Canad. Math. Bull. Vol. **55** (4), 2012 pp. 774–782
http://dx.doi.org/10.4153/CMB-2011-118-9

Pell Equations: Non-Principal Lagrange Criteria and Central Norms

R. A. Mollin and A. Srinivasan

Abstract. We provide a criterion for the central norm to be any value in the simple continued fraction expansion of $\sqrt{D}$ for any non-square integer $D > 1$. We also provide a simple criterion for the solvability of the Pell equation $x^2 - Dy^2 = -1$ in terms of congruence conditions modulo D.

1 Introduction

Suppose that $x_0 + y_0\sqrt{D}$ is the smallest positive solution of $x^2 - Dy^2 = 1$, where D is a positive non-square integer. Lagrange proved that if $D = p$ is an odd prime, then $x_0 \equiv 1 \pmod{p}$ if and only if $p \equiv 7 \pmod{8}$. In [5], the first author generalized this to involve what is known as the central norm being equal to 2; see equation (2.4). It is one of our principal results to generalize that result so that the central norm can be any value. Moreover, we prove that for any non-square positive integer $D \equiv 1, 2 \pmod{4}$ there is a solution to the Pell equation $x^2 - Dy^2 = -1$ if and only if $x_0 \equiv -1 \pmod{2D}$; see Theorem 3.5.

2 Notation and Preliminaries

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

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

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

$$A_k = q_k A_{k-1} + A_{k-2}, \qquad B_k = q_k B_{k-1} + B_{k-2},$$

Received by the editors August 19, 2009; revised November 9, 2009.
Published electronically June 14, 2011.
AMS subject classification: **11D09**, 11A55, 11R11, 11R29 .
Keywords: Pell's equation, continued fractions, central norms.

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 $k \geq 1$,

$$P_{k+1} = q_k Q_k - P_k, \quad q_k = \left\lfloor \frac{P_k + \sqrt{D}}{Q_k} \right\rfloor, \quad \text{and} \quad D = P_{k+1}^2 + Q_k Q_{k+1}. \tag{2.1}$$

We will also need the following facts (which can be found in most introductory texts in number theory, such as [7]. Also, see [3] for a more advanced exposition). First,

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

Also,

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

and

$$A_{k-1}^2 - B_{k-1}^2 D = (-1)^k Q_k. \tag{2.2}$$

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

$$A_{k\ell-1}^2 - B_{k\ell-1}^2 D = (-1)^{k\ell}. \tag{2.3}$$

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

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

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

$$Q_{\ell/2} \text{ is called the } \textit{central norm}. \tag{2.4}$$

Furthermore,

$$Q_{(2k-1)\ell/2} \mid 2D \quad \text{and} \quad q_{(2k-1)\ell/2} = 2P_{(2k-1)\ell/2}/Q_{(2k-1)\ell/2}.$$

In the next section, we will consider what are typically called the standard Pell equations (2.5)–(2.6). The *fundamental solution* of such an equation is the (unique) least pair of positive integers (x, y) 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*

$$x^2 - y^2 D = 1 \tag{2.5}$$

are given by $x = A_{k\ell-1}$ and $y = B_{kl-1}$, whereas there are no solutions to

$$x^2 - y^2 D = -1. \tag{2.6}$$

If ℓ is odd, then all positive solutions of equation (2.5) *are given by $x = A_{2k\ell-1}$ and $y = B_{2k\ell-1}$, whereas all positive solutions of equation* (2.6) *are given by $x = A_{(2k-1)\ell-1}$ and $y = B_{(2k-1)\ell-1}$.*

The proof can be found in many introductory number theory texts possessing an in-depth section on continued fractions. For instance, [7, Corollary 5.7, p. 236].

