AMBIGUOUS FORMS AND IDEALS IN QUADRATIC ORDERS

JOHN ROBERTSON

Please direct comments, corrections, or questions to
jpr2718@gmail.com

This note discusses the possible numbers of ambiguous forms, reduced ambiguous forms, ambiguous ideals, and reduced ambiguous ideals that can occur in an order of a quadratic number field and in a class in the associated class group. While we're at it, we explore possible relationships among weakly equivalent classes, improperly equivalent classes, inverses of classes, conjugates, and ambiguity.

1. Background

First a little background and notation. For the order of conductor f in the quadratic field $\mathbf{Q}(\sqrt{d})$, we consider the proper/narrow class group $H_+(\Delta)$ to be both classes of ideals and classes for forms under any of the normal isomorphisms. Unless otherwise noted, "class" means proper class of forms or strict class of ideals. Here d is a squarefree integer, not 0 or 1, and f is a positive integer. The discriminant Δ of the order is f^2d if $d \equiv 1 \pmod 4$ and is $4f^2d$ otherwise. We write $\omega = (1+\sqrt{d})/2$ when $d \equiv 1 \pmod 4$ and $\omega = \sqrt{d}$ otherwise. All forms $F = ax^2 + bxy + cy^2 = (a, b, c)$ we consider are primitive, which means that $\gcd(a, b, c) = 1$.

All ideals we consider are invertible and primitive. This last means that the ideal can be written $[a, b + f\omega]$. In fact, without further comment, when we specify an ideal, we mean the "primitive part" of the ideal. For example if $d = 5$, $f = 8$, and $I = [64, f\omega]$, then, for us I^2

Date: February 7, 2009.

is $[64, 8 + f\omega]$, not $8[64, 8 + f\omega]$. We denote by (α) the principal ideal generated by the quadratic irrational α.

2. Ambiguous and reduced forms

A form (a, b, c) is *ambiguous* if $a|b$. A (proper) class of forms is *ambiguous* if it contains an ambiguous form.

Note that definitions of ambiguous form, ambiguous ideal, and ambiguous class vary in the literature.

If a form $F = (a, b, c)$ is ambiguous, there are always an infinite number of ambiguous forms properly equivalent to F with the same a. It is therefore useful to consider the sets of all of these forms. To that end, define forms as being *special* equivalent if they are related by a transform

$$T = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n.$$

for n an integer. The form (a, b, c) is special equivalent to any form $(a, b + 2na, an^2 + bn + c)$. In particular, an ambiguous form (a, b, c) is always special equivalent, and hence properly equivalent, to a form of the form $(a, 0, c)$ or (a, a, c). We call forms $(a, 0, c)$ and (a, a, c) *special ambiguous* forms.

A form (a, b, c) with $\Delta < 0$ is said to be *reduced* if

$$|b| \leq a \leq c$$

and if either $|b| = a$ or $a = c$ then $b \geq 0$.

A form (a, b, c) with $\Delta > 0$ is said to be reduced if

$$|\sqrt{\Delta} - 2|a|| < b < \sqrt{\Delta}.$$

An equivalent set of conditions is

$$0 < b < \sqrt{\Delta} \text{ and } \sqrt{\Delta} - b < 2|a| < \sqrt{\Delta} + b.$$

In either of the above sets of conditions for $\Delta > 0$, replacing a with c gives an equivalent set of conditions.

3. Ambiguous and reduced ideals

An ideal I is *ambiguous* if $I = I'$, where I' is the conjugate of I. Because if I is invertible, $I' = I^{-1}$, an ideal is ambiguous if and only if $I^2 = (1)$. A (strict) class of ideals is *ambiguous* if it contains an ideal I for which $I \approx I'$ (strict ideal equivalence). We will see later that an ambiguous class of ideals always includes exactly two primitive ambiguous ideals.

An ideal I is *reduced* if for any $a > 0$ and α so that $I = [a, \alpha]$, not both $|\alpha| < a$ and $|\overline{\alpha}| < a$ hold.

Sections below give information on how to find reduced forms and ideals equivalent to any given form or ideal, and how to test whether an ideal is reduced.

The classes of order 1 or 2 in $H_+(\Delta)$ are the ambiguous classes. Under the usual isomorphisms, ambiguous proper classes of forms correspond to ambiguous narrow classes of ideals.

4. The number of special ambiguous forms, ambiguous ideals, and genus classes in an order

The table "Counts of Special Ambiguous Forms" tells how many special ambiguous forms there are in an order, based on the congruence class of d modulo 4, the number of distinct primes dividing Δ, and the power of 2 dividing f. In this table, A is special ambiguous forms of the form $(a, 0, c)$, B is special ambiguous forms of the form (a, a, c), and $N = 2^M$ where M is the number of distinct primes dividing Δ.

For example, if $d = 34$ and $f = 1$, then $\Delta = 136 = 2^3 \cdot 17$, so 2 primes divide Δ. This order has 8 special ambiguous forms, namely $(-34, 0, 1)$, $(-17, 0, 2)$, $(-2, 0, 17)$, $(-1, 0, 34)$, $(1, 0, -34)$, $(2, 0, -17)$, $(17, 0, -2)$, $(34, 0, -1)$.

The number of ambiguous ideals is always half the number of special ambiguous forms; this is not necessarily true class by class, but true of the sum over all classes.

