Canad. Math. Bull. Vol. **48** (1), 2005 pp. 121–132

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 $c > 1$

R. A. Mollin

Abstract. We look at the simple continued fraction expansion of $\sqrt{D}$ for any $D = 2^h c$ where $c > 1$ is odd with a goal of determining necessary and sufficient conditions for the central norm (as determined by the infrastructure of the underlying real quadratic order therein) to be 2^h. At the end of the paper, we also address the case where $D = c$ is odd and the central norm of $\sqrt{D}$ is equal to 2.

1 Introduction

In [8] we gave necessary and sufficient conditions for the parity of the period length of the simple continued fraction expansion of $\sqrt{D}$ for any nonsquare $D > 1$ in terms of solvability of the Diophantine equations $ax^2 - by^2 = \pm 1, \pm 2$. A consequence of this is the simple fact that the central norm is equal to 2 in such expansions if and only if there is a solution to the Diophantine equation $x^2 - Dy^2 = \pm 2$. However, this does not tell us the specifics pertaining to those D for which this holds. In this article, we explicitly identify those D for which this holds in terms of congruence conditions on the prime divisors of D, and parity conditions on certain numerators of convergents as well as the period length itself. This allows a complete description of those $D = 2^h c$ ($c > 1$ odd and possibly a perfect square when h is odd) with central norm equal to 2^h, heretofore only subsets of which were known—and we achieve the known results as immediate corollaries. This work was inspired by correspondence with Irving Kaplansky who sent this author a letter, dated October 29, 1998, containing conjectures for when the central norm is 2 when $D = 2pq$ for distinct primes p and q. As a consequence of the results in this paper, we achieve proofs of these conjectures as well. (See [7] for the proofs of other conjectures concerning simple continued fraction expansions inspired by correspondence with Professor Kaplansky.)

Received by the editors March 7, 2003; revised July 3, 2003.
The author's research is supported by NSERC Canada grant A8484.
AMS subject classification: 11A55, 11D09, 11R11.
Keywords: quadratic Diophantine equations, simple continued fractions, norms of ideals, infrastructure of real quadratic fields.

2 Notation and Preliminaries

Herein, we will be concerned with the simple continued fraction expansions of $\sqrt{D}$, $D \in \mathbb{N}$ (the natural numbers), D is not a perfect square. We denote this expansion by

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

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

The jth *convergent* of $\sqrt{D}$ for $j \geq 0$ is given by,

$$\frac{A_j}{B_j} = \langle q_0; q_1, q_2, \ldots, q_j \rangle = \frac{q_j A_{j-1} + A_{j-2}}{q_j B_{j-1} + B_{j-2}}. \tag{1}$$

The *complete quotients* are given by, $(P_j + \sqrt{D})/Q_j$, where $P_0 = 0$, $Q_0 = 1$, and for $j \geq 1$,

$$P_{j+1} = q_j Q_j - P_j, \tag{2}$$

$$q_j = \left\lfloor \frac{P_j + \sqrt{D}}{Q_j} \right\rfloor, \tag{3}$$

and

$$D = P_{j+1}^2 + Q_j Q_{j+1}. \tag{4}$$

We will also need the following facts (which can be found in most introductory texts on number theory, such as [6], or see [5] for a more advanced exposition).

$$A_j B_{j-1} - A_{j-1} B_j = (-1)^{j-1}. \tag{5}$$

Also,

$$A_{j-1} = P_j B_{j-1} + Q_j B_{j-2}, \tag{6}$$

and

$$A_{j-1}^2 - B_{j-1}^2 D = (-1)^j Q_j. \tag{7}$$

In particular,

$$A_{\ell-1}^2 - B_{\ell-1}^2 D = (-1)^\ell. \tag{8}$$

When ℓ is even, $P_{\ell/2} = P_{\ell/2+1}$, so by Equation (2),

$$Q_{\ell/2} \mid 2P_{\ell/2}, \tag{9}$$

https://doi.org/10.4153/CMB-2005-011-0 Published online by Cambridge University Press