Remark 2.2 For $\ell = \ell(\sqrt{D})$ let

$$x^2 - Dy^2 = (-1)^{\ell}. \tag{2.7}$$

Note that as a result of Theorem 2.1 the norm of the fundamental unit of $\mathbb{Z}[\sqrt{D}]$ is -1 if and only if ℓ is odd. If ℓ is even, (2.7) is called the *positive Pell equation*, and if ℓ is odd, it is referenced as the *negative Pell equation.* We denote the fundamental solution of the positive Pell equation by $(\mathbf{x_0}, \mathbf{y_0})$ and maintain this notation for the balance of the paper.

3 Criterion for Solvability of $x^2 - Dy^2 = -1$

All of the notation of the previous section is in force. Note especially Remark 2.2, the contents of which we employ herein.

Proposition 3.1 *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:*

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

$$ax^2 - by^2 = \pm 1. \tag{3.1}$$

Furthermore, in this case, each of the following holds, where $(x, y) = (r, s)$ is the fundamental solution of equation (3.1).

(a) $Q_{\ell/2} = a$.
(b) $A_{\ell/2-1} = ra$ *and* $B_{\ell/2-1} = s$.
(c) $A_{\ell-1} = r^2 a + s^2 b = x_0$ *and* $B_{\ell-1} = 2rs = y_0$, *since*

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

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

https://doi.org/10.4153/CMB-2011-118-9 Published online by Cambridge University Press

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

$$ax^2 - by^2 = \pm 2. \tag{3.2}$$

Moreover, in this case each of the following holds, where $(x, y) = (r, s)$ is the fundamental solution of equation (3.2).

(a) $Q_{\ell/2} = 2a$.
(b) $A_{\ell/2-1} = ra$ *and* $B_{\ell/2-1} = s$.
(c) $2A_{\ell-1} = r^2a + s^2b = 2x_0$ *and* $B_{\ell-1} = rs = y_0$, *since*

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

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

Proof All of this is proved in [4]. ■

Remark 3.2 Note that although Proposition 3.1 only deals with the case of $\sqrt{D}$ we have lost no generality (namely by excluding the maximal order $\mathbb{Z}[(1+\sqrt{D})/2]$ when $D \equiv 1 \pmod 4$), since $\ell(\sqrt{D}) \equiv \ell((1+\sqrt{D})/2) \pmod 2$. Indeed, not only do the period lengths of the orders $\mathbb{Z}[(1+\sqrt{D})/2]$ and $\mathbb{Z}[\sqrt{D}]$ have the same parity, but also when $Q_{\ell((1+\sqrt{D})/2} = 2a$, then $Q_{\ell(\sqrt{D})/2} = a$. Furthermore, note that in Proposition 3.1(ii) it is necessarily the case that $D \not\equiv 1, 2 \pmod 4$, while, as illustrated by Examples 3.3 and 3.4 below, (i) allows for $D \equiv 1, 2 \pmod 4$. To see why (ii) does not allow for $D = ab \equiv 1, 2 \pmod 4$, assume that (3.2) holds for such a D with $1 \le a < b$ and rs odd. If $D \equiv 1 \pmod 4$, then $a \equiv b \pmod 4$, so

$$\pm 2 = ar^2 - bs^2 \equiv a(r^2 - s^2) \equiv 0 \pmod 4,$$

a contradiction. If $D \equiv 2 \pmod 4$, then one of a or b is even, so (3.2) tells us that the other must be even since rs is odd, and this is a contradiction.

The above discussion on $D \equiv 1 \pmod 4$ relies on the fact that when $D \equiv 1 \pmod 8$, the fundamental unit of the order $\mathbb{Z}[(1+\sqrt{D})/2]$ is the same as the fundamental unit of the order $\mathbb{Z}[\sqrt{D}]$. When these fundamental units differ, then necessarily $D \equiv 5 \pmod 8$, in which case the fundamental unit of $\mathbb{Z}[\sqrt{D}]$ is ε_D^3, where ε_D is the fundamental unit of $\mathbb{Z}[(1+\sqrt{D})/2]$; see [3, Theorem 2.1.4, p. 53] for a proof of the above facts.

