Journal de Théorie des Nombres
de Bordeaux **7** *(1995), 447– 460*

The Palindromic Index - A Measure of Ambiguous Cycles of Reduced Ideals Without any Ambiguous Ideals in Real Quadratic Orders.

par Richard A. MOLLIN

Abstract. – Herein we introduce the palindromic index as a device for studying ambiguous cycles of reduced ideals with no ambiguous ideal in the cycle.

§1 Introduction

The theory of ambiguous classes of ideals in real quadratic fields goes back to Gauss' genus theory of binary quadratic forms. Recently, some nice papers on the topic have been written on the subject such as [4] - [5], but also some published works such as [1] and [3] contain some incorrect information. In this paper, we give a complete overview of the subject including a general criterion for an arbitrary real quadratic order (not necessarily maximal) to have ambiguous cycles of ideals (not necessarily invertible) *without* any ambiguous ideals in them. We do this via the introduction of what we call the *palindromic index* for an ideal in an ambiguous cycle over a real quadratic order. We also compare and contrast our results with those in the literature. We illustrate the results by several examples which we have placed in an Appendix at the end of the paper to improve the readability and flow of the paper, as well as to provide easily accessed illustrations of the theory.

§2 Notation and Preliminaries

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

$$r = \begin{cases} 2 \text{ if } D_0 \equiv 1 (mod\, 4) \\ 1 \text{ otherwise.} \end{cases}$$

1980 *Mathematics Subject Classification* (1985 *Revision*). 11R11, 11R29, 11R65.
Key words and phrases. Quadratic Order, Class Number, Palindromic Index, Ambiguous cycle, continued fractions, reduced ideals.
Manuscrit reçu le 21 janvier 1994.

Define $\omega_0 = (r - 1 + \sqrt{D_0})/r$ and $\Delta_0 = (\omega_0 - \omega_0')^2 = 4D_0/r^2$ where ω_0' is the algebraic conjugate of ω_0. Let $\omega_\Delta = f\omega_0 + h$ for some $f, h \in \mathbf{Z}$, and $D = (f/g)^2 D_0$ where $g = gcd(f, r)$. Thus, if $\Delta = (\omega_\Delta - \omega_\Delta')^2$, then $\Delta = f^2\Delta_0 = 4D/\sigma^2$ where $\sigma = r/g$. D_o is called the radicand associated with the discriminant Δ. Throughout the paper when referring to a discriminant Δ, we will be referring to this general setup unless otherwise specified.

Let $[\alpha, \beta] = \alpha\mathbf{Z} \oplus \beta\mathbf{Z}$, then if we set $\mathcal{O}_\Delta = [1, f\omega_0] = [1, \omega_\Delta]$, this is an order in K having conductor f and fundamental discriminant Δ_0. Let $I = [a, \quad b + c\omega_\Delta]$, with $a > 0$. It is a well-known (eg. see [10, Theorem 3.2, p.410]) that $I \not\subseteq \mathbf{Z}$ is an ideal in $\mathcal{O}_\Delta$ if and only if $c \mid a, \quad c \mid b$ and $ac \mid N(b + c\omega_\Delta)$, where N is the norm from $\mathbf{Q}(\sqrt{\Delta})$ to $\mathbf{Q}$; i.e., $N(\alpha) = \alpha\alpha'$. As shown in [10, Corollary 3.1.1, p.410] for a given ideal I in $\mathcal{O}_\Delta$ with $I \not\subseteq \mathbf{Z}$, the integers a and c are unique, and a is in fact the least positive rational integer in I. We denote the least positive rational integer in I by $L(I)$ and we denote the value of $cL(I)$ by $N(I)$, which we call the norm of I. An ideal $I = [a, b + c\omega_\Delta]$ is called primitive if $c = 1$. Moreover, if $I = [a, b + \omega_\Delta]$ is primitive, then so is its conjugate $I' = [a, b + \omega_\Delta']$. Two ideals I and J of $\mathcal{O}_\Delta$ are equivalent (denoted $I \sim J$) if there exist non-zero $\alpha, \beta \in \mathcal{O}_\Delta$ such that $(\alpha)I = (\beta)J$ (where (x) denotes the principal ideal generated by x).