where $Q_{\ell/2}$ is called the *central norm*, (via Equation (7)), and

$$q_{\ell/2} = 2P_{\ell/2}/Q_{\ell/2}. \tag{10}$$

For $\sqrt{D}$, $A_{\ell-1} + B_{\ell-1}\sqrt{D}$ is the fundamental solution of the Pell equation (8). By "fundamental solution" $X + Y\sqrt{D}$, to a norm-form equation $X^2 - DY^2 = c$, we mean that X, Y have the least positive values possible. When $c \neq \pm 1, \pm 4$ this may involve several "classes" of such solutions, so in that case, we mean the fundamental solution in its class (see [6, pp. 298–301] for instance). In general, a *positive* solution is one for which both X and Y are positive values. Similarly, for equations of the form $aX^2 - bY^2 = c$, there are classes of solutions. However, it is easy to show that if $X\sqrt{a} + Y\sqrt{b}$ and $W\sqrt{a} + Z\sqrt{b}$ are both positive solutions of the latter, then the following are equivalent: (1) $X < W$, (2) $Y < Z$, (3) $X\sqrt{a} + Y\sqrt{b} < W\sqrt{a} + Z\sqrt{b}$. Hence, there is a solution with X and Y of least positive value. We will call this the *fundamental solution* of the equation. Furthermore, the *norm* of $\alpha = X\sqrt{a} + Y\sqrt{b}$ is given by $N(\alpha) = aX^2 - bY^2$. This corresponds to the usual *norm* for elements of the form $\beta = x + y\sqrt{D}$, namely, $N(\beta) = x^2 - Dy^2$.

In [8], we proved the following results that we will need in the next section (see also [9]).

Theorem 1 *Let $D > 2$, not a perfect square. Then $\ell = \ell(\sqrt{D})$ is even if and only if one of the following holds.*

(1) *There exists a factorization $D = ab$ with $1 < a < b$ such that the Diophantine equation*

$$aX^2 - bY^2 = \pm 1 \tag{11}$$

has a solution.

(2) *There exists a factorization $D = ab$ with $1 \leq a < b$ such that the Diophantine equation*

$$ax^2 - by^2 = \pm 2 \tag{12}$$

has a solution where xy is odd.

Note that the following, proved by Lagarias [2, Lemma A-1, p. 504], is immediate from Theorem 1 (by contrapositive).

Corollary 1 *If $D > 1$ is squarefree and $f > 1$ with $\ell(\sqrt{f^2 D})$ odd, then $\ell(\sqrt{f^{2k} D})$ is odd for all $k \in \mathbb{N}$.*

Theorem 2 *Let $D > 1$, not a perfect square, and suppose that $D = ab$ with $1 < a < b$. Then if $T + U\sqrt{ab}$ is the fundamental solution of Diophantine equation*

$$x^2 - Dy^2 = 1, \tag{13}$$

and if $r\sqrt{a} + s\sqrt{b}$ is the fundamental solution of Equation (11)*, then each of the following holds.*

https://doi.org/10.4153/CMB-2005-011-0 Published online by Cambridge University Press

(a) $\ell = \ell(\sqrt{D})$ *is even.*
(b) $Q_{\ell/2} = a$ *in the simple continued fraction expansion of* $\sqrt{D}$.
(c) $A_{\ell/2-1} = ra$ *and* $B_{\ell/2-1} = s$.
(d) $T + U\sqrt{ab} = A_{\ell-1} + B_{\ell-1}\sqrt{ab} = \left(r\sqrt{a} + s\sqrt{b}\right)^2$.
(e) $r^2a - s^2b = (-1)^{\ell/2} = \left(\frac{A_{\ell/2-1}}{a}\right)^2 a - \left(B_{\ell/2-1}\right)^2 b$.
(f) *For any odd* $j \in \mathbb{N}$,

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

Theorem 3 *Let* $D = ab > 2$, *not a perfect square, with* $1 \leq a < b$. *Suppose that*

$$ax^2 - by^2 = \pm 2 \tag{14}$$

has a solution $(x, y) = (r, s) \in \mathbb{N}^2$ *where* xy *is odd. Then each of the following holds.*

(1) $\ell = \ell(\sqrt{D})$ *is even.*
(2) *If* $r\sqrt{a} + s\sqrt{b}$ *is the fundamental solution of Equation* (14), *then for any odd integer* $j \geq 1$,

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

(3) $A_{\ell/2-1} = ar$, $B_{\ell/2-1} = s$, *and* $Q_{\ell/2} = 2a$.
(4) $r^2a - s^2b = 2(-1)^{\ell/2}$.

The following is immediate from the above.

Corollary 2 *Suppose that* $D > 2$ *is an integer that is not a perfect square and* $\ell = \ell(\sqrt{D})$ *is even. Then* $Q_{\ell/2} = 2$ *if and only if there does not exist a factorization* $D = ab$ *with* $a > 2$, $b > 2$, *such that* $ax^2 - by^2 = \pm 1$; *and there does not exist a factorization* $D = ab$ *with* $a \neq 1 \neq b$ *such that* $ax^2 - by^2 = \pm 2$ *with* xy *odd.*

Theorem 4 *Suppose that* $D = ab$, *not a perfect square, where* $1 < a < b$ *with* $a = 2^t a_1$ *and* $b = 2^u b_1$ *for* $t, u \geq 0$. *If* $|r^2a - s^2b| = 1$ *has a solution* $r, s \in \mathbb{N}$, *then the following Jacobi symbol equalities hold, where* $\ell = \ell(\sqrt{ab})$ *is even,*

$$\left(\frac{b}{a_1}\right) = \left(\frac{-1}{a_1}\right)^{\ell/2+1} \text{ and } \left(\frac{a}{b_1}\right) = \left(\frac{-1}{b_1}\right)^{\ell/2}.$$

The reader may also consult the excellent paper [10] for more information on the Diophantine equation $ax^2 - by^2 = \pm 1$, which goes back to Gauss (see [1, Article 187]). There is also the seminal work of Ljunggren [3, 4].

