New York Journal of Mathematics

New York J. Math. **7** (2001) 87–97.

A Simple Criterion for Solvability of Both $X^2 - DY^2 = c$ and $x^2 - Dy^2 = -c$

R. A. Mollin

Abstract. This article provides a simple criterion for the simultaneous solvability of the Diophantine equations $X^2 - DY^2 = c$ and $x^2 - Dy^2 = -c$ when $c \in \mathbb{Z}$, and $D \in \mathbb{N}$ is not a perfect square.

Contents

1. Introduction

Lagrange used simple continued fractions to solve the Pell equation $x^2 - Dy^2 = -1$ (see [3, Corollary 5.3.3, p. 249] as well as Theorem 2.3 and Corollary 3.1 below). Also, both Gauss and Eisenstein used simple continued fractions to examine the solvability of $x^2 - Dy^2 = -4$ for $\gcd(x, y) = 1$ (see [2, Exercise 2.1.15, p. 60] as well as Lemma 3.1 below). Numerous authors have since employed the continued fraction approach to study quadratic Diophantine equations. For instance, in [8], H.C. Williams gives criteria for the solvability of $|x^2 - Dy^2| = 4$ with $\gcd(x, y) = 1$ in terms of the simple continued fraction expansion of the quadratic irrational $(1 + \sqrt{D})/2$ for field discriminants $D \equiv 5 \bmod 8$. Also, in [1], P. Kaplan and K.S. Williams use continued fractions to give criteria for the solvability of $x^2 - Dy^2 = -1, -4$ in terms of simple continued fractions. In this article, we look at the mutual solvability of the equations in the title using a combination of techniques related to continued fractions. This continues work in [4], [5] and [7].

Received January 28, 2001.

Mathematics Subject Classification. 11A55, 11R11, 11D09.

Key words and phrases. continued fractions, Diophantine equations, fundamental units, simultaneous solutions.

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

ISSN 1076-9803/01

2. Notation and preliminaries

We will be studying solutions of quadratic Diophantine equations of the general shape

$$x^2 - Dy^2 = c, \tag{2.1}$$

where $D > 0$ is not a perfect square and $c \in \mathbb{Z}$. If $x, y \in \mathbb{Z}$ is a solution of (2.1), then it is called *positive* if $x, y \in \mathbb{N}$ and it is called *primitive* if $\gcd(x, y) = 1$. Among the primitive solutions of (2.1), if such solutions exist, there is one in which both x and y have their least values. Such a solution is called a *fundamental solution.* We will use the notation

$$\alpha = x + y\sqrt{D}$$

to denote a solution of (2.1), and we let

$$N(\alpha) = x^2 - Dy^2$$

denote the *norm* of α. (Note that solutions of (2.1) can be broken down into classes where each class has a fundamental solution, so there are often several fundamental solutions — see [3, pp. 298–307]). We will be linking such solutions to simple continued fraction expansions that we now define.

Recall that a *quadratic irrational* is a number of the form

$$(P + \sqrt{D})/Q$$

where $P, Q, D \in \mathbb{Z}$ with $D > 1$ not a perfect square, $P^2 \equiv D \bmod Q$, and $Q \neq 0$. Now we set:

$$P_0 = P,\ Q_0 = Q, \text{ and recursively for } j \geq 0,$$

$$q_j = \left\lfloor \frac{P_j + \sqrt{D}}{Q_j} \right\rfloor, \tag{2.2}$$

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

and

$$D = P_{j+1}^2 + Q_j Q_{j+1}. \tag{2.4}$$

Hence, we have the simple continued fraction expansion:

$$\alpha = \frac{P + \sqrt{D}}{Q} = \frac{P_0 + \sqrt{D}}{Q_0} = \langle q_0; q_1, \ldots, q_j, \ldots \rangle,$$

where the q_j for $j \geq 0$ are called the *partial quotients* of α.

To further develop the link with continued fractions, we make the initial (well known) observation that a real number has a periodic continued fraction expansion if and only if it is a quadratic irrational (see [3, Theorem 5.3.1, p. 240]). Furthermore a quadratic irrational is said to have a *purely* periodic continued fraction expansion if it has the form

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

which means that $q_n = q_{n+\ell}$ or all $n \geq 0$, where $\ell = \ell(\alpha)$ is the period length of the simple continued fraction expansion. It is known that a quadratic irrational α has such a purely periodic expansion if and only if $\alpha > 1$ and $-1 < \alpha' < 0$, where α'

is the algebraic conjugate of α. Any quadratic irrational which satisfies these two conditions is called *reduced* (see [3, Theorem 5.3.2, p. 241]).

We now need to develop a link between the solutions of quadratic Diophantine equations with the Q_j defined in Equations (2.2)–(2.4).

