On Finding the Solutions of $n = au^2 + buv + cv^2$ in Integers u and v

Kenneth S. Williams*
Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario CANADA K1S 5B6

ABSTRACT. It is shown how to determine all the proper representations of a positive integer by a given integral, primitive, positive-definite, binary quadratic form of discriminant $-\Delta$. The method requires finding the representations of certain positive integers, which are bounded independently of n, by the principal form of discriminant $-\Delta$.

Let $aX^2+bXY+cY^2$ be an integral, primitive, positive-definite, binary quadratic form, so that a, b, c are integers such that

$$GCD(a,b,c) = 1,\ a > 0, c > 0, b^2 - 4ac < 0. \tag{1}$$

It is convenient to set

$$\Delta = 4ac - b^2, \text{ so that } \Delta \geq 3, \Delta \equiv 0 \text{ or } 3 \pmod 4, \tag{2}$$

$$d = \begin{cases} 0, & \text{if } \Delta \equiv 0 \pmod 4, \\ 1, & \text{if } \Delta \equiv 3 \pmod 4, \end{cases} \tag{3}$$

$$e = \begin{cases} \Delta/4, & \text{if } \Delta \equiv 0 \pmod 4, \\ (\Delta+1)/4, & \text{if } \Delta \equiv 3 \pmod 4, \end{cases} \tag{4}$$

$$f = (b-d)/2 = \begin{cases} b/2, & \text{if } \Delta \equiv 0 \pmod 4, \\ (b-1)/2, & \text{if } \Delta \equiv 3 \pmod 4. \end{cases} \tag{5}$$

*Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.

The form $aX^2 + bXY + cY^2$ has discriminant $b^2 - 4ac = -\Delta$. The principal form of discriminant $-\Delta$ is

$$x^2 + dxy + ey^2 = \begin{cases} x^2 + (\Delta/4)y^2, & \text{if } \Delta \equiv 0 \pmod 4, \\ x^2 + xy + ((\Delta+1)/4)y^2, & \text{if } \Delta \equiv 3 \pmod 4. \end{cases}$$

Let n be an integer ≥ 2. We are interested in determining the integral solutions (u, v) (if any) of

$$\begin{cases} n = au^2 + buv + cv^2, \\ GCD(u, v) = GCD(u, n) = GCD(v, n) = 1. \end{cases} \tag{6}$$

In this paper we show how the integral solutions of (6) can be determined from the integral solutions (x, y) of a finite number of equations

$$Q_1 = x^2 + dxy + ey^2, \tag{7}$$

where each positive integer Q_1 is bounded independently of n. It is shown in the Theorem below that each Q_1 satisfies the inequality

$$Q_1 \leq \max\left(\frac{4ac}{\Delta} + |b| + \frac{\Delta}{4}, \frac{4ac}{\Delta} + |b|\sqrt{\frac{2c}{\Delta}} + \frac{c}{2}\right). \tag{8}$$

In view of (8), when n is large in comparison with a, b, c, solving (7) is much easier than solving (6). The algorithm of [1] (see also [3]) suitably modified can be used to solve (7). Thus we have a procedure for solving (6). Before giving this procedure, we note that if (u, v) is a solution of (6) then

$$u \neq 0, \quad v \neq 0. \tag{9}$$

Moreover the inverse v^{-1} of v modulo n exists and the integer z given by

$$uv^{-1} \equiv z \pmod n, \ 0 \leq z < n, \tag{10}$$

is a solution of

$$\begin{cases} az^2 + bz + c \equiv 0 \pmod n, \\ 0 < z < n, GCD(z, n) = 1. \end{cases} \tag{11}$$

The number of integers Q_1 is just the number of solutions z of (11).

Procedure: This procedure determines all integral solutions (u, v) (if any) of (6).

Step 1. Determine all solutions z of (11). Then carry out Steps 2-5 for each z.

Step 2. Apply the Euclidean algorithm to z and n (begin by dividing z by n) to obtain quotients $\{q_i\}_{i\geq 0}$ and remainders $\{r_i\}_{i\geq 0}$, as well as the denominators $\{B_i\}_{i\geq 0}$ of the convergents to z/n. Stop at the first remainder $r_k (k \geq 0)$ which is less than or equal to $\sqrt{4cn/\Delta}$. Set

$$Q = ar_k^2 + br_k(-1)^k B_k + cB_k^2, \; Q_1 = Q/n. \tag{12}$$

Then Q_1 is a positive integer satisfying the inequality

$$Q_1 \leq M, \tag{13}$$

where

$$M = M(a,b,c) = \max\left(\frac{4ac}{\Delta} + |b| + \frac{\Delta}{4}, \frac{4ac}{\Delta} + |b|\sqrt{\frac{2c}{\Delta}} + \frac{c}{2}\right). \tag{14}$$

Step 3. Determine the solutions (x, y) of

$$x^2 + dxy + ey^2 = Q_1. \tag{15}$$

For *small* Q_1 this can be done by direct search. For *larger* values of Q_1 (remember $Q_1 \leq M$) this can be done, for example, by applying the algorithm of [1] (with minor adjustments if $GCD(\Delta, Q_1) > 1$) to

$$\begin{cases} X^2 + (\Delta/4)Y^2 = Q_1/K^2, (X,Y) = 1, & \text{if } \Delta \equiv 0 \pmod 4, \\ X^2 + \Delta Y^2 = 4Q_1/K^2, (X,Y) = 1, & \text{if } \Delta \equiv 3 \pmod 4, \end{cases}$$

for each positive integer K whose square divides Q_1, if $\Delta \equiv 0 \pmod 4$, $4Q_1$, if $\Delta \equiv 3 \pmod 4$. The required solutions are

$$(x,y) = \begin{cases} (KX, KY), & \text{if } \Delta \equiv 0 \pmod 4, \\ (K(X-Y)/2, KY), & \text{if } \Delta \equiv 3 \pmod 4. \end{cases}$$

