New York Journal of Mathematics

New York J. Math. **11** (2005) 539–545.

# Generalized Lagrange criteria for certain quadratic Diophantine equations

**R.A. Mollin**

Abstract. We consider the Diophantine equation of the form $x^2 - Dy^2 = \pm 4$, where $D$ is a positive integer that is not a perfect square, 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 criterion for the central norm to be 4 associated with principal norm 8 in the simple continued fraction expansion of $\sqrt{D}$.

Contents



## 1. Introduction

In [1], published in 1844, Eisenstein considered the problem of giving necessary and sufficient conditions for the solvability of the Diophantine equation

$$|x^2 - Dy^2| = 4 \text{ where } D \equiv 5 \pmod 8,\ D \in \mathbb{N}, \text{ and } \gcd(x, y) = 1. \tag{1.1}$$

Indeed, considerable work has been done by various authors on this problem. For instance, see [2], [9]–[10].

We know that all solutions of Equation (1.1) can be given in terms of the simple continued fraction expansions of $(1 + \sqrt{D})/2$ (see [4, Theorem 5.3.4, p. 246] for instance). When $D \not\equiv 1 \pmod 4$, $D$ must be even and work has been done in classifying solutions of the equation in terms of the simple continued fraction expansion of $\sqrt{D}$ (see [2] for instance).

In this paper we assume the solvability of $x^2 - Dy^2 = 4$ with $\gcd(x, y) = 1$, where $D$ is a positive integer that is not a perfect square, and link an analogue of

Received January 31, 2005.

*Mathematics Subject Classification.* Primary: 11D09, 11R11, 11A55. Secondary: 11R29.

*Key words and phrases.* Quadratic Diophantine equations, Continued Fractions, Central Norms.

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

ISSN 1076-9803/05

a result of Lagrange obtained in [7] to the simple continued fraction of $\sqrt{D}$. In [7], we looked at the fundamental solution $(x, y) = (x_0, y_0)$ of $x^2 - Dy^2 = 1$ and proved that $x_0 \equiv \pm 1 \pmod{D}$ if and only if the central norm is 2 in the simple continued fraction expansion of $\sqrt{D}$ (see below for definitions). This generalized a celebrated result of Lagrange. In this paper we link the fundamental solution of $x^2 - Dy^2 = 4$, $\gcd(x, y) = 1$, with central norms equal to 4, associated with a principal norm of 8, which is an exact analogue of the generalized Lagrange result.

## 2. Notation and preliminaries

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,

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

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

$$\frac{A_j}{B_j} = \langle q_0; q_1, q_2, \ldots, q_j \rangle,$$

where

$$A_j = q_j A_{j-1} + A_{j-2}, \tag{2.1}$$

$$B_j = q_j B_{j-1} + B_{j-2}, \tag{2.2}$$

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

$$P_{j+1} = q_j Q_j - P_j, \tag{2.3}$$

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

and

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

We will also need the following facts (which can be found in most introductory texts in number theory, such as [4]. Also, see [3] for a more advanced exposition).

$$A_j B_{j-1} - A_{j-1} B_j = (-1)^{j-1}. \tag{2.4}$$

Also,

$$A_{j-1}^2 - B_{j-1}^2 D = (-1)^j Q_j. \tag{2.5}$$

In particular,

$$A_{\ell-1}^2 - B_{\ell-1}^2 D = (-1)^\ell. \tag{2.6}$$

When $\ell$ is even, $P_{\ell/2} = P_{\ell/2+1}$, so by Equation (2.3),

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

where $Q_{\ell/2}$ is called the *central norm*, (via Equation (2.5)), where

$$Q_{\ell/2} \mid 2D. \tag{2.7}$$

In general, the values $Q_j$ are called the *principal norms*, since they are the norms of the principal reduced ideals in the order $\mathbb{Z}[\sqrt{D}]$, due to the association between the simple continued fraction expansion of $\sqrt{D}$ and the infrastructure of the underlying real quadratic order (see [3] for instance).

We will be considering Diophantine equations $x^2 - Dy^2 = 1, 4$. The *fundamental solution* of such an equation means the (unique) least positive integers $(x, y) = (x_0, y_0)$ satisfying it.

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

**Theorem 1** ([6]). *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 $(x, y)$:*

$$|ax^2 - by^2| = 1. \tag{2.8}$$

*Furthermore, in this case, each of the following holds, where $(x, y) = (r, s)$ is the fundamental solution of Equation (2.8):*
(a) $Q_{\ell/2} = a$.
(b) $A_{\ell/2-1} = ra$ *and* $B_{\ell/2-1} = s$.
(c) $A_{\ell-1} = r^2a + s^2b$ *and* $B_{\ell-1} = 2rs$.
(d) $r^2a - s^2b = (-1)^{\ell/2}$.

