

All Solutions of the Diophantine Equation

$$x^2 - Dy^2 = n^*$$

R.A. Mollin

Abstract

The main thrust of this article is to show how complete solutions of quadratic Diophantine equations can be given, for any positive discriminant, in terms of the continued fraction algorithm. This is in response to recent results by Zhang [4]-[6], wherein semi-simple continued fractions were introduced to generalize the well-known fact that solutions of quadratic Diophantine equations with values bounded above by \sqrt{D} , for a given field radicand D , are convergents of the simple continued fraction expansion of \sqrt{D} . We show here that Zhang's theory is not required since the continued fraction algorithm is a sufficient and more accurate mechanism for explaining how this all works, and that it actually contains a more refined version of these so-called semi-simple continued fractions. We do this by getting complete and explicit solutions for any quadratic Diophantine equation having arbitrary positive radicand D (corresponding to any real quadratic order) using only known theory, and we generalize the results of Zhang in the process. We show that solutions to these Diophantine equations arise as convergents of a continued fraction expansion of \sqrt{D} obtained via the continued fraction algorithm. We develop the entire theory from the basics, since the works of Nagell [2] and Perron [3] are insufficient to explain completely the method of obtaining all solutions to quadratic Diophantine equations via the *infrastructure*, namely the interrelationship between continued fractions and ideals, thereby filling a gap in the literature in a structure-rich fashion from a modern viewpoint.

*1991 Mathematics Subject Classification: 11D09, 11R11, 11R04, 11Y65, 11A55
Key Words and Phrases: Diophantine equations, quadratic field, continued fractions

1 Background

In this section, we look at the history and details of the continued fraction algorithm, especially as it pertains to solutions of Diophantine equations, including the Pell equation.

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

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

Define

$$\omega_0 = (\sigma_0 - 1 + \sqrt{D_0})/\sigma_0,$$

and

$$\Delta_0 = (\omega_0 - \omega'_0)^2 = 4D_0/\sigma_0^2,$$

where ω'_0 is the *algebraic conjugate* of ω_0 , i.e. $\omega'_0 = (\sigma_0 - 1 - \sqrt{D_0})/\sigma_0$. 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 $f_\Delta \in \mathbf{N}$. If we set $g = \gcd(f_\Delta, \sigma_0)$, $\sigma = \sigma_0/g$, and set

$$D = (f_\Delta/g)^2 D_0,$$

then

$$\Delta = 4D/\sigma^2,$$

and 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 $h \in \mathbf{Z}$, then ω_Δ is called the *principal surd* associated with the discriminant $\Delta = (\omega_\Delta - \omega'_\Delta)^2$. Now we bring ideal structure into the picture.

If $[\alpha, \beta] = \alpha\mathbf{Z} + \beta\mathbf{Z}$, then $\mathcal{O}_\Delta = [1, f_\Delta \omega_0] = [1, \omega_\Delta]$. This is an *order* in $K = \mathbf{Q}(\sqrt{D_0}) = \mathbf{Q}(\sqrt{\Delta})$ having *conductor* f_Δ and discriminant Δ . If $f_\Delta = 1$, then \mathcal{O}_Δ is called the *maximal order* or *ring of integers* of K . The units of \mathcal{O}_Δ form a group which we denote by U_Δ .

Let $I = [a, b + c\omega_\Delta]$, with $a > 0$. The following tells us when such a module is an ideal (see [1, Exercise 1.2.1(a), p.12]).

Theorem 1 (*Ideal Criterion*). *If $I = [a, b + c\omega_\Delta]$, then I is a non-zero ideal of \mathcal{O}_Δ if and only if $c|a$, $c|b$ and $ac|N(b + c\omega_\Delta)$.*

Note that I is a zero ideal if and only if $I \subseteq \mathbf{Z}$. Thus, if I is a non-zero ideal in \mathcal{O}_Δ , then I can be written as $[a, b + c\omega_\Delta]$ where $a, b, c \in \mathbf{Z}$, $a > 0$, $c > 0$, $c | b$ and $c | a$. In fact, for a given non-zero ideal I in \mathcal{O}_Δ , the integers a and c are unique. Indeed, a is *the least positive rational integer* in I , which we denote by $L(I)$. Also, we denote the value of $cL(I)$ by $N(I)$, called the *norm* of I . We call c a *rational integer factor* of I . Throughout, we assume our ideals to be non-zero.

If I is an \mathcal{O}_Δ -ideal with $L(I) = N(I)$, i.e. $c = 1$, then I is called *primitive* which means that I has no rational integer factors other than ± 1 . When I is primitive, then $N(I) = L(I) = |\mathcal{O}_\Delta : I|$, the *index* of I in \mathcal{O}_Δ . Moreover, if $I = [a, b + \omega_\Delta]$ is primitive, then so is its *conjugate* $I' = [a, b + \omega'_\Delta]$. A primitive ideal I is called *reduced* if there does not exist a $\beta \in I$ such that both $\beta > N(I)$, and $-N(I) < \beta' < 0$. A geometric way of looking at reduced ideals is to think of the lattice of the ideal I , and view the square, centered at the origin, with vertex $(N(I), N(I))$. If the only element of the ideal in this square is the zero element, then the ideal is reduced.

Since there are infinitely many choices for the value of b in $I = [a, b + \omega_\Delta]$, then it is valuable to have a method of being able to guarantee uniqueness in the choice. The following does this by showing that we may choose $|b| \leq a/2$ uniquely (see [1, Exercise 1.5.3, p. 28]).

Theorem 2 (*Criterion for Ideal Equality*). *If Δ is a discriminant and $I = [a, \alpha]$ is a primitive ideal in \mathcal{O}_Δ , then $I = [a, na \pm \alpha]$ for any $n \in \mathbf{Z}$.*

Now we give an elucidation of the theory of continued fractions as it pertains to the above. Continued fraction expansions will be denoted by $\langle a_0; a_1, a_2, \dots, a_l, \dots \rangle$ where $a_i \in \mathbf{R}$ are called the *partial quotients* of the continued fraction expansion. If $a_i \in \mathbf{Z}$, and $a_i > 0$ for all $i > 0$, then the continued fraction is called an *infinite simple continued fraction* (which is equivalent to being an irrational number), whereas if the expression terminates, then it is called a *finite simple continued fraction* (which is equivalent to being a rational number). If there is some $n \in \mathbf{N}$ such that $a_i \in \mathbf{Z}$ is non-zero, but possibly negative, for $i \leq n$, and $a_i > 0$ for all $i > n$, then such continued fractions have been dubbed *semi-simple continued fractions* by Zhang [4]. It is the latter which is actually explained by the continued fraction algorithm, described in detail below.

We will be discussing *quadratic irrationals* which are real numbers γ associated with a radicand D such that γ can be written in the form $\gamma = (P + \sqrt{D})/Q$ where $P, Q, D \in \mathbf{Z}, D > 0, Q \neq 0$, and $P^2 \equiv D \pmod{Q}$. The following is a setup for our discussion of the continued fraction algorithm.

Suppose that $I = [a, b + \omega_\Delta]$ is a primitive ideal in \mathcal{O}_Δ , then we define the following for the quadratic irrational $\gamma = (b + \omega_\Delta)/a$ (where g and h are defined above):

$$(P_0, Q_0) = ((\sigma_0 b + f_\Delta(\sigma_0 - 1) + h\sigma_0)/g, a\sigma_0/g), \quad (1)$$

and (for $i \geq 0$),

$$D = P_{i+1}^2 + Q_i Q_{i+1}, \quad (2)$$

$$P_{i+1} = a_i Q_i - P_i, \quad (3)$$

and

$$a_i = \lfloor (P_i + \sqrt{D})/Q_i \rfloor, \quad (4)$$

where $\lfloor x \rfloor$ is the greatest integer less than or equal to x , i.e. the *floor* of x . Therefore, $\gamma = \langle a_0; a_1, \dots, a_i, \dots \rangle$ is the simple continued fraction expansion of γ .

Remark 1 Recall that the simple continued fraction expansion of a quadratic irrational γ is called purely periodic provided that there is an integer $l \in \mathbf{N}$ such that $\gamma = \langle a_0; \overline{a_1, a_2, \dots, a_l} \rangle = \langle \overline{a_0; a_1, a_2, \dots, a_{l-1}} \rangle$.¹ The value $l = l(\gamma)$ is called the **period length** of the simple continued fraction expansion of γ . Furthermore, quadratic irrationals are purely periodic if and only if they are **reduced**, i.e. a quadratic irrational γ is purely periodic if and only if $\gamma > 1$ and $-1 < \gamma' < 0$.²

In what follows we need the notion of equivalence of ideals. Two ideals I and J of \mathcal{O}_Δ are *equivalent* (denoted by $I \sim J$) if there exist non-zero $\alpha, \beta \in \mathcal{O}_\Delta$ such that $(\alpha)I = (\beta)J$ (where (x) denotes the principal ideal generated by x).³ The following is fundamental to the discussion (see [1, Theorem 2.1.2, pp. 44-47]).

¹See [1, Chapter 2, pp. 41-63] for example.

²See [1, Theorem 2.1.1, pp. 42-43] for details.

³Note that we are not assuming that we necessarily have invertible ideals. In fact, the ideals may *not* be invertible. The notion of equivalence does not come equipped with an attendant class group structure attached to it. We need this more general approach in order to discuss the continued fraction algorithm in its greatest generality. For examples and details on this topic see [1, Chapter 1, pp. 23-30; Chapter 6, pp. 187-221].

Theorem 3 (*The Continued Fraction Algorithm.*) Let $\Delta > 0$ be a discriminant, and let $I = I_1 = [a, b + w_\Delta]$ be a primitive ideal in the order \mathcal{O}_Δ . Set $P = P_0$ and $Q = Q_0$, as defined in Equation (1), and let P_i and Q_i for $i > 0$ be defined by Equations (2) – (4) in the simple continued fraction expansion of $\gamma = \gamma_0 = (P + \sqrt{D})/Q$. If $I_i = [Q_{i-1}/\sigma, (P_{i-1} + \sqrt{D})/\sigma]$, then $I_1 \sim I_i$ for all $i \geq 1$. Also, there exists a least value $m \geq 1$ such that I_{m+i} is reduced for all $i \geq 0$.

The following consequence of Theorem 3 shows how we achieve complete solutions of Pell's equation via continued fractions. First we need to define a well-known pair of sequences. Define two sequences of integers $\{A_i\}$ and $\{B_i\}$ inductively by:

$$A_{-2} = 0, A_{-1} = 1, A_i = a_i A_{i-1} + A_{i-2} \quad (\text{for } i \geq 0), \quad (5)$$

$$B_{-2} = 1, B_{-1} = 0, B_i = a_i B_{i-1} + B_{i-2} \quad (\text{for } i \geq 0), \quad (6)$$

and

$$\langle a_0; a_1, a_2, \dots, a_{i-1}, r \rangle = \frac{rA_{i-1} + A_{i-2}}{rB_{i-1} + B_{i-2}} \quad (i \geq 0), \quad (7)$$

for any positive $r \in \mathbf{R}$, where $\{a_i\}$ is an infinite sequence of integers with $a_i > 0$ whenever $i > 0$.

