BULL. AUSTRAL. MATH. SOC. 11A55, 11J70
VOL. 51 (1995) [215–233]

A NOTE ON SYMMETRY AND AMBIGUITY

R.A. MOLLIN AND A.J. VAN DER POORTEN

We present the relationship between quadratic irrationals whose continued fraction expansion has symmetric period, and ambiguous ideal cycles in real quadratic number fields.

1. INTRODUCTION

We confine ourselves to the symmetry of the period of continued fraction expansions and the ambiguity of ideals or of ideal classes in real quadratic fields. We hope this does not disappoint readers attracted by the depth and generality of our title. It is of course known, and, as we show, is readily re-established that the notions of the title coincide. Nevertheless, this appears not well nor widely known and our incidental remarks seem worth the making. Our exposition is essentially self-contained both because the ambient literature is sometimes confusing and so that we may emphasise the congeniality of our notation and and the generality of our approach.

In particular we provide an extended discussion of ambiguous ideals and ambiguous cycles, material for which it is difficult to find a correct description in the modern literature.

We shall see that a real quadratic irrational has a pure-periodic symmetric continued fraction expansion if and only if it is greater than 1 and has norm -1, and that an element of norm -1 corresponds to to a representation of its radicand as a sum of two squares. An element with integer trace has a symmetric period in a familiar sense about to be detailed below.

Throughout δ denotes a real quadratic irrational integer with trace $\delta + \overline{\delta} = t$ and norm $\delta\overline{\delta} = n$. Thus $\overline{\delta}$ denotes its algebraic conjugate. Evidently, given a real quadratic irrational $\gamma \in \mathbb{Q}(\delta)$ we lose no generality in supposing, as we shall in the sequel, that there are rational integers P, Q so that

$$\gamma = \frac{P + \delta}{Q}$$

Received 26th April, 1994
Work supported in part by grants from the Australian Research Council and a research agreement with Digital Equipment Corporation.

with $Q \mid (\delta + P)(\overline{\delta} + P)$. This is plain because $(a\delta + b)/c = (ac\delta + bc)/c^2$, and of course c^2 divides $\text{Norm}(ac\delta + bc)$, so, for example, we need only replace δ by $ac\delta$ — and that is tantamount to dealing with an element of the order $Z[ac\delta]$ rather than an element of the order $\mathbb{Z}[\delta]$.

2. Ideals and Quadratic Forms

The point is that once $Q \mid \text{Norm}(\delta + P)$ we may remark that

Proposition 1. *For each*

$$\gamma = \frac{\delta + P}{Q}$$

there is a corresponding $\mathbb{Z}$-module $\langle Q, P + \delta \rangle$. In fact, the module is an ideal $\mathcal{I}$, that is, a $\mathbb{Z}[\delta]$-module, in the order $\mathbb{Z}[\delta]$ of the quadratic field $\mathbb{Q}(\delta)$.

Proof: To see this, it suffices to check that $\delta(P + \delta)$ is in $\mathcal{I}$. But

$$\delta(P + \delta) = -(P^2 + tP + n) + (P + t)(P + \delta) = -\text{Norm}(\delta + P) + (P + t)(P + \delta)$$

and $Q \mid \text{Norm}(\delta + P)$ completes the verification. □

Similarly, by constructing

$$(1) \qquad Q(X - \gamma Y)(X - \overline{\gamma} Y) = QX^2 - (t + 2P)XY + \left((n + Pt + P^2)/Q\right)Y^2,$$

and recalling that $Q \mid \text{Norm}(\delta + P) = n + Pt + P^2$, one associates with γ a quadratic form defined over $\mathbb{Z}$. We note that the discriminant of this form is

$$\Delta = (t + 2P)^2 - 4Q(n + Pt + P^2)/Q = t^2 - 4n.$$

In practice, one is principally interested in the two cases $\delta = \sqrt{D}$, with $t = 0$ and $n = -D$, so $\Delta = 4D$; respectively $\delta = \left(\sqrt{D} + 1\right)/2$, with $t = 1$ and $n = (1 - D)/4$, so $\Delta = D$. Since δ is an integer, the latter case applies only if $D \equiv 1 \pmod 4$. We suppose henceforth that D is squarefree. In both cases we are dealing with the real quadratic number field $\mathbb{K} = \mathbb{Q}\left(\sqrt{D}\right)$ and D is classically known as its *fundamental radicand*. In these respective cases $\Delta = 4D$, respectively $\Delta = D$, is called the *fundamental discriminant* of $\mathbb{K}$. Let f be a nonzero integer. In either case, the $\mathbb{Z}$-module $\langle 1, f\delta \rangle$ is an *order* in the ring of integers of $\mathbb{K}$. Since we have done no more than to replace δ by $f\delta$ we see that the associated discriminant is $f^2\Delta$, and that determines the *conductor* $|f|$ of the order.

We now return to our general integer $\delta \in \mathbb{K}$, remarking that the discriminant $t^2 - 4n = f^2\Delta$ reveals the conductor of the order $\mathbb{Z}[\delta]$ in $\mathbb{K}$. We note also that

$\langle a, b + c\delta \rangle$ with a, b, c positive rational integers is an ideal in $\mathbb{Z}[\delta]$ only if c divides both a and b. Indeed, a and c define the ideal and one notices that a is the least rational integer in the ideal. Moreover, ca is referred to as the *norm* of the ideal. We have that $\langle a, b + c\delta \rangle$ is an ideal of $\mathbb{Z}[\delta]$ if and only if $a \equiv b \equiv 0 \mod c$ and $\mathrm{Norm}(b + c\delta) \equiv 0 \mod ca$. If $c = 1$ and $\mathrm{Norm}(b + \delta) \equiv 0 \mod a$ then the said ideal is said to be a *primitive* ideal of $\mathbb{Z}[\delta]$; its norm is a. In the sequel we consider only primitive ideals.

Generally, of course, an ideal $(\beta_1, \beta_2, \ldots, \beta_m)$ in $\mathbb{Z}[\delta]$ is the set of all $\mathbb{Z}[\delta]$-linear combinations of the β's. If the ideal is monogenic, thus if just one generator will do, the ideal is said to be *principal*. The norm of a principal ideal (β) is just $|\mathrm{Norm}\,\beta| = |\beta\overline{\beta}|$, where $\overline{\beta}$ denotes the conjugate of β in $\mathbb{K}$. It is easy to confirm that in an order of a real quadratic number field each ideal needs at most two generators. Indeed, that follows from observing that $\mathbb{Z}[\delta]$ is isomorphic to $\mathbb{Z}^2$. Thus the ideals of Proposition 1 are in fact the most general primitive ideals of the order.

