

# When the Central Norm Equals 2 in the Simple Continued Fraction Expansion of a Quadratic Surd\*

R.A. Mollin

## Abstract

We complete the task, begun in [19], of determining when the central norm (determined by the infrastructure of the underlying real quadratic field) is equal to 2 in the simple continued fraction expansion of the associated quadratic surd.

## 1 Introduction

In [19], we showed that when the integer  $D > 1$  is not a perfect square and  $D = 2^a c$  where  $a > 1$  and  $c$  is odd, then the central norm (defined in the next section) being 2 for  $\sqrt{D}$  is directly related to the central norm of  $\sqrt{D/2^{a-1}}$  being 2. Then we settled the case for  $D = 2c$  for all except the case where  $c$  is divisible only by primes congruent to 1 modulo 8. In this note, we solve that case as well and give a new general criterion for all cases, thereby completing the project, which was motivated by correspondence with Irving Kaplansky as outlined in [19].

## 2 Notation and Preliminaries

We write the simple continued fraction expansions of  $\sqrt{D}$ ,  $D \in \mathbb{N}$  (the natural numbers),  $D$  is not a perfect square by:

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

---

\*Mathematics Subject Classification 2000: 11A55, 11D09, 11R11. Key words and phrases: quadratic Diophantine equations, simple continued fractions, infrastructure of real quadratic fields.

where  $\ell = \ell(\sqrt{D})$  is the period length of  $\sqrt{D}$ .

The  $j$ th convergent of  $\alpha$  for  $j \geq 0$  are given by,

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

If we set:  $P_0 = 0$ ,  $Q_0 = 1$ , and for  $j \geq 1$ ,

$$P_{j+1} = q_j Q_j - P_j, \quad (2)$$

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

and

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

We will also need the following facts (which can be found in most introductory texts in number theory, such as [14], or see [13] for a more advanced exposition).

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

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

and

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

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

$$Q_{\ell/2} \mid 2P_{\ell/2}, \quad (8)$$

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

$$q_{\ell/2} = 2P_{\ell/2}/Q_{\ell/2}. \quad (9)$$

We will need the following in the next section. Note that this result corrects the oversights in [15, Theorem 1.3, p. 334], [16, Theorem 1.3, p. 101], and [17, Theorem 1.2, p. 221]. (Fortunately, the correct version below is the one actually used in those papers, rather than the incorrectly stated ones. The problem only arises when the norm is not squarefree.)

**Lemma 1** *If  $D > 1$  is not a perfect square, then  $Q_j \mid 2D$  and  $Q_j \mid 2A_{j-1}$  for some  $j < \ell$  (where the  $Q_j$ ,  $A_j$ , and  $\ell$  are as defined in the previous section for  $\sqrt{D}$ ) if and only if  $j = \ell/2$ .*

*Proof.* If  $Q_j \mid 2D$  and  $Q_j \mid A_{j-1}$ , then by Equation (6)  $Q_j \mid 2P_j$  (since  $\gcd(A_{j-1}, B_{j-1}) = 1$  by Equation (5)). Now the proof follows exactly as in [18, Theorem 2.3, p. 64] (where  $Q_j$  was assumed therein to be squarefree in order to achieve the latter divisibility condition).

The converse is proved exactly as in [18, Theorem 2.3, p. 63] since no squarefreeness was needed or assumed therein.  $\square$

For work related to the work herein, which helped to inspire this author's work along with the aforementioned correspondence with Kaplansky see [1]–[12], and [21]–[23].

### 3 The Criterion

The following is a general criterion for  $Q_{\ell/2} = 2$  (where  $\ell$  is defined in the previous section as are the symbols used below) when  $D \equiv 2 \pmod{4}$  which completes the general case for reasons cited in the introduction.

**Theorem 1** *Let  $D = 2c$  where  $c > 1$  is odd (possibly a perfect square) . If  $\ell$  is even, then the following are equivalent.*

1.  $Q_{\ell/2} = 2$ .
2.  $q_{\ell/2} = P_{\ell/2}$ .
3. *There exists a solution to the Diophantine equation  $x^2 - Dy^2 = \pm 2$ .*
4. *There does not exist a factorization  $c = ab$  with  $2 < a < b$  for which there is a solution to the Diophantine equation  $ax^2 - by^2 = \pm 1$ .*
5. *There does not exist a divisor  $a > 2$  of  $D$  such that  $a \mid A_{\ell/2-1}$ .*

*Proof.* The equivalence of 1 and 2 is a consequence of Equation (9). The equivalence of 1 and 3 was proved in [20], as was the equivalence of 1 and 4. It remains to show the equivalence of 1 and 5.

