell/2+1} \pmod{2a/\alpha} \quad \text{and} \quad x_0 \equiv (-1)^{\ell/2} \pmod{2b/\alpha}. \quad (3.34)$$

Proof. See [23]. □

Corollary 3.4 [15, Theorem 3.1 and Remark 3.3, pp. 1042-1044]. *If $D > 1$ is a radicand and $\ell = \ell(\sqrt{D})$ is even, then the following are equivalent:*

(a) $Q_{\ell/2} = 2$.

(b) *There is a solution to the Diophantine equation*

$$x^2 - Dy^2 = 2(-1)^{\ell/2}.$$

(c) $x_0 \equiv (-1)^{\ell/2} \pmod{D}$.

4. Central Norms

The notation of the previous section is in force. The results of this section extend the ideas presented in [17], where only central norms as powers of 2 were considered. The following is a tool resulting from the continued fraction development presented earlier that we will employ herein.

Lemma 4.1. *Suppose that $D = m^{2d}c$, where $d, m, c \in \mathbb{N}$ with c not a perfect square. Also, let $\ell = \ell(\sqrt{D})$, $\ell' = \ell(\sqrt{c})$, $\alpha = 1$, respectively $\alpha' = 1$, if ℓ , respectively ℓ' , is even, and $\alpha = 2$, respectively $\alpha' = 2$, if ℓ , respectively ℓ' , is odd. Then if A_j, B_j , respectively, A'_j, B'_j denote the values from (2.2)-(2.3) in the simple continued fraction expansion of \sqrt{D} , respectively \sqrt{c} , then*

$$A_{\alpha\ell-1} = A'_{\alpha'k\ell'-1} \quad \text{and} \quad m^d B_{\alpha\ell-1} = B'_{\alpha'k\ell'-1} \quad \text{for some } k \in \mathbb{N}.$$

Proof. Employing Remark 2.1, we know that the fundamental solution of

$x^2 - Dy^2 = 1$ is $A_{\alpha\ell-1} + B_{\alpha\ell-1}\sqrt{D} = A_{\alpha\ell-1} + m^d B_{\alpha\ell-1}\sqrt{c}$ and the fundamental solution of $x^2 - cy^2 = 1$ is $A'_{\alpha'\ell'-1} + B'_{\alpha'\ell'-1}\sqrt{c}$. Therefore,

$$A_{\alpha\ell-1} + m^d B_{\alpha\ell-1}\sqrt{c} = (A'_{\alpha'\ell'-1} + B'_{\alpha'\ell'-1}\sqrt{c})^k = A'_{\alpha'k\ell'-1} + B'_{\alpha'k\ell'-1}\sqrt{c}$$

for some $k \in \mathbb{N}$, and the result follows. \square

Corollary 4.1. *Suppose that $D = m^2c$, where $m \in \mathbb{N}$, $\ell' = \ell(\sqrt{c})$ is odd, where c is not a perfect square. Then $\ell = \ell(\sqrt{D})$ is odd if and only if $m | B'_{k\ell'-1}$ for some odd $k \in \mathbb{N}$, where $A'_{\ell'-1} + B'_{\ell'-1}\sqrt{c}$ is the fundamental solution of $x^2 - cy^2 = -1$.*

Proof. If ℓ is odd, then from Lemma 4.1, we deduce that

$$A_{\ell-1} + mB_{\ell-1}\sqrt{c} = A'_{k\ell'-1} + B'_{k\ell'-1}\sqrt{c}$$

for some odd $k \in \mathbb{N}$, so $m | B'_{k\ell'-1}$.

Conversely, assume that $m | B'_{k\ell'-1}$ for some odd $k \in \mathbb{N}$. Therefore,

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

so ℓ is odd. \square

Example 4.1. Let $D = 5m^2$, where $m \in \mathbb{N}$. Since $\ell' = 1$, any $m | B'_{k-1}$ for k odd will result in an $\ell = \ell(\sqrt{D})$. For instance, $17 | B'_2$ and $\ell(5 \cdot 17^2) = 1$; $17 \cdot 53 | B'_8$ and $\ell(5 \cdot 17^2 \cdot 53^2) = 7$; $109441 | B'_{14}$ and $\ell(5 \cdot 109441^2) = 11$; and so forth.

Remark 4.1. We maintain the notation of Lemma 4.1 for A_j , A'_j , etc. throughout.