Step 4. Set

$$L_1 = fr_k + c(-1)^k B_k, \tag{16}$$

$$L_2 = ar_k + (d+f)(-1)^k B_k. \tag{17}$$

If $\Delta = 3$ or 4 define in addition

$$L_3 = fL_1 - cL_2 = (f^2 - ac)r_k - cd(-1)^k B_k. \tag{18}$$

Eliminate all those (x, y) determined in Step 3 which do NOT satisfy the following seven conditions:

$$r_k x - L_1 y > 0, \tag{19}$$

$$r_k x - L_1 y \equiv 0 \pmod{Q_1}, \tag{20}$$

$$(-1)^k B_k x + L_2 y \equiv 0 \pmod{Q_1}, \tag{21}$$

$$\left(\frac{r_k - z(-1)^k B_k}{n}\right) x - \left(\frac{L_1 + zL_2}{n}\right) y \equiv 0 \pmod{Q_1}, \tag{22}$$

$$GCD\left(\frac{r_k x - L_1 y}{Q_1}, \frac{(-1)^k B_k x + L_2 y}{Q_1}\right) = 1, \tag{23}$$

$$GCD\left(\frac{r_k x - L_1 y}{Q_1}, n\right) = 1, \tag{24}$$

$$GCD\left(\frac{(-1)^k B_k x + L_2 y}{Q_1}, n\right) = 1, \tag{25}$$

and the additional condition

$$L_1 x - L_3 y > 0, \text{if } \Delta = 3 \text{ or } 4. \tag{26}$$

Step 5. If no pairs (x, y) remain after the completion of Step 4 there are no solutions (u, v) of (6) satisfying (10).

Otherwise exactly one pair remains and

$$(u, v) = \left(\frac{r_k x - L_1 y}{Q_1}, \frac{(-1)^k B_k x + L_2 y}{Q_1}\right), \tag{27}$$

is a solution of (6) satisfying (10).

Step 6. All the solutions of (6) are given by

$$\begin{cases} \pm(u, v), & \text{if } \Delta > 4, \\ \pm(u, v), \pm(\frac{b}{2}u + cv, -au - \frac{b}{2}v), & \text{if } \Delta = 4, \\ \pm(u, v), \pm(\frac{(b-1)}{2}u + cv, -au - \frac{(b+1)}{2}v), & \\ \quad \pm(\frac{(b+1)}{2}u + cv, -au - \frac{(b-1)}{2}v), & \text{if } \Delta = 3, \end{cases} \tag{28}$$

where (u, v) runs through the solutions determined in Step 5.

Before proving the validity of this procedure, we give three examples.

Example 1. We seek all solutions in integers u and v of

$$\begin{cases} 577 = 3u^2 + 14uv + 17v^2, \\ GCD(u, v) = GCD(u, 577) = GCD(v, 577) = 1. \end{cases} \tag{29}$$

This example was discussed in [2], however, the algorithm developed there gives only some of the solutions of (29).

Here

$$a = 3, b = 14, c = 17, \Delta = 8, d = 0, e = 2,$$
$$f = 7, n = 577, \sqrt{4cn/\Delta} \approx 70.03$$

Step 1. $z_1 = 462, z_2 = 495$.

$z_1 = 462$. Step 2. $k = 2, r_2 = 2, B_2 = 5, Q = 577, Q_1 = 1$.

Step 3. $x^2 + 2y^2 = 1 \Rightarrow (x, y) = (\pm 1, 0)$.

Step 4. $L_1 = 99, L_2 = 41$.

(19) $2x - 99y > 0$ eliminates $(-1, 0)$.

(19)-(25) are satisfied by $(1, 0)$.

Step 5. $(u, v) = (2, 5)$.

$z_2 = 495$. Step 2. $k = 2, r_2 = 3, B_2 = 7, Q = 1154, Q_1 = 2$.

Step 3. $x^2 + 2y^2 = 2 \Rightarrow (x, y) = (0, \pm 1)$.

Step 4. $L_1 = 140, L_2 = 58$.

(19) $3x - 140y > 0$ eliminates $(0, 1)$.

(19)-(25) are satisfied by $(0, -1)$.

Step 5. $(u, v) = (70, -29)$.

Step 6. All solutions of (29) are given by
$\pm(2, 5), \pm(70, -29)$.

Example 2. We seek all solutions in integers u and v of

$$\begin{cases} 18392 = 7u^2 - 6uv + 7v^2, \\ GCD(u, v) = GCD(u, 18392) = GCD(v, 18392) = 1. \end{cases} \tag{30}$$

This example was discussed in [2] where it was solved using the algorithm developed there. (Note that in [2, Example 3] the remainder 5999 is missing for $y = 12393$ and the remainder 7 is missing for $y = 18169$.) Here

$$a = 7, b = -6, c = 7, \Delta = 160, d = 0, e = 40,$$
$$f = -3, n = 18392, \sqrt{4cn/\Delta} \approx 56.7.$$

Step 1. $z_1 = 745, z_2 = 3197, z_3 = 4165, z_4 = 8973,$
$z_5 = 9941, z_6 = 12393, z_7 = 13361, z_8 = 18169.$

$z_1 = 745$ Step 2. $k = 3, r_3 = 46, B_3 = 74, Q = 73568, Q_1 = 4$.