Let $D_0 > 1$ be a square-free positive integer and set:

$$\sigma_0 = \begin{cases} 2 & \text{if } D_0 \equiv 1 \bmod 4, \\ 1 & \text{otherwise.} \end{cases}$$

Define:

$$\omega_0 = (\sigma_0 - 1 + \sqrt{D_0})/\sigma_0, \text{ and } \Delta_0 = (\omega_0 - \omega_0')^2 = 4D_0/\sigma_0^2.$$

The value Δ_0 is called a *fundamental discriminant* or *field discriminant* with associated *radicand* D_0, and ω_0 is called the *principal fundamental surd associated with* Δ_0. Let

$$\Delta = f_\Delta^2 \Delta_0$$

for some $f_\Delta \in \mathbb{N}$. If we set

$$g = \gcd(f_\Delta, \sigma_0),\ \sigma = \sigma_0/g,\ D = (f_\Delta/g)^2 D_0, \text{ and } \Delta = 4D/\sigma^2,$$

then Δ is called a *discriminant* with associated *radicand* D. Furthermore, if we let

$$\omega_\Delta = (\sigma - 1 + \sqrt{D})/\sigma = f_\Delta \omega_0 + h$$

for some $h \in \mathbb{Z}$, then ω_Δ is called the *principal surd* associated with the discriminant

$$\Delta = (\omega_\Delta - \omega_\Delta')^2.$$

This will provide the canonical basis element for certain rings that we now define.

Let $[\alpha, \beta] = \alpha\mathbb{Z} + \beta\mathbb{Z}$ be a $\mathbb{Z}$-module. Then $\mathcal{O}_\Delta = [1, \omega_\Delta]$, is an *order* in $K = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{D_0})$ with conductor f_Δ. If $f_\Delta = 1$, then $\mathcal{O}_\Delta$ is called the *maximal order in* K. The units of $\mathcal{O}_\Delta$ form a group which we denote by U_Δ. The positive units in U_Δ have a generator which is the smallest unit that exceeds 1. This selection is unique and is called the *fundamental unit of* K, denoted by ε_Δ.

It may be shown that any $\mathbb{Z}$-submodule $I \neq (0)$ of $\mathcal{O}_\Delta$ has a representation of the form $[a, b + c\omega_\Delta]$, where $a, c \in \mathbb{N}$ with $0 \leq b < a$. We will only be concerned with *primitive* ones, namely those for which $c = 1$. In other words, I is a primitive $\mathbb{Z}$-submodule of $\mathcal{O}_\Delta$ if whenever $I = (z)J$ for some $z \in \mathbb{Z}$ and some $\mathbb{Z}$-submodule J of $\mathcal{O}_\Delta$, then $|z| = 1$. Thus, a canonical representation of a primitive $\mathbb{Z}$-submodule of $\mathcal{O}_\Delta$ is obtained by setting $\sigma a = Q$ and $b = (P - \sigma + 1)/\sigma$ for $P, Q \in \mathbb{Z}$, namely

$$I = [Q/\sigma, (P + \sqrt{D})/\sigma]. \tag{2.5}$$

Now we set the stage for linking ideal theory with continued fractions by giving a criterion for a primitive $\mathbb{Z}$-module to be a primitive ideal in $\mathcal{O}_\Delta$. A nonzero $\mathbb{Z}$-module I as given in (2.5) is called a primitive $\mathcal{O}_\Delta$-ideal if and only if $P^2 \equiv D$ mod Q (see [3, Theorem 3.5.1, p. 173]). *Henceforth, when we refer to an $\mathcal{O}_\Delta$-ideal it will be understood that we mean a* primitive *$\mathcal{O}_\Delta$-ideal.* Also, the value Q/σ is called the *norm of* I, denoted by $N(I)$. Hence, we see that I is an $\mathcal{O}_\Delta$-ideal if and only if $\alpha = (P + \sqrt{D})/Q$ is a quadratic irrational. Thus, we often write $[\alpha]$ to represent the ideal $[Q/\sigma, (P + \sqrt{D})/\sigma]$ from which it follows that the *conjugate ideal* I' of I is $[\alpha'] = [Q/\sigma, (P - \sqrt{D})/\sigma]$. When $I = I'$, we say that I is *ambiguous*.

Given the notion of a reduced quadratic irrational discussed earlier, it is not surprising that we define a *reduced ideal* I to be one which contains an element $\beta = (P+\sqrt{D})/\sigma$ such that $I = [N(I), \beta]$, where $\beta > N(I)$ and $-N(I) < \beta' < 0$, since this corresponds exactly to the reduced quadratic irrational $\alpha = \beta/N(I) > 1$ with $-1 < \alpha' < 0$, namely $I = [\alpha]$. In fact, the following holds.