An illustration of Proposition 3.1(i) when D is not square-free is given as follows, which corrects [4, Example 4, p. 175].

Example 3.3 Let $D = 2 \cdot 7^2 \cdot 13 = 1274$. Then $\ell = \ell(\sqrt{D}) = 18$, and $Q_{\ell/2} = Q_9 = 26 = a$ with $b = 49$, $r = 1020$, and $s = 743$, and

$$ar^2 - bs^2 = 26 \cdot 1020^2 - 49 \cdot 743^2 = (-1)^{\ell/2} = -1.$$

Also,

$$\begin{aligned} A_{\ell-1} + B_{\ell-1}\sqrt{D} &= x_0 + y_0\sqrt{D} = 54100801 + 1515720\sqrt{1274} \\ &= (1020\sqrt{26} + 743\sqrt{49})^2 = \Big(\frac{A_{\ell/2-1}}{a}\sqrt{a} + B_{\ell/2-1}\sqrt{b}\Big)^2 \\ &= (r\sqrt{a} + s\sqrt{b})^2. \end{aligned}$$

The following example illustrates the case where $D \equiv 1 \pmod 8$.

Example 3.4 Let $D = 41 \cdot 73 = ab = 2993 \equiv 1 \pmod 8$ has $\ell(\sqrt{D}) = 6$, $Q_{\ell/2} = Q_3 = 41$, $r = 4$, $s = 3$, and $r^2a - s^2b = -1$. Here $(x_0, y_0) = (1313, 24) = (r^2a + s^2b, rs)$.

An interesting consequence of Proposition 3.1 is the following simple criterion for the norm of the fundamental unit of a quadratic field to equal -1, namely for the existence of a solution to the negative Pell equation to be provided in terms of the fundamental solution (x_0, y_0) of the *positive* Pell equation.

Theorem 3.5 *If $D \equiv 1, 2 \pmod 4$ is a non-square positive integer, then there is a solution to the negative Pell equation if and only if $x_0 \equiv -1 \pmod{2D}$.*

Proof If there is a solution to the negative Pell equation, say (T_0, U_0), then

$$x_0 + y_0\sqrt{D} = (T_0 + U_0\sqrt{D})^2$$

so $x_0 = T_0^2 + U_0^2D \equiv -1 + 2U_0^2D \equiv -1 \pmod{2D}$ given that $T_0^2 - DU_0^2 = -1$.

Conversely, assume that $x_0 \equiv -1 \pmod{2D}$. Suppose that $\ell((1+\sqrt{D})/2)$ is even, so $\ell = \ell(\sqrt{D})$ is even. Then by Proposition 3.1 and Remark 3.2, (3.1) holds. Then $x_0 = r^2a+s^2b$ by (i)(c) and $r^2a-s^2b = (-1)^{\ell/2}$ by (i)(d). Putting these two together,

$$-1 \equiv x_0 \equiv r^2a + s^2b \equiv 2s^2b + (-1)^{\ell/2} \equiv (-1)^{\ell/2} \pmod{2b}.$$

Since $b > 1$, this makes $\ell/2$ odd. Similarly,

$$-1 \equiv x_0 \equiv r^2a + s^2b \equiv 2r^2a - (-1)^{\ell/2} \equiv (-1)^{\ell/2+1} \pmod{2a}.$$

Since $a > 1$, this makes $\ell/2$ even, a contradiction. Hence, ℓ is odd. ■

Remark 3.6 Note that Theorem 3.5 says that if $D \equiv 1 \pmod 4$ and ε_D is the fundamental unit of $\mathbb{Z}[(1+\sqrt{D})/2]$, then $N(\varepsilon_D) = -1$ if and only if $x_0 \equiv -1 \pmod D$, where (x_0, y_0) is the fundamental solution of the *positive* Pell equation. (Note that by Remark 3.2, if ε_{4D} is the fundamental unit of $\mathbb{Z}[\sqrt{D}]$ for $D \equiv 1 \pmod 4$, then $N(\varepsilon_D) = -1$ if and only if $N(\varepsilon_{4D}) = -1$.)