Corollary 1 Let $D > 0$ be any radicand with $\gamma = \sqrt{D} = \langle a_0; a_1, a_2, \dots \rangle$ and $\ell = \ell(\sqrt{D})$. If ℓ is even, then all positive solutions of $x^2 - Dy^2 = 1$ (in other words, all solutions for which $x, y > 0$), are given by $x = A_{lm-1}$ and $y = B_{lm-1}$ for $m \geq 1$, whereas there are no solutions to $x^2 - Dy^2 = -1$. If ℓ is odd, then all positive solutions of $x^2 - Dy^2 = 1$ are given by $x = A_{2lm-1}$ and $y = B_{2lm-1}$ for $m \geq 1$, whereas all positive solutions of $x^2 - Dy^2 = -1$ are given by $x = A_{(2m-1)\ell-1}$, $y = B_{(2m-1)\ell-1}$ for $m \geq 1$.

In fact, there is a more general result than the above, namely the following (see [1, Exercise 2.1.10, p. 57]).

Corollary 2 Let $D > 0$ be an arbitrary radicand and $Q \in \mathbf{Z}$ with $|Q| < \sqrt{D}$. If $x^2 - Dy^2 = Q$, then there exists a positive $i \in \mathbf{Z}$ such that $x/y = A_i/B_i = C_i$ is a **convergent** in the simple continued fraction expansion of \sqrt{D} .

Remark 2 *It is exactly Corollary 2 which Zhang [op.cit.] sought to generalize. However, as he admitted in [4], his choices for those semi-simple continued fractions are not unique. In fact, therein, he seeks to achieve what he calls minimal continued fractions, and leaves a conjecture [4, p.6] which is answered by the theory which we develop in this paper since our choices are explicit and unique.*

This author found it difficult to apply the theory developed by Zhang since it is abstract, not explicit in terms of generating solutions, and for this author at least, difficult to follow given the unusual approach which includes none of the continued fraction algorithm or ideal theory. In other words, the infrastructure was not employed in any fashion. We remedy this situation in the next section where we give complete and explicit solutions of Equation (8) based upon the infrastructure and classical theory which we are delineating in this section. Furthermore, Zhang's work must be credited with inspiring this author to develop the ideas presented in this paper.

In this paper, we will be concerned with solutions of the quadratic Diophantine equation

$$x^2 - Dy^2 = Q \tag{8}$$

where $Q \in \mathbf{Z}$ is arbitrary, and D is any radicand.

Definition 1 *If $\gcd(x, y) = 1$ ($x \neq 0, y > 0$) in equation (8), then we call $\alpha = x + y\sqrt{D}$ a **proper solution** of that equation. Furthermore, if $\alpha = x + y\sqrt{D} \in [1, \sqrt{D}]$ with $\gcd(x, y) = 1$ ($x \neq 0, y > 0$), then α is called a **primitive element** of $[1, \sqrt{D}]$.*

In the next section, we will show how proper solutions of Equation (8) are obtained from convergents of a more general principal cycle by making greater use of the continued fraction algorithm.

From Theorem 3, we get all reduced ideals equivalent to a given reduced ideal $I = [N(I), b + \omega_\Delta]$. In other words, in the simple continued fraction expansion of the quadratic irrational $(b + \omega_\Delta)/a$, where $a = N(I)$, we have, for P_i and Q_i as in Equations (1)-(4):

$$\begin{aligned} I = I_1 &= [Q_0/\sigma, (P_0 + \sqrt{D})/\sigma] \sim I_2 = [Q_1/\sigma, (P_1 + \sqrt{D})/\sigma] \\ &\sim \dots \sim I_l = [Q_{l-1}/\sigma, (P_{l-1} + \sqrt{D})/\sigma]. \end{aligned}$$

Finally, $I_{l+1} = I_1 = I$ for a complete *cycle of reduced ideals equivalent to I* of period length $l(I) = l$. Therefore, the $(P_i + \sqrt{D})/Q_i$ are the *complete quotients* of $(b + \omega_\Delta)/N(I) = \gamma$, and the a_i 's are the *partial quotients* of γ . Also, the Q_i/σ 's represent the *norms of all reduced ideals equivalent to I* . Note that $l = l(\gamma) = l(I)$ is the **period length of the cycle of reduced ideals equivalent to I** , which, in turn, is the period length of the simple continued fraction expansion of the quadratic irrational γ .

If I is not reduced in the above, then we may still invoke Theorem 3. Any ideal may be chosen, whether or not it is reduced, and whether or not its norm is positive. If we take any ideal I in \mathcal{O}_Δ , then we refer to the ideals produced by the application of the continued fraction algorithm as a cycle of ideals equivalent to I , which Theorem 3 tells us must be (eventually) purely periodic, as described above. For instance, the following illustrates the process, and will be a motivator for results in the next section.

Example 1 Suppose that $D = 13$ and $\Delta = 4 \cdot 13$, so we are dealing with the order $\mathcal{O}_\Delta = [1, \sqrt{D}]$. Consider the ideal $I = [-27, -11 + \sqrt{13}]$. Then, the continued fraction expansion of $\alpha = (-11 + \sqrt{13})/(-27)$ arising from Theorem 3 is given as follows. First we note that in this case, $\sigma = 1, \sigma_0 = 2 = f_\Delta = g, h = -1, \omega_0 = (1 + \sqrt{13})/2, \omega_\Delta = \sqrt{13}, b = -11$, and $\Delta_0 = D_0 = 13$. Thus, $D = 13$ and $(P_0, Q_0) = ((\sigma_0 b + f_\Delta(\sigma_0 - 1) + h\sigma_0)/g, \sigma_0 Q/g) = (-11, -27)$. Hence, the simple continued fraction expansion of α is:

i	0	1	2	3	4	5	6	7	8	9	10
P_i	-11	11	1	2	1	3	3	1	2	1	3
Q_i	-27	4	3	3	4	1	4	3	3	4	1
a_i	0	3	1	1	1	6	1	1	1	1	6

Therefore, $\alpha = \langle 0, 3, \overline{1, 1, 1, 6, 1} \rangle$. Given that $(1 + \sqrt{13})/3 = \langle \overline{1, 1, 1, 6, 1} \rangle$ is the simple continued fraction expansion of $(P_2 + \sqrt{13})/Q_2$, then $\alpha = \langle 0, 3, (1 + \sqrt{13})/3 \rangle$. Therefore, although $I = I_1$ is not reduced and its norm is negative, we may still invoke the continued fraction algorithm to achieve a continued fraction expansion of its associated quadratic irrational α to eventually get the reduced ideal $I_3 = [Q_2, P_2 + \sqrt{13}] = [3, 1 + \sqrt{13}]$. Also, once we reach I_3 , then we are in a cycle of principal reduced ideals since $I_3 \sim I_4 \sim I_5 \sim I_6 \sim I_7 \sim I_8 = I_3$. Furthermore, we remain in this purely periodic part of

the cycle of principal ideals after this point—ad infinitum.⁴

The process illustrated in Example 1 is of fundamental importance. Theorem 3 tells us that there always exists some minimal positive $n \in \mathbf{Z}$ such that I_{n+i} is reduced for all $i \geq 0$. We therefore introduce a refinement of the term for this integer, when $Q_n = 1$, which will be part of our classification device in the next section.

Definition 2 *Let $\Delta > 0$ be a discriminant with radicand D . If $I = I_1 = [Q_0/\sigma, (P_0 + \sqrt{D})/\sigma]$ is a primitive, principal ideal in O_Δ , and the ideals I_i are the ideals produced by the application of Theorem 3, then the least positive $n \in \mathbf{Z}$ such that $Q_n = 1$ is called the **principal reduction index** of I .*

Remark 3 *Note that I_{n+i} is reduced for all $i \in \mathbf{Z}$ with $i \geq 0$, (see [1, Theorem 2.1.2, pp. 44-47].) Also, observe that it is possible for $I_{n+1} = [Q_n/\sigma, (P_n + \sqrt{D})/\sigma]$ to be reduced without $\gamma_n = (P_n + \sqrt{D})/Q_n$ being reduced. For instance, $I_1 = [1, \sqrt{D}] = [1, \sqrt{D} + \lfloor \sqrt{D} \rfloor]$ is reduced, but $\gamma_0 = \sqrt{D}$ is not. However, whether or not γ_n is reduced, γ_{n+i} is reduced for all $i \geq 1$ (see [1, Claim 4, pg. 45]).*

In Example 1, the principal reduction index of I is $n = 5$ since $Q_5 = 1$ and I_{5+i} is reduced for all $i \geq 1$. Note that, the purely periodic part, initiated by the principal reduction index, may not be the *initial* purely periodic part as determined by Theorem 3. For instance in Example 1, the purely periodic part actually begins with $I_3 = [3, 1 + \sqrt{13}]$. However, we will be concerned with that periodic part initiated by the principal reduction index since it is intimately linked to the solution of Equation (8).

Observe that, since $[1, 3 + \sqrt{13}] = [1, \sqrt{13}]$, by Theorem 2, then we are essentially dealing with the continued fraction expansion of the principal surd $\sqrt{13}$. We will make this more explicit in the next section. Thus, the principal reduction index is a basic tool which we will use in the next section to classify all solutions to Equation (8) via the continued fraction expansion of the principal surd. In general, if the ideal $I = I_1 = [N(I), b + \omega_\Delta]$ is itself already reduced, then the purely periodic part of the cycle begins with

⁴Also, witness that $I_4 = [Q_3, P_3 + \sqrt{13}] = [3, 2 + \sqrt{13}] = I'_3$. We call $i = 4$ the **palindromic index**. See [1, pp.188-198], where we develop the structure surrounding the palindromy in ambiguous cycles.

I_1 , and this is the content of the above discussion about cycles of reduced ideals from which we get $l(I) = l(\gamma)$ where $\gamma = (b + \omega_\Delta)/N(I)$. However, even in this case we have $n > 0$ if $Q_0 \neq 1$. The relationship between $l(\gamma)$ and n when I is not reduced is illustrated by Example 1, wherein $n = 5$ and $l(\sqrt{D}) = 5$. Hence, $I_6 = [1, 3 + \sqrt{13}]$ begins the purely periodic part, initiated by $Q_n = 1$ (i.e. by the principal reduction index), of the simple continued fraction expansion of $\alpha = (-11 + \sqrt{13})/(-27)$. Since the following discussion requires an understanding of the interplay of the fundamental units in various related quadratic orders, and hence the Pell equation, we give the following results.

The next result dates back to Lagrange (see [1, Theorem 2.1.3, pp. 51-52]).

