Serdica
Mathematical Journal
Сердика
Математическо списание

For further information on
Serdica Mathematical Journal
which is the new series of
Serdica Bulgaricae Mathematicae Publicationes
visit the website of the journal http://www.math.bas.bg/~serdica
or contact: Editorial Office
Serdica Mathematical Journal
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Telephone: (+359-2)9792818, FAX:(+359-2)971-36-49
e-mail: serdica@math.bas.bg

Serdica Math. J. **28** (2002), 175-188

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

IDEAL CRITERIA FOR BOTH $X^2 - DY^2 = m_1$ AND $x^2 - Dy^2 = m_2$ TO HAVE PRIMITIVE SOLUTIONS FOR ANY INTEGERS m_1, m_2 PRIME TO $D > 0$

R. A. Mollin

Communicated by V. Drensky

Abstract. This article provides necessary and sufficient conditions for both of the Diophantine equations $X^2 - DY^2 = m_1$ and $x^2 - Dy^2 = m_2$ to have primitive solutions when $m_1, m_2 \in \mathbb{Z}$, and $D \in \mathbb{N}$ is not a perfect square. This is given in terms of the ideal theory of the underlying real quadratic order $\mathbb{Z}[\sqrt{D}]$.

1. Introduction. In [4], criteria for the existence of primitive solutions of both equations in the title were given for the case where $m_1 = -m_2$. It is the purpose of this article to generalize this to arbitrary $m_1, m_2 \in \mathbb{Z}$. The problem was inspired by work done in [3] as well as by correspondence with Keith Matthews (see Example 3.5 below). Moreover, the initial inspiration for looking at this problem was the criterion given by Lagrange for the existence of a

2000 *Mathematics Subject Classification:* 11D09, 11A55, 11R11.

Key words: continued fractions, Diophantine equations, fundamental units, simultaneous solutions, ideals, norm form equations.

solution to the negative Pell equation $x^2 - Dy^2 = -1$, namely that such a solution exists if and only if the period length of the simple continued fraction expansion of $\sqrt{D}$ is odd. One may naively ask if this holds true for $x^2 - Dy^2 = -m$, i. e. is it true that both $X^2 - DY^2 = -m$ and $x^2 - Dy^2 = m$ have primitive solutions if and only if the period length of the simple continued fraction expansion of $\sqrt{D}$ is odd. The answer is *no* and we gave a criterion in [4] for when both do have primitive solutions. It turns out, nevertheless, that one can generalize this to the arbitrary case given in the title by using ideal theory to give a simpler proof with more far-reaching applications and consequences such as the classical results of Lagrange, mentioned above, and that of Eisenstein (see Remark 3.1 below).

2. Notation and preliminaries. We will be studying solutions of quadratic Diophantine equations of the general shape

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

where $D \in \mathbb{N}$ is not a perfect square and $m \in \mathbb{Z}$. 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 a solution exists, there is one in which both x and y have their least values. Such a solution is called the *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.

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, $P^2 \equiv D \pmod{Q}$, 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 [6, Theorem 5.3.1, p. 240]). Furthermore a quadratic irrational *may* have a *purely* periodic continued fraction expansion which we denote by

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

meaning 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 [6, Theorem 5.3.2, p. 241]).

We need the following basic notation for discriminants and ideals. 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 $f_\Delta \in \mathbb{N}$ and set

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

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 $[\alpha, \beta] = \alpha\mathbb{Z} + \beta\mathbb{Z}$ denote a $\mathbb{Z}$-module. Then $\mathcal{O}_\Delta = [1, \omega_\Delta]$, is an *order*

in $K = \mathbb{Q}(\sqrt{\Delta_0}) = \mathbb{Q}(\sqrt{D_0})$ 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_0}.