(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:*

$$|ax^2 - by^2| = 2. \tag{2.9}$$

*Moreover, in this case each of the following holds, where $(x, y) = (r, s)$ is the fundamental solution of Equation (2.9):*
(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) $r^2a - s^2b = 2(-1)^{\ell/2}$.

We will require the following dual results, which are our original generalizations of the results of Lagrange that inspired the work herein. Both are proved in [7].

**Theorem 2.** *If $(x_0, y_0)$ is the fundamental solution of*

$$x^2 - Dy^2 = 1, \tag{2.10}$$

*where $D > 2$ is not a perfect square, then the following are equivalent:*

(1) $x_0 \equiv 1 \pmod{D}$.
(2) *If $\ell = \ell(\sqrt{D})$, then $\ell \equiv 0 \pmod 4$, and $Q_{\ell/2} = 2$.*
(3) *There is a solution to the Diophantine equation*

$$x^2 - Dy^2 = 2. \tag{2.11}$$

**Theorem 3.** *If $(x_0, y_0)$ is the fundamental solution of*

$$x^2 - Dy^2 = 1, \tag{2.12}$$

*where $D > 2$ is not a perfect square, then the following are equivalent:*

(1) $x_0 \equiv -1 \pmod{D}$.

(2) *If* $\ell = \ell(\sqrt{D})$, *then* $\ell \equiv 2 \pmod 4$, *and* $Q_{\ell/2} = 2$.
(3) *There is a solution to the Diophantine equation*

$$x^2 - Dy^2 = -2. \tag{2.13}$$

There is also the following result on central norms that we proved in [8]:

**Theorem 4.** *Suppose that* $D = 4^d c$, *where* $c$ *is not a perfect square,* $c$ *is odd,* $d \geq 1$, $\ell = \ell(\sqrt{D})$, *and* $\ell' = \ell(\sqrt{c})$. *If* $\ell$ *is even, then* $Q_{\ell/2} = 4^d$ *if and only if*

$$\frac{A_{\ell/2-1}}{2^d} + B_{\ell/2-1}\sqrt{c} = A_{\ell'-1} + B_{\ell'-1}\sqrt{c}, \tag{2.14}$$

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

Lastly, we will require the following in the next section.

**Theorem 5.** *Let* $D > 1$ *be an integer that is not a perfect square and suppose that* $\ell = \ell(\sqrt{D})$ *is even. Then each of the following holds:*

$$Q_{\ell/2}A_{\ell-1} = A^2_{\ell/2-1} + B^2_{\ell/2-1}D, \tag{2.15}$$

$$Q_{\ell/2}B_{\ell-1} = 2A_{\ell/2-1}B_{\ell/2-1}. \tag{2.16}$$

**Proof.** This is a consequence of [5, Lemma 3.3, p. 323]. □

## 3. Central norms 4 associated with norm 8

The following is the analogue of Theorems 2–3, and provides a criterion for the central norm to be 4, associated with norm 8, in the process.

**Theorem 6.** *Let* $D > 16$ *be an integer that is not a perfect square, and let* $\ell = \ell(\sqrt{D})$. *Also, assume that* $(x_0, y_0)$ *is the fundamental solution of*

$$x^2 - Dy^2 = 4 \text{ with } \gcd(x,y) = 1. \tag{3.1}$$

*Then the following are equivalent:*

(1) $x_0 \equiv \pm 2 \pmod{D/2}$.
(2) $\ell \equiv 0 \pmod 4$, $Q_{\ell/2} = 4$, *and the there is a solution to the Diophantine equation*

$$X^2 - DY^2 = \pm 8 \text{ with } \gcd(X,Y) = 1, \tag{3.2}$$

*where the* $\pm$ *signs correspond to those in part* (1).

**Proof.** First we assume that part (1) holds. If $x_0/2 \equiv -1 \pmod{D/4}$, then by Theorem 3, $\ell' = \ell(\sqrt{D/4}) \equiv 2 \pmod 4$, $Q_{\ell'/2} = 2$ and there is a solution to the equation

$$X^2 - DY^2/4 = -2. \tag{3.3}$$

Hence, $D/4$ is odd, since otherwise the solvability of Equation (3.1) would imply that $D/4 \equiv 0 \pmod 8$, which contradicts the solvability of Equation (3.3). Moreover, if $x_0/2$ is even, then $4(x_0/4)^2 - y_0^2 D/4 = 1$, so part (1) of Theorem 1 tells us that $Q_{\ell/2} = 4$; or $x_0/2$ is odd and $2(x_0/2)^2 - y_0^2 D/2 = 2$ and part (2) of Theorem 1 tells us that $Q_{\ell/2} = 4$. Therefore, we may invoke Theorem 1 to conclude that