Remark 2.1. At this juncture it is worth cautioning the reader concerning some data in the literature. Our notion of "primitive" given above coincides with that of [10] wherein that definition of primitive is needed to develop a full theory of continued fractions and reduced ideals; i.e., to ensure that all cycles of reduced ideals are taken into account. However, although equivalence of ideals is defined in [10] exactly as we have done above, classes of ideals are not mentioned throughout their paper. The reason is that their (and our) definition of primitive is insufficient to ensure invertibility of an ideal. To see this we recall that a fractional $\mathcal{O}_\Delta$-ideal of K is a non-zero, finitely generated $\mathcal{O}_\Delta$-submodule of $\mathbf{Q}(\sqrt{\Delta})$, and this, of course, includes all non-zero ideals of $\mathcal{O}_\Delta$, called integral ideals. Moreover any fractional $\mathcal{O}_\Delta$-ideal I of $\mathbf{Q}(\sqrt{\Delta})$ is called invertible if $I\ I^{-1} = \mathcal{O}_\Delta$ where $I^{-1} = \{x \in \mathbf{Q}(\sqrt{\Delta}) : xI \subseteq \mathcal{O}_\Delta\}$. Now we illustrate that we may have a primitive ideal which is not invertible. Let $\Delta = 1224 = 2^3 \cdot 3^2 \cdot 17$ be the discriminant with conductor $f = 3$ and order $\mathcal{O}_\Delta = [1, \sqrt{306}]$. Consider the primitive ideal $I = [9, 15 + \sqrt{306}]$. Here $I^{-1} = (\frac{1}{9})I'$ and $I\ I^{-1} = [3, \sqrt{306}] \neq \mathcal{O}_\Delta$. Thus, the ideal I is indeed primitive but not invertible, since it contains the rational integer factor 3 dividing f.

The definition of "primitive" given in [5] is sufficient (and necessary) for invertibility of ideals. However, since their definition and that of [10] conflict (in that they use the same term for different concepts) we introduce a new term here to emphasize the difference since we need both versions herein.

DEFINITION 2.1. *Let $\Delta > 0$ be a discriminant and $I = [a, (b + \sqrt{\Delta}/2]$ an ideal in $\mathcal{O}_\Delta$, then I is called* strictly primitive *if I is primitive and* $\gcd(a, b, (\Delta - b^2)/(4a)) = 1$. *(Note that this definition is the usual notion of primitive associated with quadratic* forms.*)*

The following generalizes [5, Proposition 2, p.325], and is illustrated by the example discussed in Remark 2.1.

PROPOSITION 2.1. *Let $\Delta > 0$ be a discriminant and let $I = [a, (b+\sqrt{\Delta})/2]$ be a primitive ideal of $\mathcal{O}_\Delta$. If $g = \gcd(a, b, (\Delta - b^2)/(4a))$ then $I^{-1} = (\frac{1}{a})I'$ and $I\ I' = (a)[g, \omega_\Delta]$. Thus, I is invertible if and only if I is strictly primitive.*

Proof. Since $I\ I' = (a)[a, (b + \sqrt{\Delta})/2,\ (b - \sqrt{\Delta})/2,\ (\Delta - b^2)/(4a)]$, then a check shows that $I\ I' = (a)[g, \omega_\Delta]$. Clearly then $\left(\frac{1}{a}\right) I'I \subseteq \mathcal{O}_\Delta$ and a tedious exercise verifies that indeed there are no other values $x \in \mathbf{Q}(\sqrt{\Delta})$ such that $xI \subseteq \mathcal{O}_\Delta$. Hence, if I is invertible then $\mathcal{O}_\Delta = I \quad I^{-1} = \left(\frac{1}{a}\right) I'I = [g, \omega_\Delta]$; whence $g = 1$. Conversely, if I is strictly primitive then $g = 1$ and $I^{-1}I = \mathcal{O}_\Delta$; whence I is invertible. $\square$

Much of the theory, as elucidated in [1] or [3] for example, avoids such problems by considering only ideals for which $\gcd(N(I), f) = 1$, (and such I are invertible). However, the converse does not necessarily hold. Thus the aforementioned restriction on ideals actually masks a phenomenon (not considered in [1]-[5]) which we wish to highlight; viz., that of ambiguous cycles without ambiguous ideals (see Section 3). In fact, since $\mathcal{O}_\Delta$ is not necessarily a Dedekind domain then not all ideals need be invertible, as illustrated by the above example. (In fact a Dedekind domain may be defined as a domain in which all fractional ideals are invertible.) However, we may have strictly primitive ideals I with $\gcd(N(I), f) > 1$. For example, let $\Delta = 725 = 5^2 \cdot 29$ with order $\mathcal{O}_\Delta = [1, (5 + \sqrt{725})/2]$ and conductor $f = 5$. Consider the strictly primitive ideal $I = [25, (25 + \sqrt{725})/2]$. This ideal is invertible (as are all principal ideals in a given order), since I $I^{-1} = \mathcal{O}_\Delta$ with $I^{-1} = \left(\frac{1}{25}\right) I' = \left(\frac{1}{25}\right) I$, and in fact $I = (25)$.

Now we are in a position to define ideal classes. The aforementioned notion of equivalence of ideals in $\mathcal{O}_\Delta$ is an equivalence relation, and according to the above elucidation the equivalence classes of strictly primitive ideals forms a group C_Δ under multiplication, and we call this group the ideal class group of $\mathcal{O}_\Delta$; i.e. C_Δ consists of the equivalence classes of invertible ideals of $\mathcal{O}_\Delta$. The order of C_Δ is denoted by h_Δ, the class number of $\mathcal{O}_\Delta$. The connection between the class number of the maximal order and that of an arbitrary order contained in it may be found for example in [1, Theorem 2, p. 217].