Step 3. $x^2 + 40y^2 = 4 \Rightarrow (x, y) = (\pm 2, 0)$.
Step 4. $L_1 = -656, L_2 = 544$.
(22) $3x - 22y \equiv 0 \pmod 4$ eliminates $(\pm 2, 0)$.

$z_2 = 3197$ Step 2. $k = 3, r_3 = 37, B_3 = 23, Q = 18392, Q_1 = 1$.
Step 3. $x^2 + 40y^2 = 1 \Rightarrow (x, y) = (\pm 1, 0)$.
Step 4. $L_1 = -272, L_2 = 328$.
(19) $37x + 272y > 0$ eliminates $(-1, 0)$.
(19) - (25) are satisfied by $(1, 0)$.
Step 5. $(u, v) = (37, -23)$.

$z_3 = 4165$ Step 2. $k = 4, r_4 = 41, B_4 = 53, Q = 18392, Q_1 = 1$.
Step 3. $x^2 + 40y^2 = 1 \Rightarrow (x, y) = (\pm 1, 0)$.
Step 4. $L_1 = 248, L_2 = 128$.
(19) $41x - 248y > 0$ eliminates $(-1, 0)$.
(19)-(25) are satisfied by $(1, 0)$.
Step 5. $(u, v) = (41, 53)$.

$z_4 = 8973$ Step 2. $k = 2, r_2 = 53, B_2 = 41, Q = 18392, Q_1 = 1$.
Step 3. $x^2 + 40y^2 = 1 \Rightarrow (x, y) = (\pm 1, 0)$.
Step 4. $L_1 = 128, L_2 = 248$.
(19) $53x - 128y > 0$ eliminates $(-1, 0)$.
(19)-(25) are satisfied by $(1, 0)$.
Step 5. $(u, v) = (53, 41)$.

$z_5 = 9941$ Step 2. $k = 5, r_5 = 23, B_5 = 37, Q = 18392, Q_1 = 1$.
Step 3. $x^2 + 40y^2 = 1 \Rightarrow (x, y) = (\pm 1, 0)$.
Step 4. $L_1 = -328, L_2 = 272$.
(19) $23x + 328y > 0$ eliminates $(-1, 0)$.
(19)-(25) are satisfied by $(1, 0)$.
Step 5. $(u, v) = (23, -37)$.

$z_6 = 12393$ Step 2. $k = 4, r_4 = 25, B_4 = 233, Q = 349448, Q_1 = 19$.
Step 3. $x^2 + 40y^2 = 19$ has no solutions.

$z_7 = 13361$ Step 2. $k = 7, r_7 = 1, B_7 = 223, Q = 349448, Q_1 = 19$.
Step 3. $x^2 + 40y^2 = 19$ has no solutions.

$z_8 = 18169$ Step 2. $k = 3, r_3 = 11, B_3 = 165, Q = 202312, Q_1 = 11$.
Step 3. $x^2 + 40y^2 = 11$ has no solutions.

Step 6. All solutions of (30) are given by
$(u, v) = \pm(37, -23), \pm(41, 53), \pm(53, 41),$
$\pm(23, -37)$.

Example 3. We seek all solutions in integers u and v of

$$\begin{cases} 2551 = 373u^2 + 177uv + 21v^2, \\ GCD(u, v) = GCD(u, 2551) = GCD(v, 2551) = 1. \end{cases} \tag{31}$$

This example illustrates the case $\Delta = 3$.

Here

$$a = 373, b = 177, c = 21, \Delta = 3, d = 1, e = 1,$$
$$f = 88, n = 2551, \sqrt{4cn/\Delta} \approx 267.2.$$

Step 1. $z_1 = 1101, z_2 = 1812$.

$z_1 = 1101$

Step 2. $k = 2, r_2 = 54, B_2 = 7, Q = 1155603, Q_1 = 453$.

Step 3. $x^2 + xy + y^2 = 453 \Rightarrow$
$(x, y) = \pm(4, -23), \pm(4, 19), \pm(19, -23), \pm(19, 4),$
$\pm(23, -19), \pm(23, -4)$.

Step 4. $L_1 = 4899, L_2 = 20765, L_3 = -4953$.
(19) $54x - 4899y > 0$ eliminates $(-23, 4), (-23, 19),$
$(-19, 23), (-4, 23), (4, 19), (19, 4)$.
(20) $54x - 4899y \equiv 0 \pmod{453}$ eliminates
$(-19, -4), (4, -23), (23, -19)$.
(26) $4899x + 4953y > 0$ eliminates $(-4, -19), (19, -23)$.
(19)-(26) are satisfied by $(23, -4)$.

Step 5. $(u, v) = (46, -183)$.

$z_2 = 1812$

Step 2. $k = 3, r_3 = 71, B_3 = 7, Q = 1793353, Q_1 = 703$.