Theorem 4 *Let $I = [a, b + \omega_\Delta]$ be a reduced ideal, where ϵ_Δ is the fundamental unit of \mathcal{O}_Δ . If P_i and Q_i , for $i = 1, 2, \dots, l(I) = l$, appear in the simple continued fraction expansion of $(b + \omega_\Delta)/a$, then*

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

and

$$N(\epsilon_\Delta) = (-1)^l.$$

We now describe the interplay between the fundamental units in two special orders, which has consequences for the solution of Pell's equation as well as more general equations. Since an arbitrary real quadratic order \mathcal{O}_Δ is always contained in the maximal order \mathcal{O}_{Δ_0} , then ϵ_Δ is a unit in \mathcal{O}_{Δ_0} . Therefore, $\epsilon_\Delta = \epsilon_{\Delta_0}^u$, where u is called the *unit index* of \mathcal{O}_Δ in \mathcal{O}_{Δ_0} .

In particular, if $\mathcal{O}_{\Delta_0} = [1, (1 + \sqrt{D})/2]$ for $D \equiv 1 \pmod{4}$, then set $\mathcal{O}_\Delta = [1, \sqrt{D}]$ where $\Delta = 4\Delta_0 = f_\Delta^2 D = f_\Delta^2 \Delta_0$. In this case, either $\epsilon_\Delta = \epsilon_{\Delta_0}^3$ or $\epsilon_\Delta = \epsilon_{\Delta_0}$.⁵

⁵This follows from the general class number formula for real quadratic orders. See, for example [1, footnote 1.5.9, pp. 25-26]. If $f_\Delta > 1$ is the conductor of an order \mathcal{O}_Δ with fundamental discriminant Δ_0 and unit index u , then $h_\Delta = h_{\Delta_0} \psi_{\Delta_0}(f_\Delta)/u$ where $\psi_{\Delta_0}(f_\Delta) = f_\Delta \prod (1 - (\Delta_0/p)/p)$ with the product ranging over all the distinct primes dividing f_Δ and $(*/*)$ denotes the Kronecker symbol. It is known that $h_\Delta \geq h_{\Delta_0}$. Indeed, $h_\Delta/h_{\Delta_0} \in \mathbf{Z}$, but it is an open question as to when $h_\Delta = h_{\Delta_0}$. In any case, u divides ψ_{Δ_0} . Thus, in our special case we deduce that $h_\Delta = h_{\Delta_0}$ when $\Delta \equiv 1 \pmod{8}$, and $h_\Delta = 3h_{\Delta_0}/u$ when $\Delta \equiv 5 \pmod{8}$. In other words, either $\epsilon_\Delta = \epsilon_{\Delta_0}^3$ or $\epsilon_\Delta = \epsilon_{\Delta_0}$.

Now we review the process by which all of the proper solutions of Equation (8) emanate from its fundamental solutions which we now define.

Definition 3 *If $\alpha = x + y\sqrt{D}$ is a proper solution of Equation (8), then so are certain of its **associates**, namely those $\beta \in \mathcal{O}_\Delta (= [1, \sqrt{D}])$, not necessarily maximal⁶) for which there is a $u \in U_\Delta$, $u \neq 1$ with $N(u) = 1$ such that $\beta = u\alpha$. Thus, α and β are called a **proper associated solutions** of Equation (8). These associated solutions⁷ form a class of solutions. For each such class we have an $\alpha_0 = x_0 + y_0\sqrt{D}$ with $y_0 > 0$ being the smallest value possible in its class. If $-x_0 + y_0\sqrt{D}$ is also in the class, then the class is called **ambiguous**, and so in order to ensure a unique choice of α_0 , we assume that $x_0 > 0$ in this case⁸. We call such a solution the **fundamental solution of its class**. Hence, all solutions of Equation (8) are given by certain associates of the fundamental solutions in these (finitely many⁹) classes.*

Remark 4 *An easy exercise shows that two solutions of Equation (8), $\alpha = x + y\sqrt{D}$ and $\alpha_1 = x_1 + y_1\sqrt{D}$, are in the same class if and only if both $(x_1x - y_1yD)/Q \in \mathbf{Z}$ and $(yx_1 - xy_1)/Q \in \mathbf{Z}$.*

In the next section we will need to distinguish between two types of associates of a given solution of Equation (8). We do this as follows.

Definition 4 *Suppose that α and β are proper associated solutions of Equation (8). Then β is called a **positive associate** of α if $\beta = \epsilon_\Delta^i \alpha$ where $i \in \mathbf{Z}$ is positive. If $i < 0$, then β is called a **negative associate** of α .¹⁰*

⁶Here $\Delta = 4D$ is a discriminant with radicand D , where D may be congruent to 1 modulo 4, in which case $\sigma_0 = g = 2|f_\Delta$, and we are *not* dealing with the maximal order in that situation. In any case $\sigma = 1$.

⁷As observed by Nagell [2, p. 205]. We also now see why the proper solutions of Definition 1 were chosen in that fashion, namely in order to coincide with Nagaell's notion of solutions (as well as to avoid trivialities).

⁸In the next section we will develop a unique ideal associated with each proper solution, and therefore we will be able to link all of this to ideal theory (see Definition 5).

⁹See Nagell [2, Theorem 109, pp. 207-208]. Note that, if $N(\epsilon_\Delta) = 1$ (in other words, $l(\sqrt{D})$ is even by Theorem 4), then **all** associates of α_0 are solutions of Equation (8). On the other hand, if $N(\epsilon_\Delta) = -1$, then all associates of the form $\epsilon_\Delta^{2i}\alpha_0$ for any $i \in \mathbf{Z}$ are solutions of Equation (8).

¹⁰Note that, if $N(\epsilon_\Delta) = -1$, then i must be even (see footnote 9).

Note that β is a positive associate of α if and only if α is a negative associate of β . Hence, the intersection of positive and negative associates of a given solution is empty. In other words, a positive associate can never be a negative associate of a given solution of Equation (8).

For instance, we have the following.

Example 2 Consider the Diophantine equation

$$x^2 - 13y^2 = -27. \quad (9)$$

A fundamental solution of it is $\alpha_0 = -5 + 2\sqrt{13}$. Since the fundamental unit of $\mathcal{O}_\Delta = [1, \sqrt{13}]$ is $\epsilon_\Delta = 18 + 5\sqrt{13}$, then all solutions in the class of α_0 are $\epsilon_\Delta^{2n}\alpha_0$, for $n \in \mathbf{Z}$ (since $N(\epsilon_\Delta) = -1$). For instance, $\epsilon_\Delta^2\alpha_0 = 1435 + 398\sqrt{13}$.

Similarly, $-\alpha'_0 = 5 + 2\sqrt{13}$ is a fundamental solution of the above equation, and so are all of its associates $\epsilon_\Delta^{2n}(-\alpha'_0)$, ($n \in \mathbf{Z}$). For example, $(18 + 5\sqrt{13})^2(5 + 2\sqrt{13}) = 7925 + 2198\sqrt{13}$.

In the next section, we will show how these solutions and all others in the various classes of solutions are convergents in a certain (not necessarily simple) continued fraction expansion of $\sqrt{13}$.

All of the above will be explained in a new and revealing way, using only the continued fraction algorithm.

2 Quadratic Diophantine Equations

Numerous symbols will be used and assumptions held throughout this section so we fix these in a sequence of conventions which we will state as the need arises, the first being as follows.

Convention 1 Throughout this section we assume that $\Delta > 0$ is a discriminant (not necessarily fundamental) with associated radicand D , and $\mathcal{O}_\Delta = [1, \sqrt{D}]$ (not necessarily maximal). Furthermore we set $l = l(\sqrt{D}) = l(\sqrt{D} + \lfloor \sqrt{D} \rfloor)$ (see Remark 1, and footnote 6).

First we show how proper solutions of Diophantine equations are linked to the existence of uniquely determined ideals.

Proposition 1 *If $\alpha_0 = x_0 + y_0\sqrt{D} \in \mathcal{O}_\Delta$ is primitive with $N(\alpha_0) = Q_0$, then there exists a unique primitive element $\alpha = x + y\sqrt{D} \in \mathcal{O}_\Delta$ such that*

$$\alpha\alpha'_0 = P_0 + \sqrt{D},$$

with

$$-|Q_0|/2 < P_0 \leq |Q_0|/2.$$

Also,

$$x = (x_0P_0 + Dy_0)/Q_0,$$

and

$$y = (x_0 + y_0P_0)/Q_0.$$

In this fashion, α determines a unique ideal $I = [Q_0, P_0 + \sqrt{D}]$ corresponding to α_0 .

Proof. Since $\gcd(x_0, y_0) = 1$, then $x_0y_1 - y_0x_1 = 1$ for some $x_1, y_1 \in \mathbf{Z}$. In fact, for a fixed such solution, we may give the general solution by $x = x_1 + tx_0$, and $y = y_1 + ty_0$ for some parameter $t \in \mathbf{Z}$. In other words, $x_0y - y_0x = 1$. Thus, if $\alpha = x + y\sqrt{D}$, then

$$\alpha\alpha'_0 = x_0x - y_0yD + (x_0y - y_0x)\sqrt{D} = P_0 + \sqrt{D},$$

where $P_0 = x_0x - y_0yD = x_0x_1 - y_0y_1D - tQ_0$. We may therefore choose P_0 uniquely such that $-|Q_0|/2 < P_0 \leq |Q_0|/2$, and $N(\alpha\alpha'_0) = N(\alpha)N(\alpha'_0)$. Hence, we may form the ideal¹¹

$$I = [Q_0, P_0 + \sqrt{D}].$$

Since

$$P_0 = x_0x - y_0yD, \tag{10}$$

and

$$1 = x_0y - y_0x, \tag{11}$$

then, adding y_0 times Equation (10) to x_0 times Equation (11) yields:

$$x_0 + y_0P_0 = x_0^2y - y_0^2yD = yQ_0.$$

¹¹Observe that, even if the ideal is ambiguous, (in which case $I = I' = [Q_0, -P_0 + \sqrt{D}]$), P_0 is unique since we are restricted to the choice of $P_0 = |Q_0|/2$ in this case by the *strict* inequality $-|Q_0|/2 < P_0$.

Therefore, $y = (x_0 + y_0P_0)/Q_0$. Plugging this value of y into Equation (11), we get $x = (x_0P_0 + Dy_0)/Q_0$. \square

Since α_0 is a proper solution of Equation (8) with $Q = Q_0$, then we necessarily have the following.

Corollary 3 $I_{\alpha_0} \sim 1$.

Proof. Since $I_{\alpha_0} = (\alpha'_0)[Q_0/\alpha'_0, \alpha] \sim [\alpha_0, \alpha]$, then $I_{\alpha_0} \sim [\alpha_0, \alpha]$. However, $y\alpha_0 - y_0\alpha = 1$, so $[\alpha_0, \alpha] \sim 1$. Hence, $I_{\alpha_0} \sim 1$. In fact, $I_{\alpha_0} = (\alpha'_0)$, since $[\alpha_0, \alpha] = (1) = \mathcal{O}_\Delta$. \square

Proposition 1 motivates the following definition.