Still recalling general terminology, we mention that an ideal $\mathcal{I}$ is said to be *invertible* if there exists an ideal $\overline{\mathcal{I}}$ in $\mathbb{Z}[\delta]$ so that $\mathcal{I}\overline{\mathcal{I}}$ is principal. One refers to $\overline{\mathcal{I}}$ as the ideal *conjugate* to $\mathcal{I}$. Indeed, the ideal conjugate to $\mathcal{I} = \langle Q, \delta + P \rangle$ is $\overline{\mathcal{I}} = \langle Q, \overline{\delta} + P \rangle$ where $\overline{\delta}$ is the algebraic conjugate of δ. An ideal $\langle a, b + c\delta \rangle$ is invertible if and only if it is *strictly primitive*, namely if $c = 1$ *and* $\gcd\left(a, b, (b^2 + bt + n)/a\right) = 1$. For example, $\langle 9, 15 + \sqrt{306} \rangle$, as an ideal of $\mathbb{Z}[\sqrt{306}]$, is not strictly primitive and is not invertible. Of course, in all decency one should remark that the corresponding element $(15 + \sqrt{306})/9$ is equal to $(5 + \sqrt{34})/3$ which corresponds to the strictly primitive ideal $\langle 3, 5 + \sqrt{34} \rangle$ in the order $\mathbb{Z}[\sqrt{34}]$. However, $\mathcal{I}$ is certainly invertible when it contains an element with norm prime to the conductor. In the example we had $306 = 3^2 \cdot 34$, with conductor 3. We should also mention that an ideal is called *regular* if it is invariant under multiplication by the elements of $\mathbb{K}$. One may check that any nonzero ideal which is either principal, or has norm prime to the conductor, is regular.

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

3. Periodic Continued Fractions

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

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

We shall repeatedly apply the fundamental correspondence, easily established by induction, whereby

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

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

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 $\ldots$'.

Returning to real quadratic irrationals, we now observe that

Proposition 3. *The general step $n = 0, 1, 2, \ldots$ in the continued fraction expansion of $\gamma = [a_0, a_1, \ldots, a_n, \gamma_{n+1}]$ is*

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

Note 1. The relevant formulaire is readily seen to be

$$P_h + P_{h+1} + t = a_h Q_h \text{ and } Q_h Q_{h+1} = -(\delta + P_{h+1})(\bar{\delta} + P_{h+1}) = -\left(n + P_{h+1}t + P_{h+1}^2\right);$$

it is easily verified by induction that the P_h and Q_h all are rational integers.

https://doi.org/10.1017/S0004972700014064 Published online by Cambridge University Press

NOTE 2. The literature, more precisely the 'bible' of the subject [8] and then the ensuing literature uses a somewhat different notation: it denotes the partial quotients by q_h — which we avoid so that we may adopt an alternative standard of denoting the convergents by p_h/q_h — and the convergents by A_h/B_h. More to the point: its 'standard' complete quotient is taken to be of the shape $\left(P_h+\sqrt{D}\right)/Q_h$ whereas we have $(P_h+\delta)/Q_h$. Our choice is not an arbitrary deviation even when we have no more malice in mind than just taking $\delta=\sqrt{D}$ or $\delta=\left(\sqrt{D}+1\right)/2$. Indeed, our Q_h have a uniform intrinsic meaning, whereas the older notation must distinguish those two basic cases. Specifically, our Q_h are exactly the norms of the reduced ideals. Of course, we also have the convenience of being able to deal with arbitrary orders whilst reserving D for the fundamental radicand, whereas the notation of [8] has to deal with not necessarily squarefree D.

It is a basic fact that 'Pell's equation'

$$(2)\qquad (x-\gamma y)(x-\overline{\gamma}y)=x^2-((t+2P)/Q)xy+\left((n+tP+P^2)/Q^2\right)y^2=\pm 1$$

has solutions in integers x and y, with $y\neq 0$. Indeed, by Dirichlet's box principle, and because γ is irrational, there certainly are infinitely many pairs of integers X,Y so that $|X-\gamma Y|<1/Y$, so $|(X-\gamma Y)(X-\overline{\gamma}Y)|<1+|\gamma-\overline{\gamma}|$. Hence, again by the box principle, we may choose distinct pairs X,Y and X',Y' so that

$$(X-\gamma Y)(X-\overline{\gamma}Y)=(X'-\gamma Y')(X'-\overline{\gamma}Y')=k,\ \text{say and}\ X\equiv X', Y\equiv Y'\pmod{k}.$$

Of course we remain undisturbed by it not having been specified that γ be an algebraic integer. For if not, it has a denominator d, say, and it suffices either to consider Y as replaced by dY throughout or, better, to cope with k being an element of $(1/d)\mathbb{Z}$. In any case, it is now straightforward to verify that

$$x=(XX'-(\gamma+\overline{\gamma})XY'+\gamma\overline{\gamma}YY')/k \text{ and } y=(XY'-X'Y)/k$$

yields the alleged solution to Pell's equation.

PROPOSITION 4. *Given a solution (x,y), with $y\neq 0$, to Pell's equation (2), each decomposition*

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

entails the pure-periodic continued fraction expansion

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

https://doi.org/10.1017/S0004972700014064 Published online by Cambridge University Press

PROOF: Since the cited matrix is a unimodular matrix with integer entries it may be decomposed as a product of elementary row transformations with integers a_i. Given the decomposition, suppose that

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

Then by the correspondence of Proposition 2 and the meaning of periodicity, we have

$$\begin{aligned}\alpha = [\overline{a_0, a_1, \ldots, a_r}] &= [a_0, a_1, \ldots, a_r, \alpha] \\ &\longleftrightarrow \begin{pmatrix} x & -\gamma\overline{\gamma}y \\ y & x-(\gamma+\overline{\gamma})y \end{pmatrix}\begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x\alpha-\gamma\overline{\gamma}y & x \\ y\alpha+x-(\gamma+\overline{\gamma})y & y \end{pmatrix} \\ &\longleftrightarrow \alpha = (x\alpha-\gamma\overline{\gamma}y)/(y\alpha+x-(\gamma+\overline{\gamma})y) \text{ so } y\big(\alpha^2-(\gamma+\overline{\gamma})\alpha+\gamma\overline{\gamma}\big)=0. \ \square\end{aligned}$$

NOTE 1. The continued fraction expansion so obtained may not be *admissible*: in that the a_i might not be *positive* integers for all i. The adjective 'admissible' is appropriate here in that tacitly we supposed ourselves to be obtaining the *regular* continued fraction expansion of γ, whereas our description may well have led to inadmissible partial quotients. Generally, a regular continued fraction expansion $[b_0, b_1, \ldots]$ has $b_0 \in \mathbb{Z}$ and $b_1, b_2, \ldots$ each a positive integer; that is, a partial quotient is *admissible* (other than for the 0-th partial quotient) only if it is a *positive* integer.