It may be shown that any $\mathbb{Z}$-module $I \neq (0)$ 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 $b = (P-1)/2$ if $\sigma = 2$, while $b = P$ if $\sigma = 1$ for $P, Q \in \mathbb{Z}$, namely

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

A nonzero $\mathbb{Z}$-module I as given in (2.5) is called a primitive $\mathcal{O}_\Delta$-ideal if and only if $P^2 \equiv D \pmod{Q}$ (see [6, Theorem 3.5.1, p. 173]). 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. Also, the *conjugate* ideal of I given in (2.5) is $I' = [Q/\sigma, (P - \sqrt{D})/\sigma]$. 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 $-1 < \alpha' < 0$.

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

Theorem 2.1. *Let $\Delta > 0$ be a discriminant,*

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

a reduced ideal in $\mathcal{O}_\Delta$, and $\alpha = (P+\sqrt{D})/Q$. If P_j and Q_j for $j = 1, 2, \ldots, \ell(\alpha) = \ell$ are defined by Equations (2.2)–(2.4) *in the simple continued fraction expansion of α, then*

$$\varepsilon_\Delta = \prod_{i=1}^{\ell} (P_i + \sqrt{D})/Q_i$$

and

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

P r o o f. See [5, Theorems 2.1.3–2.1.4, pp. 51–53]. □

In the next section, we will need the following (see [6, pp. 178–181]).

♦ Multiplication Formulas for Ideals

Let Δ be a discriminant, and let $I_i = [a_i, (b_i + \sqrt{\Delta})/2]$ for $i = 1, 2$ be primitive ideals in $\mathcal{O}_\Delta$. Then the following formulae hold.

$$I_1 I_2 = (d)[a_3, (b_3 + \sqrt{\Delta})/2], \tag{2.6}$$

where

$$a_3 = a_1 a_2 / d^2, \tag{2.7}$$

with

$$d = \gcd(a_1, a_2, (b_1 + b_2)/2) \tag{2.8}$$

and

$$b_3 \equiv \frac{1}{d}(\delta a_2 b_1 + \mu a_1 b_2 + \frac{\nu}{2}(b_1 b_2 + \Delta)) \pmod{2a_3}, \tag{2.9}$$

where δ, μ and ν are determined by

$$\delta a_2 + \mu a_1 + \frac{\nu}{2}(b_1 + b_2) = d. \tag{2.10}$$

We now proceed with a discussion of the solvability of

$$x^2 - Dy^2 = m \in \mathbb{Z}, \tag{2.11}$$

for any radicand $D \in \mathbb{N}$.

We will need the following later for illustrations of the main result.

Definition 2.1. *If $\tau_j = x_j + y_j\sqrt{D}$ for $j = 1, 2$ are primitive solutions of Equation* (2.11)*, then they are said to be* in the same class *provided that their ratio is a solution of Pell's equation*

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

In other words, τ_1 and τ_2 are in the same class of solutions of Equation (2.11) *if there exists a solution $\beta = u + v\sqrt{D}$ of* (2.12) *such that $\tau_1\beta = \tau_2$.*

If τ and $-\tau'$ are solutions in the same class, then that class is called ambiguous. *A solution $x_0 + y_0\sqrt{D}$ of Equation* (2.11) *for which y_0 is the least*

positive value in its class is uniquely determined and called the fundamental solution in its class. *If $x_0 + y_0\sqrt{D}$ is ambiguous, then we require, in addition, that $x_0 \geq 0$.*

An arithmetic property for determining when solutions of Equation (2.11) are in the same class is given as follows.

Proposition 2.1. *Two primitive solutions $x_j + y_j\sqrt{D}$ for $j = 1, 2$ of Equation* (2.11) *are in the same class if and only if both*

$$(x_1x_2 - y_1y_2D)/m \in \mathbb{Z} \text{ and } (y_1x_2 - x_1y_2)/m \in \mathbb{Z}.$$

Consequently, there are only finitely many classes of primitive solutions of Equation (2.11).

Proof. See [6, Proposition 6.2.1, p. 299]. □

Theorem 2.2. *Let $D \in \mathbb{N}$ not a perfect square, $m \in \mathbb{Z}$, and let $\alpha = x_0 + y_0\sqrt{D}$ be a primitive solution of*

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

Then each of the following hold.

