JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

R. A. MOLLIN
A. J. VAN DER POORTEN
H. C. WILLIAMS

Halfway to a solution of $X^2 - DY^2 = -3$

Journal de Théorie des Nombres de Bordeaux, tome 6, n° 2 (1994), p. 421-457

<http://www.numdam.org/item?id=JTNB_1994__6_2_421_0>

Journal de Théorie des Nombres,
Bordeaux **6** *(1994), 421–459*

Halfway to a Solution of $X^2 - DY^2 = -3$

by R. A. MOLLIN[1], A. J. VAN DER POORTEN[2] AND H. C. WILLIAMS[3]

ABSTRACT. – It is well known that the continued fraction expansion of $\sqrt{D}$ readily displays the midpoint of the principal cycle of ideals, that is, the point halfway to a solution of $x^2 - Dy^2 = \pm 1$. Here we notice that, analogously, the point halfway to a solution of $x^2 - Dy^2 = -3$ can be recognised. We explain what is going on.

RÉSUMÉ – Il est bien connu que le développement en fraction continue de $\sqrt{D}$ donne facilement le milieu du cycle principal des idéaux, c'est à dire le point à mi-parcourt d'une solution de $x^2 - Dy^2 = \pm 1$. Nous montrons ici que de façon analogue le point à mi-parcourt d'une solution de $x^2 - Dy^2 = -3$ peut-être reconnu. Nous expliquons ce qu'il en est.

1. Introduction

Let D be a positive integer, not a square. It is quite well known that if (X, Y) is a solution to Pell's equation $X^2 - DY^2 = 1$ then there are integers x, y so that

$$x^2 + Dy^2 = QX \text{ and } 2xy = QY\,,$$

with x/y a convergent of $\sqrt{D}$ occurring half as far along the continued fraction expansion of $\sqrt{D}$ as does the convergent X/Y. Here $x^2 - Dy^2 = Q$ with Q a divisor of $4D$ — there is an ambiguous ideal halfway along the period of reduced ideals.

Similarly, if $X^2 - DY^2 = -1$ then there are consecutive convergents x'/y' and x/y of $\sqrt{D}$, once again occurring half as far along the continued fraction expansion of $\sqrt{D}$ as does the convergent X/Y, so that

$$x'x + Dy'y = QX \text{ and } x'y + y'x = QY\,.$$

1991 *Mathematics Subject Classification.* 11A55.
Mots-clés : continued fraction, ideal, quadratic form, ambiguous cycle.
Manuscrit reçu le 24 mars 1994, version définitive le 16 décembre 1994.
[1] Research supported by NSERC Canada grant #A8484.
[2] Work supported in part by grants from the Australian Research Council and by a research agreement with Digital Equipment Corporation.
[3] Research supported by NSERC Canada grant #A7649.

Here we have $x'^2 - Dy'^2 = \pm Q$ and $x^2 - Dy^2 = \mp Q$ — reporting that D is a sum of squares $D = Q^2 + P^2$.

There is a little more to it than just that. Of course if D is not a square there is always a solution for $X^2 - DY^2 = 1$, but whilst it is additionally necessary that $D \equiv 1 \pmod 4$, or $D \equiv 2 \pmod 8$, for there to be a solution to $X^2 - DY^2 = -1$, there is no simple sufficient congruence condition on D or on its factors.

It is also well understood that if $d \mid 4D$ with $|d| < \sqrt{D}$ and d squarefree then a solution to $X^2 - DY^2 = d$ occurs halfway along the complete period. In particular a solution to $X^2 - DY^2 = \pm 2$ always has the convergent X/Y occurring halfway along the complete period. If $X^2 - DY^2 = \pm 4$ then that solution occurs a third of the way along the complete period. These matters are discussed in some detail in [4] and [5].

As regards $X^2 - DY^2 = k$,

PROPOSITION 1. *If $X^2 - DY^2 = k$ then X/Y is a convergent of $\sqrt{D}$ if $|k| < \sqrt{D}$.*

Proof. If $k < 0$ then $X < Y\sqrt{D}$ so $Y\sqrt{D} - X = k/(Y\sqrt{D} + X) < 1/2Y$, whilst if $k > 0$ then $X/\sqrt{D} - Y < 1/2X$. Hence in the first case X/Y is a convergent of $\sqrt{D}$ and in the second case Y/X is a convergent of $1/\sqrt{D}$, and again X/Y is a convergent of $\sqrt{D}$.

For large K the literature is fairly silent, beyond explaining a method — seemingly reduction of a quadratic form — which relates, for arbitrary integers K, solutions of $X^2 - DY^2 = K$ to convergents of $\sqrt{D}$.

Our finding halfway to a solution of $X^2 - DY^2 = -3$ will include our giving a necessary and sufficient condition for that equation to be solvable at all, and then our explaining how to find the solutions doing only half the expected amount of work. It will become clear that our ideas should enable one to make useful remarks about the equation with general k, including the somewhat mysterious K larger than $\sqrt{D}$.

We have already alluded to the fact that if $X^2 - DY^2 = -1$ then halfway to its solution we find consecutive complete quotients $(\sqrt{D} + P_h)/Q_h$ and $(\sqrt{D} + P_{h+1})/Q_{h+1}$, with the fact $Q_h = Q_{h+1}$ signalling halfway. Moreover, the well known symmetry of the cycle of course says that the second half of the expansion is exactly the reverse of the first half. Similarly, halfway to a solution of $X^2 - DY^2 = 1$ is signalled by successive complete quotients with $P_h = P_{h+1}$.

We find analogous signals halfway to a solution of $X^2 - DY^2 = -3$ and prove that the expansion up to that solution has *twisted* symmetry. Namely, its second half is essentially the reverse of its first half heavily disguised by having been multiplied by 3. In any case, we generalise the well known cases of halfway to a solution, and will allow them to be seen from new standpoints.

2. Notation and Principles

Throughout we take D a positive integer, not a square. We denote the conjugate of an element $\gamma \in \mathbb{Q}(\sqrt{D})$ by $\overline{\gamma}$. The following remarks are of course just rappels, and detailing or repeating them is is done in an attempt to assist the reader.

We write elements $\gamma \in \mathbb{Q}(\sqrt{D})$ as $(\sqrt{D}+P)/Q$ with integers P and Q so that

$$Q \mid (\sqrt{D}+P)(-\sqrt{D}+P)\,.$$

That loses no generality to speak of because $(a\sqrt{D}+b)/c = (ac\sqrt{D}+bc)/c^2$, and of course c^2 divides $\mathrm{Norm}(ac\sqrt{D}+bc)$, so we need only replace $\sqrt{D}$ by $ac\sqrt{D}$ — and that is tantamount to dealing with an element of the order $\mathbb{Z}[ac\sqrt{D}]$ rather than an element of the order $\mathbb{Z}[\sqrt{D}]$.

Ideals. The point is that once $Q \mid \mathrm{Norm}(\sqrt{D}+P)$, we may remark that

PROPOSITION 2. *The $\mathbb{Z}$-module $\langle Q, \sqrt{D}+P\rangle$, which corresponds to the element $(\sqrt{D}+P)/Q$, is in fact an ideal, that is, it is a $\mathbb{Z}[\sqrt{D}]$-module in the order $\mathbb{Z}[\sqrt{D}]$ of the quadratic field $\mathbb{Q}(\sqrt{D})$.*

Proof. We need only check that $\sqrt{D}(\sqrt{D}+P)$ is in the ideal. But

$$\sqrt{D}(\sqrt{D}+P) = -(P^2-D)+P(\sqrt{D}+P) = -\mathrm{Norm}(\sqrt{D}+P)+P(\sqrt{D}+P)\,,$$

whence $Q \mid \mathrm{Norm}(\sqrt{D}+P)$ completes the verification.

Similarly, by constructing

$$(1) \qquad Q(X-\gamma Y)(X-\overline{\gamma}Y) = QX^2 - 2PXY + \big((P^2-D)/Q\big)Y^2\,,$$

we associate with $(\sqrt{D}+P)/Q$ a quadratic form defined over $\mathbb{Z}$. We note that the discriminant of this form is:

$$\Delta = (2P)^2 - 4Q(P^2-D)/Q = 4D\,.$$

Working with ideals of the canonical shape $\langle Q, \sqrt{D}+P\rangle$, or, all the more with elements $(\sqrt{D}+P)/Q$, or with forms $QX^2-2PXY+\big((P^2-D)/Q\big)Y^2$, is much the same thing. But it is rather more sparing notationally to deal with elements rather than forms, and when we work with elements $(\sqrt{D}+P)/Q$, the role we give to the continued fraction algorithm is very natural. Given that, we need not have mentioned ideals at all. We do, but in so far as we mostly mention ideals only in their canonical form $\langle Q, \sqrt{D}+P\rangle$ our doing so is mostly an endeavour to make composition within a cycle of forms seem the more natural. Below we abuse language by speaking of composing elements or ideals when of course we mean composition of the corresponding forms.

Periodic Continued Fractions. We may have to be reminded that a continued fraction is an expression of the shape

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}$$

which one denotes in a space-saving flat notation by

$$[a_0\ ,\ a_1\ ,\ a_2\ ,\ a_3\ ,\ \ldots\ldots]\ .$$

Here the a_i (except perhaps a_0 which may be any element of $\mathbb{Z}$) should be positive integers. Nonetheless, the formulas are formal and do not carry any expectation of the nature of the a_i; we use that in what follows. We will repeatedly apply the fundamental correspondence, easily proved by induction, whereby:

PROPOSITION 3. *For* $n = 0,\ 1,\ 2,\ \ldots$

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\cdots\begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}$$

if and only if

$$\frac{p_n}{q_n} = [a_0\ ,\ a_1\ ,\ \ldots\ ,\ a_n]\ .$$

Of course, the 'if' part of this claim is to be read as 'for some choice of p_n and q_n so that $p_n/q_n = \ldots$ one has $\ldots$ '.

In the sequel this correspondence will be denoted by $\longleftrightarrow$.

Returning to real quadratic irrationals, we should now remark that

PROPOSITION 4. *The general step* $n = 0, 1, 2, \ldots$ *in the continued fraction expansion of* $\gamma_0 = (\sqrt{D} + P_0)/Q_0 = [a_0 , a_1 , \cdots , a_n , \gamma_{n+1}]$ *is*

$$\gamma_n = \frac{\sqrt{D} + P_n}{Q_n} = a_n - \frac{-\sqrt{D} + P_{n+1}}{Q_n}$$
$$\gamma_{n+1} = \frac{\sqrt{D} + P_{n+1}}{Q_{n+1}} .$$

Proof. The relevant formulaire is easily seen to be

$$P_n + P_{n+1} = a_n Q_n$$
$$\text{and } Q_n Q_{n+1} = -(\sqrt{D} + P_{n+1})(-\sqrt{D} + P_{n+1}) = D - P_{n+1}^2 ;$$

one verifies by induction that the P_n and Q_n all are rational integers.

Do recall that throughout we have the convention whereby, whenever we refer to an element $(\sqrt{D} + P)/Q$, always $Q \mid (D - P^2)$. So, above, of course $D - P_0^2 = a_0 Q_0$ for some *integer* a_0.

It is a basic fact:

PROPOSITION 5. *'Pell's equation'*

$$(2) \qquad (x - \gamma y)(x - \overline{\gamma} y) = x^2 - (2P/Q)xy + ((P^2 - D)/Q^2)y^2 = \pm 1$$

has solutions in integers x *and* y, *with* $y \neq 0$.

The argument, see [5], relies on several applications of the box principle, working with elements of $(1/Q)\mathbb{Z}$.

PROPOSITION 6. *Given a solution* (x, y), *with* $y \neq 0$ *to Pell's equation* (2), *each decomposition*

$$\begin{pmatrix} x & -\gamma\overline{\gamma} y \\ y & x - (\gamma + \overline{\gamma})y \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_r & 1 \\ 1 & 0 \end{pmatrix},$$

with integers a_i, *entails the pure-periodic continued fraction expansion*

$$\gamma = [\overline{a_0 , a_1 , \ldots , a_r}] .$$

Remark. Here we observe that a unimodular matrix has a decomposition of the cited form, with *integers* a_i, and then that the allegation is formally

true. Naturally, it cannot distinguish between γ and its conjugate $\overline{\gamma}$. We see below that our preference is always for that conjugate which satisfies $\gamma > 0$.