3 Central Norms

First we look at the case where the radicand is even and divisible by an even power of 2. The criterion below tells us that we can find the fundamental unit of the odd part of the radicand from halfway along the continued fraction expansion of the full radicand.

https://doi.org/10.4153/CMB-2005-011-0 Published online by Cambridge University Press

Theorem 5 *Suppose that* $D = 4^d c$, *where* c *is not a perfect square,* $c, d \in \mathbb{N}$, c *odd,* $\ell = \ell(\sqrt{D})$ *and* $\ell' = \ell(\sqrt{c})$. *If* ℓ *is even, then* $Q_{\ell/2} = 4^d$ *if and only if*

$$\frac{A_{\ell/2-1}}{2^d} + B_{\ell/2-1}\sqrt{c} = A_{\ell'-1} + B_{\ell'-1}\sqrt{c} \tag{15}$$

in the simple continued fraction expansions of $\sqrt{D}$, *respectively* $\sqrt{c}$. *Moreover, when this occurs,* $\ell' \equiv \ell/2 \pmod 2$.

Proof Suppose that $Q_{\ell/2} = 4^d$, and part 1 of Theorem 1 holds. Set $D_1 = 4c$ and $\ell_1 = \ell(\sqrt{D_1})$. Then, by a trivial induction argument,

$$A_{\ell-1} + B_{\ell-1}\sqrt{D} = A_{\ell-1} + 2^{d-1}B_{\ell-1}\sqrt{D_1} = A_{\ell_1-1} + B_{\ell_1-1}\sqrt{D_1}.$$

However, by Theorem 2,

$$A_{\ell_1-1} + B_{\ell_1-1}\sqrt{D_1} = \left(\frac{A_{\ell_1/2-1}}{2} + B_{\ell_1/2-1}\sqrt{c}\right)^2,$$

and

$$\frac{A_{\ell_1/2-1}}{2} + B_{\ell_1/2-1}\sqrt{c} = \left(A_{\ell'-1} + B_{\ell'-1}\sqrt{c}\right)^k,$$

for some $k \in \mathbb{N}$. Since $A_{\ell_1-1} + B_{\ell_1-1}\sqrt{D_1}$ is the smallest solution of

$$X^2 - 4cY^2 = 1$$

and is also the smallest solution of $x^2 - cy^2 = 1$ with y even, then $k = 1$. Hence, by Theorem 2,

$$\begin{aligned}\left(\frac{A_{\ell/2-1}}{2^d} + B_{\ell/2-1}\sqrt{c}\right)^2 &= A_{\ell-1} + B_{\ell-1}\sqrt{D} = A_{\ell_1-1} + B_{\ell_1-1}\sqrt{D_1} \\ &= \left(A_{\ell'-1} + B_{\ell'-1}\sqrt{c}\right)^2,\end{aligned}$$

and the result follows. If case 2 of Theorem 1 holds, then the result follows by a similar argument. Conversely, if Equation (15) holds, then

$$(2^d A_{\ell'-1})^2 - (2^d B_{\ell'-1})^2 c = (-1)^{\ell/2} Q_{\ell/2},$$

so

$$(-1)^{\ell'} = A_{\ell'-1}^2 - B_{\ell'-1}^2 c = (-1)^{\ell/2} Q_{\ell/2}/(2^{2d}).$$

Thus, $Q_{\ell/2} = 4^d$ and $\ell' \equiv \ell/2 \pmod 2$. ∎

https://doi.org/10.4153/CMB-2005-011-0 Published online by Cambridge University Press

Example 1 This illustrates Theorem 5 in the case where part 1 of Theorem 1 holds. Let $D = 4 \cdot 3 \cdot 7 \cdot 11$. Then $\ell = 8$, $Q_{\ell/2} = 4$, $A_{\ell/2-1} = 152$, $B_{\ell/2-1} = 5$, $\ell' = 2$, $A_{\ell'-1} = 76$, and $B_{\ell'-1} = 5$. Thus,

$$\left(\frac{A_{\ell/2-1}}{a}\sqrt{a} + B_{\ell/2-1}\sqrt{c}\right)^2 = (76 + 5\sqrt{3 \cdot 7 \cdot 11})^2 = 11551 + 380\sqrt{D}$$
$$= A_{\ell-1} + B_{\ell-1}\sqrt{D},$$

and

$$\frac{A_{\ell/2-1}}{2^d} + B_{\ell/2-1}\sqrt{c} = 76 + 5\sqrt{3 \cdot 7 \cdot 11} = A_{\ell'-1} + B_{\ell'-1}\sqrt{c}.$$

