LAGRANGE, CENTRAL NORMS, AND QUADRATIC DIOPHANTINE EQUATIONS

R. A. MOLLIN

Received 4 May 2004 and in revised form 16 January 2005

We consider the Diophantine equation of the form $x^2 - Dy^2 = c$, where $c = \pm 1, \pm 2$, and provide a generalization of results of Lagrange with elementary proofs using only basic properties of simple continued fractions. As a consequence, we achieve a completely general, simple, and elegant criterion for the central norm to be 2 in the simple continued fraction expansion of $\sqrt{D}$.

1. Introduction

As is often the case, some results get rediscovered over time. In particular, some rather striking results of Lagrange are often recreated. For instance, in [6], a result pertaining to the Pell equation for a prime discriminant was recast in the light of nonabelian cohomology groups. Yet, in [1], the authors acknowledged the fact that the result "has been discovered before," and provided an elementary proof of it and two other results related to Lagrange. In this paper, we present complete generalizations of these results (see Theorems 3.1, 3.5, and 3.9 below), and do so with only elementary properties of the simple continued fraction expansions of general $\sqrt{D}$. As a consequence, we obtain

$$x_0 \equiv \pm 1 (\mathrm{mod}\, D) \quad \text{iff } Q_{\ell/2} = 2, \tag{1.1}$$

where $x_0^2 - Dy_0^2 = 1$ is the fundamental solution, ℓ is the (even) period length of the continued fraction expansion of $\sqrt{D}$, and $Q_{\ell/2}$ is the central norm (see Theorem 3.11 below).

2. Notation and 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

$$\sqrt{D} = \langle q_0; \overline{q_1, q_2, \ldots, q_{\ell-1}, 2q_0} \rangle, \tag{2.1}$$

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

International Journal of Mathematics and Mathematical Sciences 2005:7 (2005) 1039–1047
DOI: 10.1155/IJMMS.2005.1039

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

$$\frac{A_k}{B_k} = \langle q_0; q_1, q_2, \ldots, q_k \rangle, \tag{2.2}$$

where

$$A_k = q_k A_{k-1} + A_{k-2}, \tag{2.3}$$

$$B_k = q_k B_{k-1} + B_{k-2}, \tag{2.4}$$

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

$$\begin{aligned} P_{k+1} &= q_k Q_k - P_k, \\ q_k &= \left\lfloor \frac{P_k + \sqrt{D}}{Q_k} \right\rfloor, \\ D &= P_{k+1}^2 + Q_k Q_{k+1}. \end{aligned} \tag{2.5}$$

We will also need the following facts (which can be found in most introductory texts in number theory, such as [3]; also, see [2] for a more advanced exposition):

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

Also,

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

$$D B_{k-1} = P_k A_{k-1} + Q_k A_{k-2}, \tag{2.8}$$

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

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

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

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

$$Q_{\ell+k} = Q_k, \qquad P_{\ell+k} = P_k, \qquad q_{\ell+k} = q_k. \tag{2.11}$$

When ℓ is even,

$$P_{\ell/2} = P_{\ell/2+1} = P_{(2k-1)\ell/2+1} = P_{(2k-1)\ell/2}. \tag{2.12}$$

Also $Q_{\ell/2} = Q_{(2k-1)\ell/2}$, so by (2.5),

$$Q_{(2k-1)\ell/2} \mid 2P_{(2k-1)\ell/2}, \tag{2.13}$$

where $Q_{\ell/2}$ is called the *central norm*, (via (2.9)). Furthermore,

$$Q_{(2k-1)\ell/2} \mid 2D, \tag{2.14}$$

$$q_{(2k-1)\ell/2} = 2P_{(2k-1)\ell/2}/Q_{(2k-1)\ell/2}. \tag{2.15}$$

In the next section, we will be considering what are typically called the standard Pell equations (2.16) and (2.18), 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*