The argument, detailed in [2] and [5], is a straightforward application of the correspondence of Proposition 3, once one recalls that

$$\gamma = [\overline{a_0 , a_1 , \ldots , a_r}] = [a_0 , a_1 , \ldots , a_r , \gamma] .$$

We should understand that the continued fraction expansion so obtained may not be *admissible*: in that the a_i might not be *positive* integers. Indeed in the most generally known case, if $\gamma = \sqrt{D}$ then $a_r = 0$ and

$$\sqrt{D} = [a_0 , \overline{a_1 , \ldots , a_{r-1} , 0 , a_0}] = [a_0 , \overline{a_1 , \ldots , a_{r-1} + a_0}] .$$

However, there is a unique admissible decomposition of the unimodular matrix, thus with positive integers a_i (obtained by applying the Euclidean algorithm to the rows of the matrix), exactly when the first row, respectively the first column, dominates the second: that is, precisely if $x > y > 0$ and $y > x - (\gamma + \overline{\gamma})y \geq 0$. These inequalities entail that x and y be positive and that γ is *reduced*: namely that $\gamma > 1$, whilst $0 > \overline{\gamma} > -1$. Those inequalities are precisely the well known Galois conditions for pure-periodicity.

There is an opportunity for mild confusion engendered by the frequently seen suggestion that $\sqrt{D}$ is reduced. Indeed the ideal $\langle 1, \sqrt{D} \rangle$ is reduced, but that is because it equals $\langle 1, \sqrt{D} + a_0 \rangle$, and the element $\sqrt{D} + a_0$ *is* reduced. Idealists may well see this as a justification for their position; those not troubled by an occasional need for translation will take it in their stride.

Equivalence. Two ideals $\mathcal{I}$ and $\mathcal{J}$ in the order $\mathbb{Z}[\sqrt{D}]$ are said to be *equivalent* if there exist nonzero elements β and γ in $\mathbb{Z}[\sqrt{D}]$ such that $(\beta)\mathcal{I} = (\gamma)\mathcal{J}$. It is easily checked that equivalence is an equivalence relation on the ideals compatible with multiplication of ideals. So the equivalence classes yield an abelian group called the class group of $\mathbb{Z}[\sqrt{D}]$. We will be reminded below that such class groups are of finite order.

Two numbers β and γ are said to be *equivalent* if there is a unimodular integer matrix $\left(\begin{smallmatrix} p & p' \\ q & q' \end{smallmatrix}\right)$ so that $\beta = (p\gamma + p')/(q\gamma + q')$. By decomposing the matrix as a product of elementary row transformations it follows that β and γ are equivalent if and only if their continued fraction expansions

have 'the same tail': that is, the expansions differ in at most finitely many initial partial quotients.

It is a simple exercise to confirm that the correspondence, whereby an element $(\sqrt{D}+P)/Q$ yields an ideal $\langle Q, \sqrt{D}+P\rangle$, entails that equivalent numbers yield equivalent ideals.

The import of our discussion on periodicity is that we see that each $\gamma \in \mathbb{K}$ is equivalent to just finitely many reduced elements, to wit the complete quotients appearing in its periodic continued fraction expansion. But, we recall, $(\sqrt{D}+P)/Q$ is reduced if and only if $\sqrt{D}+P > Q$ and $-Q < -\sqrt{D}+P < 0$. Thus $0 < Q < 2\sqrt{D}$ and $-\sqrt{D} < P < \sqrt{D}$ shows that there are just finitely many reduced elements and a fortiori just finitely many equivalence classes of ideals.

A reduced element $(\sqrt{D}+P)/Q$ yields a *reduced* ideal $\langle Q, \sqrt{D}+P\rangle$. One verifies that an ideal is indeed reduced if it contains no nonzero β so that both $|\beta| < Q$ and $|\beta'| < Q$. In this language the period of a continued fraction corresponds to a period of equivalent reduced ideals. Of course a period yields a complete equivalence class of reduced ideals. For if an ideal is reduced it occurs in the cycle of reduced ideals to which it is equivalent, and if it is equivalent to some ideal then it corresponds to a complete quotient occurring in the continued fraction expansion of the element corresponding to that ideal.

One says that two quadratic forms

$$Qx^2 - 2Pxy + \big((P^2-D)/Q\big)y^2 \text{ and } Q'x'^2 - 2P'x'y' + \big((P'^2-D)/Q\big)y'^2$$

are *equivalent* if there is a unimodular matrix $\left(\begin{smallmatrix} p & p' \\ q & q' \end{smallmatrix}\right)$ so that

$$(x' \quad y')\begin{pmatrix} p & p' \\ q & q' \end{pmatrix} = (x \quad y)$$

transforms the first form into the second. The forms are *properly* equivalent if the matrix has determinant $+1$; otherwise they are improperly equivalent. It is straightforward to verify that the numbers $(\sqrt{D}+P)/Q$ and $(\sqrt{D}+P')/Q'$ are equivalent only if the corresponding forms, as cited above, are equivalent. Of course if, with Gauß, we restrict ourselves to proper equivalence then we may have more proper equivalence classes of forms than we have equivalence classes of ideals.

Forms and Ideals. The product of the two ideals $\langle Q, \sqrt{D}+P\rangle$ and

$\langle Q', \sqrt{D} + P' \rangle$ is evidently generated over $\mathbb{Z}$ by the quantities

$$QQ', Q'(\sqrt{D} + P), Q(\sqrt{D} + P')$$

$$\text{and} \quad (\sqrt{D} + P)(\sqrt{D} + P') = PP' + D + (P + P')\sqrt{D}.$$

Set $G = \gcd(Q, Q', P + P')$. One may verify, by studying the classical formulas or from first principles, that the product is a rational integer multiple, namely G, of $\langle q, \sqrt{D} + p \rangle$ where $q = QQ'/G^2$ and p satisfies the three congruence conditions $p \equiv P \pmod{Q/G}$, $p \equiv P' \pmod{Q'/G}$ and $(P - p)(P' - p) \equiv 0 \pmod{QQ'/G^2}$.

The first pair of congruences determines p modulo $QQ'/G(Q, Q')$. The last congruence decides which of the remaining $(Q, Q')/G$ possibilities for $p \mod q$ is to be taken.

Correspondingly, the product of the quadratic forms

$$Qx^2 - 2Pxy + \big((P^2 - D)/Q\big)y^2 \text{ and } Q'x'^2 - 2P'x'y' + \big((P'^2 - D)/Q\big)y'^2$$

together with a substitution

$$X = Axx' + Bxy' + Cx'y + Dyy' \text{ and } Y = A'xx' + B'xy' + C'x'y + D'yy',$$

with integer coefficient $A, \ldots$ and $A', \ldots$, not all sharing a common factor, yields a form $qX^2 - 2pXY + \big((p^2 - D)/q\big)Y^2$ known as a *compound* of the given forms. In fact the Grassmann co-ordinates of the substitution matrix $\begin{pmatrix} A & B & C & D \\ A' & B' & C' & D' \end{pmatrix}$ are determined (they are essentially the six coefficients of the given forms), so the substitution is fixed up to multiplication by a 2×2 unimodular integer matrix. Note remarks on this matter by Shanks at p.182 of [7]. Thus the compound form is defined up to *equivalence* and we see that compounding is well defined on equivalence classes of forms of the same discriminant. We will refer to the particular case, where the two stated forms yield the form $qX^2 - 2pXY + \big((p^2 - D)/q\big)Y^2$, as *composition*.

In particular, one sees that the composite of a form $Qx^2 - 2Pxy + Q'y^2$ and its *opposite* $Qx^2 + 2Pxy + Q'y^2$ is equivalent to the form

$$x^2 - Dy^2 = (x - \sqrt{D}y)(x + \sqrt{D}y);$$

correspondingly the product of an ideal $\langle Q, \sqrt{D} + P \rangle$ and its conjugate

$$\langle Q, -\sqrt{D} + P \rangle = \langle Q, \sqrt{D} - P \rangle$$

is a principal ideal. Thus, it turns out that $Q \mid 2P$ is the condition for a form $Qx^2 - 2Pxy + Q'y^2$ to be properly equivalent to its opposite; the transformation is effected by $y \mapsto y$, $x \mapsto x + \big(2P/Q\big)y$. In this case the ideal $\langle Q, \sqrt{D} + P \rangle$ is its own conjugate, so its square is principal.

Ambiguity. A quadratic form $Qx^2 - 2Pxy + \big((P^2 - D)/Q\big)y^2$ is said to be *ambiguous* if it is both properly and improperly equivalent to itself. The surprising equivalence must interchange the numbers $(\sqrt{D}+P)/Q$ and its conjugate $(-\sqrt{D}+P)/Q$. Thus the form is ambiguous if and only if the element $(\sqrt{D}+P)/Q$ is equivalent to its conjugate.

In an alternative interpretation one says that an ideal $\langle Q, \sqrt{D}+P\rangle$ is ambiguous if it is equal to its conjugate. Of course an ideal equals its conjugate only if it contains the conjugate of each of its elements. Hence $\langle Q, \sqrt{D}+P\rangle$ is ambiguous if and only if it contains both $(\sqrt{D}+P)/Q$ and $(-\sqrt{D}+P)/Q$ and that is so if and only if

$$(\sqrt{D}+P)/Q + (-\sqrt{D}+P)/Q = 2P/Q \in \mathbb{Z}\,.$$

We should recall that the basic condition $Q \mid (\sqrt{D}+P)(-\sqrt{D}+P)$ is

$$(P^2 - D)/Q \in \mathbb{Z}\,.$$

Hence $2P/Q \in \mathbb{Z}$ entails $\Delta/Q \in \mathbb{Z}$. Thus the ambiguity of an ideal entails that its norm Q divides the discriminant Δ. Conversely, if an ideal has a squarefree norm dividing the discriminant then that ideal is ambiguous.

An ideal $\langle Q, \sqrt{D}+P\rangle$ is ambiguous if and only if the continued fraction expansion $(\sqrt{D}+P)/Q = [a_0\,,\,\overline{a_1\,,\,a_2\,,\,\ldots\,,\,a_{r-1}\,,\,a_r}]$ has $a_1a_2\cdots a_{r-1}$ a palindrome and $a_r = 2a_0 - 2P/Q$. In that sense ambiguity is symmetry; see [2].

One says that an equivalence class of ideals is ambiguous if it contains both an ideal and its conjugate; hence, it contains the conjugate of each ideal in the class.

Infrastructure. The literature appears to speak interchangeably of composing or *compounding* forms. It is not a bad idea to reserve one of these terms for the original operation on the equivalence classes, and the other for the specific manner of composition — corresponding neatly to multiplication of ideals in canonical form — which we mention above. Thus we may say that compounding is an operation on the ideal or form classes but that our formulas describe *composition* of forms as such and therefore of the corresponding elements. Thanks to Shanks [6] and thence to Lenstra [1] we now understand that in that way composition operates meaningfully within an ideal cycle. That is an operative principle in the sequel.

We barely need to emphasise it here, because almost throughout we work in the order $\mathbb{Z}[\sqrt{D}]$, but our notation indicates the order in which

we are active. Thus, for example, were we to work in the order $\mathbb{Z}[\delta]$, with $\delta = (\sqrt{D}+1)/2$, as we might if D were $\equiv 1 \pmod 4$, our elements would appear as $(\delta+P)/Q$ — with $Q \mid (\delta+P)(\overline{\delta}+P)$ — and the corresponding ideals as $\langle Q, \delta+P\rangle$. That, incidentally, forces a change of notation from that of Perron [3], as is alluded to at Proposition 9 below.

3. Pairs of Ideals near Halfway

Suppose that there is a solution to $X^2 - DY^2 = -3$. We shall show the existence of pairs of ideals $\langle Q_h, \sqrt{D}+P_h\rangle$ and $\langle 3Q_h, \sqrt{D}-P\rangle$ which compose to yield an ideal $\langle 3, \sqrt{D}+p\rangle$; it's because $P \equiv P_h \pmod{Q_h}$ that this works. However, the point is that the element $(\sqrt{D}+P_h)/Q_h$ is reduced and that in an easy to understand sense the ideal $\langle 3Q_h, \sqrt{D}-P\rangle$ is 'near' it. Then, given that $\langle 3, \sqrt{D}+p\rangle$ need not be a square, the ideals $\langle Q_h, \sqrt{D}+P_h\rangle$ are pretty well as close as we can get to its square root and in that sense lie halfway to it. Indeed, as one may verify experimentally, the ideals $\langle Q_h, \sqrt{D}+P_h\rangle$ we find below — if they lie in the principal cycle — do lie roughly halfway along the cycle to an ideal $\langle 3, \sqrt{D}+p\rangle$.

Of course the fact of a solution to $X^2 - DY^2 = -3$ entails the existence of an ideal $\langle 3, \sqrt{D}+p\rangle$ in the principal cycle. More than that, because of the minus sign its immediate 'neighbours' — in the sense of the continued fraction expansion or equivalently the ideal cycle, lie in the principal genus and thus have square roots lying in ambiguous cycles. It will become clear that the ideal $\langle 3, \sqrt{D}+p\rangle$ has appropriate neighbours with norm Q_h^2.