Theorem 4.1. *Let $D = m^{2d}c$, where $d \in \mathbb{N}$, $m \in \mathbb{N}$, and $c > 1$ is not a perfect square, with $\gcd(c, m) = 1$, and $\ell = \ell(\sqrt{D})$ even. Set $\ell' = \ell(\sqrt{c})$, with $\alpha' = 1$ if ℓ' is even and $\alpha' = 2$ if ℓ' is odd and α is as defined in Theorem 3.4. Then each of the following holds.*

(a) $Q_{\ell/2} = 2m^{2d}/\alpha'$ if and only if for some $k \in \mathbb{N}$,

$$A_{\ell-1} = A'_{\alpha'k\ell-1} = \frac{\alpha'}{2} \left(\frac{A_{\ell/2-1}^2}{m^{2d}} + B_{\ell/2-1}^2 c \right) \quad (4.35)$$

and

$$B'_{\alpha'k\ell-1} = \frac{\alpha' A_{\ell/2-1} B_{\ell/2-1}}{m^d} = m^d B_{\ell-1}. \quad (4.36)$$

Moreover, when $\alpha' = 2$, $\ell/2 \equiv k \pmod{2}$. Also,

$$x_0 \equiv (-1)^{\ell/2+1} \pmod{4m^{2d}/(\alpha^2\alpha')} \quad \text{and} \quad x_0 \equiv (-1)^{\ell/2} \pmod{c\alpha'}.$$

(b) $Q_{\ell/2} = 2c/\alpha'$ if and only if for some $k \in \mathbb{N}$,

$$A_{\ell-1} = A'_{\alpha'k\ell-1} = \frac{\alpha'}{2} \left(\frac{A_{\ell/2-1}^2}{c} + B_{\ell/2-1}^2 m^{2d} \right)$$

and

$$B'_{\alpha'k\ell-1} = \frac{\alpha' A_{\ell/2-1} B_{\ell/2-1} m^d}{c} = B_{\ell-1} m^d.$$

Moreover, when $\alpha' = 2$, $k \equiv \ell/2 + 1 \pmod{2}$. Also,

$$x_0 \equiv (-1)^{\ell/2+1} \pmod{4c/(\alpha^2\alpha')} \quad \text{and} \quad x_0 \equiv (-1)^{\ell/2} \pmod{\alpha' m^{2d}}.$$

(c) $Q_{\ell/2} = m^{2d}$ and $\alpha' = 1 = \alpha$ if and only if for some $k \in \mathbb{N}$,

$$A'_{k\ell-1} = \frac{A_{\ell/2-1}^2}{m^{2d}} + B_{\ell/2-1}^2 c = A_{\ell-1}$$

and

$$B'_{k\ell-1} = \frac{2A_{\ell/2-1}B_{\ell/2-1}}{m^d} = m^d B_{\ell-1}.$$

Also,

$$x_0 \equiv (-1)^{\ell/2+1} \pmod{2m^{2d}} \quad \text{and} \quad x_0 \equiv (-1)^{\ell/2} \pmod{2c}.$$

(d) $Q_{\ell/2} = \alpha'c$ if and only if for some $k \in \mathbb{N}$,

$$A'_{\alpha'k\ell'-1} = \frac{1}{\alpha'} \left(\frac{A_{\ell/2-1}^2}{c} + B_{\ell/2-1}^2 m^{2d} \right) = A_{\ell-1}$$

and

$$B'_{\alpha'k\ell'-1} = \frac{2A_{\ell/2-1}B_{\ell/2-1}m^d}{\alpha'c} = m^d B_{\ell-1}.$$

Moreover, when $\alpha' = 2$, then $k \equiv \ell/2 \pmod{2}$. Also,

$$x_0 \equiv (-1)^{\ell/2+1} \pmod{2\alpha'c/\alpha'^2} \quad \text{and} \quad x_0 \equiv (-1)^{\ell/2} \pmod{2m^{2d}/\alpha'}.$$

Proof. We establish only part (a) since parts (b)-(d) follow by an entirely analogous argument. By Lemma 4.1, $A_{\ell-1} = A'_{\alpha'k\ell'-1}$ and $m^d B_{\ell-1} = B'_{\alpha'k\ell'-1}$ for some $k \in \mathbb{N}$. Thus, by (c) in parts 1-2 of Theorem 2.2, we deduce that $Q_{\ell/2} = 2m^{2d}/\alpha'$ if and only if (4.35)-(4.36) hold. The congruence conditions on x_0 follow from Theorem 3.4 directly since $Q_{\ell/2} = 2m^{2d}/\alpha' = \alpha a$ if and only if

$$x_0 \equiv (-1)^{\ell/2+1} \pmod{4m^{2d}/(\alpha\alpha')} \quad \text{and} \quad x_0 \equiv (-1)^{\ell/2} \pmod{c\alpha'}.$$