However, our remarks do comprise a proof of Lagrange's Theorem to the effect that all real quadratic irrationals have an admissible periodic continued fraction expansion, and conversely. To see this observe that the transductions on the sequence of partial quotients

$$\begin{aligned}[\ldots, A, 0, C, \ldots] &= [\ldots, A+C, \ldots] \\ [\ldots, A, -B, C, \ldots] &= [\ldots, A-1, 1, B-2, 1, C-1, \ldots], \\ \text{whilst generally } -[A, B, C, \ldots] &= [-A-1, 1, B-1, C, \ldots],\end{aligned}$$

permit a sequential retrieval of admissibility whilst retaining periodicity; of course the length of the preperiod, and that of the period, may change.

NOTE 2. There is a unique regular decomposition of the unimodular matrix, thus with positive integers a_i, obtained by applying the Euclidean algorithm to the rows of the matrix, if and only if the first row, respectively the first column, dominates the second: that is $x > y > 0$ and $y > x-(\gamma+\overline{\gamma})y \geqslant 0$. 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 [4] for pure-periodicity of the regular.

PROPOSITION 5. *A real quadratic irrational γ has an* admissible *pure-periodic continued fraction expansion if and only if $\gamma > 1$ and $-1 < \overline{\gamma} < 0$; that is, if and only if γ is reduced.*

From here on, unless we explicitly indicate otherwise, the reader may suppose that all partial quotients appearing in continued fraction expansions are admissible.

4. SYMMETRIC CONTINUED FRACTIONS

Plainly, if $\gamma\overline{\gamma} = -1$ then the unimodular matrix is symmetric. So if there is an admissible decomposition — thus when $\gamma > 1$ and $-1 < \overline{\gamma} < 0$, that being the case when γ is *reduced* — then the unique admissible decomposition of the symmetric matrix yields a symmetric continued fraction expansion. That is, the word $a_0a_1 \dots a_r$ is a palindrome. As has been said too often: 'A palindrome is never odd or even; it is a toyota'. In summary we have the well-known result:

PROPOSITION 6. *A real quadratic irrational γ has a (admissible) pure-periodic continued fraction expansion with symmetric period if and only if $\gamma > 1$ and $\gamma\overline{\gamma} = -1$ (whence, automatically $-1 < \overline{\gamma} < 0$, so γ is reduced).*

It is fairly generally known that if γ is a real irrational quadratic integer with $\gamma > \overline{\gamma}$ then its continued fraction expansion is of the shape

$$[a_0, \overline{a_1, \dots, a_{s-1}, 2a_0 - (\gamma + \overline{\gamma})}],$$

with the word $a_1 \dots a_{s-1}$ a palindrome. To see how this fits our remarks observe the following: If the second column of

$$\begin{pmatrix} x & -\gamma\overline{\gamma}y \\ y & x - (\gamma + \overline{\gamma})y \end{pmatrix}$$

dominates the first: thus if $x - (\gamma + \overline{\gamma})y > y > 0$ and $-\gamma\overline{\gamma}y > x > 0$, then the decomposition terminates with $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, that is, $a_r = 0$. If, in other respects, the decomposition is admissible, that is if $\gamma > 1$ (and $\overline{\gamma} < 0$) then on multiplying by $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ on the right, and then by $\begin{pmatrix} \gamma + \overline{\gamma} & 1 \\ 1 & 0 \end{pmatrix}$, given that the trace $\gamma + \overline{\gamma}$ is integral, we obtain a symmetric unimodular matrix with its first row, respectively its first column, dominating the second. That corresponds to the expansion

$$\gamma = [\overline{a_0, a_1, \dots, a_{r-1}, 0}] = [a_0, \overline{a_1, \dots, a_{r-1}, 0, a_0}] = [a_0, \overline{a_1, \dots, a_{r-1} + a_0}],$$

with the word $a_1 \dots a_{r-2}$ a palindrome and with $a_{r-1} + a_0 = 2a_0 - (\gamma + \overline{\gamma})$. Familiar examples include $\gamma = \sqrt{D}$ and $\gamma = \left(\sqrt{D} + 1\right)/2$. In fact, if we recall that it is admissible for a_0 to take any value in $\mathbb{Z}$ we may deduce that:

https://doi.org/10.1017/S0004972700014064 Published online by Cambridge University Press

PROPOSITION 7. *A real quadratic irrational γ has an (admissible) continued fraction expansion*

$$[a_0, \overline{a_1, \dots, a_{r-1} + a_0}]$$

with the word $a_1 \dots a_{r-2}$ a palindrome and $a_{r-1} + a_0 = 2a_0 - (\gamma + \overline{\gamma})$, whenever $a_0 - \overline{\gamma} > 1 > \gamma - a_0$ and $\gamma + \overline{\gamma} \in \mathbb{Z}$. □

5. EQUIVALENCE

Two real numbers β and γ are said to be *equivalent* if there is a unimodular integer matrix $\begin{pmatrix} p & p' \\ q & q' \end{pmatrix}$ 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 $(\delta + P)/Q$ yields an ideal $\langle Q, \delta + P \rangle$, 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 the period of its periodic continued fraction expansion. But, we recall, $(\delta + P)/Q$ is reduced if and only if $\delta + P > Q$ and $-Q < \overline{\delta} + P < 0$. Thus $0 < Q < \delta - \overline{\delta}$ and $-\delta < P < -\overline{\delta}$ shows that there are just finitely many reduced elements and a fortiori just finitely many equivalence classes of ideals.

A reduced element $(\delta + P)/Q$ is said to yield a *reduced* ideal $\langle Q, \delta + P \rangle$. By Proposition 1 we know this is indeed an ideal of the ring $\mathbb{Z}[\delta]$. Conversely, given a strictly primitive ideal $\mathcal{I}$ of $\mathbb{Z}[\delta]$, its norm $\mathcal{I}\overline{\mathcal{I}} = \langle Q \rangle$ yields the the smallest positive integer $Q > 0$ in $\mathcal{I}$, and one may then determine $P \mod Q$. Thus the ideal determines an element $(\delta + P)/Q$ only up to addition of elements of $\mathbb{Z}$. Alternatively, $\mathbb{Z}[\delta]$ comprises Q congruence classes modulo $\mathcal{I}$. One verifies that an ideal is reduced precisely if it contains no nonzero β so that both $|\beta| < Q$ and $|\overline{\beta}| < Q$. 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 corresponds to a reduced element in a period consisting of all reduced elements equivalent to that element.