$$\ell \equiv 2\ell' \equiv 0 \pmod 4.$$

Since $D \equiv 4 \pmod 8$, Theorem 4 allows us to conclude that

$$\frac{A_{\ell/2-1}}{2} + B_{\ell/2-1}\sqrt{D/4} = A_{\ell'-1} + B_{\ell'-1}\sqrt{D/4},$$

and Theorem 5 also tells us that

$$A_{\ell'-1} + B_{\ell'-1}\sqrt{D/4} = \frac{\left(A_{\ell'/2-1} + B_{\ell'/2-1}\sqrt{D/4}\right)^2}{2},$$

so we have,

$$A_{\ell/2-1} + B_{\ell/2-1}\sqrt{D} = \left(A_{\ell'/2-1} + B_{\ell'/2-1}\sqrt{D/4}\right)^2.$$

It follows that

$$\left(A_{\ell'/2-1} + B_{\ell'/2-1}\sqrt{D/4}\right)^3 = X + Y\sqrt{D}$$

is a primitive element with norm $-8$, where

$$X = A^3_{\ell'/2-1} + 3A_{\ell'/2-1}B^2_{\ell'/2-1}D/4,$$
$$Y = 3A^2_{\ell'/2-1}B_{\ell'/2-1}/2 + B^3_{\ell'/2-1}D/8,$$

which are both integers since $A_{\ell'/2-1}B_{\ell'/2-1}$ is odd. This completes the case where $x_0 \equiv -2 \pmod{D/4}$. If $x_0 \equiv 2 \pmod{D/4}$, then we may invoke Theorem 2 to argue in a similar fashion to the above. Thus, we have shown that part (1) implies part (2).

Assume part (2) holds. Then the solvability of Equation (3.2) implies that $D$ is even and implies the solvability of the $(X/2)^2 - Y^2D/4 = \pm 2$. Then using the solvability of Equation (3.1), we may invoke Theorems 2 and 3 to get that $x_0/2 \equiv \pm 1 \pmod{D/4}$, which secures the result. □

**Example 1.** If $D = 4 \cdot 19 = 76$, then $\ell = 12$, $Q_{\ell/2} = 4$, $Q_{\ell/4} = Q_3 = 8$, $x_0 = 340 = A_{\ell/2-1} \equiv -2 \pmod{D/2}$, and the fundamental solution of $X^2 - DY^2 = -8$ is $(A_2, B_2) = (26, 3)$.

If $D = 4 \cdot 127$, then $\ell = 32$, $Q_{\ell/2} = 4$, $Q_6 = 8$, $A_{\ell/2-1} = A_{15} = x_0 = 9461248 \equiv 2 \pmod{D/2}$, and the fundamental solution of $X^2 - DY^2 = 8$ is $(A_5, B_5) = (4350, 193)$.

**Remark 1.** Note that when $D > 256$, the solution of Equation (3.2) means that $Q_j = 8$ for some $j$ in the simple continued fraction expansion of $\sqrt{D}$, where $j$ is odd when there is a minus sign and $j$ is even when there is a plus sign. This may be seen using results from [3], for instance, where the continued fraction algorithm may be employed — see [3, Theorem 2.1.2, p. 44]. The latter tells us that all norms of principal (reduced) ideals in $\mathbb{Z}[\sqrt{D}]$ must appear as one of the $Q_j$. The existence of the primitive element of norm $-8$ implies the existence of a primitive reduced ideal of norm 8. The "reduced" part merely means (in this case), that $8 < \sqrt{D}/2$, namely $D > 256$. When $D < 256$ we still have the solvability of the equation but $Q_j$ does not necessarily equal 8 for any $j$. For instance, if $D = 28$, then $\ell = 4$, $Q_{\ell/4} = 4$, but $Q_j \neq 8$ for any $j$. Moreover, $(X, Y) = (90, 17)$ is the solution of the equation. Also, the solvability of Equation (3.2) cannot be removed from condition (2) of Theorem 6. For instance, if $D = 320$, $Q_{\ell/2} = Q_2 = 4$, but $x_0 = 18 \not\equiv \pm 2 \pmod{D/2}$. This tells us that this is a criterion, not merely for central norm 4, rather as asserted in the header for the section, a criterion for central norm 4 associated with norm 8.