$$x^2 - y^2 D = 1 \tag{2.16}$$

are given by

$$x = A_{k\ell-1}, \qquad y = B_{kl-1}, \tag{2.17}$$

whereas there are no solutions to

$$x^2 - y^2 D = -1. \tag{2.18}$$

If ℓ is odd, then all positive solutions of (2.16) are given by

$$x = A_{2k\ell-1}, \qquad y = B_{2k\ell-1}, \tag{2.19}$$

whereas all positive solutions of (2.18) are given by

$$x = A_{(2k-1)\ell-1}, \qquad y = B_{(2k-1)\ell-1}. \tag{2.20}$$

Proof. This appears in many introductory number theory texts possessing an in-depth section on continued fractions. For instance, see [3, Corollary 5.3.3, page 249]. □

In the following (which we need in the next section), and all subsequent results, the notation for the A_k, B_k, Q_k, and so forth apply to the above-developed notation for the continued fraction expansion of $\sqrt{D}$.

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):*

$$ax^2 - by^2 = \pm 1. \tag{2.21}$$

Furthermore, in this case, each of the following holds, where $(x, y) = (r, s)$ is the fundamental solution of (2.21).

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

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

(c) $A_{\ell-1} = r^2 a + s^2 b$ *and* $B_{\ell-1} = 2rs$.

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

(2) *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:*

$$ax^2 - by^2 = \pm 2. \tag{2.22}$$

Moreover, in this case each of the following holds, where $(x, y) = (r, s)$ is the fundamental solution of (2.22).

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

For the proof of all this, see [4].

Lastly, we will require the following number-theoretic results.

Theorem 2.3. *If c is an odd positive integer, then the following Jacobi symbol identities hold:*

$$\begin{aligned} \left(\frac{2}{c}\right) &= (-1)^{(c^2-1)/8}, \\ \left(\frac{-1}{c}\right) &= (-1)^{(c-1)/2}. \end{aligned} \tag{2.23}$$

Proof. This may be found in introductory number theory texts. For instance, see [3, Theorem 4.2.1, page 197]. □

3. Central norms and Diophantine equations

The following extends Lagrange's [1, Theorem, page 181] to its greatest possible generality. In the proof, we use only elementary continued fraction results. The end product is that we reveal the underlying reason for the phenomenon in terms of the central norm being equal to 2.

Theorem 3.1. *Let $D > 2$ be an integer that is not a perfect square. Also assume that (x_0, y_0) is the fundamental solution of (2.16). Then the following are equivalent.*

(1) $x_0 \equiv 1 (\mathrm{mod}\, D)$.
(2) *There exists an integral solution to the equation*

$$x^2 - Dy^2 = 2. \tag{3.1}$$

(3) $\ell \equiv 0 (\mathrm{mod}\, 4)$ *and* $Q_{\ell/2} = 2$.

Proof. First we assume that part 2 holds. Using Theorem 2.2, part 2, with $a = 1$ and $b = D$, since there are integer solutions to $x^2 - Dy^2 = 2$, then letting (r, s) be the fundamental solution, $r^2 - Ds^2 = 2$, we have (using part 2(c)) that $2A_{\ell-1} = r^2 + Ds^2$. Hence,

$$2A_{\ell-1} = 2 + 2Ds^2 \equiv 2 (\mathrm{mod}\, 2D), \tag{3.2}$$

so it follows that $A_{\ell-1} \equiv 1 (\mathrm{mod}\, D)$. However, Theorem 2.2 shows that ℓ is even so that $x_0 = A_{\ell-1}$, by Theorem 2.1. We have shown that part 2 implies part 1.