Theorem 2.1. *Let Δ be a discriminant with associated radicand D. Then $I = [Q/\sigma, (P+\sqrt{D})/\sigma]$ is a reduced $\mathcal{O}_\Delta$-ideal if $Q/\sigma < \sqrt{\Delta}/2$. Conversely, if I is reduced, then $Q/\sigma < \sqrt{\Delta}$. Furthermore, if $0 \leq P - \sigma + 1 < Q < 2\sqrt{D}$ and $Q > \sqrt{D}$, then I is reduced if and only if $Q - \sqrt{D} < P < \sqrt{D}$.*

Proof. See [2, Corollaries 1.4.2–1.4.4, p. 19]. □

The following result links solutions of quadratic Diophantine equations with the Q_j as promised above.

Theorem 2.2. *Let Δ be a discriminant with radicand $D > 0$ and let $c \in \mathbb{N}$ with $c < \sqrt{\Delta}/2$. Then $x^2 - Dy^2 = \pm\sigma^2 c$ has a primitive solution if and only if $c = Q_j$ for some $j \geq 0$ in the simple continued fraction expansion of ω_Δ.*

Proof. This follows from the Continued Fraction Algorithm. for example, ee [3, Theorem 5.5.2, pp. 261–266]. □

Remark 2.1. From the continued fraction algorithm cited in the proof of Theorem 2.2, it follows that if

$$I = [Q/\sigma, (P+\sqrt{D})/\sigma]$$

is a reduced $\mathcal{O}_\Delta$-ideal, then for $\ell = \ell((P+\sqrt{D})/Q)$, the set

$$\{Q_1/\sigma, Q_2/\sigma, \ldots, Q_\ell/\sigma\}$$

represents the *norms of all reduced ideals equivalent to I*. Hence, Theorems 2.1–2.2 tell us precisely when norms of reduced ideals can be solutions of quadratic Diophantine equations.

Lastly, we will have need of the following, which may be traced back to Lagrange.

Theorem 2.3. *If $\Delta > 0$ is a discriminant, and $\ell = \ell(\sqrt{D})$ is the period length of the simple continued fraction expansion of $\sqrt{D}$ then*

$$N(\varepsilon_\Delta) = (-1)^\ell.$$

Also, either

$$\varepsilon_\Delta \in \mathbb{Z}[\sqrt{D}] \qquad \text{or} \qquad \varepsilon_\Delta^3 \in \mathbb{Z}[\sqrt{D}].$$

Proof. See [2, Theorems 2.1.3, pp. 51–52]. □

3. Solutions of quadratic equations

Theorem 3.1. *Let $c \in \mathbb{Z}$ and $D \in \mathbb{N}$ where D is not a perfect square and*

$$\gcd(c, D) = 1. \tag{3.1}$$

If

$$x^2 - Dy^2 = -c \tag{3.2}$$

has a primitive positive solution $x_0 + y_0\sqrt{D}$, then

$$x^2 - Dy^2 = c \tag{3.3}$$

has a primitive positive solution if and only if either $\ell(\sqrt{D})$ is odd, or there exists a divisor $d \in \mathbb{N}$, $d \neq 1, |c|$, of c such that

$$x^2 - Dy^2 = -d^2 \tag{3.4}$$

has a primitive solution $X + Y\sqrt{D}$ with

$$\gcd(x_0X + y_0YD, Xy_0 + x_0Y) = d, \tag{3.5}$$

and

$$\gcd(d, c/d) \bigm| 2. \tag{3.6}$$

Proof. Suppose that we have the primitive, positive solutions $x_0 + y_0\sqrt{D}$ and $x_1 + y_1\sqrt{D}$ of Equations (3.2)–(3.3), respectively. Let

$$d_0 = \gcd(x_0x_1 - y_0y_1D, x_0y_1 - x_1y_0) \tag{3.7}$$

and set

$$X = (x_0x_1 - y_0y_1D)/d_0, \text{ and } Y = (x_0y_1 - x_1y_0)/d_0.$$

Then

$$\begin{aligned} X^2 - DY^2 &= \frac{1}{d_0^2}\left[(x_0x_1 - y_0y_1D)^2 - (x_0y_1 - x_1y_0)^2D\right] \\ &= \frac{1}{d_0^2}\left[(x_0^2 - y_0^2D)(x_1^2 - y_1^2D)\right] = -\left(\frac{c}{d_0}\right)^2, \end{aligned} \tag{3.8}$$

so

$$N(X + Y\sqrt{D}) = -d^2 \tag{3.9}$$

where $c = d_0d$ and we may assume without loss of generality that $d \in \mathbb{N}$. By the choice in (3.7), $X + Y\sqrt{D}$ is primitive.