**Remark 2.** It is not a difficult task to show that the solvability of Equation (3.1), means that $x_0 \equiv \pm 2 \pmod{D}$ is not possible for odd $D$, which must in the case of that solvability, be congruent to 5 modulo 8. In other words, there is no analogue of Theorem 6 in the order $\mathbb{Z}[(1+\sqrt{D})/2]$ , nor in the order $\mathbb{Z}[\sqrt{D}]$ for odd $D$. Theorems 2–3 provide the desired generalization of Lagrange to orders wherein $D$ may be odd. The result by Lagrange is that for a prime $D = p > 2$, with $(x_0, y_0)$ the fundamental solution of the Pell Equation $x^2 - Dy^2 = 1$, then $x_0 \equiv 1 \pmod{p}$ if and only if $p \equiv 7 \pmod{8}$. Theorems 2–3 deliver the palatable fact that when $\ell(\sqrt{D})$ is even, then $x_0 \equiv \pm 1 \pmod{D}$ if and only if $Q_{\ell/2} = 2$. The following is the analogous fact derived from Theorem 6.

**Theorem 7.** *If $D$ is a positive nonsquare integer, and $(x_0, y_0)$ is the fundamental solution of Equation* (3.1)*, then $x_0 \equiv \pm 2 \pmod{D/2}$ if and only if $Q_{\ell/2} = 4$ and $Q_j = 8$ for some $j$.*

The following is the analogue of another result in [7].

**Theorem 8.** *If $D = 4c$, $c$ is odd, $\ell(\sqrt{D}) = \ell$ is even with $Q_{\ell/2} = 4$, and $Q_j = 8$ for some $j$, then the following hold:*

(1) $c \equiv 3, 7 \pmod{16}$*, if and only if $j$ is even.*
(2) $c \equiv 11, 15 \pmod{16}$ *if and only if $j$ is odd.*

**Proof.** First, we observe that it is a consequence of the results in [7] and in this paper that the only odd primes that may divide $D$ in Theorem 6 are *only* those of the form $p \equiv \pm 1 \pmod{8}$ or *only* those of the form $p \equiv 1, 3 \pmod{8}$, and $D/4 \not\equiv 1 \pmod{4}$.

Since $A_{j-1}^2 - DB_{j-1}^2 = (-1)^j 8$, the following Jacobi symbol identity holds where $D/4 = c$:

$$1 = \left(\frac{A_{j-1}^2}{c}\right) = \left(\frac{(-1)^j 8}{c}\right) = \left(\frac{(-1)^j}{c}\right)\left(\frac{2}{c}\right) = (-1)^{(4j(c-1)+c^2-1)/8},$$

from which one easily deduces the results. □

## References


[1] G. Eisenstein, *Aufgaben*, J. Reine Angew. Math. **27** (1844), 86–88, ERAM 027.0784cj.

[2] 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, MR0845899 (87g:11035), Zbl 0596.10013.

[3] R.A. Mollin, **Quadratics**, CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, 1996, MR1383823 (97e:11135), Zbl 0858.11001.

[4] R.A. Mollin, *Fundamental number theory with applications*, CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, 1998, Zbl 0943.11001.

[5] R.A. Mollin, *Polynomials of Pellian type and continued fractions*, Serdica Math. J. **27** (2001), 317–342, MR1899042 (2003c:11139).

[6] R.A. Mollin, *A continued fraction approach to the Diophantine equation $ax^2 - by^2 = \pm 1$*, JP Journal Algebra, Number Theory, and Appl. **4** (2004), 159–207, MR2049695 (2005a:11031), Zbl 1056.11017.

[7] R.A. Mollin, *Lagrange, central norms, and quadratic Diophantine equations*, International J. Math. and Math. Sci. **7** (2005), 1039–1047.

[8] R.A. Mollin, *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 nonsquare* $D > 1$, Canadian Math. Bulletin **48** (2005), 121–132, MR2118769 (2005i:11013).

[9] A.J. Stephens and H.C. Williams, *Some computational results on a problem of Eisenstein*, Théorie des nombres (Quebec, PQ, 1987) (J-M De Koninck and C. Levesque, eds.), Walter de Gruyter, Berlin, New York (1989), 869–886, MR1024611 (91c:11066), Zbl 0689.10024.

[10] H.C. Williams, *Eisenstein's problem and continued fractions*, Utilitas Math. **37** (1990), 145–158, MR1068514 (91h:11018), Zbl 0718.11010.

Department of Mathematics and Statistics, University of Calgary, Calgary, Alberta, T2N 1N4, Canada
ramollin@math.ucalgary.ca http://www.math.ucalgary.ca/~ramollin/

This paper is available via http://nyjm.albany.edu:8000/j/2005/11-25.html.