An old and difficult problem is to decide whether or not the negative Pell equation has a solution (see Lagarias [1]). Theorem 3.5 gives a criterion to do this; however, it requires finding the fundamental solution (x_0, y_0) of the positive Pell equation, which is another old and equally difficult problem. Lenstra [2] deals with this latter problem using a notion of power products. Our criterion in Theorem 3.5 links these two problems in that if one is able to find (x_0, y_0), then it is easy to check whether the negative Pell equation has a solution, namely by checking whether $x_0 \equiv -1 \pmod{D}$. Indeed one needs only a solution (x, y) that is an odd power of (x_0, y_0) as in this case $x \equiv x_0 \pmod{D}$, and the criterion applies again.

Example 3.7 If $D = 5^2 \cdot 17 = 425$, then $\ell(\sqrt{D}) = 7$,

$$x_0 + y_0\sqrt{D} = (268 + 13\sqrt{425})^2 = 143649 + 6968\sqrt{425}$$

with $x_0 \equiv -1 \pmod{425}$.

Example 3.8 Let $D = 10$, for which $\ell = l(\sqrt{D}) = 1$, so there exists a solution to $x^2 - Dy^2 = -1$, namely

$$A_{\ell-1} + B_{\ell-1}\sqrt{D} = A_0 + B_0\sqrt{10} = 3 + \sqrt{10}.$$

Thus, the fundamental solution of the positive Pell equation $x^2 - 10y^2 = 1$ is given by

$$x_0 + y_0\sqrt{D} = (A_{\ell-1} + B_{\ell-1}\sqrt{D})^2 = (3 + \sqrt{10})^2 = 19 + 6\sqrt{10}.$$

Thus, the criterion $x_0 \equiv -1 \pmod{2D}$ given in Theorem 3.5 is illustrated here as $x_0 = 19 \equiv -1 \pmod{2D}$.

Remark 3.9 If for a given radicand $D = ab \equiv 1 \pmod{4}$, $\ell(\sqrt{D})$ is even, then the very proof of Theorem 3.5 indicates that $x_0 \equiv -1 \pmod{ab}$ is impossible, since $a > 1$ and $b > 1$ are maximal in the sense that x_0 is congruent to -1 modulo all primes dividing one of them and is congruent to 1 modulo all primes dividing the other. This rather elegant condition is a notion that is exploited in a different context in Theorem 4.1.

4 Non-Principal Lagrange Criteria

The following generalizes earlier work; see Theorem 4.3. The notation of the previous sections remain in force here. As well, in what follows for $D = ab$, let $2/\alpha \le a < b$, where $\alpha = 2$ if y_0 is odd and $\alpha = 1$ if y_0 is even. Note that when $D = p^g$, where $p > 2$ is prime and $g \in \mathbb{N}$, it is not possible that $\alpha = 1$. In other words, it is not possible for $p^h = a < b = p^{g-h}$, since that would put us into part 1 of Proposition 3.1 for which $x_0 = r^2a + s^2b$ with $p \mid a$ and $p \mid b$ and since $x_0^2 - Dy_0^2 = 1$, one would conclude that $p \mid 1$, a contradiction.

Theorem 4.1 *Suppose that $\Delta = 4D$ is a discriminant with radicand $D = ab$. 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*

$$ax^2 - by^2 = (-1)^{\ell/2}\alpha, \tag{4.1}$$

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

https://doi.org/10.4153/CMB-2011-118-9 Published online by Cambridge University Press

(c) *The following congruences hold:*

$$x_0 \equiv (-1)^{\ell/2+1} \pmod{2a/\alpha} \quad \textit{and} \quad x_0 \equiv (-1)^{\ell/2} \pmod{2b/\alpha}. \tag{4.2}$$

Proof We note that Proposition 3.1 holds throughout, since we are assuming ℓ is even. First, assume that (a) holds. Then from (2.2) we have

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

Therefore,

$$a\Big(\frac{A_{\ell/2-1}}{a}\Big)^2 - B_{\ell/2-1}^2 b = \alpha(-1)^{\ell/2}$$

and by Proposition 3.1, $A_{\ell/2-1} = ra$ and $B_{\ell/2-1} = s$, namely $r\sqrt{a} + s\sqrt{b}$ is the fundamental solution to (4.1). Thus, (a) implies (b).