If $\ell(\sqrt{D})$ is even, then by Theorem 2.3 , $d \neq 1$ since (3.9) holds. Now we show that if $\ell(\sqrt{D})$ is even, $d \neq |c|$.

Let

$$X_{(+)} = x_0x_1 + y_0y_1D, \qquad Y_{(+)} = y_0x_1 + x_0y_1,$$
$$X_{(-)} = x_0x_1 - y_0y_1D, \qquad \text{and} \qquad Y_{(-)} = y_0x_1 - x_0y_1.$$

Claim 3.1. $\gcd(X_{(+)}, Y_{(+)}) = d$

Since

$$N\left(X_{(+)} + Y_{(+)}\sqrt{D}\right) = -c^2, \tag{3.10}$$

$\gcd(X_{(+)}, Y_{(+)}) \bigm| c$. Now we demonstrate that $c \bigm| Y_{(+)}Y_{(-)}$ and $c \bigm| X_{(+)}X_{(-)}$.

Multiplying $-x_1^2$ times $x_0^2 - Dy_0^2 = -c$ and adding x_0^2 times $x_1^2 - Dy_1^2 = c$ we get,

$$D(x_1^2y_0^2 - x_0^2y_1^2) = c(x_0^2 + x_1^2). \tag{3.11}$$

Therefore, $c \bigm| (y_0^2x_1^2 - x_0^2y_1^2) = Y_{(+)}Y_{(-)}$, since $\gcd(c, D) = 1$. Also,

$$\begin{aligned} X_{(+)}X_{(-)} &= x_0^2x_1^2 - y_0^2y_1^2D^2 = x_0^2x_1^2 - x_1^2y_0^2D + x_1^2y_0^2D - y_0^2y_1^2D^2 \\ &= x_1^2(x_0^2 - y_0^2D) + y_0^2D(x_1^2 - y_1^2D) = -c^2(x_1^2 - y_0^2D), \end{aligned}$$

so $c \mid X_{(+)}X_{(-)}$. We have shown that $dd_0 \mid X_{(+)}X_{(-)}$ and $dd_0 \mid Y_{(+)}Y_{(-)}$. Given that $\gcd(X_{(-)}, Y_{(-)}) = d_0$, then $\gcd(X_{(+)}, Y_{(+)}) = d$, which is Claim 3.1.

By (3.10) and Claim 3.1, if $d = |c|$, then

$$N\left(\frac{X_{(+)}}{d} + \frac{Y_{(+)}}{d}\sqrt{D}\right) = -1,$$

which is impossible if $\ell(\sqrt{D})$ is even by Theorem 2.3. We have shown that if $\ell(\sqrt{D})$ is even, then $d \neq 1, |c|$.

It remains to verify (3.5)–(3.6). We have:

$$x_0X + y_0YD = \frac{x_1(x_0^2 - y_0^2D)}{d_0} = -\frac{cx_1}{d_0} = -x_1d,$$

and

$$Xy_0 + x_0Y = \frac{y_1(x_0^2 - y_0^2D)}{d_0} = -\frac{cy_1}{d_0} = -y_1d.$$

Thus, by the primitivity of $x_1 + y_1\sqrt{D}$, we have,

$$\gcd(x_0X + y_0YD, Xy_0 + x_0Y) = d,$$

which is (3.5).

In order to establish (3.6), we need the following.

Claim 3.2. $\gcd(c, Y_{(+)}, Y_{(-)}) \mid 2$.

If p is a prime dividing both d and d_0, then p divides both $Y_{(+)}$ and $Y_{(-)}$. Hence, $p \mid 2y_0x_1$. If $p > 2$, then $p \mid y_0x_1$. If $p \mid x_1$, then $p \mid y_1$, given that $p \mid c = x_1^2 - y_1^2D$ with $\gcd(c, D) = 1$. This contradicts the primitivity of $x_1 + y_1\sqrt{D}$. Similarly, $p \nmid y_0$ given the primitivity of $x_0 + y_0\sqrt{D}$. Thus, $p = 2$. If $2^t | \gcd(c, Y_+, Y_-)$, for some $t \in \mathbb{N}$, then both $y_0x_1 \equiv x_0y_1 \bmod 2^t$ and $y_0x_1 \equiv -x_0y_1 \bmod 2^t$. Since x_0y_1 is odd in this case, then we may take the modular multiplicative inverse to get,

$$-1 \equiv (x_0y_1)^{-1}(y_0x_1) \equiv 1 \mod 2^t,$$

so $t = 1$. This establishes Claim 3.2.

Now (3.6) follows from Claims 3.1–3.2 and the fact that $\gcd(X_{(-)}, Y_{(-)}) = d_0$. This completes the proof of necessity of the conditions.