(a) *There is a unique primitive element $\beta = X_0 + Y_0\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ such that*

$$\beta\alpha' = (X_0 + Y_0\sqrt{D})(x_0 - y_0\sqrt{D}) = P_0 + \sqrt{D},$$

where

$$-|m|/2 < P_0 \leq |m|/2.$$

(b) *The solution (x_0, y_0) may be determined from β via:*

$$x_0 = \frac{X_0P_0 - Y_0D}{N(\beta)} \text{ and } y_0 = \frac{Y_0P_0 - X_0}{N(\beta)}.$$

(c) *For any solution γ in the same class as α there exists a unique element δ such that $\delta\gamma' = P_0 + \sqrt{D}$.*

(d) *There is a unique ideal*

$$I_\alpha = [N(\alpha), (P_0 + \sqrt{\Delta})/2] \sim 1.$$

Proof. See [6, Theorem 6.2.7, pp. 302–304]. □

Definition 2.2. *Given a primitive solution α of equation* (2.13)*, the ideal I_α in Theorem* 2.2 *is called the* unique ideal associated with α. *Also, α is said to* belong to the unique element P_0 *determined by Theorem* 2.2.

3. Results.

Theorem 3.1. *Let $m_1, m_2 \in \mathbb{Z}$, $D \in \mathbb{N}$, not a perfect square, and*

$$\gcd(m_1 m_2, D) = 1. \tag{3.14}$$

If

$$x^2 - Dy^2 = m_1 \tag{3.15}$$

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

$$x^2 - Dy^2 = m_2 \tag{3.16}$$

has a primitive solution if and only if there exists a divisor $d \in \mathbb{N}$, of $g = \gcd(m_1, m_2)$ such that

$$x^2 - Dy^2 = m_1 m_2/d^2 \tag{3.17}$$

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

$$\gcd(x_0 X - y_0 Y D, X y_0 - x_0 Y) = |m_1|/d. \tag{3.18}$$

Furthermore, when such a solution to (3.17) *exists, then a primitive solution of* (3.16) *is given by*

$$x_1 + y_1\sqrt{D} = \frac{x_0 X - y_0 Y D + (x_0 Y - X y_0)\sqrt{D}}{|m_1|/d}. \tag{3.19}$$

P r o o f. Suppose that (3.15)–(3.16) both have primitive solutions

$$\alpha_0 = x_0 + y_0\sqrt{D} \text{ and } \alpha_1 = x_1 + y_1\sqrt{D},$$

respectively. Then, for $\Delta = \sigma^2 D$, there exist unique, primitive, principle $\mathcal{O}_\Delta$-ideals:

$$I_{\alpha_0} = (x_0 + y_0\sqrt{D}) = [m_1, (P_0 + \sqrt{\Delta})/2],$$

and

$$I_{\alpha_1} = (x_1 + y_1\sqrt{D}) = [m_2, (P_1 + \sqrt{\Delta}])/2,$$

where α_j belongs to P_j for $j = 0, 1$ (see Definition 2.2). Thus ,we have,

$$I_{\alpha_0} I_{\alpha_1} = (I_{\alpha_0} + I_{\alpha_1})(I_{\alpha_0} \cap I_{\alpha_1}) = \gcd(I_{\alpha_0}, I_{\alpha_1})\mathrm{lcm}(I_{\alpha_0}, I_{\alpha_1}), \tag{3.20}$$

(see [7, Exercise 3.15], for instance).

Also, by the multiplication formulae (2.6)–(2.10),

$$I_{\alpha_0} I_{\alpha_1} = (d)\left[\frac{m_1 m_2}{d^2}, (P_2 + \sqrt{\Delta})/2\right],$$

where $\alpha_0\alpha_1/d$ belongs to P_2, and $d = \gcd\left(m_1, m_2, \frac{P_0+P_1}{2}\right)$. Moreover,

$$\left[\frac{m_1m_2}{d^2}, (P_2+\sqrt{\Delta})/2\right] = (X + Y\sqrt{D}),$$

where

$$X + Y\sqrt{D} = \frac{x_0x_1 + y_0y_1D + (x_1y_0 + x_0y_1)\sqrt{D}}{d}$$

with

$$X^2 - DY^2 = \frac{m_1m_2}{d^2},$$

It follows from Theorem 2.2 that $X + Y\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$, and given that $\left[\frac{m_1m_2}{d^2}, (P_2+\sqrt{\Delta})/2\right]$ is a primitive ideal generated by $X + Y\sqrt{D}$, then it is primitive. We have established (3.17). We now check that (3.18) holds.