Definition 2.2. *A primitive ideal I of $\mathcal{O}_\Delta$ is called reduced if it may be written in the form $I = [a, (b+\sqrt{\Delta})/2]$ where $-2a < b - \sqrt{\Delta} < 0 < 2a < b+\sqrt{\Delta}$. Any reduced ideal which is strictly primitive will be called strictly reduced.*

Now we give an elucidation of the theory of continued fractions as it pertains to the above. The details and proofs may also be found in [10].

Let $I = [N(I), \quad b+\omega_\Delta]$ be a primitive ideal in $\mathcal{O}_\Delta$ and denote the continued fraction expansion of $(b+\omega_\Delta)/N(I)$ by $< a_0, \overline{a_1, a_2, ..., a_\ell} >$ with period length $\ell = \ell(I)$ where $(P_0, Q_0) = ((rb + f(r-1) + hr)/g, ar/g)$ and, (for $i \geq 0$), $D = P_{i+1}^2 + Q_i Q_{i+1}$, $P_{i+1} = a_i Q_i - P_i$, and $a_i = \lfloor (P_i + \sqrt{D})/Q_i \rfloor$, with $\lfloor \quad \rfloor$ being the greatest integer function, or "floor".

From the continued fraction factoring algorithm (as given in [10]) we get all reduced ideals equivalent to a given reduced ideal $I = [N(I), \quad b+\omega_\Delta]$; i.e. in the continued fraction expansion of $(b+\omega_\Delta)/N(I)$ we have

$$I = I_0 = [Q_0/\sigma, (P_0+\sqrt{D})/\sigma] \sim I_1 = [Q_1/\sigma, (P_1+\sqrt{D})/\sigma] \sim ...$$

$$\sim I_{\ell-1} = [Q_{\ell-1}/\sigma, (P_{\ell-1}+\sqrt{D})/\sigma].$$

Finally, $I_\ell = I_0 = I$ for a complete cycle of reduced ideals of length $\ell(I) = \ell$. Therefore, the $(P_i+\sqrt{D})/Q_i$ are the complete quotients of $(b + \omega_\Delta)/N(I)$, and the Q_i/σ's represent the norms of all reduced ideals equi valent to I.

Remark 2.2 It follows from the above development that the class group C_Δ of a given order $\mathcal{O}_\Delta$ consists of classes of strictly primitive ideals, whereas if we do not consider C_Δ but merely wish to look at cycles of reduced ideals then the cycles may consist of reduced but not strictly reduced ideals. We will have need of this distinction later on.

Now we cite a couple of useful technical results which we will need throughout the paper. In what follows $\epsilon_\Delta > 1$ denotes the fundamental unit of $\mathcal{O}_\Delta$.

LEMMA 2.1. *Let $I = [a, \quad b+\omega_\Delta]$ be a reduced ideal. If P_i and Q_i for $i = 1, 2, ..., \ell(I) = \ell$ appear in the continued fraction expansion of $(b+\omega_\Delta)/a$ then $\epsilon_\Delta = \prod_{i=1}^{\ell}(P_i + \sqrt{D})/Q_i$ and $N(\epsilon_\Delta) = (-1)^\ell$.*

Proof. This is well-known (eg. see [5, Corollary 5, p.346]). An alternative form, $\epsilon_\Delta = \prod_{i=1}^{\ell}(\sqrt{D} - P_i)/Q_{i-1}$ is given in [10, Theorem 2.1, p.409] as well. We note that if $(P_i + \sqrt{D})/Q_i = \phi_i$ then $(\sqrt{D} - P_i)/Q_{i-1} = \phi_i^{-1}$. □

See Example AI in the Appendix for an illustration of Lemma 2.1.

LEMMA. *If $I = [a, \quad (b+\sqrt{\Delta})/2]$ is a primitive ideal of $\mathcal{O}_\Delta$ then $I = [a, na \pm (b+\sqrt{\Delta})/2]$ for any $\mathbb{Z}$*

Proof. This follows from the development in [10, Section 3, p.410]. □

§3 Ambiguous Classes and Cycles

The only proof given in this section is that of the last result, Theorem 3.5, which is essentially the proof of a conjecture posed in [9, Remark 2.3, p. 114]. The remaining lemmata and theorems have very easy proofs which the reader can readily reproduce.

DEFINITION 3.1. *Let $\Delta > 0$ be a discriminant. If I is a reduced ideal in $\mathcal{O}_\Delta$ then I is said to be in an ambiguous cycle if $I_j = I'$ for some integer j with $0 < j \leq l$. In particular, if $I = I'$ then I is called an ambiguous ideal.*

Observe that if I is strictly primitive then we may speak of the class of I in C_Δ in which case $I' = I_j$ means that $I \sim I'$ or $I^2 \sim 1$, the usual notion of an ambiguous ideal class in C_Δ. However, it is possible to have an ambiguous cycle which contains no ambiguous ideal. We introduce the following concept which will help to clarify (and correct errors in the literature concerning) the notion in particular of ambiguous classes without ambiguous ideals. It will be, in fact, the device by which we classify all real quadratic orders which have class groups generated by such classes. We maintain the more general setting however for reasons outlined in Section 2.