Conversely, suppose that there are $X, Y \in \mathbb{Z}$ such that (3.4)–(3.6) hold. Set

$$\alpha = \frac{(x_0 + y_0\sqrt{D})(X + Y\sqrt{D})}{d}.$$

Then $N(\alpha) = c$,

$$\alpha = \frac{x_0X + y_0YD}{d} + \frac{x_0Y + y_0X}{d}\sqrt{D} = x_1 + y_1\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$$

and $\gcd(x_1, y_1) = 1$, since $\gcd(x_0X + y_0YD, x_0Y + y_0X) = d$. □

Remark 3.1. By Corollary 2.2, a primitive solution to either of Equations (3.2) or (3.3) when $|c| < \sqrt{D}$, necessarily implies the existence of a nonnegative integer $j < \ell(\sqrt{D})$ such that $Q_j = |c|$ in the simple continued fraction expansion of $\sqrt{D}$. We also have the following classic result.

Corollary 3.1 (Lagrange — see [3, pp. 269–270])**.** *For $D \in \mathbb{N}$ not a perfect square, $x^2 - Dy^2 = -1$ has a solution if and only if $\ell(\sqrt{D})$ is odd.*

Proof. Since $c = 1$ has no proper divisors, then the result follows from Theorem 3.1. □

Example 3.1. Let $D = 65$, for which $\ell(\sqrt{D}) = 1$, so by Corollary 3.1, $x^2 - 65y^2 = -1$ has a solution. The fundamental solution is $8 + \sqrt{65}$. However, $x^2 - 65y^2 = -4$ has no primitive solutions. The following result tells us when such equations do have primitive solutions.

A well-known related result to Theorem 3.1 is the following.

Lemma 3.1 (Eisenstein — see [2, Footnote 2.1.10, p. 60])**.** *If $D \in \mathbb{N}$ is odd and not a perfect square, then* both *Pell equations*

$$x^2 - Dy^2 = -4 \tag{3.12}$$

and

$$X^2 - DY^2 = 4 \tag{3.13}$$

have primitive solutions if and only if $\varepsilon_D \notin \mathbb{Z}[\sqrt{D}]$ and $N(\varepsilon_D) = -1 = N(\varepsilon_{4D})$.

Proof. If $x_0 + y_0\sqrt{D}$ is a primitive solution of Equation (3.12), then the value $(x_0 + y_0\sqrt{D})/2$ is a unit in $\mathbb{Z}[(1 + \sqrt{D})/2]$, so $\varepsilon_D \notin \mathbb{Z}[\sqrt{D}]$. Also, $N(\varepsilon_D) = -1 = N(\varepsilon_{4D})$, since $\varepsilon_D^3 = \varepsilon_{4D}$ by Theorem 2.3. Conversely, if $\varepsilon_D \notin \mathbb{Z}[\sqrt{D}]$ and if $N(\varepsilon_D) = -1$, then Equation (3.12) has a primitive solution, and so does Equation (3.13). □

Remark 3.2. Lemma 3.1 fails if D is even. For instance, if $D = 8$, then $x^2 - Dy^2 = -4$ has primitive solution $2 + \sqrt{8}$. However, $\varepsilon_D = \varepsilon_8 = 1 + \sqrt{2} \in \mathbb{Z}[\sqrt{8}]$ and $\varepsilon_{4D} = \varepsilon_{32} = 3 + \sqrt{8} = 3 + \sqrt{8}$, with norm 1.

Now we may show that Corollary 3.1 and Lemma 3.1 are actually special cases of the following.

Corollary 3.2. *Suppose that $D \in \mathbb{N}$, $D > 1$ not a perfect square, p is a prime not dividing D, and a is a nonnegative integer. If*

$$x^2 - Dy^2 = -p^a \tag{3.14}$$

has a primitive solution, then

$$X^2 - DY^2 = p^a \tag{3.15}$$

has a primitive solution if and only if $\ell(\sqrt{D})$ is odd.

Proof. If $\ell(\sqrt{D})$ is odd, then Equation (3.15) has a primitive solution whenever Equation (3.14) has such a solution. To see this we merely we multiply a primitive solution of (3.14) by the fundamental unit of $\mathbb{Z}[\sqrt{D}]$ to get a primitive solution of (3.15) via Theorem 2.3.