Step 3. $x^2 + xy + y^2 = 703 \Rightarrow$
$(x, y) = \pm(1, 26), \pm(1, -27), \pm(6, 23), \pm(6, -29),$
$\pm(23, 6), \pm(23, -29), \pm(26, 1), \pm(26, -27),$
$\pm(27, -1), \pm(27, -26), \pm(29, -6), \pm(29, -23)$.

Step 4. $L_1 = 6101, L_2 = 25860, L_3 = -6172$.
(19) $71x - 6101y > 0$ eliminates $(1, 26), (-1, 27),$
$(6, 23), (-6, 29), (23, 6), (-23, 29), (26, 1), (-26, 27),$
$(-27, 1), (-27, 26), (-29, 6), (-29, 23)$.
(20) $71x - 6101y \equiv 0 \pmod{703}$ eliminates $(-1, -26),$
$(1, -27), (6, -29), (-23, -6), (-26, -1), (26, -27),$
$(27, -1), (27, -26), (29, -23)$.
(26) $6101x + 6172y > 0$ eliminates $(-6, -23), (23, -29)$.
(19)-(26) are satisfied by $(29, -6)$.

Step 5. $(u, v) = (55, -221)$.

Step 6. All solutions of (31) are given by
$\pm(46, -183), \pm(205, -871), \pm(251, -1054),$
$\pm(55, -221), \pm(199, -846), \pm(254, -1067)$.

The validity of the procedure described above is a consequence of the following theorem.

Theorem. *Let a, b, c be integers satisfying (1). Define Δ, d, e, f, M as in (2), (3), (4), (5), (14) respectively. Let n be an integer ≥ 2. Let z be a solution of (11). Apply the Euclidean algorithm to z and n (begin by dividing z by n) to obtain quotients $\{q_i\}_{i\geq 0}$ and remainders $\{r_i\}_{i\geq 0}$, as well as the denominators $\{B_i\}_{i\geq 0}$ of the convergents to z/n. Let $r_k (k \geq 0)$ denote the first remainder which is less than or equal to $\sqrt{4cn/\Delta}$. Define L_1, L_2, L_3, Q, Q_1 as in (16), (17), (18), (12), (12) respectively. Then Q_1 is a positive integer satisfying the inequality (13). Moreover there is at most one pair (x, y) of integers satisfing (15) and (19)-(26). If one such pair (x, y) exists then*

$$(u, v) = \left(\frac{r_k x - L_1 y}{Q_1}, \frac{(-1)^k B_k x + L_2 y}{Q_1} \right) \tag{32}$$

is a solution of (6) satisfying (10), and all solutions of (6) and (10) are given by

$$\begin{cases} \pm(u, v), & \text{if } \Delta > 4, \\ \pm(u, v), \pm(\frac{b}{2}u + cv, -au - \frac{b}{2}v), & \text{if } \Delta = 4, \\ \pm(u, v), \pm\left(\frac{(b-1)}{2}u + cv, -au - \frac{(b+1)}{2}v\right), & \\ \pm\left(\frac{(b+1)}{2}u + cv, -au - \frac{(b-1)}{2}v\right), & \text{if } \Delta = 3. \end{cases} \tag{33}$$

If no such pair exists then there is no solution (u, v) of (6) satisfying (10).

Before giving the proof of this theorem we prove a lemma.

Lemma. *Let a, b, c be integers satisfing (1). Let n be an integer ≥ 2. Let z be a solution of (11). Suppose (u, v) is a solution of (6) for which (10) holds. Then all solutions of (6) satisfying (10) are given by (33). Morever*

if $\Delta > 4$ exactly one of the two solutions in $(33)_1$ satisfies $u > 0$;

if $\Delta = 4$ exactly one of the four solutions in $(33)_2$ satisfies $u > 0$, $\frac{b}{2}u + cv > 0$;

if $\Delta = 3$ exactly one of the six solutions in $(33)_3$ satisfies $u > 0$, $\frac{(b-1)}{2}u + cv > 0$.

Proof: Suppose (u, v) and (u_1, v_1) are two solutions of (6) satisfying (10). We have

$$4n^2 = (2n)(2n) = (2au^2 + 2buv + 2cv^2)(2au_1^2 + 2bu_1v_1 + 2cv_1^2)$$

so that

$$4n^2 = (2auu_1 + buv_1 + bvu_1 + 2cvv_1)^2 + \Delta(vu_1 - uv_1)^2. \tag{34}$$

Now from (10) we have $uv^{-1} \equiv u_1 v_1^{-1} (\equiv z) \pmod{n}$ so that

$$vu_1 - uv_1 \equiv 0 \pmod{n}. \tag{35}$$

Hence, from (34) and (35), we see that there exist integers X and Y such that

$$2auu_1 + buv_1 + bvu_1 + 2cvv_1 = nX, \tag{36}$$

$$vu_1 - uv_1 = nY, \tag{37}$$

$$X^2 + \Delta Y^2 = 4. \tag{38}$$

As $\Delta \geq 3$ we see that the only solutions of (38) are

$$(X, Y) = \begin{cases} \pm(2,0), & \text{if } \Delta > 4, \\ \pm(2,0), \pm(0,1), & \text{if } \Delta = 4, \\ \pm(2,0), \pm(1,1), \pm(1,-1), & \text{if } \Delta = 3. \end{cases} \tag{39}$$

Solving the two linear equations in u_1 and v_1 which result from (36) and (37) with $(X, Y) = \pm(2, 0)$, we obtain

$$(u_1, v_1) = \pm(u, v).$$

Both $\pm(u, v)$ are integral solutions of (6) and (10).