$$\gcd(x_0X - y_0YD, x_0Y - Xy_0) = \frac{1}{d}\gcd(x_1(x_0^2 - y_0^2D), y_1(x_0^2 - y_0^2D)) =$$

$$\frac{1}{d}\gcd(x_1m_1, y_1m_1) = \frac{|m_1|}{d}\gcd(x_1, y_1) = \frac{|m_1|}{d}.$$

It remains to check (3.19). Since it is straightforward that

$$\left(\frac{x_0X - y_0YD}{m_1/d}\right)^2 - \left(\frac{x_0Y - Xy_0}{m_1/d}\right)^2 D = m_2,$$

then we are done.

To prove the converse, assume that (3.17)–(3.18) hold, and set

$$\alpha = \frac{(x_0 + y_0\sqrt{D})(X - Y\sqrt{D})}{|m_1|/d}.$$

Then $N(\alpha) = N(x_1 + y_1\sqrt{D}) = m_2$, $\alpha \in \mathbb{Z}[\sqrt{D}]$, and $\gcd(x_1, y_1) = 1$ since (3.18) holds. □

Corollary 3.1. *Suppose that $D > 0$ is a nonsquare integer, a is a nonnegative integer, and p is a prime not dividing D. If*

$$x^2 - Dy^2 = -p^a \tag{3.21}$$

has a primitive solution, then

$$X^2 - DY^2 = p^a \tag{3.22}$$

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

Proof. If $\ell(\sqrt{D})$ is odd, then by Theorem 2.1 the result holds. Conversely, if both (3.21)–(3.22) have primitive solutions, then there are principal

$\mathcal{O}_\Delta$-ideals of norm p^a and $-p^a$ with generators η_p and η_{-p} respectively. Hence, $\eta\eta_{-p}$ is a unit in $\mathcal{O}_\Delta$ so by Theorem 2.1, $\ell(\sqrt{D})$ is odd. $\square$

Remark 3.1. The special case of Corollary 3.1 where $a = 0$ is the result by Lagrange, namely that the Pell equation $x^2 - Dy^2 = -1$ has a solution if and only if $\ell(\sqrt{D})$ is odd (see [6, Corollary 5.3.3, p. 249]). The special case where $a = 2 = p$ is related to a problem of Eisenstein, namely that if the radicand $D \equiv 1 \pmod 4$, $x^2 - Dy^2 = -4$ has a primitive solution if and only if $N(\varepsilon_D) = -1$ and $\varepsilon_D \notin \mathbb{Z}[\sqrt{D}]$. In Corollary 3.1, we are assuming that $x^2 - Dy^2 = -4$ has a solution, so in this case, $\ell(\sqrt{D})$ is necessarily odd as demonstrated in the proof of the corollary. The special case where $a = 1$ is Corollary 3.2 of [4].

It turns out that Corollary 3.1 is the best that one hope to achieve in the sense that the parity of $\ell(\sqrt{D})$ determines the mutual solvability of $x^2 - Dy^2 = m$ and $X^2 - DY^2 = -m$. The following illustration shows that once m is divisible by two distinct primes, this parity is not a deciding factor in the mutual solvability of these two equations.

Example 3.1. *If $D = 34$, $m_2 = 33 = -m_1$, and $d = 3$. Then since $(x_0, y_0) = (1, 1)$ is a solution of $x^2 - Dy^2 = m_1$, and $(X, Y) = (27, 5)$ is a solution of $x^2 - Dy^2 = m_1 m_2/d^2 = -11^2$ with*

$$\gcd(x_0X - y_0YD, Xy_0 - x_0Y) = \gcd(143, 22) = 11 = |m_1|/d,$$

then

$$x_1^2 - y_1^2 D = \left(\frac{x_0X - y_0YD}{m_1/d}\right)^2 - D\left(\frac{Xy_0 - x_0Y}{m_1/d}\right)^2 = 13^2 - 2^2 \cdot 34 = 33 = m_2.$$

Notice that $\ell(\sqrt{34}) = 4$.