Definition 5 *If $\alpha_0 \in \mathcal{O}_\Delta$ is primitive, then the **unique ideal corresponding to α_0** is given by $I_{\alpha_0} = [Q_0, P_0 + \sqrt{D}]$, as determined by Proposition 1.*

This unique ideal, associated with a given solution of Equation (8), provides the anchor for an application of the continued fraction algorithm, Theorem 3, and so will provide the genesis for the complete solutions of Equation (8) via continued fractions. Since we will be discussing several different continued fraction expansions of various quadratic irrationals, we need to set some notation. We do this in the following.

Convention 2 *In what follows, $I_{\alpha_0} = [Q_0, P_0 + \sqrt{D}]$ shall denote the ideal established in Definition 5, and it will be assumed throughout to have principal reduction index n . Furthermore, it will be understood that the symbols $A_i, B_i, P_i, Q_i, a_i, n$, etc. will denote those values arising from the simple continued fraction expansion of $(P_0 + \sqrt{D})/Q_0$. Also, we set $\gamma_i = (P_i + \sqrt{D})/Q_i$ ($i \geq 0$) in that continued fraction expansion. Moreover, we use the tilde notation for the values arising from the simple continued fraction expansion of $P_n + \sqrt{D} = \tilde{\gamma}_0$. Thus, we have for example $\tilde{A}_i, \tilde{B}_i, \tilde{P}_i, \tilde{Q}_i, \tilde{a}_i$ etc. Finally, we use the symbols $\ddot{A}_i, \ddot{B}_i, \ddot{P}_i, \ddot{Q}_i, \ddot{a}_i$, etc. for the values arising from the simple continued fraction expansion of $-\alpha'_0 = (-P_0 + \sqrt{D})/Q_0$, in other words, from the unique ideal $I_{-\alpha'_0}$ corresponding to $-\alpha'_0$, which we will assume throughout to have principal reduction index \ddot{n} .*

Proposition 1 is a generalization of the result [6, Lemma 3, p. 194], which actually masks the connection between the ideal theory and the continued fraction algorithm called the *infrastructure* by Dan Shanks (see [1, Chapters 7-8, pp. 223-266]). The following example will motivate our further development of this connection. Furthermore, this example begins our trek into learning how to use the continued fraction algorithm, Theorem 3, to get a continued fraction expansion of \sqrt{D} in which all solutions of Equation (8) will be convergents.

Example 3 *If we look back at Examples (1) – (2), we see that $\alpha_0 = -5 + 2\sqrt{13}$ is a proper solution of Equation (9). The unique ideal corresponding to α_0 is given by $I_{\alpha_0} = [-27, -11 + \sqrt{13}]$ (where the α of Proposition 1 is given by $\alpha = x + y\sqrt{13} = -3 + \sqrt{13}$). In Example 1 we displayed the simple continued fraction expansion of $(-11 + \sqrt{13})/(-27)$, where the principal reduction index is $n = 5$. Furthermore, this means that $(-11 + \sqrt{13})/(-27) = \langle 0, 3, 1, 1, 1, \overline{6}, 1, 1, 1, 1 \rangle = \langle 0, 3, 1, 1, 1, 3 + \sqrt{13} \rangle$. By Equation (7),*

$$(-11 + \sqrt{13})/(-27) = \frac{A_4(3 + \sqrt{13}) + A_3}{B_4(3 + \sqrt{13}) + B_3}.$$

Hence,

$$\begin{aligned} \sqrt{13} &= -27 \frac{A_4(3 + \sqrt{13}) + A_3}{B_4(3 + \sqrt{13}) + B_3} + 11 = \\ &= \frac{(-27A_4 + 11B_4)(3 + \sqrt{13}) - 27A_3 + 11B_3}{B_4(3 + \sqrt{13}) + B_3}. \end{aligned}$$

This shows the relationship between the continued fraction expansion of $\sqrt{13}$ and that of α_0 .

Example 3 motivates the following definition of some well-known sequences related to Equations (5)-(6) (see [1, Exercise 2.1.2, pp. 54-56]).

Definition 6 *Given a quadratic irrational $\alpha = (P + \sqrt{D})/Q \in \mathcal{O}_\Delta$ with $\alpha = \langle a_0; a_1, a_2, \dots \rangle$, set*

$$G_{i-1} = Q_0 A_{i-1} - P_0 B_{i-1} \quad (i \geq -1). \quad (12)$$

Then

$$N[(G_{i-1} + B_{i-1}\sqrt{D})] = (-1)^i Q_i Q_0 \quad (i \geq 0), \quad (13)$$

where the sequences $\{A_i\}$ and $\{B_i\}$ arise from the continued fraction expansion of α via Equations (5) – (6). Also, if $\delta_{m-1} = \prod_{i=1}^m (P_i + \sqrt{D})/Q_i$, then

$$\delta_{m-1} = (G_{m-1} + B_{m-1}\sqrt{D})/Q_m. \quad (14)$$

Also, we have:

$$G_{i-1} = P_i B_{i-1} + Q_i B_{i-2} \quad (i \geq 0), \quad (15)$$

$$DB_{i-1} = P_i G_{i-1} + Q_i G_{i-2} \quad (i \geq 0), \quad (16)$$

and

$$G_i = a_i G_{i-1} + G_{i-2} \quad (i \geq 0). \quad (17)$$

Now we may examine Example 3 in light of the above.

Example 4 Notice that in Example 3, $Q_0 = -27, P_0 = -11$, and $n = l(\sqrt{13}) = l = 5$, so

$$\sqrt{13} = \frac{G_{lm+n-1}(3 + \sqrt{13}) + G_{lm+n-2}}{B_{lm+n-2}(3 + \sqrt{13}) + B_{lm+n-2}} \quad (m \geq 0).$$

Since $Q_{lm+n} = 1$, and Equation (13) tells us that

$$N(G_{lm+n-1} + B_{lm+n-1}\sqrt{13}) = (-1)^{lm+n}(-27),$$

then we get a solution of Equation (9) exactly when $lm + n$ is even, i.e. when m is odd. The first such value is therefore $lm + n - 1 = 9$, and $G_9 + B_9\sqrt{13} = 1435 + 398\sqrt{13}$. Now, if we look back to Example 2, we see that $\epsilon_{\Delta}^2 \alpha_0 = 1435 + 398\sqrt{13}$, the first positive associate of α_0 . In fact, the positive associates of α_0 are exactly the $G_{9+10j} + B_{9+10j}\sqrt{D}$ for all $j \geq 0$. We will establish this phenomenon as a general fact below.

In order to classify all solutions of Equation (8) via convergents in continued fraction expansions, we first need to establish a preliminary fact. We refer the reader to Convention 2 for notation.

The following links Definition 6 with fundamental units. This will provide us with a means of linking up the continued fraction expansion of \sqrt{D} with that of $(P_0 + \sqrt{D})/Q_0$.

Proposition 2 For any positive $m \in \mathbf{Z}$,

$$\epsilon_{\Delta}^m = \tilde{G}_{lm-1} + \tilde{B}_{lm-1}\sqrt{D},$$

(and so $\epsilon_{\Delta}^{-m} = \tilde{G}_{lm-1} - \tilde{B}_{lm-1}\sqrt{D}$).

Proof. See [1, Theorem 2.1.3, p. 51] and [1, Exercise 2.1.2, pp. 54-56]. \square

Using Proposition 2, we can now show that certain of the δ_i described in Definition 6 are always associates of α_0 for a given fundamental solution α_0 .

Proposition 3 If α_0 is a proper solution of Equation (8) which the fundamental solution in its class, $k(m) = lm+n-1$ and $\ddot{k}(m) = lm+\ddot{n}-1$ ($m \in \mathbf{Z}$) (in the negative conjugate), then:

- (1) If $\delta_{k(m)} = G_{k(m)} + B_{k(m)}\sqrt{D} \neq \alpha_0$, then $\delta_{k(m)}$ is a positive associate of α_0 for any non-negative $m \in \mathbf{Z}$ such that $k(m)$ is odd.
- (2) If $\ddot{\delta}_{\ddot{k}(m)} = \ddot{G}_{\ddot{k}(m)} + \ddot{B}_{\ddot{k}(m)}\sqrt{D} \neq \alpha_0$, then $-\ddot{\delta}_{\ddot{k}(m)}$ is a negative associate of α_0 for any non-negative $m \in \mathbf{Z}$ such that $\ddot{k}(m)$ is odd.

Proof. First we prove (1). To establish that $\delta_{k(m)}$ is a solution associated with α_0 , we invoke Remark 4. Since $k(m)$ is odd and $Q_{k(m)+1} = 1$ for all non-negative $m \in \mathbf{Z}$, then $\delta_{k(m)}$ is a proper solution of Equation (8) via Equation (13). Thus, we need only show that both

$$(x_0G_{k(m)} - y_0B_{k(m)}D)/Q_0 = E \in \mathbf{Z},$$

and

$$(y_0G_{k(m)} - x_0B_{k(m)})/Q_0 = F \in \mathbf{Z}.$$

By Proposition 1,

$$x_0P_0 = Q_0(x_0P_0 + Dy_0)/Q_0 - y_0D = Q_0x - y_0D.$$

Therefore, multiplying both sides by $B_{k(m)}$ and using Equation (12), we get:

$$x_0A_{k(m)}Q_0 - x_0G_{k(m)} = Q_0xB_{k(m)} - y_0DB_{k(m)},$$

so by rearranging,

$$(x_0G_{k(m)} - y_0DB_{k(m)})/Q_0 = x_0A_{k(m)} - xB_{k(m)}.$$

In other words, $E = x_0A_{k(m)} - xB_{k(m)} \in \mathbf{Z}$.

Similarly, by Proposition 1:

$$y_0P_0B_{k(m)} = yQ_0B_{k(m)} - x_0B_{k(m)}.$$

Again, using Equation (12):

$$y_0A_{k(m)}Q_0 - y_0G_{k(m)} = yQ_0B_{k(m)} - x_0B_{k(m)}.$$

After rearranging we get:

$$F = (y_0G_{k(m)} - x_0B_{k(m)})/Q_0 = y_0A_{k(m)} - yB_{k(m)} \in \mathbf{Z}.$$

We have demonstrated that all of the $\delta_{k(m)}$ are associates of α_0 . We now show that these associates must be positive. Suppose that $\epsilon_{\Delta}^{-i}\alpha_0 = \delta_{k(m)}$ for some $i > 0$ (where i is even if $N(\epsilon_{\Delta}) = -1$; see footnote 9), and some non-negative $m \in \mathbf{Z}$.