Suppose that (b) holds. Then if $\alpha = 2$, by Proposition 3.1(ii)(c)–(d),

$$x_0 = \frac{r^2a + s^2b}{2} = \frac{2s^2b + 2(-1)^{\ell/2}}{2} = s^2b + (-1)^{\ell/2} \equiv (-1)^{\ell/2} \pmod{b}$$

and

$$x_0 = \frac{r^2a + s^2b}{2} = \frac{2r^2a - 2(-1)^{\ell/2}}{2} = r^2a + (-1)^{\ell/2+1} \equiv (-1)^{\ell/2+1} \pmod{a}.$$

If $\alpha = 1$, then by part 1 (c)–(d) of Proposition 3.1

$$x_0 = r^2a + s^2b = 2s^2b + (-1)^{\ell/2} \equiv (-1)^{\ell/2} \pmod{2b}$$

and

$$x_0 = r^2a + s^2b = 2r^2b - (-1)^{\ell/2} \equiv (-1)^{\ell/2+1} \pmod{2a}.$$

We have shown that (4.2) holds, so we have shown that (b) implies (c).

Now assume that (c) holds. By hypothesis, a and b are maximal in the sense that a is divisible by all the primes p such that $x_0 \equiv (-1)^{\ell/2+1} \pmod{p^t}$, where $p^t \| a$ and b is divisible by all the primes q such that $x_0 \equiv (-1)^{\ell/2} \pmod{q^u}$ where $q^u \| b$. Thus the value of a in Proposition 3.1 is the value of a here so $Q_{\ell/2} = \alpha a$.

Hence, we have shown that (c) implies (a), and the logical circle is complete. ∎

Remark 4.2 With reference to the comments preceding Theorem 4.1, it is possible that $Q_{\ell/2} = 2^g$ with $\alpha = 2$ which puts us into part 2 of Proposition 3.1. For instance, if $D = 296$ with $a = 2$ and $b = 148$, we get that $Q_{\ell/2} = Q_3 = 4$ with $ar^2 - bs^2 = 2 \cdot 43^2 - 148 \cdot 5^2 = -2 = (-1)^{\ell/2}2$. Indeed, part 2 of Proposition 3.1 tells us that when $a = 2$, $Q_{\ell/2} = 4$ is forced. Observe, as well, that rs being odd in part 2 of Proposition 3.1 is a necessary hypothesis. For instance, when $D = 74$, $\ell = 5$ but $2 \cdot 43^2 - 37 \cdot 10^2 = -2$. This and more were considerations addressed in [4]. For instance, therein it is proved that if D is the power of an odd prime, then $\ell(\sqrt{D})$ is odd and $\ell(\sqrt{4D}) = \ell$ is even, with $Q_{\ell/2} = 4$—see [4, Corollaries 5–6, p. 189].

https://doi.org/10.4153/CMB-2011-118-9 Published online by Cambridge University Press

Theorem 4.3 ([5, 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) *There is a solution to the Diophantine equation $x^2 - Dy^2 = 2(-1)^{\ell/2}$.*
(b) $x_0 \equiv (-1)^{\ell/2} \pmod{D}$.

Proof If $\alpha = 1$, take $a = 2$, and if $\alpha = 2$, take $a = 1$ in Theorem 4.1. ■

Corollary 4.4 *Theorem* 4.3(a)–(b) *are equivalent to* $Q_{\ell/2} = 2$.