Conversely, assume that Equations (3.14)–(3.15) both have primitive solutions $x_0 + y_0\sqrt{D}$ and $x_1 + y_1\sqrt{D}$, respectively. Suppose that $\ell(\sqrt{D})$ is even. Then by Theorem 3.1, there is a divisor $d = p^b$ of c with $a > b > 0$ such that

$$x^2 - Dy^2 = -d^2 \tag{3.16}$$

has a primitive solution $X + Y\sqrt{D}$. By (3.6) in Theorem 3.1, $\gcd(p^b, p^{a-b})$ is 1 or 2. Hence, $p = 2$ and either $b = 1$ or $a = b + 1$. Also, since $\gcd(p, D) = 1$, then D is odd. In the case where $b = 1$, (3.16) implies that $x^2 - Dy^2 = -4$ has a primitive solution $X + Y\sqrt{D}$. Hence, $D \equiv 1 \bmod 4$ and $u = (x + y\sqrt{D})/2 \in \mathbb{Z}[(1 + \sqrt{D})/2]$ is a unit with $N(u) = N(u^3) = -1$. Since $u^3 \in \mathbb{Z}[\sqrt{D}]$, then $\ell(\sqrt{D})$ is odd by Theorem 2.3, a contradiction.

Now suppose that $a = b + 1$. Then as in the proof of (3.6) in Theorem 3.1, $\gcd(x_0x_1 + y_0y_1D, x_1y_0 + x_0y_1) = d = p^{a-1}$. Since

$$\left(\frac{x_0x_1 + y_0y_1D}{p^{a-1}}\right)^2 - \left(\frac{x_1y_0 + x_0y_1}{p^{a-1}}\right)^2 D = -p^2 = -4,$$

then by the above argument we again get a contradiction and the result is established. □

The following example was provided by the author's former graduate student, Gary Walsh.

Example 3.2. For the radicand $D = 34$ and the value $c = 33$, $1+\sqrt{34}$ is a primitive solution to $x^2 - Dy^2 = -c$ and $13 + 2\sqrt{34}$ is a primitive solution to $X^2 - DY^2 = c$. Note that $\ell(\sqrt{34}) = 4$.

Notice that in Example 3.2, c is a product of two distinct primes. Hence, Corollary 3.2 is the most that we can hope to achieve as a direct generalization of Corollary 3.1 in the sense of the odd parity of $\ell(\sqrt{D})$ determining the mutual solvability of the Equations (3.2)–(3.3).

Example 3.3. If $D = 65$ and $c = 29$, then $x_0^2 - y_0^2D = 6^2 - 65 = -29$ is a primitive solution. Also, $x_1^2 - y_1^2D = 17^2 - 2^2 \cdot 65 = 29$ is a primitive solution. Here, $\ell(\sqrt{65}) = 1$.

The following illustrates that under the hypothesis of Corollary 3.2, both $\ell(\sqrt{D})$ is odd and the condition in Theorem 3.1 are satisfied.

Example 3.4. Let $D = 145$ and $c = 2^6 = 2^a$. Here $\ell(\sqrt{145}) = 1$. We have the primitive solutions

$$x_0^2 - y_0^2D = 9^2 - 145 = -2^6 \text{ and } x_1^2 - y_1^2D = 37^2 - 3^3 \cdot 145 = 2^6.$$

Also, if $d = 32 = 2^5 = 2^{a-1}$, then

$$x^2 - Dy^2 = 51^2 - 5^2 \cdot 145 = -(32)^2 = -d^2$$

is a primitive solution, where

$$d = 32 = \gcd(x_0x + y_0yD, xy_0 + x_0y) = \gcd(1184, 96) = 32\gcd(37, 3).$$

Notice, however, that $X^2 - DY^2 = -(c/d)^2 = -4$ has no primitive solution by Lemma 3.1 since $\varepsilon_D = 12 + \sqrt{145} \in \mathbb{Z}[\sqrt{D}]$.

Remark 3.3. The existence of a solution to Equation (3.4) in Theorem 3.1 is tantamount to the existence of a reduced quadratic irrational

$$\gamma = (x + \sqrt{y^2D})/d$$

with underlying radicand y^2D. (To see that such a γ must be reduced, note that if $d > y\sqrt{D}$, then $-d^2 < -y^2D < x^2 - y^2D = -d^2$, a contradiction. Thus, $d < y\sqrt{D}$, so by Theorem 2.1, using the ideal $[d, x + \sqrt{y^2D}]$, γ is reduced.) Moreover, $N(\gamma) = -1$. The existence of such a γ is equivalent to γ having pure symmetric period namely $\gamma = \langle \overline{q_0; q_1, \dots, q_\ell} \rangle$ with $q_j = q_{\ell-j-1}$ for all integers j with $0 \le j \le \ell - 1$, which means that $q_0 q_1 \dots q_\ell$ is a palindrome.[1] Moreover, it is a fact that D is a sum of two integer squares if and only if there is an element in $\mathbb{Q}(\sqrt{D})$ of norm -1, such as γ. Moreover, $N(\gamma) = -1$ is equivalent to the ideal class of $[\gamma]$ in the class group of $\mathbb{Q}(\sqrt{D})$ having at most one ambiguous ideal. (See [6, Theorem 2.2, p. 105] for verification of the above comments.) The following illustrates these comments.