Now assume that $x_0 \equiv 1 (\mathrm{mod}\, D)$. If ℓ were odd, then by (2.10), $A_{\ell-1}^2 \equiv -1 (\mathrm{mod}\, D)$. However, by Theorem 2.1, $x_0 = A_{2\ell-1}$. Therefore, since Theorem 2.1 tells us that, in this case,

$$A_{2\ell-1} + B_{2\ell-1}\sqrt{D} = \left(A_{\ell-1} + B_{\ell-1}\sqrt{D}\right)^2 = A_{\ell-1}^2 + B_{\ell-1}^2 D + 2A_{\ell-1}B_{\ell-1}\sqrt{D}, \tag{3.3}$$

then $x_0 = A_{\ell-1}^2 + B_{\ell-1}^2 D \equiv A_{\ell-1}^2 \equiv -1 (\mathrm{mod}\, D)$, a contradiction, since $D > 2$. We have shown that ℓ is even. Thus, by Theorem 2.2, there is a factorization of $D = ab$ such that one of (2.21)-(2.22) holds.

If (2.21) holds, then by part 1(d) in Theorem 2.2, $r^2 a - s^2 b = (-1)^{\ell/2}$. However, by part 1(c) of that theorem, $x_0 = A_{\ell-1} = r^2 a + s^2 b$. It follows that

$$1 \equiv x_0 \equiv r^2 a + s^2 b \equiv (-1)^{\ell/2} + 2s^2 b (\mathrm{mod}\, D). \tag{3.4}$$

Hence, $\ell/2$ must be even since otherwise $b \mid 2$, where $1 < a < b$, which is impossible. Therefore, $a \mid 2s^2$, but by part 1(b) in Theorem 2.2, $A_{\ell/2-1} = ra$ and $B_{\ell/2-1} = s$, and by (2.6), $\gcd(A_{\ell/2-1}, B_{\ell/2-1}) = 1$, so $a \mid 2$. Since $Q_{\ell/2} = a > 1$ by part 1(a) of Theorem 2.2, then $Q_{\ell/2} = 2 = a$. Thus, part 3 holds.

Now we assume that (2.22) holds. From Theorem 2.2, parts (c)-(d),

$$2x_0 = r^2 a + s^2 b, \qquad 2(-1)^{\ell/2} = r^2 a - s^2 b. \tag{3.5}$$

Since $x_0 = 1 + ND = 1 + Nab$, for some $N \in \mathbb{N}$, then

$$2\left(1 - (-1)^{\ell/2} + Nab\right) = 2s^2 b, \tag{3.6}$$

so $b \mid (1 - (-1)^{\ell/2})$. If $\ell/2$ is odd, then $a = 1$, $b = 2 = D$, which is excluded. Hence, $\ell/2$ is even, and $Na = s^2$. Now the same argument as in the above for (2.21) shows that $\gcd(a, s) = 1$, so $a = 1$.

We have shown that part 1 implies part 3. It remains to prove that part 3 implies part 2 to complete the logical circle. However, this is an immediate consequence of Theorem 2.2. □

Corollary 3.2 [1, Theorem, page 181]. *If $D = p$ is an odd prime, then*

$$x_0 \equiv 1 (\mathrm{mod}\, p) \quad \textit{iff } p \equiv 7 (\mathrm{mod}\, 8). \tag{3.7}$$

Proof. If $p \equiv 7 (\mathrm{mod}\, 8)$, then ℓ is even by (2.10). Thus, by Theorem 2.2, (3.1) must be solvable, so Theorem 3.1 yields that $x_0 \equiv 1 (\mathrm{mod}\, p)$. Conversely, if $x_0 \equiv 1 (\mathrm{mod}\, p)$, then $x^2 - py^2 = 2$ is solvable by Theorem 3.1. Thus, x and y are both odd, so $x^2 \equiv y^2 \equiv 1 (\mathrm{mod}\, 8)$, and $p \equiv 7 (\mathrm{mod}\, 8)$. □

Note that in Theorem 3.1, all odd primes p dividing D must be of the form $p \equiv \pm 1 (\mathrm{mod}\, 8)$, and 4 does not divide D.

Remark 3.3. A dual formulation of Theorem 3.1 is that the following are equivalent.