Suppose that 5 holds and  $Q_{\ell/2} = a$ . Then by Lemma 1,  $a \mid 2D$  and  $a \mid 2A_{\ell/2-1}$ . If  $a$  is odd, then 5 forces  $a = 1$ , a contradiction. If  $a$  is divisible by 4, then by Equation (8),  $2 \mid P_{\ell/2}$ , so by Equations (5) and (7),  $4 \mid D$ , a contradiction. Hence,  $a \equiv 2 \pmod{4}$ . If  $a > 2$ , then  $(a/2) \mid D$  and  $(a/2) \mid A_{\ell/2-1}$ , so by 5  $a/2 = 1$ . Conversely, if 1 holds, then by Lemma 1, 5 must hold.  $\square$

The new condition in terms of criteria for  $Q_{\ell/2} = 2$  is 5 in Theorem 1. This completes the work done in [19]. The following completes the proof of a conjecture of Kaplansky begun in that paper.

**Corollary 1** *If  $D = 2pq$  where  $p$  and  $q$  are distinct odd primes, then*

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

*Proof.* Parts 1–4 were proved in [19]. Part 5 follows from Theorem 1. □

We conclude with an example that illustrates case 5.

**Example 1** *Let  $D = 2 \cdot 17 \cdot 41$ . Then  $\ell = 6$  and  $Q_{\ell/2} = 2$ . Here  $A_{\ell/2-1} = 112$  which is relatively prime to  $c = 17 \cdot 41$ .*

*If  $D = 2 \cdot 41 \cdot 113$ , then  $\ell = 8$ ,  $Q_{\ell/2} = 82$  and*

$$\gcd(A_{\ell/2-1}, c) = \gcd(2214, 4633) = 41.$$

**Acknowledgements:** The author's research is supported by NSERC Canada grant # A8484.

## References

- [1] J.H.E. Cohn, *Five Diophantine equations*, Math. Scand. **21** (1967), 61–70.
- [2] J.H.E. Cohn, *Squares in some recurrent sequences*, Pacific J. Math. **41** (1972), 631–646. Addendum: *Waring’s problem in quadratic number fields* Acta Arith. **20** (1972), 1–16. Acta Arith. **23** (1973), 417–418.
- [3] P. Crescenzo, *A Diophantine equation which arises in the theory of finite groups*, Advances in Math. **17** (1975), 25–29.
- [4] C. Friesen, *Legendre symbols and continued fractions*, Acta Arith. **59** (1991), 365–379.
- [5] P. Kaplan, *À propos des equation antipelliennes*, L’Ens. Math **29** (1983), 323–328.
- [6] P. Kaplan and K.S. Williams, *Pell’s equations  $x^2 - my^2 = -1, -4$  and continued fractions*, J. Number Theory **23** (1986), 169–182.
- [7] W. Ljunggren, *Zur Theorie der Gleichung  $x^2 + 1 = Dy^2$* , Avh. Norske Vid. Akad. Oslo I, no. (1942).
- [8] W. Ljunggren, *Ein Satz über die Diophantische Gleichung  $Ax^2 - By^2 = C$  ( $C = 1, 4$ )*, Tolfte Skand. Matemheirkerkongressen, Lund, 1953, 199–194 (1954).
- [9] W. Ljunggren, *On the Diophantine equation  $Ax^4 - By^2 = C$  ( $C = 1, 4$ )*, Math. Scand. **21** (1967), 149–158.
- [10] W.L. McDaniel and P. Ribenboim, *Squares and double squares in Lucas sequences*, C.R. Math. Rep. Acad. Sci. Canada **14** (1992), 104–108.
- [11] W.L. McDaniel and P. Ribenboim, *The square terms in Lucas sequences*, J. Number Theory **58** (1996), 104–123.
- [12] M. Mignotte and A. Pethö, *Sur les carrés dans certaines suites de Lucas*, J. Théorie Nombres Bordeaux **5** (1993), 333–341.
- [13] R.A. Mollin, **Quadratics**, CRC Press, Boca Raton, New York, London, Tokyo (1996).

- [14] R.A. Mollin, **Fundamental Number Theory with Applications**, CRC Press, Boca Raton, New York, London, Tokyo (1998).
- [15] R.A. Mollin, *Jacobi symbols, ambiguous ideals, and continued fractions*, Acta Arith. **LXXXV** (1998), pp. 331–349.
- [16] R.A. Mollin and K. Cheng, *Palindromy and ambiguous ideals revisited*, J. Number Theory **74** (1999), 98–110.
- [17] R.A. Mollin and A.J. van der Poorten, *Continued fractions, Jacobi symbols, and quadratic Diophantine equations*, Canad. Math. Bulletin **43** (2000), 218–225.
- [18] R.A. Mollin, *Quadratic Diophantine equations determined by continued fractions*, JP J. Algebra, Number Theory, and Apps., **1** (2001), 57–75.
- [19] 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  $c > 1$* , to appear: Canad. Math. Bulletin.
- [20] R.A. Mollin, *A continued fraction approach to the Diophantine equation  $ax^2 - by^2 = \pm 1$* , to appear.
- [21] R.J. Stroeker, *How to solve a Diophantine equation*, Amer. Math. Monthly **91**, (1984), 385–392.
- [22] H.F. Trotter, *On the norms of units in quadratic fields*, Proceed. Amer. Math. Soc. (1969), 198–201.
- [23] 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  
 Canada, T2N 1N4  
 URL: <http://www.math.ucalgary.ca/~ramollin/>  
 E-mail: ramollin@math.ucalgary.ca