One says that two quadratic forms $Qx^2 - (t + 2P)xy + \big((n + tP + P^2)/Q\big)y^2$ and $Q'x'^2 - (t + 2P')x'y' + \Big(\big(n + tP' + P'^2\big)/Q'\Big)y'^2$ are *equivalent* if there is a unimodular

https://doi.org/10.1017/S0004972700014064 Published online by Cambridge University Press

matrix $\begin{pmatrix} p & p' \\ q & q' \end{pmatrix}$ so that

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

transforms the first form into the second. The forms are *properly* equivalent if the matrix has determinant $+1$; otherwise they are improperly equivalent. Once again it is straightforward to verify that the numbers $(\delta + P)/Q$ and $(\delta + P')/Q'$ 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.

These summary remarks mean to serve as a reminder of the useful correspondence between numbers $(\delta + P)/Q$, ideals $\langle Q, \delta + P \rangle$, and quadratic forms

$$Qx^2 - (t + 2P)xy + \big((n + tP + P^2)/Q\big)y^2 .$$

It seems a compelling claim that forms are clumsy and come from an age in which one wished to hide the underlying quadratic irrational. Nonetheless, forms differ according to the sign of their leading coefficient Q; that distinction is suppressed in dealing with reduced elements $(\delta + P)/Q$, let alone when working with ideals $\langle Q, \delta + P \rangle$.

6. Symmetry

We recall that the typical step in a continued fraction expansion of a real quadratic irrational $\gamma = \gamma_0$ is

$$\begin{aligned} \gamma_n = (\delta + P_n)/Q_n &= a_n - \big(\overline{\delta} + P_{n+1}\big)/Q_n = a_n - \overline{\gamma}'_n \\ -1/\overline{\gamma}'_n = \gamma_{n+1} &= (\delta + P_{n+1})/Q_{n+1} . \end{aligned}$$

Conjugating the typical step in the algorithm, and rearranging, yields

$$\gamma'_n = (\delta + P_{n+1})/Q_n = a_n - \big(\overline{\delta} + P_n\big)/Q_n = a_n - \overline{\gamma}_n .$$

If the original step occurred in the period of γ then, by Proposition 5, $\gamma_n = (\delta + P_n)/Q_n$ is reduced, so $-1 < \big(\overline{\delta} + P_n\big)/Q_n < 0$. Thus $0 < -\big(\overline{\delta} + P_n\big)/Q_n < 1$ and $-\big(\overline{\delta} + P_n\big)/Q_n$ is a remainder. Moreover, $\gamma'_n = (\delta + P_{n+1})/Q_n > a_n \geqslant 1$, and since $-\big(\overline{\delta} + P_{n+1}\big)/Q_n$ is a remainder we have $-1 < \big(\overline{\delta} + P_{n+1}\big)/Q_n < 0$. Thus the element $(\delta + P_{n+1})/Q_n$ is reduced. Hence $(\delta + P_{n+1})/Q_n = a_n - \big(\overline{\delta} + P_n\big)/Q_n$ is also a step in some periodic expansion, namely of some element γ'.

https://doi.org/10.1017/S0004972700014064 Published online by Cambridge University Press

We shall show that if γ has a symmetric periodic expansion, as in Proposition 6 or in Proposition 7, then we may take $\gamma' = \gamma$.

Indeed, if $\gamma = [\overline{a_0, a_1, \dots, a_{r-1}}]$ is pure periodic, we have the tableaux

$$\begin{aligned}
\gamma &= (\delta + P)/Q = a_0 - (\overline{\delta} + P_1)/Q = a_0 - \overline{\gamma}_0' \\
\gamma_1 &= (\delta + P_1)/Q_1 = a_1 - (\overline{\delta} + P_2)/Q_1 = a_1 - \overline{\gamma}_1' \\
&\vdots \\
\gamma_{r-1} &= (\delta + P_{r-1})/Q_{r-1} = a_{r-1} - (\overline{\delta} + P_r)/Q_{r-1} = a_{r-1} - \overline{\gamma}_{r-1}' ,
\end{aligned}$$

where necessarily $\overline{\gamma}_{r-1}' = -1/\gamma$. Evidently, conjugation and rearrangement as above reverses the tableaux and yields $[\overline{a_{r-1}, a_{r-2}, \dots, a_0}] = -1/\overline{\gamma}$. Hence if γ has a pure-periodic *symmetric* expansion, so by Proposition 6 if and only if $\gamma > 1$ and $\gamma\overline{\gamma} = -1$, then, of course $-1/\overline{\gamma} = \gamma$ and conjugation simply reverses the tableaux showing inter alia that the word $\gamma_0\gamma_1 \dots \gamma_{r-1}$ is a palindrome.

On the other hand, suppose that γ has integral trace $a_0 = \gamma + \overline{\gamma}$. If moreover γ is reduced then by Proposition 7 we have $\gamma = [\overline{a_0, a_1, \dots, a_{r-2}}]$ with $a_1 a_2 \dots a_{r-2}$ a palindrome. In the tableaux above the final line is redundant and coincides with the first; it is

$$\gamma = (\delta + P)/Q = a_0 - (\overline{\delta} + P)/Q = a_0 - \overline{\gamma} .$$

Under conjugation and rearrangement, reversal of the tableaux leaves it invariant illustrating that, again, the word $\gamma_0\gamma_1 \dots \gamma_{r-1}$ is a palindrome.

There are two cases according to the parity of r. If $r = 2s$ is even then the central lines of the tableaux are

$$\begin{aligned}
\gamma_{s-1} &= (\delta + P_{s-1})/Q_{s-1} = a_{s-1} - (\overline{\delta} + P_s)/Q_{s-1} = a_{s-1} - \overline{\gamma}_s \\
\gamma_s &= (\delta + P_s)/Q_s = a_s - (\overline{\delta} + P_{s+1})/Q_s = a_s - \overline{\gamma}_{s-1} .
\end{aligned}$$

We have $a_{s-1} = a_s$ and the lines are conjugate to one another. Thus $P_{s-1} = P_{s+1}$ and $Q_{s-1} = Q_s$. That is

$$\mathrm{Norm}\big((\delta + P_s)/Q_s\big) = -1 .$$

If $r = 2s + 1$ is odd then the central line

$$\gamma_s = (\delta + P_s)/Q_s = a_s - (\overline{\delta} + P_{s+1})/Q_s = a_s - \overline{\gamma}_s$$

is conjugate to itself. Thus $P_s = P_{s+1}$. That is

$$\mathrm{Trace}\big((\delta + P_s)/Q_s\big) = a_s$$

is an integer.