Now we illustrate the above.

Example 4.5 If $D = 38 = 2 \cdot 19 = a \cdot b$, then $\ell = 2$, $Q_1 = 2 = a$, $y_0 = 6$, $x_0 = 37$, so $\alpha = 1$. We have $x_0 \equiv 1 \pmod{2a}$, $x_0 \equiv -1 \pmod{2b}$, and $2r^2 - 19s^2 = -1$, where $r = 3$ and $s = 1$. This illustrates Theorem 4.3.

To see that Theorem 4.1 also applies with $\alpha = 2$, let $D = 7 \cdot 17 = 119$ for which $\ell = 4$, $Q_2 = 2 = 2a$, $b = D$, $x_0 = 120 \equiv 1 \equiv (-1)^{\ell/2} \pmod{D}$, $s = 1$, and $r = 11 = y_0$ with $r^2 - s^2D = 2$.

Remark 4.6 Corollary 4.4 says, in particular, that

$$Q_{\ell/2} = 2 \text{ if and only if } x_0 \equiv (-1)^{\ell/2} \pmod{D}.$$

This is a generalization of Lagrange's criterion, which states that if $D = p$ is an odd prime, then

$$x_0 \equiv 1 \pmod{p} \text{ if and only if } p \equiv 7 \pmod{8}.$$

Note that this holds, since if $p \equiv 7 \pmod{8}$, then by (2.3) ℓ is even, and Proposition 3.1(ii) necessarily holds with $a = 1$. So by part (d) therein, $r^2 - ps^2 = (-1)^{\ell/2}2$ and since rs is odd, $(-1)^{\ell/2}2 \equiv 1 - 7 \pmod{8}$, which forces $\ell/2$ to be even. Therefore, by Theorem 4.3, $x_0 \equiv 1 \pmod{p}$. Conversely, if $x_0 \equiv 1 \pmod{p}$, then by Theorem 4.3, $\ell/2$ is even and so by part (b), $p \equiv 7 \pmod{8}$.

Theorem 4.1 is a complete generalization of the Lagrange criterion: If $D = ab$ with $\ell = \ell(\sqrt{D})$ even, $2/\alpha \le a < b$, then $Q_{\ell/2} = \alpha a$ if and only if $x_0 \equiv (-1)^{\ell/2+1} \pmod{2a/\alpha}$, and $x_0 \equiv (-1)^{\ell/2} \pmod{2b/\alpha}$.

Note as well that the relationship between Theorem 3.5 and Theorem 4.1 comes into play. By Remark 3.2, Proposition 3.1(ii) does not apply to $D \equiv 1, 2 \pmod{4}$ when ℓ is even so $\alpha = 1$ in this case. Also, if $D \equiv 1 \pmod{4}$ and ℓ is even, we cannot have $Q_{\ell/2} = 2$; see [6] for more on this matter. Thus, for $D \equiv 2 \pmod{4}$, if $a = 2$, and $\ell/2$ is odd, we can have $Q_{\ell/2} = 2$ if and only if $x_0 \equiv 1 \pmod{4}$ and $x_0 \equiv -1 \pmod{D}$. Given that Theorem 3.5 says that if $D \equiv 1, 2 \pmod{4}$, then ℓ is odd if and only if $x_0 \equiv -1 \pmod{2D}$, then necessarily $x_0 \equiv -1 \pmod{4}$ when ℓ is odd and $D \equiv 2 \pmod{4}$. This is all that distinguishes the criterion for $Q_{\ell/2} = 2$ from the criterion for ℓ to be odd in this case. For instance, let $D = 38$. Then $\ell = 2$, $Q_{\ell/2} = 2$, $\alpha = 1$, $a = 2$, and $x_0 = 37 \equiv -1 \pmod{D}$ *but* $x_0 \equiv 1 \pmod{4}$.