We lose no generality in supposing that D is squarefree, and suppose that from hereon. We may then remark that if $X^2 - DY^2 = -3$ has a solution then certainly each prime factor of D splits in $\mathbb{Q}(\sqrt{-3})$. Thus, as is easily checked by quadratic reciprocity, the only possible factors of D are 3 and primes congruent to 1 modulo 3. Hence, recalling that the maximal order of $\mathbb{Q}(\sqrt{-3})$ has basis generated by 1 and $(1+\sqrt{-3})/2$ it follows that D has representations

$$D = M^2 + MN + N^2.$$

To be precise, if D has ν different prime factors congruent to 1 modulo 3 then there are $2^{\nu-1}$ essentially different such representations — disregarding interchange of M and N, changes of sign, and — in this special case — other actions by roots of unity.

We can guarantee the parity of N; that is, we may arrange N to be odd or even according to our preference. For if M is even and N is odd then

we may interchange M and N. If both are odd, then $M+N$ is even in $D=(-M)^2-M(M+N)+(M+N)^2$. Here too we may interchange M and N if we wish. Nonetheless, the cases N odd and N even are rather different and need separate treatment.

Below we will prefer N odd. Suppose, however that $N=2Q$ is even — of course then M is odd. Then we have an equivalent representation

$$D=(M+Q)^2+3Q^2.$$

Conversely $D=A^2+3B^2$ entails $D=(A-B)^2+(A-B)\cdot 2B+(2B)^2$. Again disregarding signs, there are $2^{\nu-1}$ distinct such representations.

Out of contrariness we start with the even case. Suppose then that D has a representation $D=L^2+3Q_h^2$ with L and Q_h positive. Then it is easy to check that either the element $(\sqrt{D}+L)/Q_h$ or the element $(\sqrt{D}+L+Q_h)/Q_h$ is reduced. We set $P_h=L+gQ_h$ with $g=0$ or 1 so that $(\sqrt{D}+P_h)/Q_h$ is reduced. Because $P_h-L\equiv 0 \pmod{Q_h}$ the product of the ideals $\langle 3Q_h^2, \sqrt{D}-L\rangle$ and $\langle Q_h, \sqrt{D}+P_h\rangle$ is $Q_h\langle 3Q_h, \sqrt{D}+P\rangle$ with some $P\equiv -L \pmod{3Q_h}$. Now, consider the product of $\langle Q_h, \sqrt{D}+P_h\rangle$ and $\langle 3Q_h, \sqrt{D}+P\rangle$. It is $Q_h\langle 3, \sqrt{D}+p\rangle$ with some $p\equiv P \pmod 3$ because $P_h+P\equiv 0 \pmod{Q_h}$. Hence, indeed, we have found a pair of ideals $\langle Q_h, \sqrt{D}+P_h\rangle$ and $\langle 3Q_h, \sqrt{D}+P\rangle$ which compose to yield an ideal $\langle 3, \sqrt{D}+p\rangle$.

Since the reciprocal of $(\sqrt{D}-L)/3Q_h^2$ is $\sqrt{D}+L$ which is a neutral element for composition, and since we obtained the ideal $\langle 3Q_h, \sqrt{D}+P\rangle$ from $\langle Q_h, \sqrt{D}+P_h\rangle$ by composing with $\langle 3Q_h^2, \sqrt{D}-L\rangle$ the sense in which the ideals $\langle 3Q_h, \sqrt{D}+P\rangle$ and $\langle Q_h, \sqrt{D}+P_h\rangle$ are 'near' to one another is manifest. Moreover, for later use we remark that plainly, being equivalent to a principal ideal, the ideal $\langle 3Q_h^2, \sqrt{D}-L\rangle$ is principal.

Finally, we remark that on the one hand $\mathrm{Norm}(\sqrt{D}+P_h)=-Q_{h-1}Q_h$ and on the other hand $P_h^2-D=P_h^2-\left((P_h-gQ_h)^2+3Q_h^2\right)$. Hence

$$(3+g^2)Q_h=Q_{h-1}+2gP_h\,.$$

We will refer to an event $3Q_h=Q_{h-1}$ or $4Q_h=Q_{h-1}+2P_h$ as a *signal* — namely a signal that we may be halfway to a solution of $X^2-DY^2=-3$.

Before summarising we had best deal with the cases L or Q_h negative. In so far as we are dealing with ideals a change in sign of Q_h is irrelevant — so we assume throughout that $Q_h>0$. On the other hand $\langle Q_h, \sqrt{D}-L\rangle = \langle Q_h, -\sqrt{D}+L\rangle$ is the ideal conjugate to $\langle Q_h, \sqrt{D}+L\rangle$. A brief glance at the

continued fraction formulas reminds us that the reduced element conjugate to $(\sqrt{D}+P_h)/Q_h$ is $(\sqrt{D}+P_{h+1})/Q_h$. Our argument above should change to start with the ideal $\langle 3Q_h, \sqrt{D}+L\rangle$. It is multiplied by $\langle 3Q_h^2, \sqrt{D}-L\rangle$ as above, we might just as well say 'composed with', yielding an ideal $\langle Q_h, \sqrt{D}+P_{h+1}\rangle$. That product is then composed with $\langle 3Q_h, \sqrt{D}+L\rangle$ to yield an ideal $\langle 3, \sqrt{D}+p\rangle$. We will have set $P_{h+1} = L+gQ$ with $g = 0$ or 1. Now we conclude with the remarks that $\mathrm{Norm}(\sqrt{D}+P_{h+1}) = -Q_hQ_{h+1}$ whilst $P_{h+1}^2 - D = P_{h+1}^2 - \big((P_{h+1}-gQ_h)^2 + 3Q_h^2\big)$, whence

$$(3+g^2)Q_h = Q_{h+1} + 2gP_{h+1}\,,$$

once again with $g = 0$ or 1. These then are the conjugate signals.

PROPOSITION 7. *Each representation $D = L^2 + 3Q_h^2$ with $Q_h > 0$ yields a pair of reduced elements $(\sqrt{D}+P_h)/Q_h$ and $(\sqrt{D}+P_{h+1})/Q_h$ and,* in some ambiguous cycle, *one or other of a conjugate pair of signals*

$$\begin{aligned} 4Q_h &= Q_{h-1} + 2P_h \quad \text{or} \quad 3Q_h = Q_{h-1} \\ 4Q_h &= Q_{h+1} + 2P_{h+1} \quad \text{or} \quad 3Q_h = Q_{h+1}\,. \end{aligned}$$

Remark. We say only that, given the representation, we find one or other of the pairs of conjugate signals in *some* ambiguous cycle of the order $\mathbb{Z}[\sqrt{D}]$. Of course we can find them in the continued fraction expansion of $\sqrt{D}$ itself, thus in the *principal* cycle, only if $X^2-DY^2 = -3$ has a solution in integers (X, Y). Our ultimate purpose, hence the Theorems below, is inter alia to show that the appearance of such a signal is *necessary* as well as sufficient. Thus we hasten to emphasise that the Proposition does not rely on there being a solution to $X^2 - DY^2 = -3$. We use only the fact of the representation of D and deduce from it that there then is an ideal $\langle 3, \sqrt{D}+p\rangle$ — namely that there is a rational integer p so that $3 \mid D-p^2$.

We now turn to the representations $D = M^2+MQ_h+Q_h^2$ still supposing that $Q_h > 0$. Moreover we shall also suppose that Q_h is odd, as we may without loss of generality. If $M > 0$ it is easy to verify that the element $(\sqrt{D}+M)/Q_h$ is reduced. In analogy with the foregoing case we propose to compose the ideal $\langle Q_h, \sqrt{D}+M\rangle$ with an appropriate ideal of norm $3Q_h^2$, indeed with the ideal $\langle 3Q_h^2, \sqrt{D}-M+\frac{1}{2}(3Q_h-1)Q_h\rangle$.

By the way, we have not pulled this ideal quite out of thin air. We noted that $4D-(2M+Q_h)^2 = 3Q_h^2$ and then with some mild effort rewrote the principal ideal generated by $2\sqrt{D}-(2M+Q_h)$ in the canonical form we use

throughout. In any case, as before we obtain an ideal $\langle 3Q_h, \sqrt{D}+P\rangle$. We could have deduced that with less turgid detail since the only point is that $M - \frac{1}{2}(3Q_h - 1)Q_h \equiv M \pmod{Q_h}$. Hence $P \equiv -M \pmod{3Q_h}$. Now composing the ideals $\langle Q_h, \sqrt{D}+M\rangle$ and $\langle 3Q_h, \sqrt{D}+P\rangle$ yields an ideal $\langle 3, \sqrt{D}+p\rangle$ just as above. We set $M = P_h$. Of course $D - P_h^2 = Q_{h-1}Q_h$ and $D - P_h^2 = P_hQ_h + Q_h^2$ so we obtain $Q_{h-1} = Q_h + P_h$, an attractive signal indeed.

In the conjugate case we start with the ideal $\langle 3Q_h, \sqrt{D}+M-Q_h\rangle$. The first composition as above yields an ideal $\langle Q_h, \sqrt{D}+P_{h+1}\rangle$ corresponding to a reduced element $(\sqrt{D}+P_{h+1})/Q_h$, and when it is composed with $\langle 3Q_h, \sqrt{D}+M-Q_h\rangle$ we once again obtain an ideal $\langle 3, \sqrt{D}+p\rangle$. All this is tantamount to our setting $M = P_{h+1}$ and yields the signal $Q_{h+1} = Q_h + P_{h+1}$.

PROPOSITION 8. *Each representation $D = M^2 + MQ_h + Q_h^2$ with $Q_h > 0$ and odd yields reduced elements $(\sqrt{D}+P_h)/Q_h$ and $(\sqrt{D}+P_{h+1})/Q_h$ and a conjugate pair of signals*

$$Q_{h-1} = Q_h + P_h \quad \text{and} \quad Q_{h+1} = Q_h + P_{h+1}\,.$$

Once again, this means that given the representation we find, in *some ambiguous cycle* of the order $\mathbb{Z}[\sqrt{D}]$, the pair of conjugate signals — to wit, neighbouring P's and Q's satisfying the cited relations.

We will notice below that when $Q_{h-1} = Q_h + P_h$ then $P_{h-1} = Q_h$ and $Q_{h-2} = P_h$. Hence, automatically, $Q_{h-1} = P_{h-1} + Q_{h-2}$, which is the conjugate signal slightly displaced. Thus it actually suffices to emphasise only one of the present pair of signals. We reiterate that the Proposition does not rely on there being a solution to $X^2 - DY^2 = -3$. We use only the fact of the representation of D. Our purpose in alluding to a solution at all was to be able to say that a solution is equivalent to the presence of an ideal $\langle 3, \sqrt{D}+p\rangle$ in the principal cycle. However we have the representations as soon as $3 \mid D - p^2$ and that last is silent as to the class of the ideal $\langle 3, \sqrt{D}+p\rangle$.

4. Halfway Along the Continued Fraction Expansion

In this section we suppose that the halfway ideal $\langle Q_h, \sqrt{D}+P_h\rangle$, and therefore also its conjugate, lies in the principal cycle. We set

$$\sqrt{D} = [a_0\,,\, a_1\,,\, \ldots\,,\, a_n\,,\, (\sqrt{D}+P_{n+1})/Q_{n+1}]\,,$$

and denote the convergents variously by p_n/q_n or x_n/y_n. We write

$$N_n = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \text{ and set } J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

It will be useful to set

$$M_n = \begin{pmatrix} p_n & Dq_n \\ q_n & p_n \end{pmatrix} = \begin{pmatrix} Dq_n & p_n \\ p_n & q_n \end{pmatrix} J.$$

So $M_n J$ is symmetric, and since

$$M_n = N_n \begin{pmatrix} 1 & P_{n+1} \\ 0 & Q_{n+1} \end{pmatrix}$$

we have

$$M_n J = N_n \begin{pmatrix} 1 & P_{n+1} \\ 0 & Q_{n+1} \end{pmatrix} J = \begin{pmatrix} P_{n+1} & Q_{n+1} \\ 1 & 0 \end{pmatrix} \overleftarrow{N_n},$$

with the eccentric notation $\overleftarrow{N_n}$ for the transpose of N_n congenially reminding us that it is

$$\begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Here we have said nothing startling other than perhaps for our allegation that

PROPOSITION 9.

$$M_n = \begin{pmatrix} p_n & Dq_n \\ q_n & p_n \end{pmatrix} = N_n \begin{pmatrix} 1 & P_{n+1} \\ 0 & Q_{n+1} \end{pmatrix}.$$

This remark is central and warrants an extended explanation.