Since $\epsilon_{\Delta}^{-i} = \tilde{G}_{il-1} - \tilde{B}_{il-1}\sqrt{D}$ by Proposition 2 then,

$$G_{k(m)} = x_0\tilde{G}_{il-1} - y_0\tilde{B}_{il-1}D, \quad (18)$$

and

$$B_{k(m)} = y_0\tilde{G}_{il-1} - x_0\tilde{B}_{il-1}. \quad (19)$$

Multiplying Equation (18) by \tilde{B}_{il-1} and adding \tilde{G}_{il-1} times Equation (19), we get:

$$y_0 = \tilde{G}_{il-1}B_{k(m)} + \tilde{B}_{il-1}G_{k(m)}.$$

However,

$$\tilde{B}_j \geq \tilde{B}_{j-1} \geq 0, \quad \tilde{G}_j > \tilde{G}_{j-1} > 0$$

for all $j \geq 0$ and $B_{k(m)} > 0, G_{k(m)} > 0$ for all $k(m) \geq 0$, (for example see [1, Exercise 2.1.2(g), pp. 55]). Hence,

$$y_0 > \tilde{G}_{l(i-1)-1}B_{k(m)} + \tilde{B}_{l(i-1)-1}G_{k(m)} = v > 0.$$

However, if

$$u = \tilde{G}_{l(i-1)-1}G_{k(m)} + \tilde{B}_{l(i-1)-1}B_{k(m)}D,$$

then

$$\epsilon_{\Delta}^{-1}\alpha_0 = \epsilon_{\Delta}^{i-1}\delta_{k(m)} = u + v\sqrt{D}$$

is an associate of α_0 . Thus, by the minimality of y_0 , $v \geq y_0$, a contradiction. This secures (1).

By (1), $\ddot{\delta}_{\ddot{k}(m)}$ is a positive associate of $-\alpha'_0$, so there exists a positive $i \in \mathbf{Z}$ such that $\epsilon_\Delta^i(-\alpha'_0) = \ddot{\delta}_{\ddot{k}(m)}$. Hence, $-\ddot{\delta}'_{\ddot{k}(m)}$ is a negative associate of α_0 . This secures (2) and so the entire result. \square

Proposition 3 showed that all $\delta_{k(m)}$ are positive associates of α_0 . Now we show that the $\delta_{k(m)}$ are *all* of the positive associates of the minimum $\delta_{k(m)}$ possible for which $k(m)$ is odd, together with the related result for negative associated solutions, and that α_0 is either $\gamma_{k(m_0)}$ or $-\gamma'_{\ddot{k}(\ddot{m}_0)}$. This guarantees that we have a means of generating all solutions of Equation 8.

Theorem 5 *Suppose that α_0 is a proper solution of Equation (8), such that α_0 is fundamental in its class, $k(m) = lm + n - 1$, and $\ddot{k}(m) = lm + \ddot{n} - 1$, for any non-negative $m \in \mathbf{Z}$. Then each of the following must hold.*

- (1) *If $m = m_0$ is the least non-negative integer such that $k(m)$ is odd, then all positive associates of $\delta_{k(m_0)} = G_{k(m_0)} + B_{k(m_0)}\sqrt{D}$ are given by $\delta_{k(m)} = G_{k(m)} + B_{k(m)}\sqrt{D}$, for all $m > m_0$ such that $k(m)$ is odd.*
- (2) *All negative associates of $\delta_{k(m_0)}$ are given by $-\ddot{\delta}'_{\ddot{k}(m)} = -\ddot{G}_{\ddot{k}(m)} + \ddot{B}_{\ddot{k}(m)}\sqrt{D}$ for all $m \geq \ddot{m}_0$ such that $\ddot{k}(m)$ is odd, where $m = \ddot{m}_0$ is the least non-negative integer such that $\ddot{k}(m)$ is odd.*
- (3) *If $\alpha_0 \neq \delta_{k(m_0)}$, then $\alpha_0 = -\ddot{\delta}'_{\ddot{k}(\ddot{m}_0)}$.*

Proof. First we prove (1), which we treat by cases.

Case 1. Assume that n is even, and l is odd.

In this case $m_0 = 0$. Thus, we wish to show that

$$\epsilon_\Delta^m \delta_{n-1} = \delta_{k(m)}$$

for all even $m > 0$.

Suppose that $\epsilon_\Delta^{-m} \delta_{k(m)} = u + v\sqrt{D}$. Then by Proposition 2,

$$\epsilon_\Delta^{-m} = \tilde{G}_{lm-1} - \tilde{B}_{lm-1}\sqrt{D},$$

for all positive $m \in \mathbf{Z}$. Thus:

$$u = \tilde{G}_{lm-1}G_{k(m)} - \tilde{B}_{lm-1}B_{k(m)}D, \quad (20)$$

and

$$v = \tilde{G}_{lm-1}B_{k(m)} - \tilde{B}_{lm-1}G_{k(m)}. \quad (21)$$

First, we concentrate upon showing that $v = B_{n-1}$. From Equation (15), together with the facts that $\tilde{P}_{lm} = P_{lm+n} = \lfloor \sqrt{D} \rfloor$,¹² and $\tilde{Q}_{lm} = 1 = Q_{k(m)+1}$ for all $m > 0$, Equation (21) becomes:

$$v = (\lfloor \sqrt{D} \rfloor \tilde{B}_{lm-1} + \tilde{B}_{lm-2})B_{k(m)} - \tilde{B}_{lm-1}(\lfloor \sqrt{D} \rfloor B_{k(m)} - B_{k(m)-1}),$$

which simplifies to:

$$v = \tilde{B}_{lm-2}B_{k(m)} - \tilde{B}_{lm-1}B_{k(m)-1}. \quad (22)$$

From Equation (6), Equation (22) becomes:

$$v = \tilde{B}_{lm-2}(a_{k(m)}B_{k(m)-1} + B_{k(m)-2}) - (\tilde{a}_{lm-1}\tilde{B}_{lm-2} + \tilde{B}_{lm-3})B_{k(m)-1},$$

which, by the fact that $\tilde{a}_{lm-i} = a_{lm+n-i} = a_{k(m)-i+1}$ for all positive $i \leq lm$ and even $m > 0$, simplifies to:

$$v = \tilde{B}_{lm-2}B_{k(m)-2} - \tilde{B}_{lm-3}B_{k(m)-1}. \quad (23)$$

Again, using the aforementioned facts, we get that Equation (23) becomes:

$$\begin{aligned} v &= (\tilde{a}_{lm-2}\tilde{B}_{lm-3} + \tilde{B}_{lm-4})B_{k(m)-2} - \tilde{B}_{lm-3}(a_{k(m)-1}B_{k(m)-2} + B_{k(m)-3}) \\ &= \tilde{B}_{lm-4}B_{k(m)-2} - \tilde{B}_{lm-3}B_{k(m)-3}. \end{aligned}$$

Continuing in this fashion, we get, for any positive $i \leq lm/2 + 1$ and even $m > 0$, that:

$$v = \tilde{B}_{lm-2i}B_{k(m)-2i+2} - \tilde{B}_{lm-2i+1}B_{k(m)-2i+1}.$$

¹²In order to see that $P_{lm+n} = \lfloor D \rfloor$ for $m > 0$, we invoke [1, Theorem 2.1.2, Claims 3-4, p.45] to get that $\delta_{lm+n} = \delta_{l+n} = P_{l+n} + \sqrt{D}$ is reduced for all $m \geq 1$. Therefore, by Remark 1, $-1 < P_{l+n} - \sqrt{D} < 0$, i.e. $P_{l+n} = \lfloor D \rfloor$.

In particular, if $i = lm/2 + 1$, then

$$v = \tilde{B}_{-2}B_{n-1} - \tilde{B}_{-1}B_{n-2} = B_{n-1}.$$

To get that $u = G_{n-1}$, we use similar facts and reasoning. First we note, that from Equations (15)-(16), Equation (20) becomes (for $m > 0$ even):

$$u = \tilde{G}_{lm-1}(\lfloor \sqrt{D} \rfloor B_{k(m)} + B_{k(m)-1}) - (\lfloor \sqrt{D} \rfloor \tilde{G}_{lm-1} + \tilde{G}_{lm-2})B_{k(m)},$$

which simplifies to:

$$u = \tilde{G}_{lm-1}B_{k(m)-1} - \tilde{G}_{lm-2}B_{k(m)}. \quad (24)$$

Using Equations (6) and (17), we get that Equation (24) becomes

$$u = (\tilde{a}_{lm-1}\tilde{G}_{lm-2} + \tilde{G}_{lm-3})B_{k(m)-1} - \tilde{G}_{lm-2}(a_{k(m)}B_{k(m)-1} + B_{k(m)-2}),$$

which simplifies to

$$u = \tilde{G}_{lm-3}B_{k(m)-1} - \tilde{G}_{lm-2}B_{k(m)-2}.$$

Again, using Equations (6) and (17), we get that this becomes:

$$u = \tilde{G}_{lm-3}B_{k(m)-3} - \tilde{G}_{lm-4}B_{k(m)-2}.$$

Continuing in this fashion, we get that, for any positive $i \leq lm/2$, and odd $m > 0$,

$$u = \tilde{G}_{lm-2i+1}B_{k(m)+1-2i} - \tilde{G}_{lm-2i}B_{k(m)-2i+2}. \quad (25)$$

In particular, for $i = lm/2 + 1$,

$$u = \tilde{G}_{-1}B_{n-2} - \tilde{G}_{-2}B_{n-1} = B_{n-2} + B_{n-1}P_n = G_{n-1},$$

with the latter coming from Equation (15), since $\tilde{G}_{-2} = -\tilde{P}_0 = -P_n$ and $\tilde{G}_{-1} = \tilde{Q}_0 = 1 = Q_n$.

This establishes Case 1.

Case 2. n is odd and l is odd.

In this case $m_0 = 1$, so we seek to determine the positive associates of $\delta_{k(m_0)} = \delta_{l+n-1} = G_{l+n-1} + B_{l+n-1}\sqrt{D}$. These will now be shown to be the

$\epsilon_{\Delta}^{2t}\delta_{l+n-1} = \delta_{k(2t+1)}$ for all positive $t \in \mathbf{Z}$. We analyze $\epsilon_{\Delta}^{-2t}\delta_{k(2t+1)} = u + v\sqrt{D}$, as in Case 1 to get:

$$v = \tilde{B}_{2lt-2i}B_{k(2t+1)-2i+2} - \tilde{B}_{2t-2i+1}B_{k(2t+1)-2i+1},$$

for all positive $i \leq lt + 1$, and all positive $t \in \mathbf{Z}$. In particular, for $i = lt + 1$, we get:

$$v = \tilde{B}_{-2}B_{l+n-1} - \tilde{B}_{-1}B_{l+n-2} = B_{l+n-1}.$$

Similarly, we analyze as in Case 1 to get:

$$u = B_{k(2t+1)-2i+1}\tilde{G}_{2lt-2i+1} - B_{k(2t+1)-2i+2}\tilde{G}_{2lt-2i},$$

for any positive $i \leq lt + 1$ and any $t > 0$. In particular, for $i = lt + 1$:

$$u = B_{l+n-2}\tilde{G}_{-1} - B_{l+n-1}\tilde{G}_{-2} = B_{l+n-2} + P_n B_{l+n-1}.$$

Claim 1. $P_n = \lfloor \sqrt{D} \rfloor$.¹³

Since

$$G_{l+n-1}^2 - B_{l+n-1}^2 D = Q = N(\epsilon_{\Delta}^{-2t}\delta_{k(2t+1)}) = u^2 - v^2 D = u^2 - B_{n-1}^2 D,$$

then, $u = \pm G_{l+n-1}$. However, $u = B_{l+n-2} + P_n B_{l+n-1}$ and $G_{l+n-1} = B_{l+n-1} \lfloor \sqrt{D} \rfloor + B_{l+n-2}$. It is easy to show that $u = -G_{l+n-1}$ leads to a contradiction since $\gcd(B_{l+n-1}, B_{l+n-2}) = 1$ (see [1, Exercise 2.1.2(c), p. 54]). This establishes Claim 1 and Case 2 is secured via Equation (15).