Example 4.7 Let $D = 35 = 5 \cdot 7 = ab$ for which we have $x_0 = 6$, $y_0 = 1$, $\alpha = 2$, $\ell = \ell(\sqrt{D}) = 2$, and $Q_{\ell/2} = 10 = 2a$. Here,

$$x_0 = 6 \equiv 1 \equiv (-1)^{\ell/2+1} \pmod{a} \quad \text{and} \quad x_0 \equiv -1 \equiv (-1)^{\ell/2} \pmod{b}.$$

Also, with $r = 1 = s$, $ar^2 - by^2 = (-1)^{\ell/2}2 = -2$.

Example 4.8 Let $D = 183 = 3 \cdot 61 = ab \equiv 3 \pmod 4$ for which we have $\ell = \ell(\sqrt{D}) = 6$ and $Q_{\ell/2} = 3 = a$, and $b = 61$. Here $y_0 = 36$,

$$x_0 = 487 \equiv 1 \equiv (-1)^{\ell/2+1} \pmod{2a}, \quad \text{and} \quad x_0 \equiv -1 \equiv (-1)^{\ell/2} \pmod{b}.$$

Also, with $r = 9$, $s = 2$, $ar^2 - by^2 = (-1)^{\ell/2} = -1$.

The following illustrations look at the case where the central norm is not a prime or twice a prime.

Example 4.9 Let $D = 3 \cdot 17 \cdot 29 \cdot 61 = 90219$. then $\ell = 42$ and $Q_{\ell/2} = Q_{19} = 183 = 3 \cdot 61 = a$, and $b = 17 \cdot 29 = 493$. Here $\alpha = 1$, $y_0 = 44321930492797336$,

$$x_0 = 1331274682310917 6735 \equiv 1 \equiv (-1)^{\ell/2+1} \pmod{2a}$$

and $x_0 \equiv -1 \equiv (-1)^{\ell/2} \pmod{2b}$. Also, $r^2a - s^2b = (-1)^{\ell/2} = -1$, with its fundamental solution being

$$r\sqrt{a} + s\sqrt{b} = 190718707\sqrt{183} + 116197124\sqrt{493}.$$

Example 4.10 Let $D = 2340 = 9 \cdot 260 = a \cdot b$, with $Q_{\ell/2} = Q_4 = 9 = a$, $\alpha = 1$, $x_0 = 33281 \equiv (-1)^{\ell/2+1} \equiv -1 \pmod{18}$, $x_0 \equiv 1 \equiv (-1)^{\ell/2} \pmod{520}$, and $r\sqrt{a} + s\sqrt{b} = 129 + 16\sqrt{65}$.

References

[1] J. C. Lagarias, *On the computational complexity of determining the solvability or unsolvability of the equation $X^2 - DY^2 = -1$.* Trans. Amer. Math. Soc. **260**(1980), no. 2, 485–508.

[2] H. W. Lenstra Jr., *Solving the Pell equation.* Notices Amer. Math. Soc. **49**(2002), no. 2, 182–192.

[3] R. A. Mollin, *Quadratics.* CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, 1996.

[4] ———, *A continued fraction approach to the Diophantine equation $ax^2 - by^2 = \pm 1$.* JP J. Algebra Number Theory Appl. **4**(2004), no. 1, 159–207.

[5] ———, *Lagrange, central norms, and quadratic Diophantine equations.* Int. J. Math. Math. Sci. **2005**, no. 7, 1039–1047.

[6] ———, *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), no. 1, 121–132. http://dx.doi.org/10.4153/CMB-2005-011-0

[7] ———, *Fundamental number theory with applications.* Second ed., Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2008.

Department of Mathematics and Statistics, University of Calgary, Calgary, AB
e-mail: ramollin@math.ucalgary.ca
URL: http://www.math.ucalgary.ca/~ramollin/

Department of Mathematics, Siddhartha college, (affiliated with Mumbai University), India
e-mail: rsrinivasan.anitha@gmail.com