Next, solving the two linear equations for u_1 and v_1 resulting from (36) and (37) with $\Delta = 4$ and $(X, Y) = \pm(0, 1)$, we obtain

$$(u_1, v_1) = \pm\left(\frac{b}{2}u + cv, -au - \frac{b}{2}v\right).$$

A straightforward calculation shows that both $\pm(\frac{b}{2}u + cv, -au - \frac{b}{2}v)$ are integral solutions of (6) and (10).

Further, from (36) and (37) with $\Delta = 3$ and $(X, Y) = \pm(1, 1), \pm(1, -1)$, we obtain

$$(u_1, v_1) = \pm\left(\frac{(b+1)}{2}u + cv, -au - \frac{(b-1)}{2}v\right),$$
$$\mp\left(\frac{(b-1)}{2}u + cv, -au - \frac{(b+1)}{2}v\right).$$

Again a simple calculation shows that these are integral solutions of (6) and (10).

This completes the proof that all integral solutions of (6) and (10) are given by (33).

If $\Delta > 4$, as $u \neq 0$ by (9), we can choose a unique solution (u_1, v_1) of (6) and (10) with $u_1 > 0$ by

$$(u_1, v_1) = \begin{cases} (u, v), & \text{if } u > 0, \\ (-u, -v), & \text{if } u < 0. \end{cases}$$

If $\Delta = 4$, as $u \neq 0$ and $\frac{b}{2}u + cv \neq 0$ by (9), we can choose a unique solution (u_1, v_1) of (6) and (10) with $u_1 > 0$ and $\frac{b}{2}u_1 + cv_1 > 0$ by

$$(u_1, v_1) = \begin{cases} (u, v), & \text{if } u > 0, \frac{b}{2}u + cv > 0, \\ (\frac{b}{2}u + cv, -au - \frac{b}{2}v), & \text{if } u < 0, \frac{b}{2}u + cv > 0, \\ (-\frac{b}{2}u - cv, au + \frac{b}{2}v), & \text{if } u > 0, \frac{b}{2}u + cv < 0, \\ (-u, -v), & \text{if } u < 0, \frac{b}{2}u + cv < 0. \end{cases}$$

If $\Delta = 3$, as $u \neq 0$, $\frac{(b-1)}{2}u + cv \neq 0$ and $\frac{(b+1)}{2}u + cv \neq 0$ by (9), and noting that $u + (\frac{(b-1)}{2}u + cv) = \frac{(b+1)}{2}u + cv$, we can choose a unique solution (u_1, v_1) of (6) and (10) with $u_1 > 0$ and $\frac{(b-1)}{2}u_1 + cv_1 > 0$, by

$$(u_1, v_1) = \begin{cases} (u, v), & \text{if } u > 0, \frac{(b-1)}{2}u + cv > 0, \\ \left(-\frac{(b-1)}{2}u - cv, au + \frac{(b+1)}{2}v\right), & \text{if } u > 0, \frac{(b-1)}{2}u + cv < 0, \\ & \frac{(b+1)}{2}u + cv > 0, \\ \left(-\frac{(b+1)}{2}u - cv, au + \frac{(b-1)}{2}v\right), & \text{if } u > 0, \frac{(b+1)}{2}u + cv < 0, \\ \left(\frac{(b+1)}{2}u + cv, -au - \frac{(b-1)}{2}v\right), & \text{if } u < 0, \frac{(b+1)}{2}u + cv > 0, \\ \left(\frac{(b-1)}{2}u + cv, -au - \frac{(b+1)}{2}v\right), & \text{if } u < 0, \frac{(b-1)}{2}u + cv > 0, \\ & \frac{(b+1)}{2}u + cv < 0, \\ (-u, -v), & \text{if } u < 0, \frac{(b-1)}{2}u + cv < 0. \end{cases}$$

This completes the proof of the Lemma. □

Before proceeding we note two relations which follow easily from (2), (3), (4), (5), (12), (16) and (17):

$$(-2aL_1 + bL_2)r_k + (-bL_1 + 2cL_2)(-1)^k B_k = dQ, \tag{40}$$

$$aL_1^2 - bL_1L_2 + cL_2^2 = eQ. \tag{41}$$

We are now ready to prove the Theorem.

Proof of Theorem: We begin with some preliminaries on continued fractions. Let z be a solution of (11). Applying the Euclidean algorithm to z

and n, we obtain

$$\begin{cases} z = q_0 n + r_0, \\ n = q_1 r_0 + r_1, \\ r_{i-2} = q_i r_{i-1} + r_i (i = 2, \ldots, s), \end{cases} \tag{42}$$

where

$$s \geq 1, \tag{43}$$

$$r_0 (= z) > r_1 > r_2 > \ldots > r_{s-1} (= 1) > r_s (= 0), \tag{44}$$

and

$$\begin{cases} q_0 = [z/n] = 0, & q_1 = [n/r_0] = [n/z] \geq 1, \\ q_i = [r_{i-2}/r_{i-1}] \geq 1, & (i = 2, \ldots, s). \end{cases} \tag{45}$$

