

# Infinitely Many Quadratic Diophantine Equations Solvable Everywhere Locally, But Not Solvable Globally\*

R.A. Mollin

## Abstract

We present an infinite class of integers  $2c$ , which turn out to be Richaud-Degert type radicands, for which  $2x^2 - cy^2 = -1$  has no integer solutions, but for which  $2x^2 - cy^2 \equiv -1 \pmod{n}$  has integer solutions for any  $n \in \mathbb{N}$ . This explains a topic often seen in introductory number theory courses, that appears as a curiosity, yet for which we are able to give the underlying reasons in terms of simple continued fraction expansions.

## 1 Introduction

In many introductory number theory texts such as [6, p. 208] and [11, p. 207], the Diophantine equation  $2x^2 - 219y^2 = -1$  is discussed as having no integer solutions  $x, y$ , yet for which  $2x^2 - 219y^2 \equiv -1 \pmod{n}$  has integer solutions for all moduli  $n \in \mathbb{N}$ . In [11], Nagell is credited with having proved this as a deduction from a deeper theorem presented in [8]. Nagell remarks therein that the congruence cited above can easily be proved solvable for all moduli  $n$ . However, in neither [8] nor [11] is there any connection with the real reason underlying this phenomenon, namely central norms in continued fractions, which we will explain in the next section (see Definition 1 below). An infinite family of values  $2c$  was given more recently in [2], but again the continued fraction reasons are missing, albeit continued fractions are used in

---

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

the proof of their main result. It is this result that we generalize here and show how to generate such radicands at will that satisfy the aforementioned dual solvability/insolvability criteria.

## 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,

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

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

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

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

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

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

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

and

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

Since we use the following term throughout, we isolate it for convenience.

**Definition 1** *When  $\ell = \ell(\sqrt{D})$  is even, the value  $Q_{\ell/2}$  is called the central norm of the simple continued fraction expansion of  $\sqrt{D}$ .*

We will also need the following facts (which can be found in most introductory texts in number theory, such as [6], or see [5] for a more advanced exposition. There are also the classic references on continued fractions by Chrystal [1] and Perron [10], as well as the excellent introductory number theory texts [3], by Leveque, and [11], by Sierpiński).

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

Also,

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

and

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

In particular,

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

In [7], we proved the following results that we will need in the next section. (See also some related seminal results in [4] and [12].)

**Theorem 1** *Let  $D > 2$ , not a perfect square. Then the period length  $\ell = \ell(\sqrt{D})$  of the simple continued fraction expansion of  $\sqrt{D}$  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*

$$aX^2 - bY^2 = \pm 1 \quad (9)$$

*has a solution. (Furthermore, if such a solution exists, then  $Q_{\ell/2} = a$  in the simple continued fraction expansion of  $\sqrt{D}$ .)*

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

$$ax^2 - by^2 = \pm 2 \quad (10)$$

*has a solution where  $xy$  is odd. (Furthermore, if such a solution exists, then  $Q_{\ell/2} = 2a$  in the simple continued fraction expansion of  $\sqrt{D}$ .)*

The following is immediate from the above.

**Corollary 1** *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.*

The type of nonsquare  $D$  in which we will be primarily interested for the following section is the content of the next definition.

**Definition 2** Let  $D > 0$  be a nonsquare integer and  $s \in \mathbb{N}$  such that  $D = s^2 + r$  where  $r \mid 4s$ . Then  $D$  is said to be a radicand of Extended Richaud-Degert Type or simply ERD type.

ERD types have been extensively studied and a central source for this information is [5]. We will need the following fact which is easily deduced from [5, Theorem 3.2.1, pp. 78–80].

**Theorem 2** Let  $D = s^2 + r > 6$  be a radicand of ERD type, and let  $\ell = \ell(\sqrt{D})$  be the period length of the simple continued fraction expansion of  $\sqrt{D}$ . Then  $\ell$  is even and  $Q_{\ell/2} = 2$  if and only if  $r = \pm 2$ .