In either case we see that for each k mod r we have $\gamma_k = a_k - \overline{\gamma}_{r-k-1}$.

https://doi.org/10.1017/S0004972700014064 Published online by Cambridge University Press

7. Forms and Ideals

The product of two ideals $\langle Q, P+\delta\rangle$ and $\langle Q', P'+\delta\rangle$ is generated over $\mathbb{Z}$ by the quantities QQ', $Q'(P+\delta)$, $Q(P'+\delta)$ and $(P+\delta)(P'+\delta) = PP' - n + (t+P+P')\delta$.

Set $G = \gcd(Q, Q', t+P+P')$. One may verify, by studying the classical formulaires or from first principles, that the product is a rational integer multiple, namely by G, of $\langle q, p+\delta\rangle$ where $q = QQ'/G^2$ and p satisfies the congruences $p \equiv P \pmod{Q/G}$, $p \equiv P' \pmod{Q'/G}$ and $(P-p)(P'-p) \equiv \left(n+tp+p^2\right) \pmod{QQ'/G}$.

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 $p \bmod q$ is to be taken.

Correspondingly, a product of quadratic forms

$$Qx^2 - (t+2P)xy + \left((n+tP+P^2)/Q\right)y^2$$

$$\text{and } Q'x'^2 - (t+2P')x'y' + \left(\left(n+tP'+P'^2\right)/Q'\right)y'^2$$

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 $qX^2 - (t+2p)XY + \left((n+tp+p^2)/q\right)Y^2$ 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 determined up to multiplication by a 2×2 unimodular integer matrix. 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 shall refer to the particular case, where the stated forms yield the compound form

$$qX^2 - (2p+t)XY + \left((n+tp+p^2)/q\right)Y^2,$$

as *composition*.

In particular, one sees that the composite of a form $Qx^2 - (t+2P)xy + Q'y^2$ and its *opposite* $Qx^2 + (t+2P)xy + Q'y^2$ is equivalent to the form $x^2 - txy + ny^2 = (x-\delta y)\left(x-\bar{\delta}y\right)$. Correspondingly, the product of an ideal $\langle Q, P+\delta\rangle$ and its conjugate $\langle Q, P+\bar{\delta}\rangle = \langle Q, -t-P+\delta\rangle$ is a principal ideal.

In particular, $Q \mid (t+2P)$ is the condition for a form $Qx^2 - (t+2P)xy + Q'y^2$ to be properly equivalent to its opposite: the transformation is effected by $x \mapsto x + \left((t+2P)/Q\right)y$, $y \mapsto y$. In this case the ideal $\langle Q, P+\delta\rangle$ is its own conjugate, so its square is principal.

8. Ambiguity

A quadratic form $Qx^2-(t+2P)xy+\big((n+tP+P^2)/Q\big)y^2$ is said to be *ambiguous* — 'two-faced' might have been a better translation of the original Latin 'anceps' — if it is improperly equivalent to itself. Of course the surprising equivalence must interchange the numbers $(\delta+P)/Q$ and its conjugate $\big(\overline{\delta}+P\big)/Q$. Thus if all is well (all *is* well) the form is ambiguous if and only if the number $(\delta+P)/Q$ is equivalent to its conjugate.

In an alternative interpretation one says that an ideal $\langle Q,\delta+P\rangle$ 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 $\langle Q,\delta+P\rangle$ is ambiguous if and only if it contains both $(\delta+P)/Q$ and $\big(\overline{\delta}+P\big)/Q$ and that is so if and only if $(\delta+P)/Q+\big(\overline{\delta}+P\big)/Q=(t+2P)/Q\in\mathbb{Z}$. Not altogether surprisingly, therefore, Dickson [3] *defines* a form to be ambiguous if the trace of its roots is integral.

Thus we may say that an element $(\delta+P)/Q$ is ambiguous if $Q\,\big|\,(t+2P)$.

It is worth remarking that the basic condition $Q\,\big|\,(\delta+P)\big(\overline{\delta}+P\big)$ is

$$\big((4n-t^2)+(t+2P)^2\big)/Q\in 4\mathbb{Z}\,.$$

Hence $(t+2P)/Q\in\mathbb{Z}$ entails $f^2\Delta/Q\in\mathbb{Z}$. Thus as remarked in [7]:

Proposition 8. *The ambiguity of an ideal entails that its norm Q divides the discriminant $f^2\Delta$. Conversely, if an ideal has a squarefree norm dividing the discriminant then that ideal is ambiguous.*

We recall, compare Proposition 7, that a reduced element $\langle Q,\delta+P\rangle$ is ambiguous if and only if the corresponding continued fraction expansion

$$(\delta+P)/Q=[\overline{a_0,\,a_1,\,a_2,\,\dots\,,\,a_{r-1}}\,]$$

has $a_1a_2\cdots a_{r-1}$ a palindrome.

Thus, indeed, ambiguity is symmetry.

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. We saw at Section 6 that conjugation reverses the ordering of the ideals in an equivalence cycle whence, evidently, we have the following possibilities according to the parity of the length of the period: Since conjugation is an involution, if the length of the period is odd there must be an ideal fixed by conjugation so the cycle contains an ambiguous ideal. Since conjugation does not disturb the ordering of the ideals in the cycle, other than for reversing it, there is evidently exactly one fixed ideal, thus exactly one ambiguous ideal. The period with that ideal at its midpoint is pure symmetric. We may view the cycle of reduced ideals either as

$$\mathcal{I}_0,\mathcal{I}_1,\dots,\mathcal{I}_{s-1},\mathcal{I}_s,\overline{\mathcal{I}}_s,\overline{\mathcal{I}}_{s-1},\dots,\overline{\mathcal{I}}_1$$

with $\langle Q_0, \delta + P_0 \rangle$ ambiguous and thus with integer trace; or as pure symmetric

$$\mathcal{I}_s, \mathcal{I}_{s-1}, \dots, \mathcal{I}_1, \mathcal{I}_0, \overline{\mathcal{I}}_1, \dots, \overline{\mathcal{I}}_{s-1}, \overline{\mathcal{I}}_s$$

emphasising that $(\delta + P_s)/Q_s$ has norm -1. The former configuration is familiar from the expansion of $\sqrt{D} + a_0$ in the case that the length of the period is odd.