The continued fraction for z/n is

$$\frac{z}{n} = [q_0, q_1, q_2, \ldots, q_s]. \tag{46}$$

The ith convergent to z/n is

$$\frac{A_i}{B_i} = [q_0, q_1, q_2, \ldots, q_i] \quad (i = 0, 1, \ldots, s), \tag{47}$$

so that

$$\begin{cases} A_0 = 0, & B_0 = 1, \\ A_1 = 1, & B_1 = q_1, \\ A_2 = q_2, & B_2 = q_1 q_2 + 1, \\ \ldots & \\ A_s = z, & B_s = n, \end{cases} \tag{48}$$

and

$$\begin{cases} A_i = q_i A_{i-1} + A_{i-2} & (i = 2, \ldots, s), \\ B_i = q_i B_{i-1} + B_{i-2} & (i = 2, \ldots, s). \end{cases} \tag{49}$$

An easy induction argument on i shows that

$$r_i B_{i+1} + r_{i+1} B_i = n \quad (i = 0, 1, \ldots, s-1) \tag{50}$$

and

$$r_i = (-1)^i (B_i z - A_i n) \quad (i = 0, 1, \ldots, s), \tag{51}$$

so that

$$r_i \equiv (-1)^i B_i z \pmod{n} \quad (i = 0, 1, \ldots, s). \tag{52}$$

From $(11)_1$ and (52) we obtain

$$ar_i^2 + br_i(-1)^i B_i + cB_i^2 \equiv 0 \pmod{n} \quad (i = 0, 1, \ldots, s). \tag{53}$$

This completes the preliminaries on continued fractions.

Let $r_k (0 \leq k \leq s)$ be the first remainder $\leq \sqrt{4cn/\Delta}$. From (12) and (53) we have

$$Q = ar_k^2 + br_k(-1)^k B_k + cB_k^2 \equiv 0 \pmod{n}$$

so that $Q_1 = Q/n$ is a positive integer. We show that Q_1 satisfies the inequality (13). We consider two cases according as $k = 0$ or $k \geq 1$. If $k = 0$ we have

$$\begin{aligned}
Q_1 &= (ar_0^2 + br_0 B_0 + cB_0^2)/n && \text{(by (12))} \\
&= (ar_0^2 + br_0 + c)/n && \text{(by (48))} \\
&\leq \frac{4ac}{\Delta} + |b|\sqrt{\frac{4c}{\Delta n}} + \frac{c}{n} && (\text{as } 0 \leq r_0 \leq \sqrt{\tfrac{4cn}{\Delta}}) \\
&\leq \frac{4ac}{\Delta} + |b|\sqrt{\frac{2c}{\Delta}} + \frac{c}{2} && (\text{as } n \geq 2) \\
&\leq M. && \text{(by (14))}
\end{aligned}$$

If $k \geq 1$, appealing to (50), we have

$$r_{k-1} B_k + r_k B_{k-1} = n,$$

so that

$$r_{k-1} B_k \leq n.$$

As

$$0 \leq r_k \leq \sqrt{\frac{4cn}{\Delta}} < r_{k-1},$$

we obtain

$$B_k \leq \frac{n}{r_{k-1}} < \sqrt{\frac{\Delta n}{4c}}.$$

Then we have

$$\begin{aligned}
Q_1 &= (ar_k^2 + br_k(-1)^k B_k + cB_k^2)/n && \text{(by (12))} \\
&\leq \frac{4ac}{\Delta} + |b| + \frac{\Delta}{4} && (\text{as } 0 \leq r_k \leq \sqrt{\tfrac{4cn}{\Delta}}, 0 < B_k < \sqrt{\tfrac{\Delta n}{4c}}) \\
&\leq M. && \text{(by (14))}
\end{aligned}$$

This completes the proof of (13).

We now prove that there is at most one pair (x, y) of integers satisfying (15) and (19)-(26). Suppose (x_i, y_i) $(i = 1, 2)$ are two such pairs of integers. Set

$$u_i = \frac{r_k x_i - L_1 y_i}{Q_1},\ v_i = \frac{(-1)^k B_k x_i + L_2 y_i}{Q_1},\ (i = 1, 2). \tag{54}$$

It is clear from (20), (21) and (54) that u_i, v_i $(i = 1, 2)$ are integers. Further, for $i = 1, 2$, we have

$$\begin{aligned} & au_i^2 + bu_i v_i + cv_i^2 \\ & \quad = (a(r_k x_i - L_1 y_i)^2 + b(r_k x_i - L_1 y_i)((-1)^k B_k x_i + L_2 y_i) \\ & \quad + c((-1)^k B_k x_i + L_2 y_i)^2 / Q_1^2 \qquad \text{(by (54))} \\ & \quad = (Qx_i^2 + Qdx_i y_i + Qey_i^2)/(Q/n)^2 \\ & \qquad \text{(by (12),(40),(41))} \\ & \quad = n, \qquad \text{(by (15))} \end{aligned}$$

so that (u_i, v_i) $(i = 1, 2)$ is a solution of $(6)_1$. Clearly from (23), (24), (25) and (54), we have

$$GCD(u_i, v_i) = GCD(u_i, n) = GCD(v_i, n) = 1\ (i = 1, 2)$$

so that (u_i, v_i) $(i = 1, 2)$ satisfies $(6)_2$. Further, from (22) and (54), we see that

$$u_i - zv_i = \frac{(r_k - z(-1)^k B_k)x_i - (L_1 + zL_2)y_i}{Q_1} \equiv 0 \pmod{n}, (i = 1, 2)$$