Example 2 This illustrates Theorem 5 in the case where part 2 of Theorem 1 holds. Let $D = 4^2 \cdot 11 = 4^d \cdot c$. Then $\ell = 4$, $Q_{\ell/2} = 16$, $A_{\ell/2-1} = 40$, $B_{\ell/2-1} = 3$, $\ell' = 2$, $A_{\ell'-1} = 10$, and $B_{\ell'-1} = 3$. Hence,

$$\frac{1}{2}\left(\frac{A_{\ell/2-1}\sqrt{a}}{a} + B_{\ell/2-1}\sqrt{2c}\right)^2 = \frac{1}{2}(10\sqrt{2} + 3\sqrt{22})^2 = A_{\ell-1} + B_{\ell-1}\sqrt{D}$$
$$= 199 + 15\sqrt{D},$$

and

$$\frac{A_{\ell/2-1}}{2^d} + B_{\ell/2-1}\sqrt{c} = 10 + 3\sqrt{11} = A_{\ell'-1} + B_{\ell'-1}\sqrt{c}.$$

Now we look at the case where D is divisible by an odd power of 2.

Theorem 6 *Suppose that $D = 2^{2d-1}c$, where $d \in \mathbb{N}$, c is odd, and $\ell = \ell(\sqrt{D})$ is even. Then $Q_{\ell/2} = 2^{2d-1}$ if and only if $\ell_1 = \ell(\sqrt{2c})$ is even with $Q_{\ell_1/2} = 2$, and*

$$A_{\ell/2-1} = 2^{d-1}A_{\ell_1/2-1} \text{ and } B_{\ell/2-1} = B_{\ell_1/2-1}. \tag{16}$$

Moreover, when this holds, $\ell \equiv \ell_1 \pmod 4$.

Proof If $Q_{\ell_1/2} = 2$ and conditions (16) hold, then

$$A^2_{\ell/2-1} - B^2_{\ell/2-1}D = (-1)^{\ell/2}Q_{\ell/2} = 2^{2d-2}A^2_{\ell_1/2-1} - B^2_{\ell_1/2-1}2^{2d-1}c$$
$$= 2^{2d-2}Q_{\ell_1/2}(-1)^{\ell_1/2} = 2^{2d-1}(-1)^{\ell_1/2}.$$

Thus, $\ell_1 \equiv \ell \pmod 4$ and $Q_{\ell/2} = 2^{2d-1}$.

Conversely, suppose that $Q_{\ell/2} = 2^{2d-1}$. If part 1 of Theorem 1 holds, then $A_{\ell/2-1} = 2^{2d-1}r$, and $B_{\ell/2-1} = s$ where $2^{2d-1}r^2 - s^2c = (-1)^{\ell/2}$. Hence,

$$2^{2j-1}(r2^{d-j})^2 - s^2c = (-1)^{\ell/2},$$

for any $j = 1, \ldots, d$. Therefore, if $\ell_j = \ell(\sqrt{D_j})$ with $D_j = 2^{2j-1}c$, then

$$Q_{\ell_j/2} = 2^{2j-1},\ A_{\ell_j/2-1} = 2^{d+j-1}r = A_{\ell/2-1}/2^{d-j}.$$

https://doi.org/10.4153/CMB-2005-011-0 Published online by Cambridge University Press

In particular, if $j = 1$, we have our result. The argument is similar for the case where part 2 of Theorem 1 holds. In either case, $\ell \equiv \ell_1 \pmod 4$. ■

The following illustrates Theorem 6.

Example 3 If $D = 2^7 \cdot 129$, then $A_{\ell/2-1} = A_0 = 128 = Q_{\ell/2} = 2^7 = 2^{2d-1}$, where $r = 1$ in this case. Also, $c = 129$, $A_{\ell_1/2-1} = A_0 = 16 = 2^4 = 2^d$, and $Q_{\ell_1/2} = 2$.

Note that Theorem 6 also covers the case where c is a perfect square.

Example 4 If $D = 2^3 \cdot 3^2 = 2^{2d-1} \cdot c$, then $A_{\ell/2-1} = A_0 = 8 = Q_{\ell/2}$, and $r = 1$ in this case as well. Also, $c = 9$, $A_{\ell_1/2-1} = A_0 = 4 = 2^2 = 2^d$, and $Q_{\ell_1/2} = 2$.