We will also need some elementary number theoretic facts which we present here for the convenience of the reader. These may be found in most introductory number theory texts including the classics, [3], [9], and [11].

**Theorem 3** Let  $c \in \mathbb{Z}$ , with  $c$  odd, and  $\alpha \in \mathbb{N}$ . Then

1. There exists an  $x \in \mathbb{Z}$  such that

$$c \equiv x^2 \pmod{2^\alpha}$$

if and only if  $c \equiv 1 \pmod{g}$  where  $g = \gcd(2^\alpha, 8)$ .

2. If  $p$  is an odd prime, with  $p$  not dividing  $c$ , then there exists an  $x \in \mathbb{Z}$  such that

$$c \equiv x^2 \pmod{p^\alpha}$$

if and only if

$$\left(\frac{c}{p}\right) = 1,$$

where the brackets represent the Legendre symbol.

3. If  $p > 2$  is prime not dividing  $a \in \mathbb{Z}$ , and  $b, c \in \mathbb{Z}$  such that  $p$  does not divide  $b^2 - 4ac$ , then

$$\sum_{x=0}^{p-1} \left(\frac{ax^2 + bx + c}{p}\right) = -\left(\frac{a}{p}\right).$$

4. If  $p > 2$  is prime, then

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 3 \pmod{8}, \\ -1 & \text{if } p \equiv -1, -3 \pmod{8}. \end{cases}$$

*Proof.* These facts can be found in [6, pp. 155–158, 188, 192, and 202], for instance.  $\square$

### 3 Modular Solvability For All $n \in \mathbb{N}$

The following is our main result with the notation of the previous section in force.

**Theorem 4** *Let  $2c = a^2 + r > 6$  be a radicand of ERD type ( $r \mid 4a$ ) with  $|r| \neq 2$ ,  $c \equiv 3 \pmod{8}$ , and  $c$  is divisible only by primes congruent to 1 or 3 modulo 8. Then*

$$2x^2 - cy^2 \equiv -1 \pmod{n} \tag{11}$$

*is solvable for all  $n \in \mathbb{N}$  but*

$$2x^2 - cy^2 = -1 \tag{12}$$

*is not solvable for any integers  $x, y$ .*

*Proof.* Let  $\ell = \ell(\sqrt{2c})$  be the period length of the simple continued fraction expansion of  $\sqrt{2c}$ . First we observe that Equation (12) cannot hold since that would imply that (in the simple continued fraction expansion of  $\sqrt{2c}$ ), the central norm  $Q_{\ell/2} = 2$ , by Theorem 1, which cannot hold by Theorem 2. Note that by equation (8),  $\ell$  must be even since it implies that

$$A_{\ell-1}^2 \equiv (-1)^\ell \pmod{c}$$

and  $c \equiv 3 \pmod{4}$  making that congruence impossible for odd  $\ell$ .

To prove that congruence (11) holds for all  $n \in \mathbb{N}$ , we first observe that  $n = 1$  is the obvious case. To prove the  $n > 1$  case, by the Chinese Remainder Theorem, it suffices to prove that congruence (11) holds for  $n$  a nontrivial prime power.

Now we establish congruence (11) for  $n = 2^\alpha$  where  $\alpha > 0$ . If  $1 \leq \alpha \leq 2$ , then since  $c \equiv 3 \pmod{4}$ ,  $2 \cdot 1^2 - 3 \cdot 1^2 \equiv -1 \pmod{4}$ . When  $\alpha \geq 3$ , then  $c - 2 \equiv 1 \pmod{8}$ , so by part 1 of Theorem 3 there exists a  $z \in \mathbb{Z}$  such that

$z^2 \equiv c - 2 \pmod{2^\alpha}$ . Thus, by setting  $x = y = z^{-1}$ , where  $z^{-1}$  is the least positive multiplicative inverse of  $z$  modulo  $2^\alpha$ , we achieve:

$$2x^2 - cy^2 \equiv -1 \pmod{2^\alpha}.$$

It remains to prove congruence (11) for  $n = p^\alpha$  where  $p > 2$  is prime and  $\alpha > 0$ . We consider two cases.