Furthermore, when this occurs, say with $\alpha' = 2$, which forces $\beta = 1$, then

$$\begin{aligned} (A'_{k\ell'-1} + B'_{k\ell'-1}\sqrt{c})^2 &= A_{2k\ell'-1} + B_{2k\ell'-1} \\ &= \frac{A_{\ell/2-1}^2}{m^{2d}} + B_{\ell/2-1}^2 c + \frac{2A_{\ell/2-1}B_{\ell/2-1}}{m^d} \sqrt{c} \\ &= \left(\frac{A_{\ell/2-1}}{m^d} + \frac{B_{\ell/2-1}}{m^d} \sqrt{D} \right)^2 \end{aligned}$$

so $A'_{k\ell'-1} + B'_{k\ell'-1}\sqrt{c} = (A_{\ell/2-1} + B_{\ell/2-1}\sqrt{D})/m^d$ from which it follows that $k \equiv \ell/2 \pmod{2}$. \square

Remark 4.2. The case where $m = 1 = \alpha'$ in part (a) of Theorem 4.1 is just an instance of Theorem 2.2, part 2 with $a = 1$, namely $Q_{\ell/2} = 2$ and $k = 1$ in this

case. The special case in part (a) of Theorem 4.1, where $\alpha' = 2$ and $k = 1$ for general m is [21, Theorem 3.1, p. 5]. In previous work [23], we completely generalized Lagrange's criterion which the first author had related to the central norm being equal to 2 in [15]. The case where $m = 2$, in part (c) generalizes [17, Theorem 5, p. 125]. As well, for $m = 2$, $\alpha' = 1$, $c = 2c_1$ with c_1 odd, generalizes [17, Theorem 6, p. 126].

We have not explicitly used the fact that $\gcd(c, m) = 1$ in the proof of Theorem 4.1 is not explicitly required, but if this hypothesis is not satisfied, then cases other than (a)-(d) occur in terms of the central norm being one of the cases covered. For instance, if $D = 3^3$, where $m^{2d} = 3^2$ and $c = 3$, then none of the cases cover the fact that $Q_{\ell/2} = Q_1 = 2$, where $\alpha' = 1$ and $\alpha = 2$. However, if we let $m = 1$ and $c = D = 3^3$, then as indicated above, part (a) covers this case.

Also, note that assuming $\alpha' = 1 = \alpha$, namely ℓ' even, and y_0 is even, in part (c) is not a restriction. To see why consider what happens if ℓ' is odd. To have $Q_{\ell/2} = 2m^{2d}$ implies that one of part 1 or 2 of Theorem 2.2 holds. If it is part 1, then $a = 2m^{2d} \mid m^{2d}c$ so c is even and $b = c/2$, so (2.17) implies that ℓ' is even. If part 2 holds, then again a factorization of c cannot occur *including* the trivial one where $a = 1$, since otherwise, again ℓ' is even. Hence $\alpha' = 2$ cannot occur in part (c). In general, if ℓ' is odd, then part 2 of Theorem 2.2 cannot occur for the above reasons. Also, since we have just shown that $Q_{\ell/2} = m^{2d}$, then we are in part 1 of Theorem 2.2, where $B_{\ell-1} = y_0$ is even, so $\alpha = 1$.

We get the following recent result as a consequence of the above.

Corollary 4.2 (Redei [26]). *Suppose that $D = p^2c$, where p is a prime, c is not a perfect square, and $\ell' = \ell(\sqrt{c})$ is odd. Then each of the following holds:*

- (a) *If p is an odd prime dividing c , then $\ell = \ell(\sqrt{c})$ is odd.*
- (b) *If $p \equiv 1 \pmod{4}$ and the Legendre symbol $(c/p) = -1$, then $\ell(\sqrt{D})$ is odd.*
- (c) *If $p = 2$ or $p \equiv 3 \pmod{4}$, then $\ell(\sqrt{D})$ is even.*

Proof. If $p|c$ and $\ell(\sqrt{D})$ is even, then by Theorem 2.2, (2.17) cannot hold since there can be no factorization $c = c_1c_2$ with $1 < c_1 < c_2$ with one of c_1 dividing a and the other dividing b , given that ℓ' is odd. Similarly, (2.18) can only hold for $a = 1$, which forces $\ell(\sqrt{D})$ to be odd since $\ell(\sqrt{c})$ is odd. This is (a).

Now assume that $p \equiv 1 \pmod{4}$, $(c/p) = -1$, and $\ell(\sqrt{D})$ is even. Then by Remark 4.2, Part 1 of Theorem 2.2 holds. Therefore, $x^2p^2 - y^2c = \pm 1$ for some x, y , so the following Legendre symbol equality holds

$$1 = \left(\frac{\pm 1}{p}\right) = \left(\frac{x^2p^2 - y^2c}{p}\right) = \left(\frac{-c}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{c}{p}\right) = -1,$$

a contradiction, so $\ell(\sqrt{D})$ is odd. This is (b).