(1) $x_0 \equiv -1 (\mathrm{mod}\, D)$, and ℓ is even.

(2) There exists an integral solution to the equation

$$x^2 - Dy^2 = -2. \tag{3.8}$$

(3) $Q_{\ell/2} = 2$ and $\ell/2$ is odd.

This may be proved in a very similar fashion to that of Theorem 3.1. One must assume that ℓ is even along with $x_0 \equiv -1 (\mathrm{mod}\, D)$ since the latter is insufficient to conclude the former, unlike the dual condition 1 in Theorem 3.1 which is sufficient to conclude that ℓ is even. For instance, if $D = 74$, then $x_0 = 3699 \equiv -1 (\mathrm{mod}\, D)$. Here $\ell(\sqrt{D}) = 5$, and $x_0 = A_{2\ell-1} = A_9$.

Note that in the above dual formulation, all odd primes p dividing D must be of the form $p \equiv 1, 3 (\mathrm{mod}\, 8)$ by Theorem 2.3.

In both of these scenarios, $Q_{\ell/2} = 2$, which is the focus for the balance of the paper since it is the key to this investigation and explanation of the full generality of Lagrange's result, which we developed in Theorem 3.1.

Example 3.4. If $D = 2 \cdot 19$, then $\ell = 2$, $A_{\ell-1} = 37 \equiv -1 (\mathrm{mod}\, D)$, and $Q_{\ell/2} = 2$, which illustrates Remark 3.3. Moreover, if $D = 2 \cdot 3^7$, then $A_{\ell-1} = 456335045 \equiv -1 (\mathrm{mod}\, D)$, and $Q_{\ell/2} = 2$.

If $D = 2 \cdot 7^3$, then $\ell = 16$, $A_{\ell-1} = 10850138895 \equiv 1 (\mathrm{mod}\, D)$, and $Q_{\ell/2} = 2$, which illustrates Theorem 3.1.

Some instances with a mix of primes are as follows. If $D = 2 \cdot 7 \cdot 17$, then $\ell = 8$, $Q_{\ell/2} = 2$, and $A_{\ell-1} = 11663 \equiv 1 (\mathrm{mod}\, D)$. Similarly, if $D = 7 \cdot 17$, then $\ell = 4$, $Q_{\ell/2} = 2$, and $A_{\ell-1} = 120 \equiv 1 (\mathrm{mod}\, D)$. If $D = 2 \cdot 7 \cdot 23 \cdot 31 \cdot 47$, then $\ell = 36$, $Q_{\ell/2} = 2$, and $A_{\ell-1} = 9918684752958020825955 \equiv 1 (\mathrm{mod}\, D)$.

The following result focuses on the central norm. It also corrects [1, Theorem, page 183] and explains the phenomenon behind the result (see Remark 3.6 after the proof below).

Theorem 3.5. *If $D > 2$ is a positive integer that is not a perfect square, then the following are equivalent.*

(1) *$x^2 - Dy^2 = \pm 2$ is solvable for some integers x, y.*

(2) *ℓ is even and for any odd $j \geq 1$, $Q_{j\ell/2} = 2$.*

(3) *ℓ is even and for any odd $j \geq 1$, $q_{\ell/2} = q_{j\ell/2} = P_{j\ell/2} = P_{\ell/2}$.*

(4) *ℓ is even and for any odd $j \geq 1$, $g = \gcd(A_{j\ell/2-1}, D) \mid 2$, and if $g = 2$, then $D \equiv 2 (\mathrm{mod}\, 4)$.*

(5) *ℓ is even and for any odd $j \geq 1$, $A_{j\ell/2-1} = B_{j\ell/2} + B_{j\ell/2-2}$.*

(6) *ℓ is even and for any odd $j \geq 1$, $DB_{j\ell/2-1} = A_{j\ell/2} + A_{j\ell/2-2}$.*

Proof. Parts 1 and 2 are equivalent for $j = 1$ by Theorem 2.2; and by properties (2.11), (2.14), and (2.15), they hold for all odd $j \geq 1$.