Example 3.5. Returning to the radicand in Example 3.2, consider the reduced quadratic irrational

$$\gamma = \frac{P + \sqrt{D}}{Q} = \frac{5 + \sqrt{34}}{3} = \langle \overline{3; 1, 1, 1, 1, 3} \rangle.$$

Since $x_0^2 - Dy_0^2 = 1 - 34 = -33 = -c$ and $x^2 - Dy^2 = 5^2 - 34 = -3^2 = -d^2$, with $\gcd(x_0 x + y_0 y D, x y_0 + x_0 y) = \gcd(39, 6) = 3 = d$, then by Theorem 3.1, there exists a primitive solution to $x_1^2 - Dy_1^2 = 33 = c$. This solution is obtained in the same fashion as in the proof of Theorem 3.1, namely,

$$x_1 + y_1\sqrt{D} = \frac{x_0 x + y_0 y D}{d} + \frac{x_0 y + y_0 x}{d}\sqrt{D} = 13 + 2\sqrt{34}.$$

Also, with respect to Remark 3.3, it can be shown that the class of $[\gamma]$ has no ambiguous ideals in it using [2, Theorem 6.1.1, p. 189].

Example 3.6. Let $D = 45305 = 5 \cdot 13 \cdot 17 \cdot 41$ and $c = 7031 = 79 \cdot 89$. Suppose that we want to investigate whether there are primitive solutions to $x^2 - Dy^2 = \pm c$. Using Theorem 3.1, we would need solutions to Equation (3.4) for some divisor $d \ne 1, c$ given that $\ell(\sqrt{D}) = 16$. We have the two primitive solutions:

$$6172^2 - 29^2 \cdot 45305 = -89^2,$$

and

$$1366708^2 - 6421^2 \cdot 45305 = -79^2.$$

However, there are no solutions to either of $x^2 - Dy^2 = \pm c$. This demonstrates that we must first ensure the existence of a solution to Equation (3.2) in Theorem 3.1 before proceeding.

Suppose that we were to choose $c = 79$ or $c = 89$. Then we would still have no solutions of either equation. Corollary 3.2 explains why.

Example 3.7. Let $D = 845 = 5 \cdot 13^3$ and $c = 29$. Then

$$N(\varepsilon_{4D}) = 12238^2 - 421^2 \cdot 845 = -1,$$

where

$$\varepsilon_{4D} = 12238 + 421\sqrt{845} = \left(\frac{29 + \sqrt{845}}{2}\right)^3 = \varepsilon_D^3.$$

We have the two primitive solutions,

$$N(\alpha_0) = N(436 + 15\sqrt{845}) = 436^2 - 15^2 \cdot 845 = -29 = -c,$$

[1] We should recall, as oft does my colleague, friend, and coauthor Alf van der Poorten, that a palindrome is: *never even.* Indeed, it is: *never odd or even.* It is: *a toyota.*

and

$$N(\alpha_1) = N(407 + 14\sqrt{845}) = 407^2 - 14^2 \cdot 845 = 29.$$

Notice that,

$$\gamma = \frac{\alpha_0}{\alpha_1} = \frac{2 + \sqrt{845}}{29} = \langle \overline{1, 14, 58, 14, 1} \rangle$$

is a reduced quadratic irrational with $N(\gamma) = -1$. Moreover, in the simple continued fraction expansion of γ, we get that

$$I_3 = [Q_2, P_2 + \sqrt{D}] = [1, 29 + \sqrt{845}] = I_3'$$

is the only ambiguous ideal in the class of $[\gamma]$. See [2, Theorem 6.1.1, p. 189].

Example 3.8. Returning to the radicand in Example 3.6, $D = 45305$, we choose $c = 89 \cdot 151 = 13439$ this time. We have the primitive solution,

$$x_0^2 - y_0^2 D = N(\alpha_0) = 17879^2 - 84^2 \cdot 45305 = -c = -13439.$$

Since we know, from Example 3.6, that

$$x^2 - y^2 D = 6172^2 - 29^2 \cdot 45305 = -89^2 = -d^2,$$

and since

$$\gcd(x_0 x + y_0 y D, x_0 y + x y_0) = \gcd(220712168, 1036939) = 89 = d,$$

then by Theorem 3.1, we know that we have a solution to $x_1^2 - y_1^2 D = c$. Indeed, we have,

$$N(\alpha_1) = x_1^2 - y_1^2 D = 2479912^2 - 11651^2 \cdot 45305 = c = 13439.$$

Observe that in Example 3.5, $D = 5^2 + 3^2$ where $d = 3$. This does not happen in general. In other words, it is not always possible to get the value of d in Equation (3.4) from a representation of D as a sum of two integer squares. For instance, in this example, there exist exactly eight distinct representations of D, up to order and sign, as a sum of two integer squares (see [3, Theorem 6.1.3, pp. 279–280]). They are:

$$D = 45305 = 19^2 + 212^2 = 149^2 + 152^2 = 211^2 + 28^2 = 181^2 + 112^2 =$$

$$= 173^2 + 124^2 = 107^2 + 184^2 = 83^2 + 196^2 = 203^2 + 64^2,$$

and none of these has $d = 89$ as a divisor. Notice, as well, that

$$\gamma = \frac{\alpha_1}{\alpha_0} = \frac{2479912 + 11651\sqrt{45305}}{17879 + 84\sqrt{45305}} = \frac{6172 + \sqrt{29^2 \cdot 45305}}{89},$$

which is a reduced quadratic irrational with $N(\gamma) = -1$ having underlying radicand $D = 38101505 = 29^2 \cdot 45305$.

Remark 3.4. Notice that if both Equations (3.2)–(3.3) have primitive solutions $x_0^2 - y_0^2 D = -c$ and $x_1^2 - y_1^2 D = c$, respectively, then by Equation (3.11),

$$D \mid (x_0^2 + x_1^2) \text{ and } c \mid (x_0^2 y_1^2 - x_1^2 y_0^2).$$

For instance, in Example 3.5, $D = 34$, $c = 33$,

$$x_0^2 + x_1^2 = 1^2 + 13^2 = 170 = 5D,$$

and

$$x_0^2 y_1^2 - y_0^2 x_1^2 = 1^2 \cdot 2^2 - 1^2 \cdot 13^2 = -165 = -5c.$$

In Example 3.7, $D = 845$, $c = 29$,

$$x_0^2 + x_1^2 = 436^2 + 407^2 = 355745 = 421D,$$

and

$$x_0^2y_1^2 - y_0^2x_1^2 = 436^2 \cdot 14^2 - 15^2 \cdot 407^2 = -12209 = -421c.$$

The question naturally arises: For which values of D (if any) does it hold that $D = x_0^2 + x_1^2$. The answer is that it does hold, but only in the most trivial of cases. To see this, assume that we have the two aforementioned primitive solutions. Then by adding the two equations (3.2)–(3.3), we get $x_0^2 + x_1^2 - D(y_0^2 + y_1^2) = 0$. Thus, if $D = x_0^2 + x_1^2$, we get that $y_0^2 + y_1^2 = 1$ for which only the case $c = 1$, $y_0 = 1$, $y_1 = 0$, and $D = x_0^2 + 1$ holds (if we allow $x_1 + y_1\sqrt{D} = 1 + 0\sqrt{D}$ as a primitive solution). For instance, $D = 5 = 2^2 + 1$ is such a value. Such values of D are called narrow Richaud-Degert (RD)-types. These types and their generalizations have been studied extensively from not only the perspective of solutions of Diophantine equations, but also for the study of class numbers of quadratic orders (see [2, pp. 77–87]).

Although $D \neq x_0^2 + x_1^2$ in all except the narrow RD-types, the above argument shows that $x_0^2 + x_1^2 = D(y_0^2 + y_1^2)$ and $x_0^2y_1^2 - x_1^2y_0^2 = -c(y_0^2 + y_1^2)$.

Acknowledgements. Thanks go to the (anonymous) referee whose comments generated a clearer elucidation of the results.

References

[1] 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, MR 87g:11035, Zbl 596.10013.

[2] R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, New York, London, Tokyo, 1996, Zbl 858.11001.

[3] R. A. Mollin, *Fundamental Number Theory with Applications*, CRC Press, Boca Raton, New York, London, Tokyo, 1998, Zbl 943.11001.

[4] R. A. Mollin, *Jacobi symbols, ambiguous ideals, and continued fractions*, Acta Arith. **85** (1998), 331–349, MR 99e:11136, Zbl 916.11054.

[5] R. A. Mollin, *Criteria for simultaneous solutions of $X^2 - DY^2 = c$ and $x^2 - Dy^2 = -c$* , (to appear in Canad. Math. Bull.).

[6] R. A. Mollin and K. Cheng, *Palindromy and continuous ideals revisited*, J. Number Theory, **74** (1999), 98–110, MR 99m:11123, Zbl 923.11021.

[7] R. A. Mollin and A. J. van der Poorten, *Continued fractions, Jacobi symbols, and quadratic Diophantine equations*, Canad. Math. Bull. **43** (2000), 218–225, MR 2001a:11049.

[8] H. C. Williams, *Eisenstein's problem and continued fractions*, Utilitas Math. **37** (1990), 145–157, MR 91h:11018 Zbl 718.11010.

Dept. of Math. and Stat., 2500 University Drive, 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/2001/7-7.html.