Acta Math. Univ. Comenianae
Vol. LXXIV, 2(2005), pp. 273–278

NORM FORM EQUATIONS AND CONTINUED FRACTIONS

R. A. MOLLIN

ABSTRACT. We consider the Diophantine equation of the form $x^2 - Dy^2 = c$, where $c \mid 2D$, $\gcd(x, y) = 1$, and provide criteria for solutions in terms of congruence conditions on the fundamental solution of the Pell Equation $x^2 - Dy^2 = 1$. The proofs are elementary, using only basic properties of simple continued fractions. The results generalize various criteria for such solutions, and expose the central norm, defined by the infrastructure of the underlying real quadratic field, as the foundational key that binds all the elements.

1. Introduction

It is a basic fact that the fundamental unit $x_0 + y_0\sqrt{D}$, of a real quadratic order $\mathbb{Z}[\sqrt{D}]$ is given by certain penultimate values in the principal period of the simple continued fraction expansion of $\sqrt{D}$ (see Equation 8 below). Congruence conditions on x_0, to determine congruence conditions on the underlying radicand D, were known to Lagrange in the case where D is prime (see Corollary 2 below). We expand these notions to a much more general scenario where the central norm (see Equation (9) below), is shown to play the main role in Lagrange's result, our more general result, and in the solution of certain quadratic Diophantine equations. This includes criteria for $x_0 \equiv \pm 1$ in terms of fixed values of the central norm.

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

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

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.

Received June 21, 2004.
2000 *Mathematics Subject Classification.* Primary 11D09, 11R11, 11A55; Secondary 11R29.
Key words and phrases. Quadratic Diophantine equations, continued fractions, central norms, fundamental unit.

The jth *convergent* of α for $j \geq 0$ are given by

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

where

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

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

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 $j \geq 1$,

$$P_{j+1} = q_j Q_j - P_j, \tag{3}$$

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

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 [**3**]. Also, see [**2**] for a more advanced exposition).

$$A_j B_{j-1} - A_{j-1} B_j = (-1)^{j-1}. \tag{4}$$

Also,

$$A_{j-1} = P_j B_{j-1} + Q_j B_{j-2}, \tag{5}$$

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

and

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

In particular,

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

and it follows that $(x_0, y_0) = (A_{\ell-1}, B_{\ell-1})$ is the fundamental solution of the Pell Equation $x^2 - Dy^2 = (-1)^\ell$.

When ℓ is even, $P_{\ell/2} = P_{\ell/2+1}$, so by Equation (3),

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

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

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

and

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

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. *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).*

$$ax^2 - by^2 = \pm 1. \tag{11}$$

Furthermore, in this case, each of the following holds, where $(x, y) = (r, s)$ is the fundamental solution of Equation (11).
   (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 $1 \leq a < b$ such that the following equation has an integral solution (x, y) with xy odd.*

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

Moreover, in this case each of the following holds, where $(x, y) = (r, s)$ is the fundamental solution of Equation (12).
   (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) $r^2a - s^2b = 2(-1)^{\ell/2}$.

Proof. All of this is proved in [**4**]. □

3. Norm Form Diophantine Equations

Theorem 2. *Let D be a positive integer, not a perfect square, with $\ell = \ell(\sqrt{D})$, and let c be an integer such that $|c|$ is a prime divisor of $2D$ and $D > |c|^2$. Then the following are equivalent.*

1. *The Diophantine equation,*

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

has a solution.
2. *ℓ is even, then $c = (-1)^{\ell/2}Q_{\ell/2}$, in which case $(A_{\ell/2-1}, B_{\ell/2-1})$ is the fundamental solution of Equation (13).*
3. *ℓ is even and $A_{\ell-1} \equiv (-1)^{\ell/2} (\bmod\ 2D/|c|)$.*
4. *ℓ is even, $(-1)^{\ell/2}Q_{\ell/2} = c$,*

$$(-1)^{\ell/2}cq_{\ell/2} = 2P_{\ell/2}, \tag{14}$$

$$A_{\ell/2-1} = (-1)^{\ell/2}c(B_{\ell/2} + B_{\ell/2-2})/2, \tag{15}$$

and

$$DB_{\ell/2-1} = (-1)^{\ell/2}c(A_{\ell/2} + A_{\ell/2-2})/2. \tag{16}$$

Proof. If Equation (13) has a solution, then $|c|(x/|c|)^2 - Dy^2/|c| = \pm 1$, with $D/|c| > |c| > 1$, so by part 1 of Theorem 1, ℓ is even and

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

Therefore, part 1 implies part 2. Now assume that part 2 holds.