Explanation. We commence by observing that 'multiplication by $x - \sqrt{D}y$' is a $\mathbb{Q}$-linear map of the $\mathbb{Q}$-vector space $\mathbb{Q}(\sqrt{D})$ into itself. With respect to the basis $\{-\sqrt{D}, 1\}$ its matrix is

$$M = \begin{pmatrix} x & Dy \\ y & x \end{pmatrix}.$$

Thus M has determinant $\mathrm{Norm}(x-\sqrt{D}y) = x^2-Dy^2$ and in particular M_n has determinant $p_n^2 - Dq_n^2 = (-1)^{n+1}Q_{n+1}$ compatible with our allegation. More to the point, we apply the correspondence of Proposition 3 between matrices and continued fractions after first noticing that

$$M_n \begin{pmatrix} \sqrt{D}/Q_{n+1} & 1 \\ 1/Q_{n+1} & 0 \end{pmatrix} = \begin{pmatrix} \sqrt{D}(p_n + \sqrt{D}q_n)/Q_{n+1} & p_n \\ (p_n + \sqrt{D}q_n)/Q_{n+1} & q_n \end{pmatrix}.$$

Then

$$\begin{aligned} \sqrt{D} \longleftrightarrow \begin{pmatrix} \sqrt{D}(p_n + \sqrt{D}q_n)/Q_{n+1} & p_n \\ (p_n + \sqrt{D}q_n)/Q_{n+1} & q_n \end{pmatrix} \\ = N_n \begin{pmatrix} (\sqrt{D} + P_{n+1})/Q_{n+1} & 1 \\ 1 & 0 \end{pmatrix} \\ \longleftrightarrow [a_0\,, \ldots, a_n\,, (\sqrt{D} + P_{n+1})/Q_{n+1}]\,, \end{aligned}$$

explaining that the constants P_{n+1} and Q_{n+1} do indeed define the next complete quotient exactly as our notation had suggested.

It therefore seems appropriate to consider the M_n to define the sequences (P_n) and (Q_n), via the statement of the proposition. Were we working in an order different from $\mathbb{Z}[\sqrt{D}]$ this would force a change of notation from that of Perron [3].

In any case, with that cleared up, we next remark that the product of any two matrices of the shape M is again of that shape. That is

$$MM' = \begin{pmatrix} x & Dy \\ y & x \end{pmatrix} \begin{pmatrix} x' & Dy' \\ y' & x \end{pmatrix} = \begin{pmatrix} X & DY \\ Y & X \end{pmatrix}.$$

That's plain without computation on remarking that

$$(x - \sqrt{D}y)(x' - \sqrt{D}y') = (X - \sqrt{D}Y)\,,$$

with $X = xx' + Dyy'$ and $Y = xy' + x'y$.

We shall interpret our idea for finding the halfway point to a solution of $X^2 - DY^2 = -3$ in terms of the observation that multiplication of matrices M corresponds to composing the corresponding forms, as is clear, of course, in the light of the remark just made. Accordingly we are now in a position to compose, so to speak, the corresponding continued fraction expansions.

Representations $D = M^2+MN+N^2$ with N odd. It seems convenient to suppress subscripts as long as practicable. Our argument runs as follows. Suppose Q odd. The representation $D = P^2 + PQ + Q^2$ yields the ideal $\langle Q, \sqrt{D} + P\rangle$ and it corresponds to, say,

$$\begin{pmatrix} x & Dy \\ y & x \end{pmatrix} = \begin{pmatrix} x & x' \\ y & y' \end{pmatrix} \begin{pmatrix} 1 & P \\ 0 & Q \end{pmatrix}.$$

Expanding $\sqrt{D}$ we may[1] write

$$\sqrt{D} = [P + \tfrac{1}{2}(Q-1)\,,1\,,1\,,(\sqrt{D}+P-\tfrac{1}{2}Q(3Q-1))/3Q^2]$$

so the ideal $\langle 3Q^2, \sqrt{D} + P - \frac{1}{2}Q(3Q-1)\rangle$ corresponds explicitly to the matrix

$$\begin{pmatrix} 2P+Q & P+\frac{1}{2}(Q+1) \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & P-\frac{1}{2}Q(3Q-1) \\ 0 & 3Q^2 \end{pmatrix}.$$

The conjugate of the ideal corresponds to the adjoint of the matrix[2]. Hence the first composition yields the matrix product

$$\begin{pmatrix} x & x' \\ y & y' \end{pmatrix} \begin{pmatrix} 1 & P \\ 0 & Q \end{pmatrix} \begin{pmatrix} 3Q^2 & -P+\frac{1}{2}Q(3Q-1) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -P-\frac{1}{2}(Q+1) \\ -2 & 2P+Q \end{pmatrix}$$

$$= \begin{pmatrix} x & x' \\ y & y' \end{pmatrix} \begin{pmatrix} 3Q^2 & \frac{1}{2}Q(3Q-1) \\ 0 & Q \end{pmatrix} \begin{pmatrix} 1 & -P-\frac{1}{2}(Q+1) \\ -2 & 2P+Q \end{pmatrix}$$

$$= -Q \begin{pmatrix} x & x' \\ y & y' \end{pmatrix} \begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & Q-P \\ 0 & 3Q \end{pmatrix},$$

the last line after a little work. We recognise the intermediate matrices as reciprocals and may therefore interpret the product as telling us of the following configuration in the expansion:

$$\vdots$$

$$(\sqrt{D}+Q_h-P_h)/3Q_h = 0 - (-\sqrt{D}+P_h-Q_h)/3Q_h$$

$$(\sqrt{D}+P_h-Q_h)/P_h = 1 - (-\sqrt{D}+Q_h)/P_h$$

$$(\sqrt{D}+Q_h)/(P_h+Q_h) = 1 - (-\sqrt{D}+P_h)/Q_{h-1}$$

$$(\sqrt{D}+P_h)/Q_h =$$

[1] "No, you may not", we hear you say. "$P+\frac{1}{2}(Q-1)$ is not the integer part of $\sqrt{D}$". To that one of us replies "Up a gumtree" (an Antipodean response to nonsense). Our assertion is an identity showing that a certain ideal is principal. The fact that it is not *the* usual continued fraction expansion of $\sqrt{D}$ is quite irrelevant.

[2] Strictly speaking, it corresponds to the inverse, but since the correspondence with continued fractions disregards multiplication by nonzero constants we effectively obtain the adjoint.

More compactly

$$(\sqrt{D}+Q_h-P_h)/3Q_h = [0\,,1\,,1\,,(\sqrt{D}+P_h)/Q_h]\,.$$

Of course we have recalled that $D = P_h^2+P_hQ_h+Q_h^2$ and $Q_{h-1} = Q_h+P_h$.

Whatever, we may now compose the ideal $\langle 3Q, \sqrt{D}+Q-P\rangle$ with $\langle Q, \sqrt{D}+P\rangle$. Here one might notice, the absurd way is by the use of false transposition[3], that also

$$\begin{pmatrix} x & Dy \\ y & x \end{pmatrix} = \begin{pmatrix} P & Q \\ 1 & 0 \end{pmatrix}\begin{pmatrix} y & x \\ y' & x' \end{pmatrix}.$$

We obtain

$$\begin{pmatrix} x & x' \\ y & y' \end{pmatrix}\begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & Q-P \\ 0 & 3Q \end{pmatrix}\times$$
$$\times\begin{pmatrix} P & Q \\ 1 & 0 \end{pmatrix}\begin{pmatrix} y & x \\ y' & x' \end{pmatrix}$$
$$= Q\begin{pmatrix} x & x' \\ y & y' \end{pmatrix}\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} y & x \\ y' & x' \end{pmatrix}$$
$$= Q\begin{pmatrix} x & x' \\ y & y' \end{pmatrix}\begin{pmatrix} 2y-y' & 2x-x' \\ 2y'-y & 2x'-x \end{pmatrix},$$

corresponding to some ideal $\langle 3, \sqrt{D}+p\rangle$. The first matrix corresponds to the continued fraction

$$[a_0\,,a_1\,,\ldots,a_{h-1}] = [a_0\,,w]$$

and since it is well known, and easily seen by the matrix correspondence, that

$$y/y' = [a_{h-1}\,,a_{h-2}\,,\ldots,a_1] = [\overleftarrow{w}\,],$$

the second matrix corresponds to that expansion 'multiplied symmetrically' by 3, to wit to the continued fraction of

$$\frac{2y/y'-1}{2-y/y'}\,.$$

[3]That is, transposition in the wrong diagonal. This should not be confused with "students' transposition" where one over-enthusiastically transposes in both diagonals. Mind you, the students have a point. The "double transpose" of a product of 2×2 matrices is the product of the double transposes. There is none of this nonsense of having to remember to reverse the order of multiplication.

Of course the matrix

$$\begin{pmatrix} 2y - y' & 2x - x' \\ 2y' - y & 2x' - x \end{pmatrix}$$

expands as a product of matrices of the shape

$$\begin{pmatrix} a_h & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{h+1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & p \\ 0 & 3 \end{pmatrix}.$$

The decomposition is tantamount to performing the euclidean algorithm on the rows of the 2×2 matrix. That is plain given that the continued fraction expansion of a rational is effectively the euclidean algorithm on its numerator and denominator. We give numerical details in our examples below. In particular, above,

$$\frac{2y - y'}{2y' - y} = [a_h\,,\, a_{h+1}\,,\, \ldots\,,\, a_n\,].$$

To ensure that we have expressed matters correctly we had better confirm that all the entries $2y' - y$, $2x - x'$, $\ldots$, are positive. We note that is so if and only if the partial quotient $a_{h-1} = 1$. Fortunately, always $Q_h = P_{h-1}$, and so $a_{h-1} = 1$, because the element $(\sqrt{D} + Q_h)/(Q_h + P_h)$ is reduced when $D = P_h^2 + P_h Q_h + Q_h^2$.

THEOREM I. *Let $x^2 - Dy^2 = (-1)^h Q_h$ and suppose that $Q_{h-1} = Q_h + P_h$ in the principal cycle. Then $X^2 - DY^2 = -3$, where*

$$Q_h^2 X = 4Dxy - (2P_h + Q_h)(x^2 + Dy^2)$$
$$Q_h^2 Y = 2(x^2 + Dy^2) - 2(2P_h + Q_h)xy\,.$$

Moreover the continued fraction expansion of X/Y is twisted symmetric. Its first half is the expansion of x/y, say $[a_0, \overrightarrow{w}]$, and its second part is the expansion of $(2[\overleftarrow{w}] - 1)/(2 - [\overleftarrow{w}])$ — thus the reverse of that first half, omitting the zero-th partial quotient, twisted by multiplication by a transformation of determinant 3.

Proof. Having been signalled by $Q_{h-1} = Q_h + P_h$ we have

$$P_h^2 - D = -Q_h Q_{h-1} = -Q_h^2 - Q_h P_h$$

and thus the representation $D = P_h^2 + P_h Q_h + Q_h^2$. But then we have seen explicitly that

$$\begin{pmatrix} x & Dy \\ y & x \end{pmatrix} \begin{pmatrix} 2P_h + Q_h & -2D \\ -2 & 2P_h + Q_h \end{pmatrix} \begin{pmatrix} x & Dy \\ y & x \end{pmatrix} = -Q_h^2 \begin{pmatrix} X & DY \\ Y & X \end{pmatrix},$$

yielding the claims.

We will not need the conjugate case; see however the discussion below of the conjugate case when N is even.