If the length of the period is even there is either no ambiguous ideal, in which case the period is pure symmetric, or exactly two ambiguous ideals. This is clear because an order reversing involution has at most two fixed points. The cycle of reduced ideals is appropriately viewed as either being of the shape

$$\mathcal{I}_0, \dots, \mathcal{I}_{s-1}, \overline{\mathcal{I}}_{s-1}, \dots, \overline{\mathcal{I}}_0 ,$$

with both $(\delta + P_0)/Q_0$ and $(\delta + P_{s-1})/Q_{s-1}$ of norm -1; or of the shape

$$\mathcal{I}_0, \dots, \mathcal{I}_{s-1}, \mathcal{I}_s, \overline{\mathcal{I}}_{s-1}, \dots, \overline{\mathcal{I}}_1 ,$$

with both $\mathcal{I}_0$ and $\mathcal{I}_s$ ambiguous, thus with $(\delta + P_0)/Q_0$ and $(\delta + P_s)/Q_s$ having integer trace. The latter configuration is familiar from the expansion of $\sqrt{D} + a_0$ in the case that the length of the period is even; the former is less familiar since it cannot refer to the principal class.

In this brief summary we presented the various periods so that their symmetry is manifest. Essentially, this was just a matter of arranging that the initial ideal of the period is ambiguous or corresponds to a complete quotient of norm -1. Were we to have commenced the period with an arbitrary ideal the ambiguity of the cycle would still be evident from the presence of pairs of conjugate ideals. Symmetry would be disguised, but could readily be detected by comparing the distance between conjugate ideals — their 'palindromic index' — with the length of the period; (see [7]).

9. Sums of two squares

We recall that the discriminant $f^2\Delta$ of the order $\mathbb{Z}[\delta]$ is given by $f^2\Delta = t^2 - 4n$, where t is the trace of δ, and n is its norm. Hence with $\gamma = (\delta + P)/Q$, the condition $\gamma\overline{\gamma} = -1$ is $(\delta + P)(\overline{\delta} + P) = -Q^2$ and that becomes

$$f^2\Delta = t^2 - 4n = (2Q)^2 + (2P + t)^2 ,$$

expressing the discriminant as the sum of two squares. Conversely, any decomposition $f^2\Delta = (2a)^2 + b^2$ with a and b relatively prime yields a reduced element of norm -1, therefore a pure symmetric cycle and hence an ambiguous ideal class. Incidentally, if t is odd then $\Delta = D$ whilst if t is even $\Delta = 4D$ and we may divide through by 4. So it

is helpful to speak in terms of the radicand f^2D rather than the discriminant. If the length of the period is odd the ambiguous class contains an ambiguous reduced ideal. If the length of the period is even it does not, but it contains a second ideal corresponding to an element of norm -1 and therefore to a second decomposition as a sum of two squares. Indeed, as noted in [7],

PROPOSITION 9. *There is an ambiguous ideal class without ambiguous reduced ideals if and only if the radicand f^2D is a sum of two relatively prime squares, and the length of the period is even; that is, the norm of the fundamental unit is* 1.

Incidentally, it really is relevant to insist on representations as a sum of *relatively prime* squares. To see this note once again the example $\gamma = \left(15+\sqrt{306}\right)/9$. It has norm -1 so its continued fraction expansion is pure periodic symmetric; it happens, of period length 6. The continued fraction corresponds to an ambiguous *cycle* of reduced ideals which contains no ambiguous ideal. However, here $306 = 15^2 + 9^2$, and the squares are not relatively prime. The point is that the ideals alluded to here, such as $\langle 9, 15+\sqrt{306}\rangle$ are not *strictly* primitive ideals of the order $\mathbb{Z}[\sqrt{306}]$, and thus are not invertible. Restricting ourselves to invertible ideals one sees that the class group is generated by $\langle 5, 1+\sqrt{306}\rangle$ and there is no ambiguous *class* of the order $\mathbb{Z}[\sqrt{306}]$ without ambiguous ideals. The point is, though, that the continued fraction expansion of γ is in truth the expansion of $\left(5+\sqrt{34}\right)/3$ and reports correctly that $\mathbb{Z}[\sqrt{34}]$ has an ambiguous ideal *class* without ambiguous ideals. We reiterate that the ideal class group of an order is the group of *invertible* ideals modulo principal ideals.

It may be interesting to recall (see [5]) that $r(n)$, the number of representations of n as a sum of squares counting variations of signs and order as distinct representations is given as follows: if $n = 2^a \prod p^b \prod q^c$, where p denotes primes $\equiv 1 \mod 4$ and q those primes $\equiv 3 \mod 4$, then $r(n) = 0$ if any c is odd, whilst if every c is even,

$$r(n) = 4\prod_p (b+1).$$

We are of course concerned with the number of different strictly primitive elements of norm -1 and allow neither variations of sign nor the summands having an odd common factor. But there remains a distinction according to the parity of the trace, because if t is odd only one summand is even:

PROPOSITION 10. *Suppose that the odd primes dividing Δ all are $\equiv 1 \mod 4$ and let μ denote the number of distinct such prime divisors. If the trace t is odd (and hence $t+2P$ is always odd) then the order $\mathbb{Z}[\delta]$ (of discriminant $f^2\Delta$) contains exactly $2^{\mu-1}$ different primitive reduced elements of norm -1; whilst if t is even, there are 2^μ such elements.*

https://doi.org/10.1017/S0004972700014064 Published online by Cambridge University Press

In the case of period of even length, thus when Pell's equation $\text{Norm}(X - \delta Y) = -1$ has no solution, or in yet different words when the fundamental unit of $\mathbb{Q}(\delta)$ has norm $+1$: we saw at Section 8 that each symmetric cycle (and thus ambiguous class) of reduced ideals contains either two ambiguous reduced ideals, or it contains two reduced ideals corresponding to elements of norm -1, and hence to decompositions of the discriminant as a sum of two squares.

Now consider the number of reduced ideals corresponding to elements of norm -1. We can see that if there is one such reduced ideal then there must be at least as many as there are ambiguous reduced ideals. That is obvious because, clearly, the composition of an ambiguous ideal class without ambiguous reduced ideals and of an ambiguous ideal class with ambiguous reduced ideals yields an ambiguous ideal class without ambiguous reduced ideals. Similarly, there must be as many ambiguous ideal classes with ambiguous reduced ideals as there are ambiguous ideal classes without ambiguous reduced ideals. That is plain because the composite of two ambiguous ideal classes without ambiguous reduced ideals is an ambiguous ideal class with ambiguous reduced ideals. Thus there are either no ambiguous ideal classes without ambiguous reduced ideals or their number coincides with the number of ambiguous ideal classes with ambiguous reduced ideals. One can compare our counts of sums of squares with explicit counts of primitive ambiguous reduced ideals in orders.

We may conclude that if there are 2^ν ambiguous ideal classes in all and if there is at least one such class without ambiguous reduced ideals, then the set of all ambiguous classes is generated by exactly ν ambiguous ideal classes without ambiguous reduced ideals. To see this note that the subgroup of ambiguous classes with ambiguous reduced ideals is generated by $\nu - 1$ classes. Hence to obtain a set of generators for the group of all ambiguous ideal classes it suffices to take one ambiguous class without an ambiguous reduced ideal, and to note that it, and its products with each of those $\nu - 1$ classes provide the said generators.