If $p = 2$ or $p \equiv 3 \pmod{4}$, and $\ell(\sqrt{D})$ is odd, then $A_{\ell-1}^2 - DB_{\ell-1}^2D = -1$, so $-1 \equiv A_{\ell-1}^2 \pmod{p}$, a contradiction if $p > 2$, and if $p = 2$, then $A_{\ell-1}^2 \equiv -1 \pmod{4}$, a contradiction. Thus, $\ell(\sqrt{D})$ is even, and this is (c). \square

The following are illustrations of Theorem 4.1 for the various cases.

Example 4.2. Let $D = 5^2 \cdot 27 = m^{2d} \cdot c = 675$ for which $\ell = \ell' = 2$, $Q_{\ell/2} = 50 = 2 \cdot m^{2d}$, $A_{\ell/2-1} = 25$, $B_{\ell/2-1} = 1$, $A_{\ell'-1} = 26$ and $B_{\ell'-1} = 5$, where

$$A_{\ell-1} = \frac{1}{2} \left(\frac{A_{\ell/2-1}^2}{m^{2d}} + B_{\ell/2-1}^2 c \right) = \frac{1}{2} \left(\frac{25^2}{5^2} + 1^2 \cdot 27 \right) = 26 = A_{\ell'-1}$$

and

$$m^d B_{\ell-1} = \frac{A_{\ell/2-1} B_{\ell/2-1}}{m^d} = \frac{25 \cdot 1}{5} = 5 = B_{\ell'-1}.$$

Also,

$$x_0 = 26 \equiv 1 \equiv (-1)^{\ell/2+1} \pmod{4m^{2d}/(\alpha^2\alpha')}$$

and

$$x_0 \equiv -1 \equiv (-1)^{\ell/2} \pmod{c\alpha'}.$$

This illustrates part (a) of Theorem 4.1 when $\alpha' = 1$ and $\alpha = 2$.

Example 4.3. Let $D = 5^2 \cdot 101 = m^{2d} \cdot c$, for which $\ell = 2$, $\ell' = 1$, $A_{\ell/2-1} = 50$, $B_{\ell/2-1} = 1$,

$$A'_{\alpha'k\ell'-1} = A'_{2\ell'-1} = 201 = A_{\ell/2-1}^2/m^{2d} + B_{\ell/2-1}^2c = A_{\ell-1},$$

$$B'_{2\ell'-1} = 20 = 2A_{\ell/2-1}B_{\ell/2-1}/m^d = m^d B_{\ell-1},$$

and $Q_{\ell/2} = Q_1 = 5^2 = m^{2d}$. Also,

$$x_0 = 201 \equiv 1 \equiv (-1)^{\ell/2+1} \pmod{4m^{2d}/(\alpha^2\alpha')}$$

and

$$x_0 \equiv -1 \equiv (-1)^{\ell/2} \pmod{c\alpha'}.$$

This illustrates part (a) of Theorem 4.1 when $\alpha' = 2$ and $\alpha = 1$.

Example 4.4. Let $D = 8^2 \cdot 17 = m^{2d} \cdot c$, for which $\ell = 2$, $\ell' = 1$, $A_{\ell/2-1} = 32$, $B_{\ell/2-1} = 1$,

$$A'_{\alpha'k\ell'-1} = A'_{2\ell'-1} = 33 = A_{\ell/2-1}^2/m^{2d} + B_{\ell/2-1}^2c = A_{\ell-1},$$

$$B'_{2\ell'-1} = 8 = 2A_{\ell/2-1}B_{\ell/2-1}/m^d = m^d B_{\ell-1},$$

and $Q_{\ell/2} = Q_1 = 8^2 = m^{2d}$. Also,

$$x_0 = 33 \equiv 1 \equiv (-1)^{\ell/2+1} \pmod{4m^{2d}/(\alpha^2\alpha')}$$

and

$$x_0 \equiv -1 \equiv (-1)^{\ell/2} \pmod{c\alpha'}.$$

This illustrates part (a) of Theorem 4.1 when $\alpha' = \alpha = 2$.

Example 4.5. Let $D = 3^2 \cdot 38 = m^{2d} \cdot c$, for which $\ell = \ell' = 2$, $A_{\ell/2-1} = 18$, $B_{\ell/2-1} = 1$,

$$A'_{\alpha'k\ell'-1} = A'_{\ell'-1} = 37 = \frac{1}{2}(A_{\ell/2-1}^2/m^{2d} + B_{\ell/2-1}^2c) = A_{\ell-1},$$

$$B'_{2^{\ell'-1}} = 6 = A_{\ell/2-1} B_{\ell/2-1} / m^d = m^d B_{\ell-1},$$

and $Q_{\ell/2} = Q_1 = 2 \cdot 3^2 = 2m^{2d}$. Also,

$$x_0 = 37 \equiv 1 \equiv (-1)^{\ell/2+1} \pmod{4m^{2d}/(\alpha^2\alpha')}$$

and

$$x_0 \equiv -1 \equiv (-1)^{\ell/2} \pmod{c\alpha'}.$$

This illustrates part (a) of Theorem 4.1 when $\alpha' = \alpha = 1$.