Also note that when $Q_{\ell_1/2} = 2$ in the absence of the satisfaction of conditions (16) in Theorem 6, then not only do we not have $Q_{\ell/2} = 2^{2d-1}$, but also $Q_{\ell/2}$ may not be even. For instance, if $D = 2^3 \cdot 7$, then $\ell_1 = \ell(\sqrt{14}) = 4$ and $Q_{\ell_1/2} = 2$. However, $\ell = \ell(\sqrt{56}) = 2$ and $Q_{\ell/2} = 7$.

Note as well that Theorem 6 says nothing about the case where $d = 1$ and thus it is predicated upon the solution of that problem which is given in the following more detailed result, where we cover all cases except when c is divisible only by primes congruent to 1 modulo 4. (See Remark 1 below for comments on that case.)

Theorem 7 *Let $D = 2c$, and $\ell = \ell(\sqrt{D})$, where $c > 1$ is odd (possibly a perfect square). Then ℓ is even and we have criteria for $Q_{\ell/2} = 2$ in each of the following.*

(a) *If $c \equiv 1 \pmod 8$ and c is divisible by a prime congruent to 7 modulo 8, then $Q_{\ell/2} = 2$ if and only if each of the following holds.*
   (1) *$\ell/2$ is even,*
   (2) *$A_{\ell/2-1} \equiv 2 \pmod 4$, and*
   (3) *There does not exist a factorization $c = ab$ with $a \neq 1$, $b \neq 1$, such that $a \equiv 1 \equiv b \pmod 8$ and $2ax^2 - by^2 = \pm 1$ for any integers x, y.*

(b) *If $c \equiv 1 \pmod 8$ and c is divisible by a prime congruent to 3 modulo 8, then $Q_{\ell/2} = 2$ if and only if each of the following holds.*
   (1) *$\ell/2$ is odd.*
   (2) *$A_{\ell/2-1} \equiv 0 \pmod 4$.*
   (3) *There does not exist a factorization $c = ab$ with $a \neq 1$, $b \neq 1$, such that $a \equiv 1 \equiv b \pmod 8$ and $2ax^2 - by^2 = \pm 1$ for any integers x, y.*

(c) *If $c \equiv 3 \pmod 8$, then $Q_{\ell/2} = 2$ if and only if each of the following holds.*
   (1) *$\ell/2$ is odd.*
   (2) *$A_{\ell/2-1} \equiv 2 \pmod 4$.*
   (3) *There does not exist a factorization $c = ab$ with $a \neq 1$, $b \neq 1$ such that $a \equiv 1 \pmod 8$, $b \equiv 3 \pmod 8$, and $2ax^2 - by^2 = -1$ for any integers x, y.*

https://doi.org/10.4153/CMB-2005-011-0 Published online by Cambridge University Press

(d) *If* $c \equiv 7 \pmod 8$, *then* $Q_{\ell/2} = 2$ *if and only if each of the following holds.*

(1) $\ell/2$ *is even.*

(2) $A_{\ell/2-1} \equiv 0 \pmod 4$.

(3) *There does not exist a factorization* $c = ab$ *with* $a \neq 1$, $b \neq 1$ *such that* $a \equiv 1 \pmod 8$, $b \equiv 7 \pmod 8$, *and* $2ax^2 - by^2 = 1$ *for any integers* x, y.

Proof In all parts, (a)–(d), D is divisible by a prime congruent to 3 modulo 4, so $x^2 - Dy^2 = -1$ cannot hold from which Equation (8) tells us that ℓ is even. Moreover, for all parts (a)–(d), part 2 of Theorem 1 cannot hold (given that XY cannot be odd in that case when D is even), so part 1 of Theorem 1 must hold.

For part (a), if $Q_{\ell/2} = 2$, then by Theorems 1–2, we must have

$$2r^2 - cs^2 = (-1)^{\ell/2}$$

for some natural numbers r, s, and $A_{\ell/2-1} = 2r$. If $\ell/2$ is odd, then given any prime $p \mid c$, with $p \equiv 7 \pmod 8$,

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

a contradiction, so $\ell/2$ is even. Therefore, $1 = 2r^2 - cs^2 \equiv 2r^2 - 1 \pmod 8$, so r is odd. Hence, $A_{\ell/2-1} \equiv 2 \pmod 4$. If there were a factorization $c = ab$ with $a \neq 1$, $b \neq 1$ and $2ax^2 - by^2 = \pm 1$ then by Theorem 2, $A_{\ell/2-1} = 2ax$, forcing $a = 1$, a contradiction; or $A_{\ell/2-1} = by = 2r$, also a contradiction since by is odd. Conversely, suppose that (1)–(3) hold. If there exist $a \neq 1$, $b \neq 1$ such that $2ar^2 - bs^2 = \pm 1$ for some $r, s \in \mathbb{N}$, then by (3), $a \equiv 3 \pmod 8$, so $\pm 1 \equiv 6r^2 - 3 \equiv \pm 3 \pmod 8$, a contradiction. Therefore, $a = 1$, so $Q_{\ell/2} = 2$. The cases $a \equiv b \equiv 5 \pmod 8$ and $a \equiv b \equiv 7 \pmod 8$ are similar. Also, in (b)–(d) we only cover one case since the others are similar.