DEFINITION 3.2. *Let $\Delta > 0$ be a discriminant and let $I = [a, \quad (b+\sqrt{\Delta})/2]$ be a reduced ideal in $\mathcal{O}_\Delta$ with $0 < (\sqrt{\Delta} - b)/(2a) < 1$. If I is in an ambiguous cycle then in the continued fraction expansion of $(b+\sqrt{\Delta})/(2a)$,* *we must have $I' = I_p$ for some integer $p \in Z$ with $1 \leq p \leq \ell(I)$. We call $p = p(I)$ the palindromic index of I, since for a given I as above, p is unique.*

We will suppress the I and just write p for $p(I)$ and ℓ for $\ell(I)$ whenever the context is clear. It follows from [7, Lemma 3.5, p.831] that an ambiguous ideal class (or more generally an ambiguous cycle of ideals) can have at most 2 reduced ambiguous ideals.

In order to give our criterion we need a couple of useful technical lemmas.

LEMMA 3.1. *If $I = [a, \quad (b+\sqrt{\Delta})/2]$ is a reduced ideal in $\mathcal{O}_\Delta$ with $0 < (\sqrt{\Delta}-b)/2a < 1$ then in the continued fraction expansion of $(b+\sqrt{\Delta})/2a$ we have that $a_i = \lfloor (P_i+\sqrt{D})/Q_i \rfloor$; whence, $I' = [Q_i/\sigma, \quad (P_i+\sqrt{D})/\sigma]' = [Q_i/\tau, (-P_i+\sqrt{D})/\sigma] = = [Q_i/\sigma, \quad (P_{i+1}+\sqrt{D})/\sigma]$. .*

The next lemma generalizes observations made in [6, p.65].

LEMMA 3.2. *Let I, ℓ and p be as in Definition 3.2, then $(I_i)' = I_{p-i}$ for $0 \leq i \leq p$; whence, $a_i = a_{p-i}$, $Q_i = Q_{p-i}$ and $P_{i+1} = P_{p-i}$. Moreover, if $\ell \geq p+2$, then $(I_i)' = I_{\ell+p-i}$ for $p+1 \leq i \leq \ell-1$; whence $a_i = a_{\ell+p-i}$, $\quad Q_i = Q_{\ell+p-i}$ and $P_i = P_{\ell+p-i+1}$.*

Now we are in a position to give the aforementioned criterion, which follows easily from the above two lemmata.

THEOREM 3.1. *Let $\Delta > 0$ be a discriminant and let I be a reduced ideal in $\mathcal{O}_\Delta$. Then I is in an ambiguous cycle without an ambiguous ideal if and only if $\ell(I) = \ell$ is even and $p(I) = p$ is odd.*

Remark. If we consider the continued fraction expansion of $(15+\sqrt{306})/9$ given in Example A1 of the Appendix then we see that the primitive ideal $I = [9, 15+\sqrt{306}]$ has $p(I) = \ell(I) - 1 = 5$; whence, I is in an ambiguous cycle with no ambiguous ideal. However, there does not exist an ambiguous class without ambiguous ideals in C_s.

This example is no accident as the following generalization of [6, Lemma 6, p.65] shows, (see also [4, Lemma 5, p.275]).

LEMMA 3.3. *Let $\Delta > 0$ and $I = [a, (b+\sqrt{\Delta})/2]$ be a reduced ideal in an ambiguous cycle and $0 < (\sqrt{\Delta}-b)/(2a) < 1$, then $\Delta = 4a^2+b^2$ if and only if $I' = I_{\ell-1}$, i.e. $p = \ell - 1$.*

The following generalizes a well-known result which can be found in [1] for example.

LEMMA 3.4. *Let $\Delta > 0$ be a discriminant. In $\mathcal{O}_\Delta$ there exists an ambiguous cycle of reduced ideals, containing no ambiguous ideal if and only if $N(\epsilon_\Delta) = 1$ and D is a sum of 2 squares.*

Remark 3.1 Now we need a definition which will lead us into a result which basically says that, if we have one ambiguous cycle of reduced ideals without ambiguous ideals then we also have the maximum possible. For maximal orders this means that, if we have one such class, then we may generate the class group entirely by such classes. See Example A2 in the Apppendix for an illustration pertaining to non-maximal orders, and Example A3 for maximal orders.