Our example at Section 11 illustrates this and other of our remarks.

REMARK. Amongst many other helpful remarks the referee observes that it is not at all clear whether an ambiguous class without ambiguous reduced ideals does or does not contain ambiguous ideals. This is indeed not clear and we have therefore been irritatingly careful to speak about ideal classes without ambiguous *reduced* ideals.

In the case of period of odd length, thus when Pell's equation $\text{Norm}(X - \delta Y) = -1$ has a solution, or in yet different words when the fundamental unit of $\mathbb{Q}(\delta)$ has norm -1: we saw at Section 8 that each symmetric cycle (and thus ambiguous class) of reduced ideals contains exactly one ambiguous ideal and one ideal corresponding to an element of norm -1. Thus there are the same number of ambiguous reduced ideals as there are reduced ideals corresponding to elements of norm -1.

It is well known that, given that Δ has decompositions as sums of squares, there are no simple criteria for determining whether the fundamental unit has norm -1 or not. The canonical examples to illustrate this are $\Delta = 65 = 5 \cdot 13$ and $\Delta = 221 = 13 \cdot 17$. The one completely evident exception to the said difficulty is when $\Delta = p$ with $p \equiv 1 \mod 4$. Then there is just one appropriate sum of squares so necessarily the ambiguous ideal class has one ambiguous ideal and one ideal corresponding to an element of norm -1; so the fundamental unit must have norm -1.

10. Forms

There is an evident difficulty in the correspondence we recalled between ideals $\langle Q, \delta + P \rangle$ and forms $Qx^2 - (2P + t)xy + Q'y^2$ in that conjugate ideals give the same form. An appropriate way to deal with that is to observe that the ideals $\langle Q, \delta + P \rangle$ and $\langle Q, -\delta - P \rangle$ are the same whilst of course in general the 'corresponding' forms $Qx^2 - (2P + t)xy + Q'y^2$ and $Qx^2 + (2P + t)xy + Q'y^2$ are not; they are equivalent under the transformation $x \mapsto x$; $y \mapsto -y$ but not generally properly equivalent. One terms them *conjugate* forms. Accordingly conjugate forms are equivalent if and only if the corresponding ideal belongs to an ambiguous class. All the more, the form $Qx^2 - (2P + t)xy + Q'y^2$ and its negative $-Qx^2 + (2P + t)xy - Q'y^2$ are certainly different; whilst the corresponding ideals coincide.

The resolution of these difficulties is that a given form $Qx^2 - (2P + t)xy + Q'y^2$ by convention corresponds to, its 'first zero': the element $(\delta + P)/Q$, and thus to the ideal $\langle Q, \delta + P \rangle$, rather than to the element $(\overline{\delta} + P)/Q$, and therefore to the ideal $\langle Q, \overline{\delta} + P \rangle$. Exchanging the ideals by conjugating reminds one that $\overline{\delta} + P = P + t - \delta$ so conjugating the ideal $\langle Q, \delta + P \rangle$ yields the ideal $\langle Q, \delta - P - t \rangle$. Then the conjugate form indeed does correspond to the conjugate ideal.

Nevertheless, we do have the negatives of all the forms, potentially leading to twice as many classes of forms as of ideals. That is indeed the case if those negatives are not already properly equivalent to the 'positive' forms; they are properly equivalent if and only if there is a unit of norm -1. Thus one gets twice as many classes of forms as of ideals if and only if there is no unit of norm -1. We note that in a cycle of forms the leading coefficients Q alternate in sign. It also follows that all ambiguous cycles of forms are of even length and each contains a pair of ambiguous forms. In this case an ambiguous cycle is precisely one containing a pair of ambiguous forms.

We also recall how to count the number of primitive ambiguous reduced ideals. We mentioned that an ideal $\langle Q, \delta + P \rangle$ is ambiguous if and only if $2P + t = Qa$ for some integer a. Set $n + Pt + P^2 = QQ'$, where, of course, Q' is an integer. Indeed the ideal corresponds to the form $Qx^2 - (2P + t)xy + Q'y^2$. Then

$$f^2\Delta = t^2 - 4n = (2P + t)^2 - 4(n + Pt + P^2) = Q(Qa^2 - 4Q').$$

There are now two cases according as t is even, whence $f^2\Delta \equiv 0 \mod 4$, or t is odd (and $f^2\Delta \equiv 1 \mod 4$). Let ν be the number of different primes dividing Δ.

Suppose t is odd. Then Q is odd and we must have $\gcd\left(Q, Qa^2 - 4Q'\right) = 1$ since otherwise the given form is not primitive. Note that the notion *primitive form* corresponds to the notion *strictly primitive ideal*. Thus the smaller, Q, of each pair of factors of Δ prime to its cofactor yields an ambiguous reduced ideal $\langle Q, \delta + P\rangle$ and there are exactly $2^{\nu-1}$ distinct such ideals. We note that Q with square factors from f^2 fails to yield strictly primitive ideals in the order.

Now suppose t is even. We note that only the choices $a = 0$, and $a = 1$ when possible, correspond to different reduced ideals, and observe that we must have $\gcd(Q, Q') = 1$, since otherwise the form is not primitive. It follows that, corresponding to the case $a = 0$, we obtain reduced ambiguous ideals $\langle Q, \delta + P\rangle$ with $Q \mid P$ for the smaller, Q, of each pair of factors of $\Delta/4$ prime to its cofactor. For the choice $a = 1$ to be possible we must have $f^2\Delta \equiv 12 \mod 16$ or $\equiv 0 \mod 32$ and $4 \mid Q$. In those cases we obtain a second ambiguous ideal for each of the choices already made in the case $a = 0$.

11. An example

An example of appropriate complexity to carry conviction is

$$D = 45305 = 5 \cdot 13 \cdot 17 \cdot 41 .$$

Since $D \equiv 1 \mod 4$, we set $\delta = \left(1 + \sqrt{45305}\right)/2$ and we have $\Delta = D$.

Our remarks at Section 10 immediately above readily allow us to list the 8 reduced ambiguous ideals

$$\langle 1, 105 + \delta\rangle , \quad \langle 5, 102 + \delta\rangle , \quad \langle 13, 97 + \delta\rangle , \quad \langle 17, 93 + \delta\rangle ,$$
$$\langle 41, 102 + \delta\rangle , \quad \langle 65, 97 + \delta\rangle , \quad \langle 85, 42 + \delta\rangle , \quad \langle 205, 102 + \delta\rangle .$$

We do not know a priori (until we discover the parity of the length of the period) whether these belong to the $8 = 2^3$ different ambiguous classes, or whether there are $4 = 2^2$ ambiguous classes without reduced ambiguous ideals. In the latter case the present ideals belong in pairs to the remaining $4 = 2^2$ ambiguous classes.