If $(-1)^{\ell/2}Q_{\ell/2} = c$, then by part 1 of Theorem 1,

$$|c|A_{\ell-1} \equiv A_{\ell/2-1}^2 + B_{\ell/2-1}^2 D \equiv c + 2B_{\ell/2-1}^2 D \equiv c \pmod{2D},$$

so $A_{\ell-1} \equiv (-1)^{\ell/2} \pmod{2D/|c|}$. We have shown that part 2 implies part 3. Now assume that part 3 holds.

Since ℓ is even, we may invoke Theorem 1. If part 1 of that theorem holds, then $D = ab$ with $1 < a < b$, $Q_{\ell/2} = a$,

$$(-1)^{\ell/2} \equiv A_{\ell-1} \equiv r^2 a + s^2 b \equiv 2s^2 b + (-1)^{\ell/2} \pmod{2D/|c|}.$$

It follows that $a \mid s^2|c|$. However, by Equation (4),

$$\gcd(ra, s) = \gcd(A_{\ell/2-1}, B_{\ell/2-1}) = 1,$$

so $a \mid |c|$. Thus, $Q_{\ell/2} = a = |c|$. If part 2 of Theorem1 holds, then a similar argument yields that $Q_{\ell/2} = |c|$, namely that $(-1)^{\ell/2}Q_{\ell/2} = c$. Therefore, Equation (10) implies that Equation (14) holds. Next, we show that Equation (15) holds.

By Equations (5) and (14),

$$A_{\ell/2-1} = P_{\ell/2}B_{\ell/2-1} + Q_{\ell/2}B_{\ell/2-2} = (-1)^{\ell/2}cq_{\ell/2}B_{\ell/2-1}/2 + (-1)^{\ell/2}cB_{\ell/2-2} =$$
$$(-1)^{\ell/2}c(q_{\ell/2}B_{\ell/2-1} + 2B_{\ell/2-2})/2 = (-1)^{\ell/2}c(B_{\ell/2} + B_{\ell/2-2}),$$

where the last equality follows from Equation (2).

To complete the establishment of part 4, we now prove that Equation (16) holds. By Equations (6) and (14),

$$\begin{aligned} 2DB_{\ell/2-1} &= 2P_{\ell/2}A_{\ell/2-1} + 2Q_{\ell/2}A_{\ell/2-2} = q_{\ell/2}(-1)^{\ell/2}cA_{\ell/2-1} + 2(-1)^{\ell/2}cA_{\ell/2-2} \\ &= (-1)^{\ell/2}c(q_{\ell/2}A_{\ell/2-1} + 2A_{\ell/2-2}) = (-1)^{\ell/2}c(A_{\ell/2} + A_{\ell/2-2}), \end{aligned}$$

where the last equality follows from Equation (1). It remains to complete the circle of equivalences by showing that part 4 implies part 1. However, this is immediate from Equation (7), where $(x, y) = (A_{\ell/2-1}, B_{\ell/2-1})$. $\square$

Remark 1. Theorem 2 completely generalizes [**1**, Theorem p. 183], wherein only $c = \pm 2$ is considered. Moreover, they miss the importance of the central norm which we now illustate and highlight as concluding features of this note.

Example 1. Let $D = 2337 = 3 \cdot 19 \cdot 41$, for which $\ell = 18$, $Q_{\ell/2} = 41$, $c = -41$,

$$A_{\ell-1} = 672604673 \equiv 113 \equiv -1 \equiv (-1)^{\ell/2} \pmod{2D/|c|},$$

$$A_{\ell/2-1}^2 - B_{\ell/2-1}^2 D = 117424^2 - 2429^2 D = -c = (-1)^{\ell/2}Q_{\ell/2} = -41,$$

$q_{\ell/2} = 2$, $P_{\ell/2} = 41 = (-1)^{\ell/2}c = Q_{\ell/2}$,

$$A_{\ell/2-1} = 117424 = 41(5293 + 435)/2 = (-1)^{\ell/2}c(B_{\ell/2} + B_{\ell/2-2})/2,$$

and

$$DB_{\ell/2-1} = 5676573 = 41(255877 + 21029)/2 = (-1)^{\ell/2} c(A_{\ell/2} + A_{\ell/2-2})/2.$$

Example 2. Let $D = 4715 = 5 \cdot 23 \cdot 41$, where $\ell = 4$, $Q_{\ell/2} = c = 46$,

$$A_{\ell-1} = 206 \equiv (-1)^{\ell/2} \pmod{2D/c},$$

$$A^2_{\ell/2-1} - B^2_{\ell/2-1} D = 69^2 - 4715 = 46 = c = (-1)^{\ell/2} Q_{\ell/2},$$