DEFINITION 3.3. *Let $\Delta > 0$ be a discriminant and let s be one half the excess of the number of divisors of $D = \sigma^2\Delta/4$ of the form $4j+1$ over those divisors of the form $4j+3$. Thus s corresponds to the number of distinct sums of squares $D = a^2 + b^2$ (where distinct here means that, although $\gcd(a,b)$ is not necessarily one, we always assume that both a and b are positive, but we do not count as distinct those which differ only by the order of the factors. For example, the 8 solutions of $x^2 + y^2 = 5 : (1,2),(-1,2),(1,-2),(-1,-2),(2,1),(2,-1),(-2,1)$ and $(-2,-1)$ are considered as only one solution.*

THEOREM 3.2. *Let $\Delta > 0$ be a discriminant, then if there exists an ambiguous cycle of reduced ideals without ambiguous ideals there are s such cycles when $D = \sigma^2\Delta/4$ is even and when D is odd there are $s/2$ of them.*

Remark 3.2 In [1, pp. 190, 225] it is asserted that there can be at most one ambiguous class without an ambiguous ideal in it, when considering, $C_\Delta$for the maximal order. This is shown to be incorrect by Theorem 3.2. What we think that Professor Cohn meant to say was that $|C_{\Delta,2}| \,/\, |C_{\Delta,1}| = 2$ where $C_{\Delta,2}$ is the elementary abelian 2-subgroup of C_Δ and $C_{\Delta,1}$ is the subgroup of C_Δ consisting of classes with ambiguous ideals. In fact from Lemma 3.4 and Theorem 3.2, we see that there exists an ambiguous class without ambiguous ideals if and only if there exist 2^t ambiguous classes without ambiguous ideals, where t is the number at distinct prime divisors at Δ. In order to clarify the situation, we give the following criterion.

THEOREM 3.2. *Let $\Delta > 0$ be a discriminant not divisible by the odd power of any prime congruent to* 3 *modulo* 4 *in its canonical prime of factorization* *then the following are equivalent :*

i) $D = \sigma^2\Delta/4$ *is a sum of two squares and* $N(\epsilon_\Delta) = 1$.

ii) *There are* s *ambiguous cycles of reduced ideals without ambiguous ideals in* $\mathcal{O}_\Delta$ *when* D *is even, and there are* $s/2$ *of them when* D *is odd.*

iii) *There exists an ambiguous cycle of reduced ideals without ambiguous ideals in* $\mathcal{O}_\Delta$.

Remark 3.3. When $\mathcal{O}_\Delta$ is the maximal order Theorem 3.3 says that if t is the number of distinct primes dividing Δ (not divisible by any prime congruent to 3 *modulo* 4) and there exists an ambiguous class without ambiguous ideals then there are 2^t such classes.

Example A3 in the Appendix not only illustrates Theorem 3.3 for maximal orders but also shows that by a judicious choice of an ideal I in an ambiguous class without ambiguous ideals (namely the ones arising from the pairs of representations as sums of squares) we may always guarantee that $p(I) = \ell(I) - 1$.

Part of the impetus for studying and clarifying the above data on ambiguous classes was to see if [7. Lemma 3.5, p.831] could be generalized to hold for ambiguous classes. The answer is no. We do however have a general result for ambiguous classes which yields [7, ibid] as an immediate consequence, which follows easily from Lemma 3.2.

THEOREM 3.4. *Let* $\Delta > 0$ *be a discriminant and let* $I = [a, \quad (b+\sqrt{\Delta})/2]$ *with* $0 < (\sqrt{\Delta}-b)/2a < 1$ *be a reduced ideal in an ambiguous cycle of* $\mathcal{O}_\Delta$. *Let* Q_i *be in the continued fraction expansion of* $(\sqrt{\Delta}+b)/2a$, *then* $I = I'$ *if and only if one of the following holds:*

i) $p = \ell$ *and* $i = 0$ *or* ℓ.

ii) p *is even and* $i = p/2$.

iii) p *and* ℓ *have the same parity and* $i = (p+\ell)/2$.

Remark 3.4. We note that the main result of [3, Theorem 3.1, p.75] was shown to be false in [8] where we considered class groups of quadratic orders (with positive or negative discriminants) generated by ambiguous ideals. Therein we gave a general criteria (which yielded as an immediate consequence a correct version of [3, op.cit.]) for the class group of a maximal quadratic order (in real or complex quadratic fields) to be generated by ambiguous ideals. This criterion was given in terms of canonical quadratic polynomials.

Remark 3.5. The reader should note that a correct and very appealing treatment of ideal classes in real quadratic fields is contained in [2].

We conclude with a proof of a conjecture made in [9] using the results of this section. In [9] we classified and enumerated all discriminants $\Delta > 0$ such that there is exactly one non-inert prime less than $\sqrt{\Delta}/2$ (with one possible exception whose existence would be a counterexample to the generalized Riemann hypothesis) using a well-known result of Tatuzawa. Additionally we used this result to show that certain forms for Δ cannot exist with the aforementioned property (again with one possible exception remaining). We now give an unconditional proof of this result as a nice application of the theory developed to this point.