Parts 2 and 3 are equivalent by (2.15).

If part 2 holds, then by (2.9), part 4 must hold.

If part 4 holds, then by (2.9),

$$A^2_{j\ell/2-1} - B^2_{j\ell/2-1}D = (-1)^j Q_{j\ell/2}, \tag{3.9}$$

and by (2.14),

$$Q_{j\ell/2} \mid 2D. \tag{3.10}$$

Let p be a prime dividing both $Q_{j\ell/2}$ and D. Then by (3.9), $p \mid A_{j\ell/2-1}$. Therefore, $p = g = 2$ and $D \equiv 2 (\mathrm{mod}\, 4)$, by hypothesis. Since (2.6) tells us that $\gcd(A_{j\ell/2-1}, B_{j\ell/2-1}) = 1$, then (3.9) tells us that 4 cannot divide $Q_{j\ell/2}$, so $Q_{j\ell/2} = 2$. If $\gcd(D, Q_{j\ell/2}) = 1$, then $Q_{\ell/2} \mid 2$, by (3.10). Hence, $Q_{j\ell/2} = 2$ since $Q_{j\ell/2} = 1$ can only occur when j is even (see (2.9)-(2.10)). We have completed the proof that parts 2 and 4 are equivalent. (Note that in the case of part 4, the condition $g = 2$ being tied to $D \equiv 2 (\mathrm{mod}\, 4)$ prevents $4 \mid Q_{j\ell/2}$ from occurring—see Remark 3.6 after the proof.)

If part 5 holds, then by (2.4),

$$A_{j\ell/2-1} = B_{j\ell/2} + B_{j\ell/2-2} = q_{j\ell/2}B_{j\ell/2-1} + 2B_{j\ell/2-2}, \tag{3.11}$$

and by (2.7),

$$A_{j\ell/2-1} = P_{j\ell/2}B_{j\ell/2-1} + Q_{j\ell/2}B_{j\ell/2-2}. \tag{3.12}$$

Hence,

$$B_{j\ell/2-1}(q_{j\ell/2} - P_{j\ell/2}) = B_{j\ell/2-2}(Q_{j\ell/2} - 2). \tag{3.13}$$

Since $P_{j\ell/2} = q_{j\ell/2}Q_{j\ell/2}/2$ from (2.15), then (3.13) becomes

$$B_{j\ell/2-1}q_{j\ell/2}(2 - Q_{j\ell/2}) = 2B_{j\ell/2-2}(Q_{j\ell/2} - 2). \tag{3.14}$$

If $Q_{j\ell/2} \neq 2$, then

$$-B_{j\ell/2-1}q_{j\ell/2} = 2B_{j\ell/2-2}, \tag{3.15}$$

which is impossible since $B_{j\ell/2-1}$, $q_{j\ell/2}$, and $B_{j\ell/2-2}$ are all positive (unless $j\ell/2 = 1$, in which case (3.15) becomes $-B_0q_1 = 0$, again impossible since $B_0 = 1$ and $q_1 \geq 1$). We have shown that part 5 implies part 2. That part 2 implies part 5 is easy using (2.7).

It remains to bring part 6 into the picture. If part 6 holds, then by (2.3),

$$DB_{j\ell/2-1} = A_{j\ell/2} + A_{j\ell/2-2} = q_{j\ell/2}A_{j\ell/2-1} + 2A_{j\ell/2-2}, \tag{3.16}$$

and by (2.8), this also equals $P_{j\ell/2}A_{j\ell/2-1} + Q_{j\ell/2}A_{j\ell/2-2}$. Hence,

$$A_{j\ell/2-1}(q_{j\ell/2} - P_{j\ell/2}) = (Q_{j\ell/2} - 2)A_{j\ell/2-2}, \tag{3.17}$$

but by (2.15), $Q_{j\ell/2}q_{j\ell/2} = 2P_{j\ell/2}$, so (3.17) becomes

$$A_{j\ell/2-1}q_{j\ell/2}(2 - Q_{j\ell/2}) = (Q_{j\ell/2} - 2)2A_{j\ell/2-2}. \tag{3.18}$$