$q_{\ell/2} = 1$, $(-1)^{\ell/2} cq_{\ell/2} = 46 = 2P_{\ell/2}$,

$$A_{\ell/2-1} = 69 = 46(2+1)/2 = (-1)^{\ell/2} c(B_{\ell/2} + B_{\ell/2-2})/2,$$

and

$$DB_{\ell/2-1} = 4715 = 46(137 + 68)/2 = (-1)^{\ell/2}(A_{\ell/2} + A_{\ell/2-2})/2.$$

A key consequence of Theorem 2 involves condition 3. When $|c| = 2$, the result boils down to a rather pleasant criterion for the central norm to be 2, in terms of congruence conditions on the fundamental solution of the Pell Equation.

Corollary 1. *If D is a positive nonsquare integer and $\ell = \ell(\sqrt{D})$ is even, then $A_{\ell-1} \equiv (-1)^{\ell/2} (\mathrm{mod}\ D)$ if and only if $Q_{\ell/2} = 2$.*

Proof. If $Q_{\ell/2} = 2$, then by Theorem 1, either Equation (11) holds with $a = 2$ or Equation (12) holds with $a = 1$. In the former case, D is even so Equation (13) holds with $c = \pm 2$, and in the latter case, D is odd so Equation (13) holds with $c = \pm 2$. By Theorem 2, in either case, $A_{\ell-1} \equiv (-1)^{\ell/2} (\mathrm{mod}\ D/2)$. Conversely, if $A_{\ell-1} \equiv (-1)^{\ell/2} (\mathrm{mod}\ D)$, then by Theorem 2, $Q_{\ell/2} = 2$. □

The following celebrated result of Lagrange is shown to essentially be a central norm 2 issue.

Corollary 2 (Lagrange)**.** *If $p > 2$ is prime and (x_0, y_0) is the fundamental solution of $x^2 - py^2 = 1$, then $x_0 \equiv 1 (\mathrm{mod}\ p)$ if and only if $p \equiv 7 (\mathrm{mod}\ 8)$.*

Proof. If $x_0 \equiv 1 \pmod{p}$ and $\ell = \ell(\sqrt{p})$ is odd, then by Equation (8), $A^2_{\ell-1} \equiv -1 (\mathrm{mod}\ p)$, and $x_0 = A_{2\ell-1} = A^2_{\ell-1} + B^2_{\ell-1} p \equiv -1 (\mathrm{mod}\ p)$, a contradiction. Thus, ℓ is even, and $x_0 = A_{\ell-1}$. Thus, by Theorem 1, the only possibility is part 2 which tells us that $Q_{\ell/2} = 2$, and Theorem 2 tells us that $\ell/2$ even, so the following Legendre symbol equalities hold.

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

which implies by elementary number theory (see [**3**, Corollary 4.1.6, p. 192], for instance), $p \equiv \pm 1 (\mathrm{mod}\ 8)$. However, $p \equiv 1 (\mathrm{mod}\ 8)$ is precluded by the fact that $x^2 - py^2 = 2$, via Equation (13).

Conversely, if $p \equiv 7 (\mathrm{mod}\ 8)$, ℓ is even by Equation (8). Thus, by Theorem 1, $Q_{\ell/2} = 2$, and by a simple Legendre symbol argument as above, $\ell/2$ is even. Thus, by Theorem 2, $x_0 \equiv 1 (\mathrm{mod}\ p)$. □

Remark 2. A consequence of the proof of Corollary 2 is that $x_0 \equiv 1 \pmod p$ if and only if $p \equiv 7 \pmod 8$ if and only if $\ell \equiv 0 \pmod 4$ and $Q_{\ell/2} = 2$. Central norm 2 plays an important part in such results, not previously highlighted in the literature.

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

References

1. Lin Q. and Ono T., *On two questions of Ono*, Proc. Japan Acad. **78**, Ser. A (2002), 181–184.
2. Mollin R. A. *Quadratics*, CRC Press, Boca Raton, London, New York, Washington D.C. (1996).
3. ———, *Fundamental Number Theory with Applications*, CRC Press, Boca Raton, London, New York, Washington D.C. (1998).
4. ———, *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.

R. A. Mollin, Department of Mathematics and Statistics,University of Calgary, Calgary, Alberta, Canada, T2N 1N4, *e-mail*: `ramollin@math.ucalgary.ca`