**Case 1:**  $\left(\frac{-2}{p}\right) = 1$ .

By part 2 of Theorem 3, there exists a  $z \in \mathbb{Z}$  such that  $z^2 \equiv -2 \pmod{p^\alpha}$ . By letting  $j$  be the least positive multiplicative inverse of 2 modulo  $p^\alpha$ , we get:

$$2(jz)^2 - c \cdot 0^2 \equiv -1 \pmod{p^\alpha}.$$

**Case 2:**  $\left(\frac{-2}{p}\right) = -1$ .

By part 4 of Theorem 3,  $p$  cannot divide  $c$  since  $c$  is divisible only by primes congruent to 1 or 3 modulo 8. Hence, we may invoke part 3 of Theorem 3 (take  $a = -c$ ,  $b = 0$ ,  $c = 1$ , and  $x = t$  therein) to get the existence of an integer  $t$  such that

$$\left(\frac{1 - ct^2}{p}\right) = -1.$$

Hence,

$$\left(\frac{2ct^2 - 2}{p}\right) = 1.$$

Therefore, by part 2 of Theorem 3, there exists a  $z \in \mathbb{Z}$  such that

$$z^2 \equiv 2ct^2 - 2 \pmod{p^\alpha}.$$

If we let  $j$  be the least positive multiplicative inverse of 2 modulo  $p^\alpha$ , and set  $x = jz$ ,  $y = t$ , then

$$2x^2 - cy^2 \equiv -1 \pmod{p^\alpha}.$$

By the Chinese Remainder Theorem, we may piece the information together and we have the result for any  $n \in \mathbb{N}$ .  $\square$

Immediate from the above is the following recent result that helped to motivate the findings herein.

**Corollary 2** [Kimura and Williams [2]] *Let  $a > 1$  divisible only by primes congruent to 1 or 3 modulo 8. Then*

$$2x^2 - (2a^4 + a^2)y^2 = -1$$

*has no integer solutions, whereas*

$$2x^2 - (2a^4 + a^2)y^2 \equiv -1 \pmod{n}$$

*has integer solutions for all  $n \in \mathbb{N}$ .*

The following example, cited at the outset, fits quite nicely into our framework (but is missed by the more restrictive scenario given in Corollary 2).

**Example 1** *Let  $c = 219$ , then  $2c = 21^2 - 3 = 2 \cdot 3 \cdot 73$  is of ERD type satisfying the hypothesis of Theorem 4. Hence,  $2x^2 - 219y^2 = -1$  has no integer solutions whereas,  $2x^2 - 219y^2 \equiv -1 \pmod{n}$  has solutions for all  $n \in \mathbb{N}$ .*

The hypothesis that  $c$  must be divisible by only primes congruent to 1 or 3 modulo 8 is necessary since otherwise there are integers for which congruence (11) must fail.

**Example 2** *Let  $c = 105$ . Then  $2c = 14^2 + 14$  which is an ERD type of suitable form, but  $5 \mid c$ , and this ensures that congruence (11) fails for  $p = 5$  since  $2x^2 - 105y^2 \equiv -1 \pmod{5}$  is tantamount to stating that  $\left(\frac{-2}{5}\right) = 1$  which is false by part 4 of Theorem 3.*

The condition in Theorem 4 requiring  $|r| \neq 2$  is the lynchpin of the discussion, in view of Theorem 1, since the solvability of Equation (12) says that  $Q_{\ell/2} = 2$ , and by Theorem 2 this cannot happen unless  $|r| = 2$  for ERD types. The balance of our argument that all other (nontrivial) congruences hold is the particular nature of the ERD type of radicand. These observations seem to have been missed in all earlier work on the subject.