On the other hand one can readily compute all decompositions of Δ as a sum of two squares by noticing $5 = 1^2 + 2^2$, $13 = 3^2 + 2^2$, $17 = 1^2 + 4^2$ $41 = 5^2 + 4^2$ and recalling that

$$\left(x^2 + y^2\right)\left(x'^2 + y'^2\right) = \left(xy' \pm x'y\right)^2 + \left(xx' \mp yy'\right)^2 .$$

https://doi.org/10.1017/S0004972700014064 Published online by Cambridge University Press

That yields a list reporting that $\Delta =$

$$(2\cdot 101+1)^2+4\cdot 32^2\,,\quad (2\cdot 41+1)^2+4\cdot 98^2\,,\quad (2\cdot 9+1)^2+4\cdot 106^2\,,$$
$$(2\cdot 74+1)^2+4\cdot 76^2\,,\quad (2\cdot 86+1)^2+4\cdot 62^2\,,\quad (2\cdot 53+1)^2+4\cdot 92^2\,,$$
$$(2\cdot 105+1)^2+4\cdot 14^2\,,\quad (2\cdot 90+1)^2+4\cdot 56^2\,.$$

Now, for instance, in the continued fraction expansion of $(9+\delta)/106$ it happens that $Q_{12}=Q_{13}=76$, with $P_{13}=74$, so we see that the ideals $\langle 106, 9+\delta\rangle$ and $\langle 76, 74+\delta\rangle$ belong to the same ambiguous ideal class, $\mathcal{C}_1$, say, of course without ambiguous reduced ideals. Similarly, on expanding $(105+\delta)/14$ we notice that $Q_9=Q_{10}=56$, with $P_{10}=90$, and conclude that the ideals $\langle 14, 105+\delta\rangle$ and $\langle 56, 90+\delta\rangle$ belong to the same ambiguous ideal class, $\mathcal{C}_2$, say, without ambiguous reduced ideals. Finally, on expanding $(86+\delta)/62$ we find that $Q_{11}=Q_{12}=92$, with $P_{12}=53$, so we have that the ideals $\langle 62, 86+\delta\rangle$ and $\langle 92, 53+\delta\rangle$ belong to the same ambiguous ideal class, $\mathcal{C}_3$, say, without ambiguous reduced ideals. Of course it follows that the two remaining ideals $\langle 98, 41+\delta\rangle$ and $\langle 14, 105+\delta\rangle$ belong to the same ambiguous ideal class, $\mathcal{C}_4$, say, again without ambiguous reduced ideals.

There are thus $4=2^2$ such classes and, of the $8=2^3$ ambiguous classes in all, the other $4=2^2$ are the ambiguous classes each containing a pair of ambiguous reduced ideals. The remarks of Section 9 entail that any 3 of the ambiguous classes without ambiguous reduced ideals generate the entire subgroup of ambiguous classes; thus, for example, it follows that $\mathcal{C}_1\mathcal{C}_2\mathcal{C}_3=\mathcal{C}_4$, which the energetic reader may check by composing representative ideals. The ambiguous classes with ambiguous reduced ideals are the principal class $\mathcal{C}_0$ represented by the reduced ideal $\langle 1, 105+\delta\rangle$, and the classes $\mathcal{C}_1\mathcal{C}_2$, $\mathcal{C}_2\mathcal{C}_3$, and $\mathcal{C}_1\mathcal{C}_3$. We remarked that any 2, say $\mathcal{C}_1\mathcal{C}_2$ and $\mathcal{C}_1\mathcal{C}_3$ of these classes generate the subgroup of classes with ambiguous reduced ideals — which is indeed plain; it is also manifest that, as remarked, say $\mathcal{C}_1$, and its products with those 2 generators gives the generators of the entire subgroup of ambiguous classes.

12. Acknowledgements

For the second of us, these remarks result from a challenge from Hugh Williams to show that the matrix formulaire for continued fractions does indeed readily identify symmetry in the expansion, and ambiguity. Eventually writing this response was materially assisted by extensive conversations with Thomas Schmidt, then a Macquarie University Research Fellow. It must be well known, but does not seem widely known, that symmetry in continued fraction expansions corresponds respectively to the integrality of the trace — ambiguous ideals; or to elements of norm -1 — thus to a decomposition as a sum of two squares. That warranted emphasising, but to do that, and to use our

preferred notation, required a report from first principles. In writing on the present subject one's debt is of course to Gauß; but, realistically one must acknowledge so useful a source as Harvey Cohn's [2], notwithstanding its confusing exercise 9, p.190. For forms one may turn to Dickson [3] or, all the way back to Mathews [6]. It is painful that the variety of notations, terminologies and notions makes the subject rather more difficult than it should be. We hope not to have added to that confusion. Achieving that goal has been greatly assisted by the extraordinarily helpful advice of the referee.

References

[1] D.A. Buell, *Binary quadratic forms: classical theory and modern computations* (Springer-Verlag, Berlin, Heidelbrg, New York, 1989).

[2] H. Cohn, *A second course in number theory*, reprinted as *Advanced number theory*, (Dover Books, 1980) (Wiley, 1962).

[3] L.E. Dickson, *Introduction to the theory of numbers* (University of Chicago Press, Chicago, 1929) (reprinted by Dover Books, 1957).

[4] É. Galois, 'Démonstration d'un théorème sur les fractions continues périodiques', *Ann. Mat. Pura. Appl.* **19** (1828–1829), (*Oeuvres de Galois* [80,83] ; as cited in Oskar Perron, Sections 22–23 *op. cit.*), 294.

[5] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers* (Oxford University Press).

[6] G.B. Mathews, *Theory of numbers* (Chelsea, New York, 1960).

[7] R.A. Mollin, 'The palindromic index — a measure of ambiguous ideal classes without ambiguous ideals in class groups of real quadratic orders', *Journal de Théorie des Nombres de Bordeaux* (to appear).

[8] O. Perron, *Die Lehre von den Kettenbrüchen*, (Chelsea reprint of 1929 edition) (Teubner, Leipzig).

[9] A.M. Rockett and P. Szüsz, *Continued fractions* (World Scientific Publishing Co., Singapore, 1992).

School of Mathematics
University of Calgary
Alberta
Canada
e-mail: ramollin@acs.ucalgary.ca

Centre for Number Theory Research
Macquarie University
New South Wales 2109
Australia
e-mail: alf@mpce.mq.edu.au