Now, by assuming that $Q_{j\ell/2} \neq 2$, we argue in a similar fashion to the above and achieve a contradiction. Thus, part 6 implies part 2. Conversely, if part 2 holds, then using (2.3) and (2.8), we easily deduce that part 2 implies part 6, which completes the proof. □

Remark 3.6. If condition 4 in Theorem 3.5 did not have the stipulation that $g = 2$ must entail $D \equiv 2 (\mathrm{mod}\, 4)$, the result would fail. For instance, if $D = 8$, then $A_{\ell/2-1} = A_0 = 2$, so $g = 2$, but $Q_{\ell/2} = 4$.

Condition 4 is where the error in [1, Theorem, page 183] occurs. They attempt to prove that the condition is $\gcd(A_{j\ell/2-1}, D) = 1$. The following example is a counterexample to their claim that the conditions 1–3 and 5-6 of Theorem 3.5 are equivalent to the relatively primality cited above.

Example 3.7. Let $D = 2 \cdot 17 \cdot 41$. Then $\ell = 6$, $Q_{\ell/2} = 2$, $A_{\ell/2-1} = 112$, and $\gcd(D, A_{\ell/2-1}) = 2$. This is condition 4 of Theorem 3.5 with nontriviality of the gcd condition, which contradicts the assertion in [1] on the contrary. Moreover, it points to the central norm $Q_{\ell/2} = 2$, being the underlying feature of Theorem 3.5.

Remark 3.8. Condition 2 of Theorem 3.5 implicitly tells us that $\ell/2$ is odd if and only if condition 1 has the minus sign and $\ell/2$ is even if and only if condition 1 has the plus sign.

Observe that, as a consequence of the above development, when $Q_{\ell/2} = 2$ in the simple continued fraction expansion of $\sqrt{D}$, we may never have a prime $p \equiv 5 (\mathrm{mod}\, 8)$ dividing D. Moreover, we may never have *both* primes of the form $p \equiv 3 (\mathrm{mod}\, 8)$ *and* primes of the form $p \equiv 7 (\mathrm{mod}\, 8)$ dividing D. Thus, when $Q_{\ell/2} = 2$, the odd primes must be either *only* primes of the form $p \equiv \pm 1 (\mathrm{mod}\, 8)$ dividing D, or *only* primes of the form $p \equiv 1, 3 (\mathrm{mod}\, 8)$ dividing D. Lastly, 4 cannot divide D when $Q_{\ell/2} = 2$.

A motivation for the authors of [1] to present their result discussed in Remark 3.6 and Example 3.7 was the following result of Lagrange from 1770. For a prime p, $\ell(\sqrt{p})$ is odd if $p = 2$ or $p \equiv 1 (\mathrm{mod}\, 4)$. A related known result for which they provide a proof as well is the following. If $p \equiv 7 (\mathrm{mod}\, 8)$, then $\ell(\sqrt{p}) \equiv 0 (\mathrm{mod}\, 4)$, and if $p \equiv 3 (\mathrm{mod}\, 8)$, then $\ell(\sqrt{p}) \equiv 2 (\mathrm{mod}\, 4)$. We now generalize this result in an elementary fashion.

Theorem 3.9. *If $D = 2^a c$, where $a \in \{0, 1\}$, $c \equiv 3 (\mathrm{mod}\, 4)$, and $Q_{\ell/2} = 2$, then the following hold.*

(1) $c \equiv 3 (\mathrm{mod}\, 8)$ *if and only if* $\ell \equiv 2 (\mathrm{mod}\, 4)$.