For part (b), if $Q_{\ell/2} = 2$, then as above, $2r^2 - cs^2 = (-1)^{\ell/2}$, and $A_{\ell/2-1} = 2r$. If $\ell/2$ is even, then for any prime $p \mid c$, with $p \equiv 3 \pmod 8$,

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

a contradiction, so $\ell/2$ is odd. Therefore, $-1 = 2r^2 - cs^2 \equiv 2r^2 - 1 \pmod 8$, forcing r to be even, namely $A_{\ell/2-1} \equiv 0 \pmod 4$. We have shown that (1) and (2) hold, and (3) holds by the same reasoning as in the proof for (a). Conversely, suppose that (1)–(3) hold. If there exist integers r, s and a factorization $c = ab$ with $1 \leq a < 2b$ such that $ar^2 - 2bs^2 = (-1)^{\ell/2} = -1$, then by Theorem 2, $A_{\ell/2-1} = ar \equiv 0 \pmod 4$, a contradiction since ar is clearly odd. Hence, there exists a factorization $c = ab$ with $1 \leq 2a < b$ such that $2ar^2 - bs^2 = -1$ and $A_{\ell/2-1} = 2ar \equiv 0 \pmod 4$, so r is even. If $a > 1$, then $-1 \equiv -b \pmod 8$, forcing $a \equiv b \equiv 1 \pmod 8$. This contradicts (3) unless $a = 1$, so $Q_{\ell/2} = 2$.

https://doi.org/10.4153/CMB-2005-011-0 Published online by Cambridge University Press

For part (c), suppose that $Q_{\ell/2} = 2$. Then as above, there are $r, s \in \mathbb{N}$ with $2r^2 - cs^2 = (-1)^{\ell/2}$ and $A_{\ell/2-1} = 2r$. If $\ell/2$ is even, $1 \equiv 2r^2 - 3 \pmod 8$, so $r^2 \equiv 2 \pmod 4$, which is not possible, so $\ell/2$ is odd. Thus,

$$-1 \equiv 2r^2 - 3 \pmod 8,$$

forcing r to be odd. Therefore, $A_{\ell/2-1} \equiv 2 \pmod 4$. This establishes (1) and (2). Part (3) must also hold by Theorem 2 since *any* factorization $c = ab$ with $1 < a < b$ such that $2ax^2 - by^2 = -1$ would imply that $A_{\ell/2-1} = 2ax$, which is impossible since $A_{\ell/2-1} = 2r$ where $\gcd(r, c) = 1$. Conversely, suppose parts (1)–(3) hold. As above, there exists a factorization $c = ab$ with $a \neq 1$, $b \neq 1$, and $2ar^2 - bs^2 = -1$ for some $r, s \in \mathbb{N}$, where r is odd by part (2). If $a > 1$, then by part (3), $a \equiv 3 \pmod 8$ and $b \equiv 1 \pmod 8$. Hence,

$$-1 \equiv 2ar^2 - bs^2 \equiv 6 - 1 \equiv 5 \pmod 8,$$

a contradiction. Therefore, $a = 1$, so $Q_{\ell/2} = 2$.

For part (d), if $Q_{\ell/2} = 2$, then as above, there exist $r, s \in \mathbb{N}$ such that $2r^2 - cs^2 = (-1)^{\ell/2}$ and $A_{\ell/2-1} = 2r$. If $\ell/2$ is odd, then

$$-1 \equiv 2r^2 - 7 \equiv -5, -7 \pmod 8,$$

which is not possible. Thus, $\ell/2$ is even. Therefore, $1 \equiv 2r^2 - 7 \pmod 8$, which implies that r is even. Hence, $A_{\ell/2-1} \equiv 0 \pmod 4$. This is (1) and (2). Part (3) follows as above. Conversely, suppose that (1)–(3) hold. If there exist $x, y \in \mathbb{N}$ such that $2ax^2 - by^2 = 1$ for $a > 1$, then by (2) and (3)

$$2ax^2 - by^2 = 1 \equiv 6x^2 - 1 \equiv -1 \pmod 8,$$

which is not possible. Thus, $a = 1$ so $Q_{\ell/2} = 2$. ∎

The following is immediate from the above and is partly motivated by the more general study herein based upon correspondence with Irving Kaplansky, and proves his conjectures in the aforementioned correspondence.