Case 3. Both n and l are even.

In this case, $m_0 = 0, \delta_{k(0)} = G_{n-1} + B_{n-1}\sqrt{D}$, and we need to show that $\epsilon_{\Delta}^m \delta_{k(0)} = \delta_{k(m)}$ for all non-negative $m \in \mathbf{Z}$. As above, we analyze $\epsilon_{\Delta}^{-m} \delta_{k(m)} = u + v\sqrt{D}$. The exact same reasoning as in Case 1 holds, with no restriction on m this time. In this fashion, we get that $u = G_{n-1}$, and $v = B_{n-1}$.

Case 4. n is odd and l is even.

In this case, $lm + n$ is never even. We must show that this case cannot occur. If $x_0^2 - y_0^2 D = Q$, and n is odd, then $G_{n-1}^2 - B_{n-1}^2 D = (-1)^n Q = -Q$,

¹³This fails to be true in other cases. For instance look at Example 6 following. Therein, $n = 2, l = 5$ and $P_n = 2 \neq \lfloor \sqrt{D} \rfloor = 3$.

by Equation (13). However, by the continued fraction algorithm (see [1, Claim 2, p. 45]), we have the ideal equality:

$$I_{\alpha_0} = (x_0 - y_0\sqrt{D}) = (G_{n-1} - B_{n-1}\sqrt{D}).$$

Hence, $x_0 - y_0\sqrt{D} = u(G_{n-1} - B_{n-1}\sqrt{D})$ for some unit $u \in \mathcal{O}_\Delta$. However, by Theorem 4, $N(u) = 1$ since l is even. Therefore, $Q = N(x_0 - y_0\sqrt{D}) = N(G_{n-1} - B_{n-1}\sqrt{D}) = -Q$, a contradiction. This secures (1).

To prove (2), we need to establish the following.

Claim 2. $I_{\alpha_0} = I_{\delta_{k(m)}}$ for all $m \geq 0$ such that $k(m)$ is odd.

By Proposition 1, there exists a unique \bar{P}_0 such that

$$-|Q_0|/2 < \bar{P}_0 \leq |Q_0|/2$$

and $\bar{x}, \bar{y} \in \mathbf{Z}$ with

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

and

$$\bar{\alpha}\delta'_{k(m)} = (\bar{x} + \bar{y}\sqrt{D})(G_{k(m)} - B_{k(m)}\sqrt{D}) = \bar{P}_0 + \sqrt{D}.$$

Thus,

$$\bar{P}_0 = \bar{x}G_{k(m)} - \bar{y}B_{k(m)}D, \tag{26}$$

and

$$1 = \bar{y}G_{k(m)} - \bar{x}B_{k(m)}. \tag{27}$$

By simultaneously solving Equations (26)-(27), for \bar{x} , and \bar{y} we get:

$$\bar{x} = (G_{k(m)}\bar{P}_0 + B_{k(m)}D)/Q_0, \tag{28}$$

and

$$\bar{y} = (B_{k(m)}\bar{P}_0 + G_{k(m)})/Q_0. \tag{29}$$

Since a solution of Equations (28)-(29) is given by

$$\bar{x} = (G_{k(m)}P_0 + B_{k(m)}D)/Q_0,$$

and

$$\bar{y} = A_{k(m)}$$

with

$$\bar{P}_0 = P_0,$$

then by the uniqueness of \bar{P}_0 , these are the only solutions.¹⁴ This is Claim 2.

As a consequence of Claim 2, we have:

$$I_{\delta_{\ddot{k}(\ddot{m}_0)}} = I_{-\alpha_0} = I_{-\delta'_{k(m_0)}}.$$

Hence, by part (1), all positive associates of $-\delta'_{k(m_0)}$ are given by the $\delta_{\ddot{k}(m)}$ for all $m \geq 0$ such that $\ddot{k}(m)$ is odd. In other words, all negative associates of $\delta_{k(m_0)}$ are given by the $-\delta'_{\ddot{k}(m)}$. This is (2).

If $\delta_{k(m_0)} \neq \alpha_0$, then $\delta_{k(m_0)} = \epsilon_{\Delta}^i \alpha_0$ for some positive i , by Proposition 3. In other words, α_0 is a negative associate of $\delta_{k(m_0)}$. Hence, $\alpha_0 = -\delta'_{\ddot{k}(m)}$ for some $m \geq 0$ such that $\ddot{k}(m)$ is odd, by part 2. However, by the minimality of y_0 , and the fact that $\ddot{B}_{\ddot{k}(m)} \geq \ddot{B}_{\ddot{k}(\ddot{m}_0)}$ for all $m \geq \ddot{m}_0$, then $\alpha_0 = -\delta'_{\ddot{k}(\ddot{m}_0)}$, which is (3), and thus the whole result. \square

It is worth isolating the results of Case 4 in the above proof, since they are of interest in their own right.

Corollary 4 *If n (or \ddot{n}) is odd, then l must be odd. Also, if l is even, then there cannot be solutions of both $x^2 - Dy^2 = Q$ and $u^2 - Dv^2 = -Q$ for $x, y, u, v \in \mathbf{Z}$.*

We observe that Corollary 1 is an immediate consequence of Theorem 5. In fact, this is just the case where $n = 0$. To see this we observe that, when $Q_0 = 1$, $P_0 = 0$, and l is even, then $G_{k(m)} = A_{k(m)} = A_{lm-1}$. Thus, the $A_{lm-1} + B_{lm-1}\sqrt{D}$ are all the solutions of Pell's equation $x^2 - Dy^2 = 1$. Indeed, Proposition 2 gives us that $\epsilon_{\Delta}^m = A_{lm-1} + B_{lm-1}\sqrt{D}$ since $A_{lm-1} = \tilde{A}_{lm-1}$ and $B_{lm-1} = \tilde{B}_{lm-1}$ ($m \geq 1$) in this case. To see how this fits into our scheme more clearly, we note that, by Proposition 1, if $\epsilon_{\Delta} = x_0 + y_0\sqrt{D}$, then $P_0 = 0$, $x = Dy_0$, and $y = x_0$. Here $x_0 = A_{l-1}$ and $y_0 = B_{l-1}$.

If $Q_0 = -1$, then l is odd, and Theorem 5 differs from Corollary 1 in its presentation since we allow for negative Q_0 , and its associated unique ideal via Proposition 1. This makes our presentation more palatable since we always have a unique continued fraction expansion to associate with the given solution. In our case, all positive solutions of $x^2 - Dy^2 = -1$ are given by $G_{k(m)} + B_{k(m)}\sqrt{D}$ for any $m \geq 0$ such that $k(m)$ is odd. For instance we have the following.

¹⁴This \bar{x} is, in turn, equal to $P_0 A_{k(m)} + Q_{-1} B_{k(m)}$, where $D = P_0^2 + Q_0 Q_{-1}$.

Example 5 Consider $\Delta = 4 \cdot 17$. The continued fraction expansion arising from $-\sqrt{17}$ is :

i	0	1	2	3	4
P_i	0	5	3	4	4
Q_i	-1	8	1	1	1
a_i	-5	1	7	8	8

Hence, $n = 2$, $l = 1$ and $k(m_0) = 1$ for $m_0 = 0$. Also, $G_1 = 4$, and $B_1 = 1$, with

$$\begin{aligned} \epsilon_\Delta &= G_1 + B_1\sqrt{D} = \prod_{i=1}^{k(m_0)+1} (P_i + \sqrt{D})/Q_i = \prod_{i=1}^l (\tilde{P}_i + \sqrt{D})/\tilde{Q}_i \\ &= \tilde{G}_{l-1} + \tilde{B}_{l-1}\sqrt{D} = \tilde{G}_0 + \tilde{B}_0\sqrt{D} = 4 + \sqrt{17}. \end{aligned}$$

Finally, we observe that:

$$\epsilon_\Delta^m = \prod_{i=1}^{m+1} (P_i + \sqrt{D})/Q_i,$$

for any $m \geq 2$ since $(P_i + \sqrt{D})/Q_i = 4 + \sqrt{D}$ for all $i \geq 3$.

Now we bring in the connection with a continued fraction expansion of \sqrt{D} . We need to motivate this by referring back to an earlier example.

Example 6 Looking back to Example 2, we see that another class of solutions to Equation (9) is given by the fundamental solution $-\alpha'_0 = 5 + 2\sqrt{13}$. We now look at the unique ideal corresponding to $-\alpha'_0$, namely $I_{-\alpha'_0} = [-27, 11 + \sqrt{13}]$, where the α of Proposition 1 is $x + y\sqrt{13} = -3 - \sqrt{13}$. The continued fraction expansion of $(11 + \sqrt{13})/(-27)$ is given as follows:

i	0	1	2	3	4	5	6	7	8	9	10	11
\tilde{P}_i	11	16	2	3	1	2	1	3	3	1	2	1
\tilde{Q}_i	-27	9	1	4	3	3	4	1	4	3	3	4
\tilde{a}_i	-1	2	5	1	1	1	1	6	1	1	1	1

Notice that $\ddot{n} = 2$ for $I_{-\alpha'_0}$ and $-\alpha'_0 = \ddot{G}_1 + \ddot{B}_1\sqrt{D} = 5 + 2\sqrt{13} = \ddot{\delta}_{\ddot{k}(\ddot{m}_0)}$ since $\ddot{m}_0 = 0$. Also, $\alpha_0 = -\ddot{\delta}'_1 = -\ddot{G}_1 + \ddot{B}_1\sqrt{D} = -5 + 2\sqrt{13}$, since $\alpha_0 \neq \delta_{k(m)}$ for any $m \geq 0$. In fact, $\delta_{k(m_0)} = G_9 + B_9\sqrt{D} = 1435 + 398\sqrt{13} = \epsilon_\Delta^2 \alpha_0$ since $n = 5$ for I_{α_0} , thereby making $k(m_0) = lm_0 + n - 1 = 5 \cdot 1 + 5 - 1 = 9$ the minimum value for $k(m)$ to be odd. The next positive associate of α_0 is:

$$\delta_{19} = G_{19} + B_{19}\sqrt{D} = 1862635 + 516602\sqrt{13} = \epsilon_\Delta^2 \delta_{k(m_0)} = \epsilon_\Delta^4 \alpha_0.$$

Thus we see that all positive associates of α_0 are the $\delta_{k(m+1)} = G_{k(m+1)} + B_{k(m+1)}\sqrt{13} = \epsilon_\Delta^m \alpha_0$ for all even $m > 0$. This is case 2 of Theorem 5.