Having given a depiction of Theorem 4.1 for each of the four cases in part (a), we merely give one instance of each case for (b)-(d).

Example 4.6. Let $D = 3^2 \cdot 7 = m^{2d} \cdot c$, for which $\ell = 2$, $\ell' = 4$, $Q_{\ell/2} = 14 = 2c$, $A_{\ell/2-1} = 7$, $B_{\ell/2-1} = 1$,

$$A'_{\alpha'k\ell'-1} = A'_3 = \frac{1}{2}(7^2/7 + 1^2 \cdot 3^2) = 8 = A_{\ell-1} = \frac{1}{2}(A_{\ell/2-1}^2/c + B_{\ell/2-1}^2 m^{2d}),$$

$$B_3 = 3 = m^d B_{\ell-1} = A_{\ell/2-1} B_{\ell/2-1} m^d / c.$$

Also,

$$x_0 = 8 \equiv 1 \equiv (-1)^{\ell/2+1} \pmod{4c/(\alpha^2\alpha')} \quad \text{and} \quad x_0 \equiv -1 \equiv (-1)^{\ell/2} \pmod{\alpha' m^{2d}}.$$

This illustrates part (b) of Theorem 4.1 when $\alpha' = 1$ and $\alpha = 2$.

Example 4.7. Let $D = 3^2 \cdot 23 = m^{2d} \cdot c$, for which $\ell = 8$, $\ell' = 4$, $Q_{\ell/2} = 9 = m^{2d}$, $A_{\ell/2-1} = 72$, $B_{\ell/2-1} = 5$,

$$A'_{\alpha'k\ell'-1} = A'_7 = 72^2/3^2 + 5^2 \cdot 23 = 1151 = A_{\ell-1} = A_{\ell/2-1}^2/m^{2d} + B_{\ell/2-1}^2 c,$$

$$B'_7 = 240 = m^d B_{\ell-1} = 2A_{\ell/2-1} B_{\ell/2-1} / m^d.$$

Also,

$$x_0 = 2251 \equiv -1 \equiv (-1)^{\ell/2+1} \pmod{2m^{2d}/\alpha^2} \quad \text{and} \quad x_0 \equiv 1 \equiv (-1)^{\ell/2} \pmod{2c}.$$

This illustrates part (c) of Theorem 4.1.

Example 4.8. Let $D = 7^2 \cdot 3 = m^{2d} \cdot c$, for which $\ell = 2 = \ell'$, $Q_{\ell/2} = 3 = c$, $A_{\ell/2-1} = 12$, $B_{\ell/2-1} = 1$,

$$A'_{\alpha'k\ell-1} = A'_7 = 12^2/3 + 1^2 \cdot 7^2 = 97 = A_{\ell-1} = A_{\ell/2-1}^2/c + B_{\ell/2-1}^2 m^{2d},$$

$$B'_7 = 56 = m^d B_{\ell-1} = 2A_{\ell/2-1}B_{\ell/2-1}m^d/c.$$

Also,

$$x_0 = 97 \equiv 1 \equiv (-1)^{\ell/2+1} \pmod{2\alpha'c/\alpha^2} \quad \text{and} \quad x_0 \equiv -1 \equiv (-1)^{\ell/2} \pmod{2m^{2d}/\alpha'}.$$

This illustrates part (d) of Theorem 4.1 when $\alpha' = \alpha = 1$.

As an auxiliary note to Theorem 3.1 and the discussion surrounding it, we have the following. In the theorem, \mathcal{C}_D denotes the *wide* or ordinary ideal class group of $\mathbb{Z}[\sqrt{D}]$, and \mathcal{C}_D^+ denotes its *narrow* ideal class group. Also, if $I \sim J$ denotes equivalence in the wide ideal class group, then an *ambiguous class of ideals* therein is one for which $I \sim I'$, where I' is the conjugate ideal to I and an *ambiguous ideal* is one for which $I = I'$.

Theorem 4.2. *If $D > 1$ is a non-square integer, then the following are equivalent:*

(a) $x^2 - Dy^2 = -1$ has a solution.

(b) If $x_0 + y_0\sqrt{D}$ is the fundamental solution of $x^2 - Dy^2 = 1$, then $x_0 \equiv -1 \pmod{2D}$.