Corollary 3 *If $D = 2p^e q^f$ where p and q are distinct odd primes, and $e, f \in \mathbb{N}$ are odd, then $\ell = \ell(\sqrt{D})$ is even and each of the following holds.*

(1) *If $p \equiv 7 \equiv q \pmod 8$, then $Q_{\ell/2} = 2$ if and only if $\ell/2$ is even and $A_{\ell/2-1} \equiv 2 \pmod 4$.*
(2) *If $p \equiv q \equiv 3 \pmod 8$, then $Q_{\ell/2} = 2$.*
(3) *If $p \equiv 1 \pmod 8$ and $q \equiv 3 \pmod 8$, with $p > 2q$, then $Q_{\ell/2} = 2$ if and only if $\ell/2$ is odd and $A_{\ell/2-1} \equiv 2 \pmod 4$.*
(4) *if $p \equiv 1 \pmod 8$ and $q \equiv 7 \pmod 8$ with $p > 2q$, then $Q_{\ell/2} = 2$ if and only if $\ell/2$ is even and $A_{\ell/2-1} \equiv 0 \pmod 4$.*

The following illustrates the results above.

https://doi.org/10.4153/CMB-2005-011-0 Published online by Cambridge University Press

Example 5 If $D = 2{\cdot}7{\cdot}23 = 2{\cdot}a{\cdot}b$, then $\ell = 4$, $a \equiv b \equiv 7 \pmod 8$ and $A_{\ell/2-1} = 6$, with $Q_{\ell/2} = 2$. This illustrates part (a) above. Although condition (3) is vacuous when c is divisible by only two primes, it is necessary for more primes. For instance, if $D = 2{\cdot}47{\cdot}71{\cdot}103{\cdot}127$, $\ell = 8$, $A_{\ell/2-1} \equiv 2 \pmod 4$, but $2{\cdot}47{\cdot}71{\cdot}7^2 - 103{\cdot}127{\cdot}5^2 = 1$, and $Q_{\ell/2} = 6674 = 2 \cdot 47 \cdot 71 = P_{\ell/2}$. However, if $D = 2 \cdot 7 \cdot 23 \cdot 31 \cdot 47 = 2c$, $Q_{\ell/2} = Q_{18} = 2$, $A_{\ell/2-1} \equiv 2 \pmod 4$ and there does not exist such a factorization of $c = 234577$. Unlike part (2) of Corollary 3, there are instances where $Q_{\ell/2} \neq 2$ when c is divisible by only two primes. For instance, if $D = 2 \cdot 7 \cdot 31$, then $\ell = 4$, $Q_{\ell/2} = 7$, and $A_{\ell/2-1}$ is odd.

If $D = 2 \cdot 3^2$, then $\ell/2 = 1$, $Q_{\ell/2} = 2$, and $A_{\ell/2-1} = 4$. This illustrates part (b). Note that condition (3) is vacuous in part (b) if c is only divisible by two primes, but is necessary for more primes. For instance, if $D = 2{\cdot}3{\cdot}7{\cdot}11{\cdot}151$, conditions (1) and (2) are satisfied since $\ell/2 = 1$, and $A_{\ell/2-1} = 264 \equiv 0 \pmod 4$, but $Q_{\ell/2} = 66 = 2{\cdot}3{\cdot}11$. Here we have, $2 \cdot 3 \cdot 11 \cdot 4^2 - 7 \cdot 151 = -1$. Moreover, part (2) of Corollary 3 tells us that conditions (1) and (2) always hold when c is divisible by exactly two distinct primes.

If $D = 2 \cdot 3 \cdot 17$, then $\ell = 2$, $A_{\ell/2-1} = 10$ and $Q_{\ell/2} = 2$. This illustrates part (c). Note that condition (3) cannot be eliminated even in the case where c is divisible by only two primes. For instance, if $D = 2 \cdot 89 \cdot 179$, then $\ell = 2$, $A_{\ell/2-1} = 178 \equiv 2 \pmod 4$, but $Q_{\ell/2} = 178 = 2 \cdot 89$, and we have that $2 \cdot 89 - 179 = -1$. Also, as with the previous case, we need conditions (1) and (2). For instance, if $D = 2 \cdot 3 \cdot 73$, then $\ell = 4$ and $Q_{\ell/2} = 3$.

If $D = 2 \cdot 17 \cdot 23$, then $\ell = 4$, $Q_{\ell/2} = 2$, and $A_{\ell/2-1} = 28 \equiv 0 \pmod 4$. This illustrates part (d). The following illustrates the necessity of condition (3) even when c is divisible by only two primes. Let $D = 2 \cdot 17 \cdot 103$. Then $\ell = 24$, $A_{\ell/2-1} = 477916 \equiv 0 \pmod 4$. However, $Q_{\ell/2} = 34 = 2{\cdot}17$, and $2{\cdot}17{\cdot}13174^2 - 7569^2{\cdot}103 = 1$. Again, parts (1) and (2) are required when c is divisible by only two primes. For instance, if $D = 2 \cdot 23 \cdot 73$, $Q_{\ell/2} = Q_7 = 23$.