(2) $c \equiv 7 (\mathrm{mod}\, 8)$ *if and only if* $\ell \equiv 0 (\mathrm{mod}\, 4)$.

Proof. By Theorem 2.2, $A_{\ell/2-1}^2 - DB_{\ell/2-1}^2 = (-1)^{\ell/2} 2$. Thus, by Theorem 2.3, the following Jacobi symbol identity holds:

$$1 = \left(\frac{A_{\ell/2-1}^2}{c}\right) = \left(\frac{(-1)^{\ell/2} 2}{c}\right) = \left(\frac{(-1)^{\ell/2}}{c}\right)\left(\frac{2}{c}\right) = (-1)^{(2\ell(c-1)+c^2-1)/8}, \tag{3.19}$$

from which one easily deduces the results. □

Corollary 3.10 (Lagrange). *If $p \equiv 3 (\mathrm{mod}\, 4)$, ℓ is even and $\ell \equiv 2 (\mathrm{mod}\, 4)$ if and only if $p \equiv 3 (\mathrm{mod}\, 8)$, or (equivalently) $\ell \equiv 0 (\mathrm{mod}\, 4)$ if and only if $p \equiv 7 (\mathrm{mod}\, 8)$.*

Proof. That ℓ is even follows from (2.10), and that $Q_{\ell/2} = 2$ follows from Theorem 2.2. □

We close with a result that brings together all the features we have been discussing, while at the same time presenting a general criterion for the central norm to be 2. The following completes a study begun by the author into the search for such a general criterion (see [5]).

THEOREM 3.11. *Suppose that D is a positive integer that is not a perfect square, that $(x, y) = (x_0, y_0)$ is the fundamental solution of (2.16), and that $\ell = \ell(\sqrt{D})$ is even. Then*

$$x_0 \equiv \pm 1 (\mathrm{mod}\, D) \quad \textit{iff } Q_{\ell/2} = 2. \tag{3.20}$$

Proof. If $x_0 \equiv \pm 1(\mathrm{mod}\, D)$, then by Theorem 3.1 and its dual formulation in Remark 3.3, $Q_{\ell/2} = 2$. Conversely, given the two cases in Theorem 3.1 and Remark 3.3, then we need only to show that $Q_{\ell/2} = 2$ implies a solution to one of $x^2 - Dy^2 = \pm 2$, but this is immediate from Theorem 3.5. □

Theorem 3.11 tells us that when ℓ is even, the condition $x_0 \equiv \pm 1(\mathrm{mod}\, D)$ is equivalent to all the conditions in Theorem 3.5.

Theorem 3.11 is a result which Lagrange might well have appreciated as a classification and generalization of the results he gave us.

Acknowledgments

The author's research is supported by NSERC Canada Grant no. A8484. Also, thanks go to two anonymous referees for so carefully going over the paper to make it more readable and accessible.

References

[1] Q. Lin and T. Ono, *On two questions of Ono*, Proc. Japan Acad. Ser. A Math. Sci. **78** (2002), no. 10, 181–184.

[2] R. A. Mollin, *Quadratics*, CRC Press Series on Discrete Mathematics and Its Applications, CRC Press, Florida, 1996.

[3] ———, *Fundamental Number Theory with Applications*, CRC Press, Florida, 1998.

[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] ———, *Necessary and sufficient conditions for the central norm to equal a power of 2 in the simple continued fraction expansion of $\sqrt{D}$ for any non-square $D > 1$*, to appear in Canad. Math. Bull.

[6] T. Ono, *On certain exact sequences for $\Gamma_0(m)$*, Proc. Japan Acad. Ser. A Math. Sci. **78** (2002), no. 6, 83–86.

R. A. Mollin: Department of Mathematics and Statistics, University of Calgary, Calgary, AB, Canada T2N 1N4

E-mail address: ramollin@math.ucalgary.ca