There is a mirror image result when the  $-1$  is replaced by a  $+1$  in congruence (11) and equation (12). We present it and an illustration as a closing feature of this note. We display it without proof since it is verified in an analogous fashion to Theorem 4.

**Theorem 5** *Let  $2c = a^2 + r > 6$  be a radicand of ERD type ( $r \mid 4a$ ) with  $|r| \neq 2$ ,  $c \equiv 1 \pmod{8}$ , and  $c$  is divisible only by primes congruent to 1 or 7 modulo 8, with at least one prime congruent to 7 modulo 8. Then*

$$2x^2 - cy^2 \equiv 1 \pmod{n}$$

*is solvable for all  $n \in \mathbb{N}$ , but  $2x^2 - cy^2 = 1$  is not solvable for any integer  $x, y$ .*

**Example 3** *Let  $c = 2 \cdot 7 \cdot 31 = 434 = 21^2 - 7$  for which  $2x^2 - 217y^2 = 1$  is not solvable. Here  $Q_{\ell/2} = 7 = Q_2$  in the simple continued fraction expansion of  $\sqrt{2c}$ . Yet  $2x^2 - 217y^2 \equiv 1 \pmod{n}$  is solvable for all  $n \in \mathbb{N}$ .*

The methodologies used herein provide significantly simpler tools for investigating such results and are more revealing than those in other sources such as those cited above. For instance, in [11] a “direct proof” (more than a page in length) using elementary number theory is given to show that  $2x^2 - 219y^2 \equiv -1 \pmod{n}$  has solutions for any  $n \in \mathbb{N}$ , but  $2x^2 - 219y^2 = -1$  has no integer solutions. Such facts are now easy consequences of the above continued fraction approach.

**Acknowledgements:** The author’s research is supported by NSERC Canada grant # A8484. Moreover, thanks go to the referee for comments that improved the presentation and readability of the paper.

## References

- [1] G. Chrystal, **Textbook of Algebra** (1889), **II**, reprinted by Chelsea, New York (1964), and reprinted by AMS Chelsea (1999).
- [2] N. Kimura and K.S. Williams, *Infinitely many insolvable Diophantine equations  $f(x_1, x_2) = 0$  such that  $f(x_1, x_2) \equiv 0 \pmod{m}$  is solvable for every  $m$* , to appear: Amer. Math. Monthly.
- [3] W.J. Leveque, **Fundamentals of Number Theory**, Addison-Wesley (1977).

- [4] W. Ljunggren, *Ein Satz über die Diophantische Gleichung  $Ax^2 - By^2 = C$*  ( $C = 1, 4$ ), Tolfte Skand. Matemheirkerkongressen, Lund, 1953, 199–194 (1954).
- [5] R.A. Mollin **Quadratics**, CRC Press, Boca Raton, London, New York, Washington D.C. (1996).
- [6] R.A. Mollin **Fundamental Number Theory with Applications**, CRC Press, Boca Raton, London, New York, Washington D.C. (1998).
- [7] R.A. Mollin, *A continued fraction approach to the Diophantine equation  $ax^2 - by^2 = \pm 1$* , to appear JP Journal of Algebra, Number Theory, and Applications.
- [8] T. Nagell, *On a special class of Diophantine equations of the second degree*, Ark. Mat. **3** (1954), 51–65.
- [9] T. Nagell, **Number Theory**, Almqvist and Wiksell, Stockholm (1951), reprinted by Chelsea, New York (1981).
- [10] O. Perron, *Die Lehre von den Kettenbrüchen*, Bd. **1** Teubner, Leipzig (1954).
- [11] W. Sierpiński, **Elementary Theory of Numbers**, North-Holland (PWN), Amsterdam, New York, Oxford (1988).
- [12] 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](mailto:ramollin@math.ucalgary.ca)