(c) D is a sum of two integer squares and there does not exist an ambiguous class of ideals in \mathcal{C}_D without any ambiguous ideals in them.

(d) Every element of order 2 in \mathcal{C}_D is the image of an ambiguous class of ideals under the natural mapping $\rho : \mathcal{C}_D^+ \mapsto \mathcal{C}_D$ and -1 is a quadratic residue modulo D .

(e) There exist $A, B, C \in \mathbb{N}$ with

$$C^2 = A^2 + B^2, \quad \text{where } \gcd(A, B) = 1, \quad D = a^2 + b^2 \quad \text{and} \quad |aA - bB| = 1. \quad (4.37)$$

Proof. The equivalence of (a) and (b) is proved in [23, Theorem 3.1]. The equivalence of (a) and (c) is proved in [11, Lemma 6.1.3, p. 191]. The equivalence of (a) and (d) is proved in [20]. The equivalence of (a) and (e) is proved in [4].

Since the equivalence of (a) and (e) is intimately linked to the results herein with our continued fraction approach, we provide a proof that does not appear explicitly in the literature. (However, we acknowledge the contribution of Kaplan and Williams in [6] connecting continued fractions intimately with the solution of Pell's equations $x^2 - Dy^2 = -1, -4$ – see also [11, Exercises 2.1.14-2.1.15, pp. 59-60]. Moreover, this proof is instructive in the connection with continued fractions that is very rarely made.

If (a) holds, then $\ell = \ell(\sqrt{D})$ is odd and from (2.5) and (2.11),

$$D = P_{(\ell+1)/2}^2 + Q_{(\ell+1)/2}^2. \quad (4.38)$$

Now we need to show the critical result as follows.

Claim 4.1. $B_{\ell-1} = B_{(\ell-1)/2}^2 + B_{(\ell-3)/2}^2$.

We employ the general result for units of quadratic orders proved, for instance in [22, Theorem 3, p. 44], from which it follows that the ensuing matrix equations hold, where the q_j comes from (2.1),

$$\begin{aligned} & \begin{pmatrix} A_{(\ell-1)/2} & A_{(\ell-3)/2} \\ B_{(\ell-1)/2} & B_{(\ell-3)/2} \end{pmatrix} \cdot \begin{pmatrix} A_{(\ell-1)/2} & B_{(\ell-1)/2} \\ A_{(\ell-3)/2} & B_{(\ell-3)/2} \end{pmatrix} & (4.39) \\ & = \begin{pmatrix} A_{\ell-1} & A_{\ell-2} \\ B_{\ell-1} & B_{\ell-2} \end{pmatrix} \cdot \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \\ & = \prod_{j=0}^{\ell-1} \begin{pmatrix} q_j & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \\ & = \begin{pmatrix} DB_{\ell-1} & A_{\ell-1} \\ A_{\ell-1} & B_{\ell-1} \end{pmatrix}, & (4.40) \end{aligned}$$

from which the claim follows from the right lower entries in (4.39) and (4.40).

Another result, we need, is the following:

Claim 4.2. $A_{(\ell-3)/2} = Q_{(\ell+1)/2}B_{(\ell-1)/2} - P_{(\ell+1)/2}B_{(\ell-3)/2}$.

Since $Q_{(\ell+1)/2} = Q_{(\ell-1)/2}$, using (2.3)-(2.4) and (2.7), we get

$$\begin{aligned} & Q_{(\ell+1)/2}B_{(\ell-1)/2} - P_{(\ell+1)/2}B_{(\ell-3)/2} \\ &= Q_{(\ell-1)/2}(q_{(\ell-1)/2}B_{(\ell-3)/2} + B_{(\ell-5)/2}) - B_{(\ell-3)/2}(q_{(\ell-1)/2}Q_{(\ell-1)/2} - P_{(\ell-1)/2}) \\ &= Q_{(\ell-1)/2}B_{(\ell-5)/2} + B_{(\ell-3)/2}P_{(\ell-1)/2} \\ &= A_{(\ell-3)/2}, \end{aligned}$$

which is Claim 4.2.