An example. One can see that $122831^2 - 1729 \cdot 2954^2 = -3$ after a brief computation. In detail,

$$
\begin{array}{lcl}
(\sqrt{1729}\ +\ 0\ )/1 & = & 41 - (-\sqrt{1729} + 41\ )/1 \\
(\sqrt{1729} + 41\ )/48 & = & 1 - (-\sqrt{1729}\ +\ 7\ )/48 \\
(\sqrt{1729}\ +\ 7\ )/35 & = & 1 - (-\sqrt{1729} + 28\ )/35 \\
(\sqrt{1729} + 28\ )/27 & = & 2 - (-\sqrt{1729} + 26\ )/27 \\
(\sqrt{1729} + 26\ )/39 & = & 1 - (-\sqrt{1729} + 13\ )/39 \\
(\sqrt{1729} + 13\ )/40 & = & 1 - (-\sqrt{1729} + 27\ )/40 \\
(\sqrt{1729} + 27\ )/25 & = & 2 - (-\sqrt{1729} + 23\ )/25 \\
(\sqrt{1729} + 23\ )/48 & = & 1 - (-\sqrt{1729} + 25\ )/48 \\
(\sqrt{1729} + 25\ )/23 & = & 2 - (-\sqrt{1729} + 21\ )/23 \\
(\sqrt{1729} + 21\ )/56 & = & 1 - (-\sqrt{1729} + 35\ )/56 \\
(\sqrt{1729} + 35\ )/9 & = & 8 - (-\sqrt{1729} + 37\ )/9 \\
(\sqrt{1729} + 37\ )/40 & = & 1 - (-\sqrt{1729}\ +\ 3\ )/40 \\
(\sqrt{1729}\ +\ 3\ )/43 & = & 1 - (-\sqrt{1729} + 40\ )/43 \\
(\sqrt{1729} + 40\ )/3 & = & \ldots
\end{array}
$$

n	x_n	y_n
0	41	1
1	42	1
2	83	2
3	208	5
4	291	7
5	499	12
6	1289	31
7	1788	43
8	4865	117
9	6653	160
10	58089	1397
11	64742	1557
12	122831	2954

Here $Q_7 = 48 = 23 + 25 = Q_8 + P_8$. Incidentally, $a_7 = 1$ whence $P_7 = Q_8$ as in the continued fraction configuration we mentioned above. That's clear of course because an element $(\sqrt{D} + Q)/(Q + P)$ is reduced if $D = P^2 + PQ + Q^2$. We read off that

$$\begin{pmatrix} y_7 & x_7 \\ y_6 & x_6 \end{pmatrix} = \begin{pmatrix} 43 & 1788 \\ 31 & 1289 \end{pmatrix}.$$

We purport that the continued fraction expansion $[41\ ,\ 1\ ,\ 1\ ,\ 2\ ,\ 1\ ,\ 1\ ,\ 2\ ,\ 1]$ continues with the expansion corresponding to

$$\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} 43 & 1788 \\ 31 & 1289 \end{pmatrix}.$$

Note that all entries in the product are positive exactly because $a_7 = 1$. Indeed, the product expands to yield

$$\begin{pmatrix} 55 & 2287 \\ 19 & 790 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 8 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 40 \\ 0 & 3 \end{pmatrix},$$

that is $55/19 = [2\ ,\ 1\ ,\ 8\ ,\ 1\ ,\ 1]$ and $2287/790 = [2\ ,\ 1\ ,\ 8\ ,\ 1\ ,\ 1\ ,\ 40/3]$, precisely as predicted[4].

[4]Our joy was great and not a little tinged with surprise at this vindication.

We should also confirm that

$$Q_8^2X = 4\cdot 1729x_7y_7 - (2P_8+Q_8)(x_7^2+1729y_7^2)$$
$$= 4{\cdot}1729{\cdot}1788{\cdot}43-(2{\cdot}25+23)(1788^2+1729{\cdot}43^2) = 64977599 = 23^2{\cdot}122831\,,$$

and

$$Q_8^2Y = 2(x_7^2+1729y_7^2) - 2(2P_8+Q_8)x_7y_7$$
$$= 2(1788^2+1729\cdot 43^2) - 2(2\cdot 25+23)1788\cdot 43 = 1562666 = 23^2\cdot 2954\,.$$

Representations $D = M^2+MN+N^2$ with N even. We now return to representations $D = M^2+MN+N^2$ with N even. Appropriately expanding $\sqrt{D}$ we obtain

$$\sqrt{D} = [M+\tfrac{1}{2}N\,,\,(\sqrt{D}+M+\tfrac{1}{2}N)/\tfrac{3}{4}N^2\,]\,,$$

immediately yielding the ideal $\langle \frac{3}{4}N^2, \sqrt{D}+M+\frac{1}{2}N\rangle$. Accordingly we set $N = 2Q$ and $L = M+Q$ and note that one or other of the elements $(\sqrt{D}+L)/Q$ or $(\sqrt{D}+L+Q)/Q$ is reduced. As before we write $P = L+gQ$ with $g = 0$ or 1. The first composition corresponds to

$$\begin{pmatrix} x & Dy \\ y & x \end{pmatrix}\begin{pmatrix} L & -D \\ -1 & L \end{pmatrix}$$
$$= \begin{pmatrix} x & x' \\ y & y' \end{pmatrix}\begin{pmatrix} 1 & P \\ 0 & Q \end{pmatrix}\begin{pmatrix} 3Q^2 & gQ-P \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ -1 & P-gQ \end{pmatrix}$$
$$= Q\begin{pmatrix} x & x' \\ y & y' \end{pmatrix}\begin{pmatrix} 3Q & g \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ -1 & P-gQ \end{pmatrix}$$
$$= Q\begin{pmatrix} x & x' \\ y & y' \end{pmatrix}\begin{pmatrix} -g & gP-(3+g^2)Q \\ -1 & P-gQ \end{pmatrix}$$
$$= -Q\begin{pmatrix} x & x' \\ y & y' \end{pmatrix}\begin{pmatrix} g & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & gQ-P \\ 0 & 3Q \end{pmatrix},$$

telling us of the following configuration in an expansion:

$$\vdots$$
$$(\sqrt{D}+P_h)/Q_h \;= g-(-\sqrt{D}+gQ_h-P_h)/Q_h$$
$$(\sqrt{D}+gQ_h-P_h)/3Q_h = \;\ldots$$

If $g = 0$ this just reports that $Q_{h-1} = 3Q_h$, in the proper continued fraction expansion. Of course we have recalled that $D = (P_h - gQ_h)^2 + 3Q_h^2$ and $(3 + g^2)Q_h = Q_{h-1} + 2gP_h$.

Now, the second composition with the ideal $\langle Q, \sqrt{D} + P \rangle$ corresponds to

$$\begin{pmatrix} x & x' \\ y & y' \end{pmatrix} \begin{pmatrix} g & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & gQ - P \\ 0 & 3Q \end{pmatrix} \begin{pmatrix} P & Q \\ 1 & 0 \end{pmatrix} \begin{pmatrix} y & x \\ y' & x' \end{pmatrix}$$
$$= Q \begin{pmatrix} x & x' \\ y & y' \end{pmatrix} \begin{pmatrix} g & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} g & 1 \\ 3 & 0 \end{pmatrix} \begin{pmatrix} y & x \\ y' & x' \end{pmatrix}$$
$$= Q \begin{pmatrix} x & x' \\ y & y' \end{pmatrix} \begin{pmatrix} g & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} g & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} y & x \\ y' & x' \end{pmatrix}$$

Firstly suppose that $g = 1$. Then the first two matrices correspond to the continued fraction

$$[a_0 , a_1 , \ldots , a_{h-1} , 1] = [a_0 , w , 1] ,$$

whence the last two matrices correspond to the expansion

$$[1 , a_{h-1} , a_{h-2} , \ldots , a_1] = [1 , \overleftarrow{w}] .$$

Thus the continued fraction expansion of X/Y, where $X^2 - DY^2 = -3$, is twisted symmetric with the symmetry *twisted* in that the second half of the expansion is the reverse of the first half — omitting the zero-th partial quotient, *and* is divided by 3. If $g = 0$ we again have twisted symmetry. The first half of the expansion is $[a_0 , w]$ and the second half is the continued fraction expansion of the rational $[\overleftarrow{w}]$ multiplied by 3.

THEOREM II. *Suppose that either* $g = 0$ *or* $g = 1$ *and* $(3 + g^2)Q_h = Q_{h-1} + 2gP_h$ *in the principal cycle, and* $x^2 - Dy^2 = (-1)^h Q_h$. *Then* $X^2 - DY^2 = -3$, *where*

$$Q_h^2 X = 2Dxy - (P_h - gQ_h)(x^2 + Dy^2)$$
$$Q_h^2 Y = (x^2 + Dy^2) - 2(P_h - gQ_h)xy .$$

Moreover the continued fraction expansion of X/Y *is twisted symmetric. Its first half is the expansion of* x/y *with* g *appended and its second half is the reverse of that first half — omitting the zero-th partial quotient, and is twisted by division by* 3. [*That entails that when* $g = 0$ *its first half is*

the expansion of x/y and its second half is the reverse of that first half — omitting the zero-th partial quotient, and is twisted by multiplication by 3.]

Proof. Having been signalled by $(3+g^2)Q_h = Q_{h-1} + 2gP_h$ we have

$$P_h^2 - D = -Q_h Q_{h-1} = 2gQ_hP_h - (g^2+3)Q_h^2$$

and thus the representation $D = (P_h - gQ_h)^2 + 3Q_h^2$. But then we have seen explicitly that

$$\begin{pmatrix} x & Dy \\ y & x \end{pmatrix} \begin{pmatrix} P_h - gQ_h & -D \\ -1 & P_h - gQ_h \end{pmatrix} \begin{pmatrix} x & Dy \\ y & x \end{pmatrix} = -Q^2 \begin{pmatrix} X & DY \\ Y & X \end{pmatrix},$$

yielding the claims.

Another example. It is easy to see that $34798636^2 - 1891 \cdot 800233^2 = -3$ and also $35308981699^2 - 1891 \cdot 811968962^2 = -3$. With $\sqrt{\beta} = \sqrt{1891}$,

	n	x_n	y_n
$(\beta + 0)/1 = 43 - (\overline{\beta} + 43)/1$	0	43	1
$(\beta + 43)/42 = 2 - (\overline{\beta} + 41)/42$	1	87	2
$(\beta + 41)/5 = 16 - (\overline{\beta} + 39)/5$	2	1435	33
$(\beta + 39)/74 = 1 - (\overline{\beta} + 35)/74$	3	1522	35
$(\beta + 35)/9 = 8 - (\overline{\beta} + 37)/9$	4	13611	313
$(\beta + 37)/58 = 1 - (\overline{\beta} + 21)/58$	5	15133	348
$(\beta + 21)/25 = 2 - (\overline{\beta} + 29)/25$	6	43877	1009
$(\beta + 29)/42 = 1 - (\overline{\beta} + 13)/42$	7	59010	1357
$(\beta + 13)/41 = 1 - (\overline{\beta} + 28)/41$	8	102887	2366
$(\beta + 28)/27 = 2 - (\overline{\beta} + 26)/27$	9	264784	6089
$(\beta + 26)/45 = 1 - (\overline{\beta} + 19)/45$	10	367671	8455
$(\beta + 19)/34 = 1 - (\overline{\beta} + 15)/34$	11	632455	14544
$(\beta + 15)/49 = 1 - (\overline{\beta} + 34)/49$	12	1000126	22999
$(\beta + 34)/15 = 5 - (\overline{\beta} + 41)/15$	13	5633085	129539
$(\beta + 41)/14 = 6 - (\overline{\beta} + 43)/14$	14	34798636	800233
$(\beta + 43)/3 = 28 - (\overline{\beta} + 41)/3$	15	979994893	22536063
$(\beta + 41)/70 = 1 - (\overline{\beta} + 29)/70$	16	1014793529	23336296
$(\beta + 29)/15 = 4 - (\overline{\beta} + 31)/15$	17	5039169009	115881247
$(\beta + 31)/62 = 1 - (\overline{\beta} + 31)/62$	18	6053962538	139217543
$(\beta + 31)/15 = 4 - (\overline{\beta} + 29)/15$	19	29255019161	672751419
$(\beta + 29)/70 = 1 - (\overline{\beta} + 41)/70$	20	35308981699	811968962
$(\beta + 41)/3 = \ldots$			

where $4Q_6 = 4 \cdot 25 = 58 + 2 \cdot 21 = Q_5 + 2P_6$, and also $Q_{12} = 49 = 15 + 34 = Q_{13} + P_{13}$. We should also notice that it happens to happen that $4Q_6 = 4 \cdot 25 = 42 + 2 \cdot 29 = Q_7 + 2P_7$. We have that

$$\begin{pmatrix} y_5 & x_5 \\ y_4 & x_4 \end{pmatrix} = \begin{pmatrix} 348 & 15133 \\ 313 & 13611 \end{pmatrix}.$$

Our arguments pretend to show that the expansion $[43\,,\,2\,,\,16\,,\,1\,,\,8\,,\,1]$ continues with the partial quotient 1 and then with the partial quotients corresponding to

$$\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 348 & 15133 \\ 313 & 13611 \end{pmatrix} = \begin{pmatrix} 661 & 28744 \\ 1044 & 45399 \end{pmatrix}.$$

According to our description we should have

$$\begin{pmatrix} 661 & 28744 \\ 1044 & 45399 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \times$$
$$\times \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 6 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 43 \\ 1 & 3 \end{pmatrix}.$$

This is indeed the case. The displayed detail of this decomposition is

661	28744	
1044	45399	0
661	28744	1
383	16655	1
278	12089	1
105	4566	2
68	2957	1
7	1609	1
31	1348	1
6	261	5
1	43	6
0	3	

We also note that, as alleged,

$$Q_6^2 X = 2 \cdot 1891 x_5 y_5 - (P_6 - Q_6)(x_5^2 + 1891 y_5^2)$$
$$= 2 \cdot 1891 \cdot 15133 \cdot 348 - (21 - 25)(15133^2 + 1891 \cdot 348^2) = 25^2 \cdot 34798636$$

and

$$\begin{aligned} Q_6^2 Y &= (x_5^2 + 1891 y_5^2) - 2(P_6 - Q_6) x_5 y_5 \\ &= (15133^2 + 1891 \cdot 348^2) - 2(21 - 25)15133 \cdot 348 = 25^2 \cdot 800233 . \end{aligned}$$

The continued fraction expansion following the signal $Q_{12} = 49 = 15+34 = Q_{13} + P_{13}$ should correspond to

$$\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} y_{12} & x_{12} \\ y_{11} & x_{11} \end{pmatrix} = \begin{pmatrix} 31454 & 1367797 \\ 6089 & 264784 \end{pmatrix} .$$

Indeed,

$$31454/6089 = [5\,,\,6\,,\,28\,,\,1\,,\,4\,,\,1\,,\,4\,,\,1]$$

in accordance with prediction and showing that the present identity signals the other solution to $X^2 - 1891Y^2 = -3$. Indeed our first signal arose from the representation $1891 = 4^2 + 3 \cdot 25^2 = 21^2 - 21.50 + 50^2$ whilst this second signal arises from the representation $1891 = 34^2 + 34 \cdot 15 + 15^2$. It is not unamusing to compound these two representations obtaining both $D^2 = 279^2 - 279 \cdot 2015 + 2015^2$ and $D^2 = 1464^2 - 1464 \cdot 2135 + 2135^2$. It follows that $1891 = 31 \cdot 61$. That's clear because the greatest common divisor of 279 and 2015 is 31, and the greatest common divisor of 1464 and 2135 is 61.