THEOREM 3.5. *Let $\Delta = q^2 + 4q$ where both q and $q + 4$ are primes with $\sqrt{\Delta} > q > \sqrt{\Delta}/2$. Furthermore, if $r < \sqrt{\Delta}/2$ is a prime such that $(\Delta/r) = 1$ and $p^{h_\Delta} > \sqrt{\Delta}$ then r is not the only non-inert prime less that $\sqrt{\Delta}/2$.*

Proof. Assume that r is the only non-inert prime less than $\sqrt{\Delta}/2$. Since $N(\epsilon_\Delta) = N\left((q + 2 + \sqrt{\Delta})/2\right) = 1$ then the period length of any reduced ideal is even by Lemma 2.1. In particular, if $I = [r, b + \omega_\Delta]$ then $l(I) = l$ is even. If h_Δ is even then $I^{h_\Delta/2}$ is in an ambiguous class, and as shown in [9], $I^{h_\Delta/2}$ is reduced. If $p(I^{h_\Delta/2}) = p$ is even then by Lemma 3.2, $P_{p/2} = q$, $Q_{p/2} = 2q$ and $\Delta = q^2 + Q_{p/2}Q_{p/2-1} = q^2 + 4q$; whence $Q_{p/2-1} = 2$. This means $I^{h_\Delta/2} \sim I$, a contradiction. Thus p is odd and so by Theorem 3.1, $I^{h_\Delta/2}$ is in an ambiguous class without an ambiguous ideal. Moreover $Q_{(p-1)/2} = Q_{(p+1)/2}$ and $\Delta = P^2_{(p+1)/2} + Q^2_{(p+1)/2}$, by Lemma 3.2. Since $Q_{(p+1)/2} < \sqrt{\Delta}$ then $\mathrm{Q}_{(r+1)/2} = 2p^j$, so $I^{h_\Delta/2} \sim I^{\pm j}$, i.e. $j \equiv h_\Delta/2(mod \quad h_\Delta)$. However, $r^{h_\Delta} > \sqrt{\Delta}$ so $j = h_\Delta/2$; i.e. $Q_{(p+1)/2} = 2r^{h_\Delta/2}$. Yet, by definition $Q_p = 2p^{h_\Delta/2}$ and is the first such Q_i with this property, a contradiction. Hence h_Δ is odd. Now, if there exists a $Q_i < \sqrt{\Delta}$ for any i with $0 < i < \ell$ in the continued fraction expansion of $(b + \omega_\Delta)/r$ then $Q_i = 2r^j$ for some $j \geq 0$; whence, $I \sim I^{\pm j}$. Therefore $j \equiv \pm 1(mod \quad h_\Delta)$, but $p^{h_\Delta} > \sqrt{\Delta}$ forcing $j = h_\Delta - 1$ or $j = 1$. If $j = 1$ then $I \sim I'$ and if $j = h_\Delta - 1$ then $I \sim I^{h_\Delta - 1} \sim I^{-1} \sim I'$. In either case I is in an ambiguous class. Since h_Δ is odd then $I \sim 1$. However, in the continued fraction expansion of ω_Δ, the principal class, the period length $\ell(1) = 2$, and $Q_1 = 2q \neq 2r$, a contradiction. Hence, there does not exist any integer i with $0 < i < \ell(I) = \ell$ such that $Q_i < \sqrt{\Delta}$ in the continued fraction expansion of $(b + \omega_\Delta)/r$. Yet $\Delta = P_i^2 + Q_iQ_{i-1}$ for $0 < i < \ell$, and we cannot have <u>both</u> Q_i <u>and</u> Q_{i-1} bigger than $\sqrt{\Delta}$. Thus,

$\ell = 2$ with $Q_1 = 2s > \sqrt{\Delta}$, s a prime. Also $P_1 = P_2 = a_1 Q_1 - P_1$; whence $P_1 = sa_1$ which forces s to divide Δ since $\Delta = P_1^2 + 4s$. Thus $s = q$ and so $\Delta = q^2(P_1/q)^2 + 4rq = q^2 + 4q$, a contradiction. $\square$

It is hoped that the introduction of the palindromic index and the ramifications of it elucidated herein have made this beautiful topic more understandable.

Acknowledgements. The author's research is supported by NSERC Canada grant #A8484. The author also welcomes the referee for comments which led to a more compact paper.