We can exploit this example further by illustrating the proof of Theorem 3.1 involving the use of ideals. We have that $\alpha_0 = x_0 + y_0\sqrt{34} = 1 + \sqrt{34}$ is a primitive solution of $x^2 - 34y^2 = m_1$, and $\alpha_1 = x_1 + y_1\sqrt{34} = 13 + 2\sqrt{34}$ is a primitive solution of $x^2 - 34y^2 = m_2$. Thus we have the primitive, principle ideals (in $\mathbb{Z}[\sqrt{D}]$):

$$I_{\alpha_0} = (1 + \sqrt{34}) = [-33, -1 + \sqrt{34}] = [m_1, P_0 + \sqrt{D}],$$

and

$$I_{\alpha_1} = (13 + 2\sqrt{34}) = [33, 10 + \sqrt{34}] = [m_2, P_1 + \sqrt{D}]$$

where α_0 belongs to $P_0 = -1$ and α_1 belongs to $P_1 = 10$. Thus,

$$I = I_{\alpha_0} I_{\alpha_1} = (3)(27 + 5\sqrt{34}) = (3)[-11^2, 43 + \sqrt{34}] = (3)[m_1 m_2/d^2, P_2 + \sqrt{D}],$$

where

$$27 + 5\sqrt{34} = \frac{(1+\sqrt{34})(13+2\sqrt{34})}{3} = \alpha_0\alpha_1/d$$

belongs to $P_2 = 43$.

On the other end of the spectrum from the consideration in Example 3.1 is the case where $\gcd(m_1, m_2) = 1$. In this case, both (3.15)–(3.16) have primitive solutions when $x^2 - Dy^2 = m_1m_2$ has one with the gcd condition (3.18) satisfied. For instance, we have the following.

Example 3.2. *Let* $D = 221$, $m_1 = -100$ *and* $m_2 = -43$. *Then*

$$x_0 + y_0\sqrt{D} = 431 + 29\sqrt{221}$$

is a primitive solution of $x^2 - Dy^2 = m_1$. *Also, since* $\gcd(m_1, m_2) = 1$, *we choose* $d = 1$ *in Theorem* 3.1. *We calculate a primitive solution*

$$X + Y\sqrt{D} = 25317 + 1703\sqrt{221}$$

of $x^2 - Dy^2 = m_1m_2$. *Thus by Theorem* 3.1,

$$\frac{x_0X - y_0YD}{|m_1|} + \frac{x_0Y - Xy_0}{|m_1|}\sqrt{D} = -29 + 2\sqrt{221}$$

is a primitive solution of $x^2 - 221y^2 = -43$.

The following depicts the essential nature of the gcd condition (3.18) in Theorem 3.1.

Example 3.3. *If* $D = 29$, $m_1 = 455$ *and* $m_2 = 65$, *then we have the primitive solution* $x_0 + y_0\sqrt{D} = 22 + \sqrt{29}$ *to* $x^2 - Dy^2 = m_1 = 455$. *Also, for* $d = 13$, *we have the primitive solution* $X + Y\sqrt{D} = 318 + 59\sqrt{29}$ *to*

$$x^2 - Dy^2 = m_1m_2/d^2 = 175, \tag{3.23}$$

where

$$\gcd(x_0X - y_0YD, Xy_0 - x_0Y) = \gcd(5285, 980) = 35 = m_1/d.$$

Hence, by Theorem 3.1, *we must have a primitive solution* $x_1 + y_1\sqrt{D}$ *to*

$$x^2 - Dy^2 = m_2, \tag{3.24}$$

and it is achieved via

$$(x_1, y_1) = \left(\frac{x_0X - y_0YD}{m_1/d}, \frac{Xy_0 - x_0Y}{m_1/d}\right) = \left(\frac{5285}{35}, \frac{980}{35}\right) = (151, 28).$$