The signal $4Q_6 = Q_7 + 2P_7$ is in fact conjugate to a signal happening to coincide in position with the signal conjugate to $4Q_6 = Q_5 + 2P_6$. We shall see in the next section that it of course leads naturally to the first solution, by exactly computations already provided.

The conjugate cases. We now deal with the formulas appropriate to the conjugate cases. To obtain these cases we consider the ideal $\langle 3Q_h, \sqrt{D}+L\rangle$ composed sequentially with $\langle 3Q_h^2, \sqrt{D}-L\rangle$ and then with $\langle 3Q_h, \sqrt{D}+L\rangle$. The compositions correspond sequentially to a matrix product

$$\begin{aligned} &\begin{pmatrix} x & Dy \\ y & x \end{pmatrix} \begin{pmatrix} L & -D \\ -1 & L \end{pmatrix} \\ &\qquad = \begin{pmatrix} x & x' \\ y & y' \end{pmatrix} \begin{pmatrix} 1 & L \\ 0 & 3Q \end{pmatrix} \begin{pmatrix} 3Q^2 & -L \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ -1 & L \end{pmatrix} \\ &\qquad\qquad = 3Q \begin{pmatrix} x & x' \\ y & y' \end{pmatrix} \begin{pmatrix} Q & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ -1 & L \end{pmatrix} . \end{aligned}$$

The last pair of matrices may be 'simplified' to yield

$$\begin{pmatrix} 0 & -1 \\ -1 & -g \end{pmatrix} \begin{pmatrix} 1 & -L-gQ \\ 0 & Q \end{pmatrix}$$

$$\text{or } -\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} g & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -L-gQ \\ 0 & Q \end{pmatrix}.$$

Setting $L = P_{h+1} - gQ_h$, these matrices detail respectively the following equivalent configurations in a notional continued fraction expansion:

$$\begin{aligned} &\vdots \\ (\sqrt{D} - P_{h+1})/Q_h &= -g - (-\sqrt{D} + L)/Q_h \\ (\sqrt{D} + L)/3Q_h &= \quad \dots \end{aligned}$$

which is $(\sqrt{D} - P_{h+1})/Q_h = [-g\,,\,(\sqrt{D}+L)/3Q_h]$; or

$$\begin{aligned} (\sqrt{D} + L)/3Q_h &= 0 - (-\sqrt{D} - L)/3Q_h \\ (\sqrt{D} - L)/Q_h &= g - (-\sqrt{D} + P_{h+1})/Q_h \\ (\sqrt{D} + P_{h+1})/Q_{h+1} &= 0 - (-\sqrt{D} - P_{h+1})/Q_{h+1} \\ (\sqrt{D} - P_{h+1})/Q_h &= \dots \end{aligned}$$

This is $(\sqrt{D}+L)/3Q_h = [0\,,g\,,0\,,(\sqrt{D}-P_{h+1})/Q_h]$. If $g = 0$ either expansion just reports that $Q_{h+1} = 3Q_h$. Of course we have recalled that $D = (P_{h+1} - gQ_h)^2 + 3Q_h^2$ and $(3+g^2)Q_h = Q_{h+1} + 2gP_{h+1}$.

The second composition now yields

$$-3Q\begin{pmatrix} x & x' \\ y & y' \end{pmatrix} \begin{pmatrix} Q & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -L \end{pmatrix} \begin{pmatrix} L & 3Q \\ 1 & 0 \end{pmatrix} \begin{pmatrix} y & x \\ y' & x' \end{pmatrix}$$

$$= -3Q^2 \begin{pmatrix} x & x' \\ y & y' \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} y & x \\ y' & x' \end{pmatrix},$$

corresponding to some ideal $\langle 3, \sqrt{D} + p \rangle$.

THEOREM III. *Suppose that* $(3+g^2)Q_h = Q_{h+1} + 2gP_{h+1}$ *in the principal cycle, with either* $g = 0$ *or* $g = 1$, *and* $x^2 - Dy^2 = (-1)^{h+1}3Q_h$. *Then* $X^2 - DY^2 = -3$, *where*

$$\begin{aligned} 3Q_h^2 X &= 2Dxy - (P_{h+1} - gQ_h)(x^2 + Dy^2) \\ 3Q_h^2 Y &= (x^2 + Dy^2) - 2(P_{h+1} - gQ_h)xy\,. \end{aligned}$$

Moreover, the continued fraction expansion of X/Y is twisted symmetric. Its first half is the expansion of x/y and its second half is the reverse of that first half — omitting the zero-th partial quotient, and is twisted by division by 3.

Proof. We have seen explicitly that

$$\begin{pmatrix} x & Dy \\ y & x \end{pmatrix} \begin{pmatrix} P_h - gQ_h & -D \\ -1 & P_h - gQ_h \end{pmatrix} \begin{pmatrix} x & Dy \\ y & x \end{pmatrix} = -3Q^2 \begin{pmatrix} X & DY \\ Y & X \end{pmatrix},$$

yielding the claims.

This is all very well if x/y is a convergent, but it is not if $g = 1$. However, above, we saw the continued fraction configuration

$$\begin{aligned} &\vdots \\ (\sqrt{D} + P_{h+1})/Q_{h+1} &= 0 \quad - (-\sqrt{D} - P_{h+1})/Q_{h+1} \\ (\sqrt{D} - P_{h+1})/Q_h &= -g - (-\sqrt{D} + L)/Q_h \\ (\sqrt{D} + L)/3Q_h &= \quad \dots \end{aligned}$$

so

$$\begin{pmatrix} x & x' \\ y & y' \end{pmatrix} = \begin{pmatrix} x_h & x_{h-1} \\ y_h & y_{h-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -g & 1 \\ 1 & 0 \end{pmatrix}.$$

Hence we have the alternative

COROLLARY. *Set $x_h^2 - Dy_h^2 = (-1)^{h+1}Q_{h+1}$ and $x_{h-1}^2 - Dy_{h-1}^2 = (-1)^h Q_h$. Suppose that either $g = 0$ or $g = 1$ and $(3 + g^2)Q_h = Q_{h+1} + 2gP_{h+1}$ in the principal cycle. Then $X^2 - DY^2 = -3$, where*

$$\begin{aligned} 3Q_h^2 X = {} & 2D(x_h - gx_{h-1})(y_h - gy_{h-1}) \\ & - (P_{h+1} - gQ_h)\big((x_h - gx_{h-1})^2 + D(y_h - gy_{h-1})\big) \end{aligned}$$

$$\begin{aligned} 3Q_h^2 Y = {} & \big((x_h - gx_{h-1})^2 + D(y_h - gy_{h-1})^2\big) \\ & - 2(P_{h+1} - gQ_h)(x_h - gx_{h-1})(y_h - gy_{h-1}). \end{aligned}$$

Moreover, the continued fraction expansion of X/Y is twisted symmetric. Its first half is the expansion of x_{h-1}/y_{h-1} followed by the partial quotient $a_h - g$ and its second half is the reverse of that first half — omitting the zero-th partial quotient, and is twisted by division by 3.

If this seems too contorted one could replace the last paragraph by

Moreover, the continued fraction expansion of X/Y is twisted symmetric. Its first half is the expansion of x_h/y_h and its second half is the reverse of that first half — omitting the zero-th partial quotient, and is twisted by the linear fractional transformation $\begin{pmatrix} 3+g^2 & -g \\ -g & 1 \end{pmatrix}$.

Yet a further example. It's clear that $1352234^2 - 5719 \cdot 17881^2 = -3$ and $545397694^2 - 5719 \cdot 7211959^2 = -3$. Here

$$\sqrt{5719} = [75\,,1\,,1\,,1\,,1\,,1\,,16\,,5\,,1\,,1\,,5\,,1\,,1\,,49\,,1\,,6\,,1\,,\ldots]$$

where $Q_7 = 27 = 3 \cdot 9 = 3Q_6$ and $Q_9 = 75 = 3 \cdot 25 = 3Q_{10}$. These signals belong respectively to the representations $5719 = 74^2 + 3 \cdot 9^2 = 65^2 + 65 \cdot 18 + 18^2$ and $5719 = 62^2 + 3.25^2 = 37^2 + 37.50 + 50^2$. One notes that $Q_{13} = Q_{17} = 3$.

This and the next example have been 'concised' on the advice of the referee. The reader can readily compute the relevant table [a spreadsheet program is optimal].

The first signal is a conjugate case. We have that

$$\begin{pmatrix} y_6 & x_6 \\ y_5 & x_5 \end{pmatrix} = \begin{pmatrix} 133 & 10058 \\ 8 & 605 \end{pmatrix}.$$

Our arguments suggest that the expansion $[75\,,1\,,1\,,1\,,1\,,1\,,16]$ continues with the partial quotients corresponding to

$$\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 133 & 10058 \\ 8 & 605 \end{pmatrix} = \begin{pmatrix} 133 & 10058 \\ 24 & 1815 \end{pmatrix}$$
$$= \begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 74 \\ 0 & 3 \end{pmatrix}.$$

This is indeed the case. We also note that, again as suggested,

$$3Q_6^2X = 2 \cdot 5719x_6y_6 - P_7(x_6^2 + 5719y_6^2)$$
$$= 2 \cdot 5719 \cdot 10058 \cdot 133 - 74(10058^2 + 5719 \cdot 133^2) = 3 \cdot 9^2 \cdot 1352234$$

and

$$3Q_6^2Y = (x_6^2 + 5719y_6^2) - 2P_7x_6y_6$$
$$= (10058^2 + 5719 \cdot 133^2) - 2 \cdot 74 \cdot 10058 \cdot 133 = 3 \cdot 9^2 \cdot 17881\,.$$

In respect of the second signal we have that

$$\begin{pmatrix} y_9 & x_9 \\ y_8 & x_8 \end{pmatrix} = \begin{pmatrix} 1479 & 111848 \\ 806 & 60953 \end{pmatrix}.$$

Our claim is that the expansion $[75\,,1\,,1\,,1\,,1\,,16\,,5\,,1\,,1]$ continues with the partial quotients corresponding to

$$\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1479 & 111848 \\ 806 & 60953 \end{pmatrix} = \begin{pmatrix} 4437 & 335544 \\ 806 & 60953 \end{pmatrix}$$
$$= \begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 49 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\times$$
$$\times \begin{pmatrix} 6 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 73 \\ 0 & 3 \end{pmatrix}.$$

We also note that just as suggested,

$$Q_{10}^2 X = 2\cdot 5719 x_9 y_9 - P_{10}(x_9^2 + 5719 y_9^2)$$
$$= 2\cdot 5719\cdot 111848\cdot 1479 - 62(111848^2 + 5719\cdot 1479^2) = 25^2\cdot 545397694$$

and

$$Q_{10}^2 Y = (x_9^2 + 5719 y_9^2) - 2P_{10} x_9 y_9$$
$$= (111848^2 + 5719\cdot 1479^2) - 2\cdot 62\cdot 111848\cdot 1479 = 25^2\cdot 7211959\,.$$

And yet another example. It takes one only a few moments to confirm that $169911899891^2 - 9139\cdot 1777356134^2 = -3$ and that similarly we have $54144725563676^2 - 9139\cdot 566378577169^2 = -3$. Here

$$\sqrt{9139} = [95\,,1\,,1\,,2\,,20\,,1\,,5\,,2\,,2\,,1\,,1\,,1\,,1\,,1\,,5\,,$$
$$1\,,3\,,18\,,1\,,6\,,7\,,1\,,1\,,63\,,5\,,\ldots].$$

One may see the signal $4Q_{16} = 4\cdot 49 = 10 + 2\cdot 93 = Q_{17} + 2P_{17}$ arising from the representation $D = 44^2 + 3\cdot 49^2 = 5^2 - 5\cdot 98 + 98^2$. There is also $Q_{13} = 107 = 30 + 77 = Q_{14} + P_{14}$ arising from the representation $D = 30^2 + 30\cdot 77 + 77^2$.