Similarly, by Theorem 5, the $-\ddot{\delta}'_{\ddot{k}(m)}$ are negative associates of α_0 , and by Theorem 5 all positive associates of $-\alpha'_0$ are the $\ddot{\delta}_{\ddot{k}(m)}$ for all m such that $\ddot{k}(m) = 5m + 1$ is odd, so m is even. The first positive associate of $-\alpha'_0 = \ddot{\delta}_{\ddot{k}(\ddot{m}_0)}$ is $\epsilon_\Delta^2(-\alpha'_0) = \ddot{G}_{11} + \ddot{B}_{11}\sqrt{13} = \ddot{\delta}_{\ddot{k}(2)} = 7925 + 2198\sqrt{13}$. In general, $\epsilon_\Delta^m(-\alpha'_0) = \ddot{\delta}_{\ddot{k}(m)}$, so $\epsilon_\Delta^{-m} \alpha_0 = -\ddot{\delta}'_{\ddot{k}(m)}$ for any even $m > 0$. Therefore, we have all of the negative associates of α_0 in this fashion. The first occurs for $m = 2$, namely, $\epsilon_\Delta^{-2} \alpha_0 = -7925 + 2198\sqrt{13}$.

The only other possible fundamental solution of Equation (9) is $12 + 3\sqrt{13}$. However, this is not a proper solution. Hence, all proper solutions of $x^2 - 13y^2 = -27$ are given by total of the $\pm G_{k(m)} + B_{k(m)}\sqrt{D}$ for all $m \geq 0$ such that $k(m)$ is odd, and the $\pm \ddot{G}_{\ddot{k}(m)} + \ddot{B}_{\ddot{k}(m)}\sqrt{D}$ for all $m \geq 0$ such that $\ddot{k}(m)$ is odd.

Example 6 suggests the following which is immediate from Theorem 5.

Theorem 6 All proper solutions of Equation (8) are given by the values $\pm G_{k(m)} + B_{k(m)}\sqrt{D}$ for all $m \geq 0$ such that $k(m)$ is odd, and the $\pm \ddot{G}_{\ddot{k}(m)} + \ddot{B}_{\ddot{k}(m)}\sqrt{D}$ for all $m \geq 0$ such that $\ddot{k}(m)$ is odd, as we allow the α_0 to range over all fundamental proper solutions of Equation (8) .

Now that we have all solutions of Equation (8) via the infrastructure, we explain what is behind the work of Zhang [4]-[6] wherein solutions are listed as convergents in a *semi-simple* continued fraction expansion of \sqrt{D} .

Lemma 1 Suppose that $\alpha_0 = x_0 + y_0\sqrt{D} \in \mathcal{O}_\Delta$ is a primitive element such that $I_{\alpha_0} = [Q_0, P_0 + \sqrt{D}]$, and $n + lm \geq 1$. If $\gamma_0 = (P_0 + \sqrt{D})/Q_0 = \langle a_0; a_1, \dots \rangle$, then for any non-negative $m \in \mathbf{Z}$,

$$\sqrt{D} = \langle -P_{lm+n}; -a_{lm+n-1}, -a_{n+lm-2}, \dots, -a_1, -a_0 + \gamma_0 \rangle.$$

Furthermore, $P_{lm+n} = \lfloor \sqrt{D} \rfloor$ if $m > 0$.¹⁵

Proof. Since $\gamma_{i+1} = 1/(-a_i + \gamma_i)$ (see the proof of [1, Theorem 2.1.1, pp. 42-43], for instance), and $Q_{lm+n} = 1$, then $\gamma_{lm+n} = P_{lm+n} + \sqrt{D}$. Therefore,

$$\begin{aligned} \sqrt{D} &= \gamma_{lm+n} - P_{lm+n} = -P_{lm+n} + \frac{1}{-a_{lm+n-1} + \gamma_{lm+n-1}} = \\ &= -P_{lm+n} + \frac{1}{-a_{lm+n-1} + \frac{1}{-a_{lm+n-2} + \gamma_{lm+n-2}}} = \dots \end{aligned}$$

Hence,

$$\sqrt{D} = \langle -P_{lm+n}; -a_{lm+n-1}, -a_{lm+n-2}, \dots, -a_1, -a_0 + \gamma_0 \rangle.$$

To see that $P_{lm+n} = \lfloor D \rfloor$ for $m > 0$, we invoke footnote 12. This completes the proof. \square

Lemma 1 motivates the following.

Definition 7 *The continued fraction expansion of \sqrt{D} (for $lm + n \geq 1$), in Lemma 1 is called **the (lm+n)th continued fraction expansion of \sqrt{D}** arising from I_{α_0} , which is uniquely determined by l , m , and n since the simple continued fraction expansion of γ_0 , upon which this expansion is based, is uniquely determined by Theorem 3.*

At this juncture, we must ensure that we can distinguish between the values arising from Equations (1)-(7), in comparisons of the continued fraction expansions of \sqrt{D} via Definition 7, and that of others defined above. We need to set some notation. We do this as follows.

Convention 3 *We use the hat notation to denote values arising from the continued fraction expansion of \sqrt{D} as given in Definition 7, such as \hat{A}_i , and $\hat{\delta}_i$.*

With this notation in place we have the following result from Lemma 1.

¹⁵If γ_n is reduced, then $P_n = \lfloor \sqrt{D} \rfloor$ as well. However, as observed in Remark 3, it is possible for I_{n+1} to be reduced without γ_n being reduced (see Example 6 for instance).

Corollary 5 For the $(lm + n)$ th continued fraction expansion of \sqrt{D} given in Lemma 1, we have $\hat{P}_i = -P_{lm+n+1-i}$ for $1 \leq i \leq lm + n$ with $\hat{P}_0 = 0$, and $\hat{Q}_i = Q_{lm+n-i}$ for $1 \leq i \leq lm + n$ with $\hat{Q}_0 = 1$.

Proof. Since $\hat{Q}_0 = 1 = Q_{lm+n}$, and $\hat{a}_0 = \hat{P}_1 = -P_{lm+n}$, then

$$D = \hat{P}_1^2 + \hat{Q}_1 = P_{lm+n}^2 + Q_{lm+n-1},$$

so $\hat{Q}_1 = Q_{lm+n-1}$. As induction hypothesis, assume $\hat{P}_i = -P_{lm+n+1-i}$ and $\hat{Q}_i = Q_{lm+n-i}$ whenever $1 \leq i < lm + n$. Since we also have established that $\hat{a}_i = -a_{lm+n-i}$, whenever $1 \leq i < lm + n$, then

$$\hat{P}_{lm+n} = \hat{a}_{lm+n-1}\hat{Q}_{lm+n-1} - \hat{P}_{lm+n-1} = -a_1Q_1 + P_2 = -P_1.$$

Also,

$$\hat{Q}_{lm+n} = (D - \hat{P}_{lm+n}^2)/\hat{Q}_{lm+n-1} = (D - P_1^2)/Q_1 = Q_0.$$

This completes the proof. \square

We observe that Equations (5)-(6) hold for the \hat{A}_i and \hat{B}_i despite the fact that the partial quotients are negative. We must caution the reader that although the continued fraction expansion of \sqrt{D} as given in Definition 7 satisfies Equations (1)-(3) and (5)-(7), it does *not* respect Equation (4). The reason is that the values of the partial quotients a_i are positive for all $i \geq 1$ in the simple continued fraction expansion of any quadratic irrational. This is implicit in Theorem 3. In point of fact, the use of the floor of an integer as the definition of the partial quotient in Equation (4) is precisely what keeps those partial quotients positive (for all $i \geq 1$) in the *simple* continued fraction expansion of a given quadratic irrational. However, our continued fraction expansion of \sqrt{D} , as given in Definition 7, has negative partial quotients. Thus, the equation $\hat{a}_i = (\hat{P}_{i+1} + \hat{P}_i)/\hat{Q}_i$ is the one which applies in this case. The following illustrates this process.

Example 7 By Lemma 1, we get that

$$\sqrt{13} = \langle -3; -1, -1, -1, -3, (-11 + \sqrt{13})/(-27) \rangle.$$

The corresponding table is :

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
\hat{P}_i	0	-3	-1	-2	-1	-11	11	1	2	1	3	3	1	2	1	3
\hat{Q}_i	1	4	3	3	4	-27	4	3	3	4	1	4	3	3	4	1
\hat{a}_i	-3	-1	-1	-1	-3	0	3	1	1	1	6	1	1	1	1	6

In the above table, columns 5-15 are given by Equations (1) – (4), as in Example 1. However, in columns 0-4, Equation (4) fails. Instead we use $\hat{a}_i = (\hat{P}_{i+1} + \hat{P}_i)/\hat{Q}_i$, as determined by Equation (3).

The above motivates the following criterion.

Lemma 2 *Suppose that $\alpha_0 = x_0 + y_0\sqrt{D} \in \mathcal{O}_\Delta$ is a primitive element, and $k(m) = lm + n - 1$ for any non-negative $m \in \mathbf{Z}$ such that $k(m)$ is odd, then the following are equivalent.*

- (1) α_0 is a proper solution of Equation (8).
- (2) $Q = Q_0 = \hat{Q}_{k(m)+1}$.
- (3) $\hat{A}_{k(m)}^2 - \hat{B}_{k(m)}^2 D = Q = Q_0$.
- (4) $G_{k(m)}^2 - B_{k(m)}^2 D = Q = Q_0$.

Proof. Implicit in the hypotheses of (2)-(4), is the existence of I_{α_0} which guarantees (1) via Proposition 1. Hence, we have that (2) \Rightarrow (1), (3) \Rightarrow (1), and (4) \Rightarrow (1).

If (1) holds, then by Corollary 5, $Q = Q_0 = \hat{Q}_{lm+n}$ for any non-negative $m \in \mathbf{Z}$. Thus, (1) \Rightarrow (2). Also, if (1) holds, then $\hat{P}_0 = 0$, $\hat{Q}_0 = 1$ and so $\hat{G}_i = \hat{A}_i$ ($i \geq -2$). Since $\hat{Q}_{k(m)+1} = Q_0 = Q$ by Corollary 5, then $\hat{A}_{k(m)}^2 - \hat{B}_{k(m)}^2 D = Q$, by Equation (13). In other words, (1) \Rightarrow (3).

Finally, since $Q_{k(m)+1} = Q_n = 1$, then by Equation (13), we have that (1) \Rightarrow (4). \square

There is something stronger which is contained within Lemma 2. We isolate this as follows.