Appendix

I. Examples

Example A1. Let $\Delta = 1224 = 2^3 \cdot 3^2 \cdot 17$, $D = 306 = 2 \cdot 3^2 \cdot 17$, $D_0 = 2 \cdot 17 = 34$ and $\Delta_0 = 2^3 \cdot 17$; whence, $f = 3$, $\sigma = r = g = 1$ and $\mathcal{O}_\Delta = [1, 3\sqrt{34}] = [1, f\omega_0] = [1, \sqrt{306}]$. Consider the ideal $I = [9, 15 + \sqrt{306}]$, then the continued fraction expansion of $(15 + \sqrt{306})/9$ is

i	0	1	2	3	4	5	6
P_i	15	12	6	9	6	12	15
Q_i	9	18	15	15	18	9	9
a_i	3	1	1	1	1	3	3,

and

$$\begin{aligned}\epsilon_\Delta &= 35 + 2\sqrt{306} \\ &= [(12 + \sqrt{306})/18][(6 + \sqrt{306})/15][(9 + \sqrt{306})/15] \\ &\cdot [(6 + \sqrt{306})/18][(12 + \sqrt{306})/9][(15 + \sqrt{306})/9].\end{aligned}$$

In fact if we consider $\mathcal{P}_5 = [5, 1 + \sqrt{306}]$ and look at the continued fraction expansion of $(1 + \sqrt{306})/5$ we get

i	0	1	2	3	4
P_i	1	14	8	14	16
Q_i	5	22	11	10	5
a_i	3	1	2	3	6

and,

$$\epsilon_\Delta = [(14 + \sqrt{306})/22][(8 + \sqrt{306})/11][(14 + \sqrt{306}/10][(16 + \sqrt{306})/5].$$

Moreover, by [1, op.cit.], $h_\Delta = 4$ and since $\mathcal{P}_5 \sim \mathcal{P}'_{11}\mathcal{P}_2 \sim \mathcal{P}_{11}$ where $\mathcal{P}_{11}$ lies over 11 then $\mathcal{P}_{11}^2 \sim \mathcal{P}_2 \not\sim 1$; whence, P_5 has order 4. Hence, $C_\Delta =< P_5 >$.

Example A2. Let $\Delta = 2^3 \cdot 13^2 \cdot 5^2 \cdot 17$ then $D = 143650 = 2 \cdot 13^2 \cdot 5^2 \cdot 17$ with $\sigma = r = g = 1$ and $f = 2 \cdot 5 \cdot 13$. D is representable as a sum of squares in 9 distinct ways; viz.,

$$\begin{aligned} D &= 379^2 + 3^2 = 363^2 + 109^2 = 333^2 + 181^2 \\ &= 267^2 + 269^2 = 195^2 + 325^2 = 377^2 + 39^2 \\ &= 375^2 + 55^2 = 143^2 + 351^2 = 305^2 + 225^2 \end{aligned}$$

and each one of these yields an ambiguous cycle without any ambiguous ideals. However the last 5 of these arise from 13 and 5; i.e. they give rise to ideals which are not strictly primitive and therefore do not represent classes in C_Δ. For example, $I = [195, 325+\sqrt{143650}]$ has continued fraction expansion for $(325 + \sqrt{143650})/195$ being

i	0	1	2	3	4	5	6
P_i	325	260	130	195	130	260	325
Q_i	195	390	325	325	390	195	195
a_i	3	1	1	1	1	3	3

an ambiguous cycle with $p(I) = 5 = \ell(I) - 1$, thus without any ambiguous ideals, but I is not strictly primitive. However the first 4 representatives of D as a sum of 2 squares do represent classes in C_Δ; viz.,

$$\begin{aligned} J &= [3,\ 379 + \sqrt{D}] &\sim&\ [363,\ 109 + \sqrt{D}] \\ L &= [181,\ 33 + \sqrt{D}] &\sim&\ [267,\ 269 + \sqrt{D}] \\ M &= [379,\ 3 + \sqrt{D}] &\sim&\ [109,\ 363 + \sqrt{D}] \\ N &= [333,\ 181 + \sqrt{D}] &\sim&\ [269,\ 267 + \sqrt{D}]. \end{aligned}$$

Moreover, $C_{(\Delta,2)} =< J > \times < L > \times < M > \times < N >$ the 2-part of a class group generated by ambiguous classes without ambiguous ideals.

Example A3. Let $\Delta = D_0 = 45305 = 5 \cdot 13 \cdot 17 \cdot 41$ and let

$$I = [106, \quad (19 + \sqrt{45305})/2].$$

We choose this since the ambiguous classes without ambiguous ideals arise from the representations as sums of 2 relatively prime squares. Here $\Delta =$

$19^2+4\cdot 106^2$. The continued fraction expansion of $(19+\sqrt{45305})/212$ is

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13
P_i	19	193	187	85	195	169	153	187	117	91	87	125	155	149
Q_i	212	38	272	140	52	322	68	152	208	178	212	140	152	152
a_i	1	10	1	2	7	1	5	2	1	1	1	2	2	2

	14	15	16	17	18	19	20	21	22	23	24	25	26
	155	125	87	91	117	187	153	169	195	85	187	193	19
	140	212	178	208	152	68	322	52	140	272	38	212	212
	2	1	1	1	2	5	1	7	2	1	10	1	1

Here we see, as predicted by Lemma 3.3, $p(I)=25=\ell(I)-1$ and by Theorem 3.1 this is an ambiguous class without an ambiguous ideal. We also see that I generates the representation $\Delta=149^2+4\cdot 76^2$ since $P_{13}=149$ and $Q_{13}=Q_{12}=152$. Note as well that although $Q_{15}=212$ this does not represent the conjugate, by Lemma 3.2, because there is no symmetry about 15.