so that as $GCD(v_i, n) = 1$ we have $u_i v_i^{-1} \equiv z \pmod{n}$, showing that (u_i, v_i) $(i = 1, 2)$ satisfies (10). From (19) and (54) we see that

$$u_1 > 0 (i = 1, 2),\ \text{if } \Delta > 4,$$

and from (16),(18),(19), (26) and (54) we see that

$$u_i > 0,\ fu_i + cv_i > 0\ (i = 1, 2),\ \text{if } \Delta = 3 \text{ or } 4.$$

Hence, by the Lemma, we have

$$u_1 = u_2,\ v_1 = v_2.$$

Then, from (54), we deduce

$$\begin{cases} r_k(x_1 - x_2) - L_1(y_1 - y_2) = 0, \\ (-1)^k B_k(x_1 - x_2) + L_2(y_1 - y_2) = 0. \end{cases} \tag{55}$$

As

$$\begin{vmatrix} r_k & -L_1 \\ (-1)^k B_k & L_2 \end{vmatrix} = r_k L_2 + (-1)^k B_k L_1$$

$$= r_k(ar_k + (d+f)(-1)^k B_k) + (-1)^k B_k(fr_k + c(-1)^k B_k) \quad \text{(by (16),(17))}$$

$$= ar_k^2 + br_k(-1)^k B_k + cB_k^2 \quad \text{(by (5))}$$

$$= Q, \quad \text{(by (12))}$$

we deduce from (55) as $Q \neq 0$ that $x_1 - x_2 = y_1 - y_2 = 0$, so that $(x_1, y_1) = (x_2, y_2)$ as asserted.

It is clear from the above argument that if (x, y) is an integral solution of (15) satisfying (19)-(26) then $(u, v) = (\frac{r_k x - L_1 y}{Q_1}, \frac{(-1)^k B_k x + L_2 y}{Q_1})$ is an integral solution of (6) and (10) for which

$$\begin{cases} u > 0, & \text{if } \Delta > 4, \\ u > 0, fu + cv > 0, & \text{if } \Delta = 3 \text{ or } 4. \end{cases} \tag{56}$$

Hence by the Lemma all solutions of (6) and (10) are given by (33).

If there is no integral solution of (15) satisfying (19)-(26) we show that there is no integral solution of (6) and (10). We do this by proving that if (6) and (10) have an integral solution then there is an integral solution of (15) for which (19)-(26) hold. Let (u, v) be an integral solution of (6) for which (10) holds. By the Lemma (u, v) can be chosen uniquely so that (56) holds. Appealing to (5), (10), $(11)_1$ and (52), we have for $i = 0, 1, \ldots, s$

$$\begin{cases} r_i(au + fv) + (-1)^i B_i((d+f)u + cv) \equiv 0 \pmod{n}, \\ r_i v - (-1)^i B_i u \equiv 0 \pmod{n}. \end{cases} \tag{57}$$

Hence we can define integers c_i and d_i for $i = 0, 1, \ldots, s$, by

$$\begin{cases} c_i = (r_i(au + fv) + (-1)^i B_i((d+f)u + cv))/n, \\ d_i = (r_i v - (-1)^i B_i u)/n. \end{cases} \tag{58}$$

A straightforward calculation making use of (2), (3), (4), (5), $(6)_1$, $(11)_1$ and (58) shows that for $i = 0, 1, \ldots, s$ we have

$$(ar_i^2 + br_i(-1)^i B_i + cB_i^2)/n = c_i^2 + dc_i d_i + ed_i^2. \tag{59}$$

From (5), (58) and (59) we obtain for $i = 0, 1, \ldots, s$

$$\begin{cases} u = \frac{r_i c_i - (fr_i + c(-1)^i B_i) d_i}{c_i^2 + dc_i d_i + ed_i^2}, \\ v = \frac{(-1)^i B_i c_i + (ar_i + (d+f)(-1)^i B_i) d_i}{c_i^2 + dc_i d_i + ed_i^2}. \end{cases} \tag{60}$$

We set

$$x = c_k,\ y = d_k, \tag{61}$$

where the integer k $(0 \leq k \leq s)$ is such that r_k is the first remainder $\leq \sqrt{4cn/\Delta}$. Clearly x and y are integers with $(x, y) \neq (0, 0)$. We show that (x, y) is a solution of (15) satisfying (19)-(26).

First we show that (x, y) satisfies (15). This is clear as

$$\begin{aligned} x^2 + dxy + ey^2 &= c_k^2 + dc_k d_k + ed_k^2 = (ar_k^2 + br_k(-1)^k B_k + cB_k^2)/n \\ &= Q/n = Q_1, \end{aligned}$$

by (61), (59) and (12).

Next we show that (x, y) satisfies (19). We have

$$\begin{aligned} r_k x - L_1 y &= r_k c_k - (fr_k + c(-1)^k B_k) d_k \\ &\qquad\qquad \text{(by (16),(61))} \\ &= u(c_k^2 + dc_k d_k + ed_k^2) \qquad \text{(by } (60)_1\text{)} \\ &> 0, \qquad\qquad \text{(by (56))} \end{aligned}$$

as required.

The congruence (20) holds as

$$\begin{aligned} r_k x - L_1 y &= u(c_k^2 + dc_k d_k + ed_k^2) = u(ar_k^2 + br_k(-1)^k B_k + cB_k^2)/n \\ &= uQ/n = uQ_1, \end{aligned} \tag{62}$$

by (12) and (59).