Corollary 6 *With the hypothesis as in Lemma 2, we have that $\hat{A}_{k(m)} = G_{k(m)}$ and $\hat{B}_{k(m)} = -B_{k(m)}$.*

Proof. By Equation (15), $G_{k(m)}/B_{k(m)} = P_{k(m)} + B_{k(m)-1}/B_{k(m)}$. Thus, by [1, Exercise 2.1.1(c), p.54],

$$\begin{aligned} G_{k(m)}/B_{k(m)} &= P_{k(m)+1} + 1/\langle a_{k(m)}; a_{k-1}, \dots, a_2, a_1 \rangle \\ &= \langle P_{k(m)+1}; a_{k(m)}, a_{k-1}, \dots, a_1 \rangle. \end{aligned}$$

Hence, $-G_{k(m)}/B_{k(m)} = \langle -P_{k(m)+1}; -a_{k(m)}, -a_{k-1}, \dots, -a_1 \rangle$, and so by [1, Exercise 2.1.2(b), p. 54], $\hat{A}_{k(m)}/\hat{B}_{k(m)} = -G_{k(m)}/B_{k(m)}$. Thus, $\hat{A}_{k(m)}B_{k(m)} = -\hat{B}_{k(m)}G_{k(m)}$. Since $\gcd(\hat{A}_{k(m)}, \hat{B}_{k(m)}) = 1$ (see [1, Exercise 2.1.2(c), p. 54]), then $|B_{k(m)}| = |\hat{B}_{k(m)}|$ and $|\hat{A}_{k(m)}| = |G_{k(m)}|$. However, since $\hat{A}_{-1} = 1$, and $\hat{A}_0 = -P_{k(m)+1}$, then $\hat{A}_i < 0$ when $i > 0$ is even. Also, since $\hat{B}_{-1} = 0$, $\hat{B}_0 = 1$, and $\hat{B}_1 = -a_{k(m)}$ then $\hat{B}_i < 0$ when $i > 0$ is odd. Hence, given that $k(m)$ is odd, then $\hat{A}_{k(m)} = G_{k(m)}$ and $\hat{B}_{k(m)} = -B_{k(m)}$. \square

Now we link up the notion of convergents for these *new* continued fraction expansions of \sqrt{D} with the solutions which have already classified.

Definition 8 *If $\sqrt{D} = \langle b_0; b_1, \dots \rangle$ is the $(lm + n)$ th continued fraction expansion of \sqrt{D} as given in Definition 7, then $\hat{C}_{k(m)} = \hat{A}_{k(m)}/\hat{B}_{k(m)} = \langle b_0; b_1, \dots, b_{k(m)} \rangle$ is called the **k(m)th convergent** in the $(lm + n)$ th continued fraction expansion of \sqrt{D} arising from I_{α_0} .*

The above notion of convergent coincides with the notion given in Corollary 2. We may now summarize our findings in the following.

Theorem 7 *If $\alpha_0 = x_0 + y_0\sqrt{D}$ is a primitive element of \mathcal{O}_Δ such that $I_{\alpha_0} = [Q_0, P_0 + \sqrt{D}]$ has principal reduction index n , then the following are equivalent.*

- (1) α_0 is a proper solution of Equation (8).
- (2) *There exists a non-negative $m \in \mathbf{Z}$ such that either $x_0/y_0 = \pm\hat{C}_{k(m)} = \langle -P_{lm+n}; -a_{k(m)}, -a_{k(m)-1}, \dots, -a_1 \rangle$ in the $lm + n$ th continued fraction expansion of \sqrt{D} arising from I_{α_0} , or $x_0/y_0 = \pm\hat{C}_{\check{k}(m)}$ in the $lm + n$ th continued fraction expansion of \sqrt{D} arising from $I_{-\alpha'_0}$*
- (3) x_0/y_0 is one of the values $\pm G_{k(m)}/B_{k(m)}$ for some $m \geq 0$ such that $k(m)$ is odd, or one of the values $\pm\check{G}_{\check{k}(m)}/\check{B}_{\check{k}(m)}$ for some $m \geq 0$ such that $\check{k}(m)$ is odd.

Proof. By Theorem 6, we have the equivalence of (1) and (3). Also, from Corollaries 5 and 6 we have the equivalence of (1) and (2), since (in the case where $x_0 + y_0\sqrt{D} = \pm G_{k(m)} + B_{k(m)}\sqrt{D}$ for instance),

$$\hat{C}_{k(m)} = \hat{A}_{k(m)}/\hat{B}_{k(m)} = \langle \hat{a}_0; \hat{a}_1, \dots, \hat{a}_{k(m)} \rangle$$

$$= \langle -P_{lm+n}; -a_{k(m)}, -a_{k(m)-1}, \dots, -a_1 \rangle = -G_{k(m)}/B_{k(m)}.$$

The result now follows from Lemma 2. \square

Remark 5 *We now see that, via Corollary 6, all of the so-called semi-simple continued fractions are really just the values arising from the infrastructure as we have developed it herein. Furthermore, Zhang has given numerous results on the use of the semi-simple continued fractions applied to Richaud-Degert types of radicands (see [1, pp.77 – 95]). We do not analyze these results herein since they all follow in greater generality from our theory.*

We conclude with some illustrations of the latter results. The following illustrates Theorem 7

Example 8 *Let $\beta = 4936 + 1369\sqrt{13} = x_0 + y_0\sqrt{13}$ and $Q_0 = 3$. From Proposition 1, $P_0 = -1, x = 4287$, and $y = 1189$. Thus, the simple continued fraction expansion of $(-1 + \sqrt{13})/3$ is given by:*

i	0	1	2	3	4	5	6	7
P_i	-1	1	3	3	1	2	1	3
Q_i	3	4	1	4	3	3	4	1
a_i	0	1	6	1	1	1	1	6

so that $n = 2$ for I_β , and $l = 5$. Here, $G_{11} = 4936, B_{11} = 1369$, (observing that $I_{\alpha_0} = I_\beta$ where $\alpha_0 = 4 + \sqrt{13}$ by Claim 2 in the proof of Theorem 5, and $\epsilon_{\Delta}^2 \alpha_0 = \beta = \delta_{11} = \delta_{k(2)}$). We now show that $-4936/1369$ is the 11th convergent in the 12th continued fraction expansion of $\sqrt{13}$ arising from I_β , which is:

i	0	1	2	3	4	5	6	7	8	9	10	11	12
\hat{P}_i	0	-3	-1	-2	-1	-3	-3	-1	-2	-1	-3	-3	-1
\hat{Q}_i	1	4	3	3	4	1	4	3	3	4	1	4	3
\hat{a}_i	-3	-1	-1	-1	-1	-6	-1	-1	-1	-1	-6	-1	0

Here, $\hat{A}_{11} = 4936$ and $\hat{B}_{11} = -1369$, so

$$-4936/1369 = \hat{A}_{11}/\hat{B}_{11} = \langle -3; -1, -1, -1, -1, -6, -1, -1, -1, -1, -6, -1 \rangle$$

is the 11th convergent in the 12th continued fraction expansion of $\sqrt{13}$ arising from I_β .

Notice as well, in this example, that the class of β is not sufficient to get all solutions of $x^2 - 13y^2 = 3$. We cannot get $\tau = 256 + 71\sqrt{13}$ for instance. For this solution, we need $I_{-\beta'} = I_{-\delta'_{k(2)}} = [3, 1 + \sqrt{13}]$. The simple continued fraction expansion of $(1 + \sqrt{13})/3$ is:

i	0	1	2	3	4	5	6	7	8
\bar{P}_i	1	2	1	3	3	1	2	1	3
\bar{Q}_i	3	3	4	1	4	3	3	4	1
\bar{a}_i	1	1	1	6	1	1	1	1	6

Thus, $\ddot{n} = 3$, $\ddot{m}_0 = 1$ and $l = 5$. Here, $\ddot{G}_7 = 256$ and $\ddot{B}_7 = 71$, i.e. $\ddot{\delta}_{\ddot{k}(1)} = \ddot{\delta}_7 = 256 + 71\sqrt{13} = \tau$, so $-256/71$ is the 7th convergent in the 8th continued fraction expansion of \sqrt{D} arising from $I_{-\beta'}$.

Observe that in the above example, $Q_0 < \sqrt{D}$. Thus, our approach is different from the classical approach given in Corollary 2 and is more general.

Finally, we give an illustration of our results from an ambiguous class wherein all associated solutions come from a *single* class since $I_{\alpha_0} = I_{-\alpha'_0}$. When $\delta_{k(m_0)}$ and $\delta'_{\ddot{k}(m)}$ are in the same class, then it follows from Remark 4 that $Q_0 | \Delta$ and $Q_0 | 2G_{k(m_0)}$.

Example 9 Consider the fundamental solution $\alpha_0 = 3 + \sqrt{15}$ of $x^2 - 15y^2 = -6$. By Proposition 1, $x_0 = 3, y_0 = 1, x = -4, y = -1$ and $P_0 = 3$. The simple continued fraction expansion of $(3 + \sqrt{15})/(-6)$ is:

i	0	1	2	3	4	5
P_i	3	9	2	3	3	3
Q_i	-6	11	1	6	1	6
a_i	-2	1	5	1	6	1

Hence, $l = n = 2$ and $\alpha_0 = G_1 + B_1\sqrt{D}$. Since $k(m_0) = 1$ and $k(m) = 2m + 1$ for any $m \geq 0$, then $\delta_{k(m)} = G_{k(m)} + B_{k(m)}\sqrt{D} = \epsilon_{\Delta}^m \alpha_0$, where $\epsilon_{\Delta} = 4 + \sqrt{15}$. Also, $\epsilon_{\Delta}^{-m-1} \alpha_0 = -G_{k(m)} + B_{k(m)}\sqrt{D}$ for all $m \geq 0$. Thus, all proper solutions of $x^2 - 15y^2 = -6$ are given by the $\pm G_{k(m)} + B_{k(m)}\sqrt{D}$.

In summary, we have now developed complete, explicit, computationally palatable means of getting all solution to Equation (8). Moreover, this is

the first instance where a *unique* method of *going back* in the continued fraction expansion is presented.

Acknowledgments : The author welcomes the opportunity to recognize the support of this research by NSERC Canada grant # A8484.

References

- [1] R.A. Mollin, **Quadratics**, CRC Press, Boca Raton, New York, London, Tokyo, (1995).
- [2] T. Nagell, **Number Theory**, Chelsea, New York (1981).
- [3] O. Perron, **Die Lehre von den Kettenbrüchen**, (Chelsea reprint of 1929 edition), Teubner, Leipzig.
- [4] Zhang Xianke, *Semi-simple continued fractions and Diophantine equations for real quadratic fields*, International Centre for Theoretical Physics, IC/94/257 (1994), 1-9.
- [5] Zhang Xianke, Solutions of the Diophantine equations related to real quadratic fields, Chinese Science Bull., **37** (1992), 885-889.
- [6] Zhang Xianke, Determination of solutions and solvabilities of Diophantine equations and quadratic fields, in *Algebraic Geometry and Algebraic Number Theory* (ed. Feng Ke-Qin), Nankai Series in Pure App. Math. **3**, World Sci. Pub., Singapore, (Proceed. Special Program, 1989-1990), 189-199.

Mathematics Department,
University of Calgary,
Calgary, Alberta,
T2N 1N4, Canada
e-mail address: ramollin@math.ucalgary.ca
Web: <http://www.math.ucalgary.ca/~ramollin/>