Notice that the gcd *condition given above is essential. For instance, we have primitive solutions such as* $(X, Y) = (2698, 501)$ *to Equation* (3.23)*. However,*

$$\gcd(x_1, y_1) = \gcd(x_0X - y_0YD, Xy_0 - x_0Y) = \gcd(44827, 8324) = 1 \neq m_1/d$$

and (x_1, y_1) *does not give a solution of* (3.24)*. Similarly, the primitive solution* $(X, Y) = (146, 27)$ *of Equation* (3.23) *has*

$$\gcd(x_0X - y_0YD, Xy_0 - x_0Y) = \gcd(2429, 448) = 7 = m_2/d \neq m_1/d,$$

and $((x_0X - y_0YD)/7, (x_0Y - Xy_0)/7) = (347, -64)$ *does not yield a solution of* (3.24)*.*

The gcd condition (3.18) in Theorem 3.1 also takes on special meaning when m_2 is a perfect square.

Example 3.4. *Let* $D = 106$*,* $m_1 = 1575$*, and* $m_2 = 225 = 3^2 \cdot 5^2$*. Then we have a primitive solution* $(x_0, y_0) = (41, 1)$ *to* $x^2 - Dy^2 = m_1$*. If we set* $d = 25$*, then we have the primitive solution* $(X, Y) = (6929, 673)$ *to*

$$x^2 - Dy^2 = m_1 m_2/d^2 = 567 \tag{3.25}$$

where

$$\gcd(x_0X - y_0YD, Xy_0 - x_0Y) = \gcd(212751, 20664) = 63 = m_1/d. \tag{3.26}$$

Thus, by Theorem 3.1*,*

$$(x_1, y_1) = \left(\frac{x_0X - y_0YD}{m_1/d}, \frac{x_0Y - Xy_0}{m_1/d} \right) = (3377, 328)$$

is a primitive solution of $x^2 - Dy^2 = m_2$*.*

Notice that there are other primitive solutions to (3.25)*. However, not all satisfy* (3.26)*. For instance,* $(X, Y) = (2399, 233)$ *satisfies* (3.25)*, but not* (3.26) *since* $\gcd(x_0X - y_0YD, Xy_0 - x_0Y) = 7 = n \neq m_1/d = 63$*. Similarly, the primitive solution* $(3791129, 368227)$ *to* (3.25) *does not satisfy* (3.26) *since the* $\gcd(x_0X - y_0YD, Xy_0 - x_0Y) = 9$*. However, note that*

$$\varepsilon_{4 \cdot 106} = 4005 + 389\sqrt{106}$$

is the fundamental unit of $\mathbb{Z}[\sqrt{106}]$ *and*

$$(-4005 + 389\sqrt{106})^2(3791129 + 368227\sqrt{106}) = 2399 - 233\sqrt{106},$$

so the solutions $(2399, -233)$ *and* $(3791129, 368227)$ *are in the same class of solutions to* (3.25) *à la Definition* 2.1*, but not in the class of* $(6929, 673)$ *by Proposition* 2.1*.*

The following is an example from a communication from Keith Matthews

in 1999, who was studying, at that time, a paper [10] by Wilhelm Patz published in the late 1940s. This correspondence and the interchange surrounding it was one of the inspirations for the writing of this paper and several other outcroppings such as [1] – [2].

Example 3.5. *Patz* [10] *used simple continued fraction expansions to solve* $x^2 - Dy^2 = np$ *where* $p = 2^{31} - 1$ *and* $D = 13$ *for certain small values of* n. *His method is a special case of the* Lagrange-Matthews-Mollin *algorithm described in* [1]–[2]. *In particular Patz considered the case*

$$x^2 - 13y^2 = -p = 1 - 2^{31}. \tag{3.27}$$

Matthews observed that

$$x_0^2 - y_0^2 D = 49696^2 - 26183^2 \cdot 13 = -3p.$$

From this, he wanted to achieve a solution of (3.27).