Now, we set $a = P_{(\ell+1)/2}$, $b = Q_{(\ell+1)/2}$, $A = 2B_{(\ell-1)/2}B_{(\ell-3)/2}$, $B = B_{(\ell-1)/2}^2 - B_{(\ell-3)/2}^2$, and $C = B_{\ell-1}$. Then we get

$$\begin{aligned} A^2 + B^2 &= (2B_{(\ell-1)/2}B_{(\ell-3)/2})^2 + (B_{(\ell-1)/2}^2 - B_{(\ell-3)/2}^2)^2 \\ &= (B_{(\ell-1)/2}^2 + B_{(\ell-3)/2}^2)^2 = C^2, \end{aligned}$$

from Claim 4.1 with $\gcd(A, B) = 1$ from (2.6). Also, $D = a^2 + b^2$ and

$$\begin{aligned} aA - bB &= P_{(\ell+1)/2}2B_{(\ell-1)/2}B_{(\ell-3)/2} - Q_{(\ell+1)/2}(B_{(\ell-1)/2}^2 - B_{(\ell-3)/2}^2) \\ &= B_{(\ell-3)/2}(P_{(\ell+1)/2}B_{(\ell-1)/2} + Q_{(\ell+1)/2}B_{(\ell-3)/2}) \\ &\quad - B_{(\ell-1)/2}(Q_{(\ell+1)/2}B_{(\ell-1)/2} - P_{(\ell+1)/2}B_{(\ell-3)/2}) \\ &= B_{(\ell-1)/2}A_{(\ell-3)/2} + B_{(\ell-3)/2}A_{(\ell-1)/2} \\ &= (-1)^{(\ell-1)/2}, \end{aligned}$$

so $|aA - bB| = 1$.

Conversely, assume that the conditions in (4.37) hold. Then setting $x = |aA - bB|$ and $y = C$ yields $x^2 - Dy^2 = -1$. \square

Corollary 4.3. *If -1 is a quadratic residue modulo D and $h_D = |\mathcal{C}_D|$ is odd, then ℓ is odd.*

Proof. Since h_D is odd, there can be no element of order 2 in \mathcal{C}_D so vacuously condition (d) is satisfied. \square

Example 4.9. If $D = p \equiv 1 \pmod{4}$ is prime or $D = 2$, then h_D is odd and $\ell(\sqrt{D})$ is odd – see [12, Theorem 3.70, p. 262] and [12, Exercise 3.90, p. 168] for instance.

Remark 4.3. It is valuable to note the continued fraction connection of the equivalence of (a) and (e) in Theorem 4.2, where solution of the negative Pell's equation is linked to Pythagorean triples, which is essentially due to Euler, albeit he would not have formulated the result in the following terms. In a first course in number theory, a lemma is derived that essentially says the following. When -1 is a quadratic residue of $D > 1$, then each solution $D = a^2 + b^2$ with $a, b \in \mathbb{N}$ and $\gcd(a, b) = 1$ determines a unique $m_{a,b} \in \mathbb{N}$ modulo D such that $a \equiv m_{a,b}b \pmod{D}$ and $m_{a,b}^2 \equiv -1 \pmod{D}$. Conversely, if $m^2 \equiv -1 \pmod{D}$, then there are unique relatively prime $a, b \in \mathbb{N}$ such that $D = a^2 + b^2$ with $a \equiv mb \pmod{D}$. What the above equivalence of (a) and (e) brings into focus is the exact intimate relationship that unfolds with respect to m and delineates exactly what that m happens to be. Let us explain.

The criterion for odd $\ell(\sqrt{D})$ given in Theorem 3.1 says that $x_0 \equiv -10 \pmod{2D}$, where (x_0, y_0) is the fundamental solution of $x^2 - Dy^2 = 1$. Thus, in the simple continued fraction expansion of \sqrt{D} , this means that $A_{\ell-1}^2 + B_{\ell-1}^2 D \equiv -1 \pmod{2D}$ so $A_{\ell-1}^2 \equiv -1 \pmod{D}$. The unique m discussed above can be deduced, via [11, Exercise 2.1.14, pp. 59-60] for instance, to be $m \equiv (-1)^{(\ell-1)/2} A_{\ell-1} \pmod{D}$ and it follows that

$$(-1)^{(\ell-1)/2} Q_{(\ell+1)/2} + A_{\ell-1} P_{(\ell+1)/2} = D(B_{(\ell-1)/2}^2 - B_{(\ell-3)/2}^2).$$

Thus, in the notation of Theorem 4.2,

$$b + ma = (-1)^{(\ell-1)/2} DB,$$

which shows the connection with our results herein in a precise fashion.

Acknowledgement

The first author gratefully acknowledges the support of NSERC Canada grant #A8484.