Remark 1 The case where c is divisible by only primes congruent to 1 modulo 8 is special (in the notation of Theorem 7) in that there appears to be no necessary and sufficient conditions for $Q_{\ell/2} = 2$ (when ℓ is even) beyond that given in Corollary 2, namely that $Q_{\ell/2} = 2$ if and only if there is no factorization $c = ab$ with $a \neq 1 \neq b$ such that $2ax^2 - by^2 = \pm 1$ for any $x, y \in \mathbb{Z}$. It is perhaps worthy of note that if $Q_{\ell/2} = 2$, then $A_{\ell/2-1} \equiv 1 + (-1)^{\ell/2} \pmod 4$, which can be shown using the above techniques. However, this is far from sufficient. For example, if $D = 2 \cdot 17 \cdot 137$, then $\ell = 2$, $A_{\ell/2-1} \equiv 0 \pmod 4$, but $Q_{\ell/2} = 2 \cdot 17$.

The following provides cases where $D \equiv 2 \pmod 4$ and $Q_{\ell/2} \neq 2$ under any hypothesis.

Theorem 8 *Let $D = 2c$ where $c > 1$ is odd* (possibly a perfect square). Then in each of the following cases, when $\ell = \ell(\sqrt{D})$ is even, $Q_{\ell/2} \neq 2$.

(1) c is divisible by a prime $p \equiv 5 \pmod 8$.
(2) c is divisible by primes $p_j \equiv 3 \pmod 8$, and $p_k \equiv 7 \pmod 8$.

https://doi.org/10.4153/CMB-2005-011-0 Published online by Cambridge University Press

Proof As in the proof of Theorem 7, if ℓ is even, then part (2) of Theorem 1 must hold. Thus, if $Q_{\ell/2} = 2$, then there exist $r, s \in \mathbb{N}$ such that

$$2r^2 - cs^2 = (-1)^{\ell/2}.$$

If part (1) holds, then

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

a contradiction.

If part (2) holds, then

$$(-1)^{\ell/2} = \left(\frac{(-1)^{\ell/2}}{p_j}\right) = \left(\frac{2r^2 - cs^2}{p_j}\right) = \left(\frac{2}{p_j}\right) = -1.$$

However,

$$(-1)^{\ell/2} = \left(\frac{(-1)^{\ell/2}}{p_k}\right) = \left(\frac{2r^2 - cs^2}{p_k}\right) = \left(\frac{2}{p_k}\right) = 1,$$

a contradiction. ∎

We conclude with some comments in the case where D is odd. When $D \equiv 1 \pmod 4$, it is not possible for $Q_{\ell/2} = 2$ when ℓ is even. The reason is that, when ℓ is even, and D is odd, then part (2) of Theorem 1 must hold if $Q_{\ell/2} = 2$ (by Theorems 2–3). Hence, there exist odd $X, Y \in \mathbb{N}$ such that $X^2 - DY^2 = (-1)^{\ell/2}2$, so $D \equiv 1 + (-1)^{\ell/2+1} \pmod 8$, whence $D \equiv 3 \pmod 4$. When $D \equiv 3 \pmod 4$, the only criterion seems to be the one we found in [8], namely Corollary 2.

Acknowledgements The author welcomes the opportunity to thank the referee for comments which led the author to strengthen the results of the paper in an even more concise form.

References

[1] C F. Gauss, *Disquisitiones Arithmeticae.* Springer-Verlag, New York, 1986.
[2] 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), 485–508.
[3] W. Ljunggren, *Ein Satz über die Diophantische Gleichung* $Ax^2 - By^4 = C (C = 1, 2, 4)$. Matematiska Inst., Lund, 1954, pp. 188–194.
[4] ———, *On the Diophantine equation* $Ax^4 - By^2 = C (C = 1, 4)$). Math. Scand. **21**(1967), 149–158.
[5] R. A. Mollin, *Quadratics.* CRC Press, Boca Raton, FL, 1996.
[6] ———, *Fundamental Number Theory with Applications.* CRC Press, Boca Raton, FL, 1998 .
[7] ———, *Proof of some conjectures by Kaplansky.* C.R. Math. Acad. Sci. Soc. R. Can. **23**(2001), 60–64.
[8] ———, *A continued fraction approach to the Diophantine equation* $ax^2 - by^2 = \pm 1$. JP J. Algebra Number Theory Appl. **4**(2004), 159–207.

[9] P. J. Rippon and H. Taylor, *Even and odd periods in continued fractions of square roots*, preprint (2001).
[10] D. T. Walker, *On the Diophantine equation* $mX^2 - nY^2 = \pm 1$, Amer. Math. Monthly **74**(1967), 504–513.

Department of Mathematics and Statistics
University of Calgary
Calgary, Alberta
T2N 1N4
e-mail: ramollin@math.ucalgary.ca