If we take $m_1 = -3p$, $m_2 = -p$, *and* $d = p$ *in Theorem* 3.1, *then*

$$X^2 - DY^2 = 256^2 - 71^2 \cdot 13 = 3 = m_1 m_2/d^2$$

with

$$\gcd(x_0 X - y_0 Y D, X y_0 - x_0 Y) = \gcd(11444733, 3174432) = |m_1|/d = 3.$$

Thus, by Theorem 3.1,

$$\frac{x_0 X - y_0 Y D + (X y_0 - x_0 Y)\sqrt{D}}{|m_1|/d} = -3814911 + 1058144\sqrt{13}$$

is a primitive solution of (3.27).

Remark 3.2. Another interpretation of what Theorem 3.1 says is that if there exists a primitive solution $x_0 + y_0\sqrt{D}$ of $x^2 - Dy^2 = m_1$, then $x^2 - Dy^2 = m_2$ has a primitive solution precisely when there exists a quadratic irrational

$$\gamma = \frac{x + \sqrt{Dy^2}}{d},$$

where $x, y, d \in \mathbb{Z}$, $d \mid \gcd(m_1, m_2)$, and

$$N(\gamma) = m_1 m_2/d^2$$

with $\gcd(x_0 x - y_0 y D, x y_0 - x_0 y) = |m_1|/d$. In particular, if $m_1 = -m_2$, then this is tantamount to saying that $DY^2 = x^2 + d^2$ and if $y = 1$, then we have that D itself is a primitive sum of two integer squares. For instance, we have the following.

Example 3.6. *Returning to Example* 3.1, *we have that* $x_0 + y_0\sqrt{34} =$

$1 + \sqrt{34}$ *is a primitive solution of* $x^2 - 34y^2 = -33$ *and* $13 + 2\sqrt{34}$ *is a primitive solution of* $x^2 - 34y^2 = 33 = m_2$. *Furthermore,*

$$\gamma = \frac{-1 + \sqrt{34}}{13 - 2\sqrt{34}} = \frac{(-1 + \sqrt{34})(13 + 2\sqrt{34})}{33} = \frac{55 + 11\sqrt{34}}{33} =$$

$$\frac{5 + \sqrt{34}}{3} = \langle \overline{3; 1, 1, 1, 1, 3} \rangle,$$

which is an example of a reduced quadratic irrational with pure symmetric period (see [9]). *Moreover,*

$$D = 34 = 3^2 + 5^2 = d^2 + X^2,$$

(see [9] for connections with ideal classes having no ambiguous ideals in them.)

Acknowledgements. This author's research is supported by NSERC Canada grant # A8484. Also, thanks go to the referee for comments that led not only to a more refined and shorter version than the original, but also a more general result.

REFERENCES

[1] K. R. Matthews. The Diophantine equation $x^2 - Dy^2 = N$, $D > 0$. *Exposition. Math.* **18** (2000) 323–331.

[2] R. A. Mollin. Simple continued fraction solutions for Diophantine equations. *Exposition. Math.* **19** (2001), 55–73.

[3] R. A. Mollin. All solutions of the Diophantine equation $x^2 - Dy^2 = n$. *Far East J. Math. Sci.*, Special Volume (1998), Part III, 257–293.

[4] 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.).

[5] R. A. Mollin. Quadratics. CRC Press, Boca Raton, New York, London, Tokyo, 1996.

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

[7] R. A. Mollin. Algebraic Number Theory. Chapman and Hall/CRC, Boca Raton, New York, London, Tokyo, 1999.

[8] R. A. Mollin. Simple Continued Fraction Solutions for Diophantine Equations (to appear in Exposition. Math.).

[9] R. A. Mollin, K. Cheng. Palindromy and Ambiguous ideals revisited. *J. Number Theory* **74** (1999), 110.

[10] W. Patz. Über die Gleichung $X^2 - DY^2 = \pm c \cdot (2^{31} - 1)$, wo c möglichst klein. Sitzungsber. Math.-Naturw. Kl. Bayer. Akad. Wiss. Munchen (1948), 21–30.

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`

Received February 5, 2002
Revised April 8, 2002