References

- [1] P. Barrucand and H. Cohn, Note on primes of the type $x^2 + 32y^2$, class number and residuacity, *J. Reine Angew. Math.* 238 (1969), 67-70.
- [2] P. E. Conner and J. Hurrelbrink, *Class Number Parity*, World Scientific Publishers Co., Singapore, New Jersey, Hong Kong, 1998.
- [3] G. P. L. Dirichlet, Einige neue Sätze über unbestimmte Gleichungen, *Abh. Kön. Akad. Wiss. Berlin* (1834), 649-664, *Gesammelte Werke I*, 221-236.
- [4] A. Grytchuk, F. Lucas and M. Wójtowicz, The negative Pell equation and Pythagorean triples, *Proc. Japan Acad. Ser. A Math. Sci.* 76 (2000), 91-94.
- [5] Chr. U. Jensen, On the solvability of a certain class of non-Pellian equations, *Math. Scand.* 10 (1962), 71-84.
- [6] P. Kaplan and K. S. Williams, Pell's equation $x^2 - Dy^2 = -1, -4$ and continued fractions, *J. Number Theory* 23 (1986), 169-182.
- [7] E. Lehmer, On the quartic character of quadratic units, *J. Reine Angew. Math.* 268/269 (1974), 294-301.
- [8] D. H. Lehmer, *Selected Papers of D. H. Lehmer*, D. McCarthy, ed., Vols. I-III, The Charles Babbage Research Centre, St. Pierre, Canada, 1981.
- [9] A. M. Legendre, *Thorie des Nombres*, Third Edition, Paris, Chez Firmin Didot Frres, Libraires, 1830.
- [10] H. W. Lenstra, Jr., Solving the Pell equation, *Notices Amer. Math. Soc.* 49 (2002), 182-192.
- [11] R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, New York, London, Tokyo, 1996.
- [12] R. A. Mollin, *Algebraic Number Theory*, Chapman & Hall/CRC Press, Boca Raton, New York, London, Tokyo, 1999.
- [13] R. A. Mollin, Polynomials of Pellian type and continued fractions, *Seridica Math. J.* 27 (2001), 317-342.
- [14] R. A. Mollin, A continued fraction approach to the Diophantine equation $ab^2 - by^2 = \pm 1$, *JP Jour. Algebra, Number Theory & Appl.* 4 (2004), 159-207.

- [15] R. A. Mollin, Lagrange, central norms, and quadratic Diophantine equations, *Internat. J. Math. Math. Sci.* 7 (2005), 1039-1047.
- [16] R. A. Mollin, Generalized Lagrange criteria for certain quadratic Diophantine equations, *New York J. Math.* 11 (2005), 539-545.
- [17] 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 $c > 1$, *Canada. Math. Bull.* 48 (2005), 121-132.
- [18] R. A. Mollin, *Fundamental Number Theory with Applications*, Second Edition, Chapman & Hall/CRC, Taylor & Francis Group, Boca Raton, London, New York, 2008.
- [19] R. A. Mollin, *Advanced Number Theory with Applications*, Chapman & Hall/CRC, Taylor & Francis Group, Boca Raton, London, New York, 2009.
- [20] R. A. Mollin, Characterization of $D = P^2 + Q^2$ when $\gcd(P, Q) = 1$ and $x^2 - Dy^2 = -1$ has no integer solutions, *Far East J. Math. Sci. (FJMS)* 32 (2009), 285-294.
- [21] R. A. Mollin, Central norms and continued fractions, *Internat. J. Pure Appl. Math.* 55 (2009), 1-8.
- [22] R. A. Mollin and K. Cheng, Matrices and continued fractions, *Int. Math. J.* 1 (2003), 41-58.
- [23] R. A. Mollin and A. Srinivasan, Pell equations: non-principal Lagrange criteria and central norms, (to appear).
- [24] J. Perrot, Sur l'équation $t^2 - Dy^2 = -1$, *J. Reine Angew. Math.* 102 (1888), 185-223.
- [25] D. Pumplün, Über die Klassenzahl und die Grundeinheit des reellquadratischen Zahlkörpers, *J. Reine Angew. Math.* 230 (1968), 167-210.
- [26] L. Rédei, Über die Pellsche Gleichung $x^2 - Dy^2 = -1$, *J. Reine Angew. Math.* 173 (1935), 193-221.
- [27] P. Stevehagen, Frobenius distributions for real quadratic orders, *J. de Théor. Nombres Bordeaux* 7 (1995), 121-132.

<p>Paper # PPH-0910086-MS</p> <p>Kindly return the proof after correction to:</p> <p style="text-align: center;"><i>The Publication Manager Pushpa Publishing House Vijaya Niwas 198, Mumfordganj Allahabad-211002 (India)</i></p> <p>along with the print charges* by the <u>fastest mail</u></p> <p>*Invoice attached</p>	<p>Proof read by:</p> <p>Copyright transferred to the Pushpa Publishing House</p> <p>Signature:</p> <p>Date:</p> <p>Tel:</p> <p>Fax:</p> <p>e-mail:</p> <p>Number of additional reprints required</p> <p>Cost of a set of 25 copies of additional reprints @ U.S. Dollars 15.00 per page. (25 copies of reprints are provided to the corresponding author ex-gratis)</p>
--	--