According to our arguments the continued fraction expansion

$$[95\,,1\,,1\,,2\,,20\,,1\,,5\,,2\,,2\,,1\,,1\,,1\,,1\,,1\,,5\,,1]$$

will have the partial quotient $2 = 3 - 1$ appended. In matrix terms that yields

$$\begin{pmatrix} x_{15} & x_{14} \\ y_{15} & y_{14} \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 21578407 & 18318798 \\ 225720 & 191623 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 61475612 & 21578407 \\ 643063 & 225720 \end{pmatrix}.$$

Now dividing the reversed continued fraction by 3 supplies the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 643063 & 61475612 \\ 225720 & 21578407 \end{pmatrix} = \begin{pmatrix} 643063 & 61475612 \\ 677160 & 64735221 \end{pmatrix}$$

It will be more instructive to display the sequence of calculations providing the decomposition of this matrix, rather than to allege the result. One has in detail

643063	61475612	
677160	64735221	0
643063	61475612	1
34097	3259609	18
29317	2802650	1
4780	456959	6
637	60896	7
321	30687	1
316	30209	1
5	478	63
1	95	5
0	3	

Recall that the first two columns are the sequence of 2×2 matrices obtained as we split off each partial quotient matrix by employing the euclidean algorithm on the rows of the matrices. The a_n, now properly seen to be the quotients of that euclidean algorithm, are displayed in the third column. The last 2×2 matrix displays $P_{25} = p = 95$ and, of course, $Q_{25} = 3$.

Evidently all is well, with truth prevailing. We were halfway to the second solution. Indeed

$$\begin{aligned} 3Q_{16}^2 X &= 2 \cdot 9139(x_{16} - gx_{15})(y_{16} - gy_{15}) \\ &\quad - (P_{17} - gQ_{16})\big((x_{16} - gx_{15})^2 + 9139(y_{16} - gy_{15})^2\big) \\ &= 2 \cdot 9139 \cdot 61475612 \cdot 643063 - (93 - 49)(61475612^2 + 9139 \cdot 643063^2) \\ &= 3 \cdot 49^2 \cdot 54144725563676 \end{aligned}$$

and $3Q_{16}^2Y$

$$= ((x_{16}-gx_{15})^2+9139(y_{16}-gy_{15})^2)-2(P_{17}-gQ_{16})(x_{16}-gx_{15})(y_{16}-gy_{15})$$
$$= (61475612^2 + 9139 \cdot 643063^2) - 2(93-49)61475612 \cdot 643063$$
$$= 3 \cdot 49^2 \cdot 566378577169\,,$$

verifying our formulas.

According to the signal $Q_{13} = 107 = 30+77 = Q_{14}+P_{14}$, the continued fraction expansion

$$[95\,,\,1\,,\,1\,,\,2\,,\,20\,,\,1\,,\,5\,,\,2\,,\,2\,,\,1\,,\,1\,,\,1\,,\,1\,,\,1]$$

continues with the expansion corresponding to

$$\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} 34097 & 3259609 \\ 21138 & 2020753 \end{pmatrix} = \begin{pmatrix} 47056 & 4498465 \\ 8179 & 781897 \end{pmatrix}.$$

The decomposition details are

47056	4498465	
8179	781897	5
6161	588980	1
2018	192917	3
107	10229	18
92	8795	1
15	1434	6
2	191	7
1	97	1
1	94	1
0	3	

precisely as predicted. The last 2×2 matrix displays $P_{23} = p = 94$ and, of course, $Q_{23} = 3$.

We also confirm that

$$Q_{14}^2X = 4 \cdot 9139x_{13}y_{13} - (2P_{14}+Q_{14})(x_{13}^2 + 9139y_{13}^2)$$
$$= 4 \cdot 9139 \cdot 3259609 \cdot 34097 - (2 \cdot 77 + 30)(3259609^2 + 9139 \cdot 34097^2)$$
$$= 30^2 \cdot 169911899891\,,$$

and

$$Q_8^2Y = 2(x_{13}^2 + 9139y_{13}^2) - 2(2P_{14}+Q_{14})x_{13}y_{13}$$
$$= 2(3259609^2 + 9139 \cdot 34097^2) - 2(2 \cdot 77 + 30)3259609 \cdot 34097$$
$$= 30^2 \cdot 1777356134\,.$$

5. Signals in Arbitrary Cycles

Our preceding discussion shows that if there is a solution to $X^2 - DY^2 = -3$ then D has representations $D = M^2 + MN + N^2$ and there are signals

$$\begin{array}{lll} 4Q_h = Q_{h-1} + 2P_h & \text{or} \quad 3Q_h = Q_{h-1} & \text{or} \quad Q_{h-1} = Q_h + P_h \\ 4Q_h = Q_{h+1} + 2P_{h+1} & 3Q_h = Q_{h+1} & Q_{h+1} = Q_h + P_{h+1}. \end{array}$$

That is, there are reduced elements $(\sqrt{D} + P_h)/Q_h$, or $(\sqrt{D} + P_{h+1})/Q_h$ yielding the signal, with $Q_h = N$ or $2Q_h = N$ according as N is odd or even, occurring in some continued fraction cycle.

A priori, signals may occur in any cycle whatsoever. Our arguments only entail that if a signal occurs in some ideal class, or cycle — thus if there is a reduced element $(\sqrt{D}+P_h)/Q_h$ corresponding to an ideal $\langle Q_h, \sqrt{D}+P_h\rangle$ in that cycle, respectively a reduced element $(\sqrt{D}+P_{h+1})/Q_h$ corresponding to an ideal $\langle Q_h, \sqrt{D} + P_{h+1}\rangle$ in that cycle if we are referring to a conjugate signal from the second line in the list above — then there is an ideal $\langle 3, \sqrt{D} + p\rangle$ in the ideal class that is the square of the signalling class.

However, if there is a solution to $X^2 - DY^2 = -3$ then, in particular, the ideal $\langle 3, \sqrt{D} + p\rangle$ must lie in the principal class. Hence, if there is a solution, the signals must occur in ambiguous classes, for those are precisely the classes whose square is principal. Conversely, if there is a signal in some ambiguous class then there is a principal ideal $\langle 3, \sqrt{D}+p\rangle$, thence a solution to $X^2 - DY^2 = -3$, and all signals must occur in ambiguous classes.

We shall address the question whether there are signals in the principal class, given that there is a solution to $X^2 - DY^2 = -3$. We also briefly explain how a signal in an arbitrary cycle containing an ambiguous ideal permits one to construct a solution to $X^2 - DY^2 = -3$.

Counting ambiguous classes and representations. We will be dealing with squarefree D divisible by primes congruent to 1 (mod 3), and possibly by 3. If D is divisible by exactly ν different primes congruent to 1 (mod 3) then there are exactly 2^ν ambiguous ideals, respectively $2^{\nu+1}$ ambiguous ideals, in the order $\mathbb{Z}[\sqrt{D}]$ — according as $3 \nmid D$ or $3 \mid D$. Half of these ambiguous ideals have odd norm S dividing D and half have even norm $2S$ dividing $2D$. These matters are well known; there is a fresh discussion in [2].

We have to distinguish the cases $D \equiv 1 \pmod 4$ and $D \equiv -1 \pmod 4$. In the latter case we have nothing to add at this point. In the former case we note that the maximal order of $\mathbb{Q}(\sqrt{D})$ is in fact $\mathbb{Z}[(\sqrt{D}+1)/2]$. We now remark that

PROPOSITION 10. *Suppose* $D \equiv 1 \pmod 4$. *Then if an ideal* $\langle 2S, \sqrt{D}+R\rangle$ *is an ambiguous ideal, then it is an ideal of the order* $\mathbb{Z}[(\sqrt{D}+1)/2]$. *So any ideal* $\langle Q, \sqrt{D}+P\rangle$ *of* $\mathbb{Z}[\sqrt{D}]$ *equivalent to it must have* Q *even. Conversely, if an ideal* $\langle Q, P+\sqrt{D}\rangle$ *has even norm* Q *but is not an ideal of* $\mathbb{Z}[(\sqrt{D}+1)/2]$, *then* $4 \mid Q$ *and* $4 \parallel (D-P^2)$.

Proof. Set $\delta = (\sqrt{D}+1)/2$. Our first claim is that the ideal $\langle 2S, \sqrt{D}+R\rangle$ is an ideal $\langle S, \delta+(R-1)/2\rangle$ of the order $\mathbb{Z}[\delta]$. Now, since $D \equiv 1 \pmod 4$ and $2S \mid (R^2-D)$, certainly R is odd and $4 \mid (R^2-D)$, and since the ideal is ambiguous, $2S \mid 2R$ so $S \mid D$. Thus S is odd. Our first claim reduces to $S \mid \left((\frac{1}{4}(1-D)+\frac{1}{2}(R-1)+\frac{1}{4}(R-1)^2\right) = \frac{1}{4}(R^2-D)$, which is the case.

Conversely, $\langle Q, P+\sqrt{D}\rangle$ is not an ideal of $\mathbb{Z}[\delta]$ if $\frac{1}{2}Q \nmid \frac{1}{4}(P^2-D)$ notwithstanding that $Q \mid (P^2-D)$. It is easy to see that this is so only if $4 \mid Q$ whilst $4 \parallel (P^2-D)$, as alleged.

In the case of the signal $Q_{h-1} = Q_h + P_h$, or $Q_{h+1} = Q_h + P_{h+1}$, we have Q_h odd. For the remaining signals we have $D = L^2 + 3Q_h^2$. A simple check modulo 4 confirms that Q_h is even exactly when $D \equiv 1 \pmod 4$.

Suppose that $3Q_h = Q_{h-1}$ or $3Q_h = Q_{h-1}$. Since $(P_h^2 - D) = -Q_{h-1}Q_h$, respectively $(P_{h+1}^2 - D) = -Q_hQ_{h+1}$, plainly $4 \mid Q_h$ cannot be accompanied by $4 \parallel (P_h^2-D)$, nor respectively $4 \parallel (P_{h+}^2-D)$. Quite similarly, neither $4Q_h = Q_{h-1}+2P_h$ nor $4Q_h = Q_{h+1}+2P_{h+1}$ allow both $4 \mid Q_h$ and $4 \parallel (P_h^2-D)$, respectively $4 \parallel (P_{h+}^2-D)$. Thus if Q_h is even our signals must occur in cycles of the order $\mathbb{Z}[(\sqrt{D}+1)/2]$. Hence, if $D \equiv 1 \pmod 4$ at most the signal $Q_{h-1} = Q_h + P_h$, as always closely accompanied by $Q_{h+1} = Q_h + P_{h+1}$, can occur in the principal cycle of the order $\mathbb{Z}[\sqrt{D}]$.

Relating signals to a solution. We will generalise the remarks of the previous section, for the case when a signal occurs in an arbitrary ambiguous cycle. The central remark there was that the presence of a complete quotient $(\sqrt{D}+P_h)/Q_h$ in the principal cycle entails an equation $(x-\sqrt{D}y)(x+\sqrt{D}y) = x^2-Dy^2 = (-1)^hQ_h$ and corresponds to a matrix decomposition

$$\begin{pmatrix} x & Dy \\ y & x \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_{h-1} & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & P_h \\ 0 & Q_h \end{pmatrix}$$
$$= N_{h-1}\begin{pmatrix} 1 & P_h \\ 0 & Q_h \end{pmatrix}.$$

Suppose now that $(\sqrt{D}+P_h)/Q_h$ is a complete quotient of an arbitrary element $\gamma = (\sqrt{D}+R)/S$. That is,

$$\gamma = [b_0\,,\, b_1\,,\, \ldots\,,\, b_{h-1}\,,\, (\sqrt{D}+P_h)/Q_h\,].$$

In effect, we have set $P_0 = R$ and $Q_0 = S$. For use below, we recall that the element γ is ambiguous if and only if $S \mid 2R$.