The congruence (21) holds as

$$\begin{aligned} (-1)^k B_k x + L_2 y &= (-1)^k B_k c_k + (ar_k + (d+f)(-1)^k B_k) d_k \\ &\qquad\qquad \text{(by (17),(61))} \\ &= v(c_k^2 + dc_k d_k + ed_k^2) \qquad \text{(by } (60)_2\text{)} \\ &= v(ar_k^2 + br_k(-1)^k B_k + cB_k^2)/n \\ &\qquad\qquad \text{(by (59))} \\ &= vQ/n, \qquad\qquad \text{(by (12))} \end{aligned}$$

that is

$$(-1)^k B_k x + L_2 y = vQ_1. \tag{63}$$

Next we show that the congruence (22) holds. We first show that $(r_k - z(-1)^k B_k)/n$ and $(L_1 + zL_2)/n$ are integers. We have

$$\begin{aligned} v(r_k - z(-1)^k B_k) &\equiv r_k v - (-1)^k B_k u \pmod{n} \\ &\qquad\qquad \text{(by (10))} \\ &\equiv 0 \pmod{n}, \qquad\qquad \text{(by } (57)_2\text{)} \end{aligned}$$

so that (as $GCD(v,n)=1$) $r_k - z(-1)^k B_k \equiv 0 \pmod{n}$. Also

$$\begin{aligned} v(L_1+zL_2) &\equiv v(fr_k + c(-1)^k B_k) + u(ar_k + (d+f)(-1)^k B_k) \pmod{n} \\ &\qquad \text{(by (10),(16),(17))} \\ &\equiv r_k(au+fv) + (-1)^k B_k((d+f)u+cv) \pmod{n} \\ &\equiv 0 \pmod{n}, \qquad \text{(by } (57)_1\text{)} \end{aligned}$$

so that $L_1 + zL_2 \equiv 0 \pmod{n}$. Then

$$\begin{aligned} (r_k - z(-1)^k B_k)x - (L_1+zL_2)y &= (r_k x - L_1 y) - z((-1)^k B_k x + L_2 y) \\ &= uQ_1 - zvQ_1 \\ &\qquad \text{(by (62),(63))} \\ &= \frac{(u-zv)}{n} Q, \qquad \text{(by (12))} \end{aligned}$$

where $(u-zv)/n$ is an integer by (10) and thus

$$\frac{r_k - z(-1)^k B_k)}{n} x - \frac{(L_1+zL_2)}{n} y = \frac{(u-zv)}{n} Q_1,$$

completing the proof of (22).

The equalities (23), (24) and (25) hold as, by (62), (63) and $(6)_2$, we have

$$\begin{aligned} GCD\left(\frac{r_k x - L_1 y}{Q_1}, \frac{(-1)^k B_k x + L_2 y}{Q_1}\right) &= GCD(u,v) = 1, \\ GCD\left(\frac{r_k x - L_1 y}{Q_1}, n\right) &= GCD(u,n) = 1, \\ GCD\left(\frac{(-1)^k B_k x + L_2 y}{Q_1}, n\right) &= GCD(v,n) = 1. \end{aligned}$$

Finally we show that (x,y) satisfies (26) when $\Delta = 3$ or 4. We have

$$\begin{aligned} L_1 x - L_3 y &= (fr_k + c(-1)^k B_k)c_k - ((f^2-ac)r_k - cd(-1)^k B_k)d_k \\ &\qquad \text{(by (16),(18),(61))} \\ &= f(r_k c_k - (fr_k + c(-1)^k B_k)d_k) + c((-1)^k B_k c_k \\ &\quad + (ar_k + (d+f)(-1)^k B_k)d_k) \\ &= (fu+cv)(c_k^2 + dc_k d_k + ed_k^2) \qquad \text{(by (60))} \\ &> 0. \qquad \text{(by (56))} \end{aligned}$$

This completes the proof of the Theorem. □

We conclude by remarking that the detailed analysis carried out in the proof of the Theorem in [2] shows that if a, b, c satisfy

$$\Delta \geq 16, |b| \leq (\Delta - 16)/8$$

then we must have $(u, v) = (r_k, (-1)^k B_k)$ in (32), that is,

$$\frac{r_k x - L_1 y}{Q_1} = r_k, \frac{(-1)^k B_k x + L_2 y}{Q_1} = (-1)^k B_k.$$

Solving for x and y, we obtain $x = Q_1$, $y = 0$. Then, from (15), we deduce $Q_1^2 = Q_1$ so that $Q_1 = 1$ and $(x, y) = (1, 0)$.

The author would like to thank the referee for valuable comments on the first draft of this paper.

References

[1] K. Hardy, J.B. Muskat, and K.S. Williams, A deterministic algorithm for solving $n = fu^2 + gv^2$ in coprime integers u and v, *Mathematics of Computation* **55** (1990), 327–343.

[2] K. Hardy, J.B. Muskat, and K.S. Williams, Solving $n = au^2 + buv + cv^2$ using the Euclidean algorithm, *Utilitas Mathematica* **38** (1990), 225–236.

[3] J.B. Muskat, A refinement of the Hardy-Muskat-Williams algorithm for solving $n = fu^2 + gv^2$, *Utilitas Mathematica* **41** (1992), 109–117.