Now we consider $J=[14,\quad (211+\sqrt{45305})/2]$ which arises from $\Delta=211^2+4\cdot 14^2$. The continued fraction expansion of $(211+\sqrt{45305})/28$ is

i	0	1	2	3	4	5	6	7	8	9	10
P_i	211	209	197	139	93	65	195	197	35	155	181
Q_i	28	58	112	232	158	260	28	232	190	112	112
a_i	15	7	3	1	1	1	14	1	1	3	3

	11	12	13	14	15	16	17	18	19	20
	155	35	197	195	65	93	139	197	209	211
	190	232	28	260	158	232	112	58	28	28
	1	1	14	1	1	1	3	7	15	15

We see that J also generates $\Delta=181^2+4\cdot 56^2$ since $P_{10}=181$ and $Q_{10}=Q_9=112$. Here $p(J)=19=\ell(J)-1$ so it's an ambiguous class without an ambiguous ideal. Note as above that although $Q_6=28$ this does not represent the conjugate.

Finally we let $L=[62,\quad (173+\sqrt{\Delta})/2]$ which arises from $\Delta=173^2+4\cdot 62^2$.

The continued fraction expansion of $(173+\sqrt{\Delta})/124$ is

i	0	1	2	3	4	5	6	7	8	9	10	11
P_i	173	199	169	195	205	123	61	165	155	111	137	77
Q_i	124	46	364	20	164	184	226	80	266	124	214	184
a_i	3	8	1	20	2	1	1	4	1	2	1	1

12	13	14	15	16	17	18	19	20	21	22	23	24
107	77	137	111	155	165	61	123	205	195	169	199	173
184	214	124	266	80	226	184	164	20	364	46	124	124
1	1	2	1	4	1	1	2	20	1	8	3	3

Thus $p(L) = 23 = \ell(L) - 1$ and again, as predicted, we have an ambiguous class without an ambiguous ideal. Moreover the other sum of 2 squares which L generates is $\Delta = 107^2 + 4 \cdot 92^2$ since $P_{12} = 107$ and $Q_{12} = Q_{11} = 184$. As above although $Q_9 = 124$ this does not represent the conjugate due to lack of palindromy.

We note that there is one more pair of representations of Δ as a sum of squares (since there are $2^{t-1} = 8$ such representation); viz., $\Delta = 83^2 + 4 \cdot 98^2 = 203^2 + 4 \cdot 32^2$. The ideal which arises from this pair is $M = [98, \quad (83 + \sqrt{45305})/2]$. However, $M \sim IJK$, whereas there are no such relationships between I, J and L; whence $C_\Delta =< I > \times < J > \times < L >$, a class group generated by ambiguous classes without ambiguous ideals.

Bibliography

[1] H. COHN, *A second course in number theory*, John Wiley and Sons Inc., New York/London (1962).

[2] H. COHEN, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, Graduate Texts in Mathematics **138**, (1993).

[3] F. HALTER-KOCH, *Prime-producing quadratic polynomials and class numbers of quadratic orders in* Computational Number Theory, (A. Pethö, M. Pohst, H.C. Williams, and H.G. Zimmer eds.) Walter de Gruyter, Berlin (1991), 73–82.

[4] F. HALTER-KOCH, P. KAPLAN, K. S. WILLIAMS and Y. YAMAMOTO, *Infrastructure des Classes Ambiges D'Idéaux des ordres des corps quadratiques réels*, L'Enseignement Math **37** (1991), 263–292.

[5] P. KAPLAN and K. S. WILLIAMS, *The distance between ideals in the orders of real quadratic fields*, L'Enseignment Math. **36** (1990), 321–358.

[6] S. LOUBOUTIN, *Groupes des classes d'ideaux triviaux*, Acta. Arith. LIV (1989), 61–74.

[7] S. LOUBOUTIN, R. A. MOLLIN and H. C. WILLIAMS, *Class numbers of real quadratic fields, continued fractions, reduced ideals, prime-producing quadratic polynomials, and quadratic residue covers*, Can. J. Math. **44** (1992), 824–842.

[8] R. A. MOLLIN, *Ambiguous Classes in Real Quadratic Fields*, Math Comp. **61** (1993), 355–360.

[9] R. A. MOLLIN and H. C. WILLIAMS, *Classification and enumeration of real quadratic fields having exactly one non-inert prime less than a Minkowski bound*, Can. Math. Bull. **36** (1993), 108–115.

[10] H. C. WILLIAMS and M. C. WUNDERLICH, *On the parallel generation of the residues for the continued fraction factoring algorithm*, Math. Comp. **77** (1987), 405–423.

Richard A. MOLLIN
Department of Mathematics
University of Calgary
Calgary, Alberta
T2N 1N4
CANADA
e-mail address: ramollin@acs.ucalgary.ca.