We need little more than to observe that

$$(Sx - Ry) - \sqrt{D}y = S(x - \frac{\sqrt{D}+R}{S}y).$$

It is then plain that our earlier remark becomes that the presence of a complete quotient $(\sqrt{D}+P_h)/Q_h$ in the continued fraction expansion of $\gamma = (\sqrt{D}+R)/S$ entails an equation

$$(x-\gamma y)(x-\overline{\gamma}y) = x^2 - (2R/S)xy - \big((-D+R^2)/S^2\big)y^2 = (-1)^h Q_h\,,$$

and corresponds to a matrix decomposition

$$\begin{aligned} S^{-2}\begin{pmatrix}1&0\\0&S\end{pmatrix}\begin{pmatrix}1&R\\0&1\end{pmatrix}\begin{pmatrix}Sx-Ry & Dy\\ y & Sx-Ry\end{pmatrix}\begin{pmatrix}1&-R\\0&1\end{pmatrix}\begin{pmatrix}S&0\\0&1\end{pmatrix} \\ = \begin{pmatrix}x & -\gamma\overline{\gamma}y\\ y & x-(\gamma+\overline{\gamma})y\end{pmatrix} \\ = \begin{pmatrix}b_0&1\\1&0\end{pmatrix}\begin{pmatrix}b_1&1\\1&0\end{pmatrix}\cdots\begin{pmatrix}b_{h-1}&1\\1&0\end{pmatrix}\begin{pmatrix}1&(P_h-R)/S\\0&Q_h/S\end{pmatrix}. \end{aligned}$$

PROPOSITION 11. *Suppose that* $(\sqrt{D}+P)/Q$ *and* $(\sqrt{D}+P')/Q'$ *are complete quotients of* $\gamma = (\sqrt{D}+R)/S$ *yielding the norms* $(x-\gamma y)(x-\overline{\gamma}y) = \pm Q$ *and* $(x'-\gamma y')(x'-\overline{\gamma}y') = \pm Q'$. *If* γ *is ambiguous then composition of the ideals* $\langle Q, \sqrt{D}+P\rangle$ *and* $\langle Q', \sqrt{D}+P'\rangle$ *corresponds to the matrix product*

$$\begin{aligned} &\begin{pmatrix}1&-R\\0&1\end{pmatrix}\begin{pmatrix}S&0\\0&1\end{pmatrix}\begin{pmatrix}x & -\gamma\overline{\gamma}y\\ y & x-(\gamma+\overline{\gamma})y\end{pmatrix}\times \\ &\qquad\times\begin{pmatrix}x' & -\gamma\overline{\gamma}y'\\ y' & x'-(\gamma+\overline{\gamma})y'\end{pmatrix}\begin{pmatrix}1&0\\0&S\end{pmatrix}\begin{pmatrix}1&R\\0&1\end{pmatrix} \end{aligned}$$

and yields a matrix corresponding to an ideal in the principal cycle.

Proof. The product of the inner pair of matrices is again a matrix of their shape. The outer matrices conjugate that product to yield a matrix

$$S\begin{pmatrix}X & DY\\ Y & X\end{pmatrix}$$

with

$$X = Sxx' - \big((R^2 - D)/S\big)yy' - R\big((xy' + x'y) + (2R/S)yy'\big)$$
$$Y = xy' + x'y - (2R/S)yy'.$$

Suppose that G is the greatest common divisor of Q, Q' and $(P + P')$, and is therefore the greatest common divisor of X and Y. Then, according to our remarks in §4 above, the product corresponds to an ideal of norm QQ'/G^2 in the principal cycle.

It is rather interesting to notice the role played by the integrality of $2R/S$, that is, the ambiguity of γ, in ensuring that X and Y be integers. Of course this is only a mechanical restatement of the fact that we are going to arrive in the principal cycle only if we started from a cycle with ambiguous forms.

In summary: Each pair of signal and ambiguous ideal in the same cycle yields a solution to $X^2 - DY^2 = -3$ by the formulas and arguments of §4. We suffer only the additional complication of having to conjugate by appropriate matrices depending on the given ambiguous ideal.

Relating signals and ambiguous ideals. It is plain that the equation $X^2 - DY^2 = -3$ has either no, one or two solutions. Of course in saying that we refer to *primitive* non-associated solutions; we identify solutions differing only by multiplication by a unit of $\mathbb{Q}(\sqrt{D})$. We now remark that if the equation has s solutions then there are at most s distinct pairs of conjugate signals in each ambiguous cycle. Our remarks immediately above showed that events in an arbitrary ambiguous cycle are mapped to the principal cycle by matrix conjugation. Thus it is sufficient to consider just the principal cycle. Then our remark is clear from infrastructural considerations. Were we to have more than s signals in the first half of the principal cycle, we would obtain more than s primitive solutions to $X^2 - DY^2 = -3$. We should add that signals are to be considered distinct if they arise from different representations or are of different kind — the two 'kinds' being those signals arising from a representation $D = L^2 + 3Q^2$ and those arising from a representation $D = M^2 + MQ + Q^2$ with Q odd. That means that 'happens to happenings', such as we saw in the example $D = 1891$, or such as we always see for signals of the second kind, do not constitute distinct signals.

It remains to count solutions, representations and signals, and ambiguous ideals.

THEOREM IV. *Suppose* $X^2 - DY^2 = -3$ *has* $s > 0$ *primitive solutions and that* D *is squarefree and is divisible by* ν *distinct primes congruent to* 1 *modulo* 3.

If $3 \mid D$ *then* $s = 1$. *The solution belongs to the ambiguous ideal halfway along the principal cycle. There are indeed two ambiguous ideals per cycle that contains an ambiguous ideal, but, nonetheless, just one conjugate pair of signals in each such cycle. In all there are* $2^{\nu+1}$ *ambiguous ideals, and hence* 2^{ν} *cycles containing an ambiguous ideal. There are just* $2^{\nu-1}$ *essentially distinct representations of* D *with discriminant* -3 *but each gives rise to signals of the two kinds. Thus there are* 2^{ν} *conjugate pairs of distinct signals, one conjugate pair for each cycle containing an ambiguous ideal.*

Henceforth, $3 \nmid D$. *If* $D \equiv -1 \pmod 4$ *then* $s = 2$. *The two solutions are conjugate so there is just one belonging to an ideal in the first half of the principal cycle. There are two ambiguous ideals per cycle containing an ambiguous ideal, and two conjugate pairs of signals are permitted in each such cycle. Indeed, there are* 2^{ν} *ambiguous ideals in all, and hence* $2^{\nu-1}$ *cycles containing an ambiguous ideal. There are just* $2^{\nu-1}$ *essentially distinct representations of* D *with discriminant* -3 *but each gives rise to signals of the two kinds. Thus there are* 2^{ν} *conjugate pairs of distinct signals, two conjugate pairs for each cycle containing an ambiguous ideal.*

If $D \equiv 1 \pmod 4$ *then* $s = 1$ *or* 2 *according as the fundamental unit of* $\mathbb{Q}(\sqrt{D})$ *has norm* -1 *or* $+1$. *In either case there are just* $2^{\nu-1}$ *ambiguous ideals of odd norm and as many as* $2^{\nu-1}$ *essentially distinct representations of* D *with discriminant* -3. *Thus there is a signal of the second kind, to wit a signal arising from a representation* $D = M^2 + MQ + Q^2$ *with* Q *odd, for each ambiguous ideal of odd norm. Hence in either case there are exactly* s *conjugate pairs of signals of the second kind in each ideal cycle containing ambiguous ideals of odd norm. Similarly, there are exactly* s *conjugate pairs of signals of the first kind in each ideal cycle containing ambiguous ideals of even norm.*

COROLLARY. *If* $X^2 - DY^2 = -3$ *has a solution then that solution is signalled, halfway to the solution, in the principal cycle. Specifically, there is at least one signal of the second kind in the principal cycle if* $D \equiv 1 \pmod 4$. *Moreover, in that case the continued fraction expansion of* $(\sqrt{D} + 1)/2$ *displays at least one signal of the first kind.*

Proof. Other than to mention that our appeals were to Proposition 10 in the case $D \equiv 1 \pmod 4$, we only need to justify our allegations concerning

the number of solutions s. The point about $s \neq 0$ is that it expects to be 2, in that the principal cycle, being ambiguous, contains the conjugate of each of its ideals. If $3 \mid D$, however, an ideal $\langle 3, \sqrt{D} + p \rangle$ is conjugate to itself, whilst if the fundamental unit has norm -1 then conjugation also reverses sign, and the conjugate equation shows a norm 3, rather than -3.

6. Concluding Remarks and Acknowledgements

We will always know whether $X^2 - DY^2 = -3$ has solutions, and will be able to compute the solutions if there are any, twice as fast as is naïvely practicable. We have detected new symmetry, albeit twisted, in the continued fraction expansions of certain quadratic irrationals. On the other hand our ideas are plainly too close to the surface to enable us to give sufficient criteria for the existence of solutions in terms of D alone. Of course the presence of signals in all cycles containing ambiguous ideals is both sufficient and necessary, but knowing about halfway signals is only twice as good as knowing in the first place that the continued fraction expansion of $\sqrt{D}$ explicitly reveals the solutions, if there are any. We should also confess to glossing over various questions when $D \equiv 1 \pmod 4$. Our arguments show signals of the first kind, which by Proposition 10 cannot appear in the cycle containing $\langle 1, \sqrt{D} \rangle$, signalling solutions to $X^2 - DY^2 = -3$. But there are also signals, this time properly in the order $\mathbb{Z}[(\sqrt{D} + 1)/2]$ signalling solutions to $(2X - 1)^2 - DY^2 = -12$, rather than to the equation under consideration here. In any case, there will be more about such matters in various sequels.

We have gone to some pains to stay with the equation $X^2 - DY^2 = -3$, yet to lay out our arguments as to readily allow generalisation. Some generalisations, such as that halfway to a solution of $X^2 - DY^2 = -q$ is signalled at least in some cycles with ambiguous ideals if D has a representation $D = L^2 + qQ^2$, or if $q = \square \pm 1$ and D has a representation $D = \square \cdot M^2 \pm MN + N^2$, are fairly evident. We have looked at a variety of such examples. We are conscious that much of what we explain is well known, but not widely known, and that it remains necessary to provide dictionaries translating between the languages of forms, ideals and continued fractions.

The visits — during which many of the present ideas were developed — by the Canadian co-authors to the *ceNTRe* for Number Theory Research at Macquarie University, Sydney were made possible by a grant from the Australian Research Council. We are indebted to Thomas A. Schmidt, then a Macquarie University Research Fellow, for useful discussions during the

critical early stages of the present work.

We are grateful to the referee for his helpful advice.

References

[1] H. W. LENSTRA Jr, *On the calculation of regulators and class numbers of quadratic fields*, J. V. ARMITAGE ed., Journées Arithmétiques 1980, LMS Lecture Notes **56**, Cambridge, 1982, pp. 123–151..

[2] R. A. MOLLIN and A. J. VAN DER POORTEN, *A note on symmetry and ambiguity*, Bull. Austral. Math. Soc. **51** (1995), 215–233.

[3] Oskar PERRON, *Die Lehre von den Kettenbrüchen*, (Chelsea reprint of 1929 edition).

[4] A. J. VAN DER POORTEN, *An introduction to continued fractions*, Diophantine Analysis, LMS Lecture Notes in Math. **109**, ed. J. H. LOXTON and A. J. VAN DER POORTEN, Cambridge University Press, 1986, pp. 99–138.

[5] A. J. VAN DER POORTEN, *Fractions of the period of the continued fraction expansion of quadratic integers*, Bull. Austral. Math. Soc **44** (1991), 155–169.

[6] D. SHANKS, *Class number, a theory of factorization, and genera*, Proc. Symp. Pure Math., **20** (1969 Institute on Number Theory), Amer. Math. Soc., Providence 1971, pp. 415–440, see also *The infrastructure of a real quadratic field and its applications*, Proc. Number Theory Conference, Boulder, 1972.

[7] D. Shanks, *On Gauß and composition*, Number Theory and Applications, Richard A. MOLLIN ed. (NATO – Advanced Study Institute, Banff, 1988), Kluwer Academic Publishers, Dordrecht, 1989, pp. 163–204.

Richard A. Mollin
School of Mathematics
University of Calgary, Alberta T2N 1N4 Canada
ramollin@acs.ucalgary.ca

Alfred J. van der Poorten
Centre for Number Theory Research
Macquarie University NSW 2109 Australia
alf@mpce.mq.edu.au

Hugh C. Williams
Department of Computer Science
University of Manitoba
Winnipeg, Manitoba R3T 2N2 Canada
Hugh_Williams@macmail.cs.umanitoba.ca