The number of genus classes is equal to the number of ambiguous classes, and is 1/4 the number of special ambiguous forms for $d > 0$, and 1/2 the number of special ambiguous forms for $d < 0$.

Counts of Special Ambiguous Forms

d modulo 4	A or B	$2 \nmid f$	$2^1 \| f$	$2^2 \| f$	$8 \mid f$
1	A	0	N	$2N$	$2N$
1	B	$2N$	0	0	$2N$
2	A	$2N$	$2N$	$2N$	$2N$
2	B	0	$2N$	$2N$	$2N$
3	A	N	$2N$	$2N$	$2N$
3	B	N	0	$2N$	$2N$

TABLE 1. All forms are primitive

Possible counts for $\Delta < 0$

Class is Ambig?	Reduced Ideals	Ambig Ideals	Reduced Ambig Ideals	Reduced Forms	Special Classes of Ambig Forms	Reduced Ambig Forms
No	1	0	0	1	0	0
Yes	1	2	1	1	2	1
Yes	2	2	0	1	2	0

TABLE 2. Any class has the counts in some row; all forms and ideals are primitive

5. Numbers of reduced and ambiguous forms and ideals in a class for $\Delta < 0$

The table "Possible counts for $\Delta < 0$" tells how many ambiguous ideals, reduced ambiguous ideals, special ambiguous forms, and reduced ambiguous forms can be in a class when $\Delta < 0$. For example, any ambiguous class in $H_+(\Delta)$ always has exactly two primitive ambiguous ideals. But, when $\Delta < 0$, neither or exactly one of these ambiguous ideals might be reduced. We give examples of some of the more interesting possibilities.

The order $d = -15$, $f = 1$ (the maximal order for the field $\mathbf{Q}(\sqrt{-15})$) has an ambiguous class that does not have any reduced ambiguous ideals. This is the one non-principal class, which includes the ambiguous ideals $[3, 1 + \omega]$ and $[5, 2 + \omega]$, where $\omega = (1 + \sqrt{-15})/2$. Neither of these ideals is reduced ($|1 + \omega| = \sqrt{6} = 2.45$, $|2 + \omega| = \sqrt{10} = 3.16$). This class does have two reduced ideals, namely $[2, \omega]$ and $[2, 1 + \omega]$ ($|\omega| = \sqrt{4} = 2$).

The special ambiguous forms in the non-principal class of the maximal order of $\mathbf{Q}(\sqrt{-15})$ are $(3, 3, 2)$ and $(5, 5, 2)$, neither of which is properly equivalent to a reduced ambiguous form. The one reduced form in this class is $(2, 1, 2)$. The repeating "2" in this example is no coincidence. If (a, a, c) is a form in a given class (for an order with a negative discriminant), and $a/3 < c < a$, then the reduced form in the class will be (c, b, c) where $0 < b = a - 2c < c$ if $c < a/2$ and $0 < b = 2c - a < c$ if $c > a/2$. While we're at it, for completeness we note that if $a/4 < c < a/3$, then the reduced form in the class is (a', a', c) where $0 < a' = 4c - a < c$.

The order with $d = -70$, $f = 12$ has three ambiguous classes that do not have reduced ambiguous ideals. As an example, one of these classes is that with the ambiguous ideals $[180, 90 + f\omega]$ and $[224, 112 + f\omega]$. Here $f\omega = 12\sqrt{-70}$. The reduced ideals in this class are $[101, 11 + f\omega]$ and $[101, 90 + f\omega]$. This order also has three classes that do not have reduced ambiguous forms, namely the three classes that correspond to the three classes without reduced ambiguous ideals. The ambiguous forms (or representatives of the special classes of ambiguous forms) in the class that corresponds under the standard isomorphism to the ideal class just discussed are $(180, 180, 101)$ and $(224, 224, 101)$, neither of which is reduced. The reduced form in this class is $(101, 22, 101)$.

For $d = -55$, $f = 1$, all three kinds of class occur.

6. Numbers of reduced and ambiguous forms and ideals in a class for $\Delta > 0$

The table "Possible counts for $\Delta > 0$" tells how many ambiguous ideals and reduced ambiguous ideals can be in a class when $\Delta > 0$. Whether or not the class is ambiguous, the number of reduced forms

Possible counts for $\Delta > 0$

$N(\epsilon)$	Class is Ambig?	Reduced Ideals (N)	Ambig Ideals	Reduced Ambig Ideals
-1	No	Odd ≥ 3	0	0
-1	Yes	Odd ≥ 1	2	1
$+1$	No	≥ 2	0	0
$+1$	Yes	Odd ≥ 1	2	1
$+1$	Yes	Even ≥ 2	2	0 or 2

TABLE 3. Any class has the counts in some row; all forms and ideals are primitive

is twice the number of reduced ideals. An ambiguous class has exactly 4 special ambiguous forms and exactly 2 reduced ambiguous forms.

As an example where $\Delta > 0$, and the norm of the fundamental unit is -1, take $d = 145$, $f = 1$ ($12^2 - 145 \cdot 1^2 = -1$). Here $H_+(145)$ is cyclic of order 4, and so has two ambiguous classes. The non-principal class has the two ambiguous ideals $[5, 2 + \omega]$ and $[29, 14 + \omega]$, of which only the first is reduced. This class also has the four ambiguous forms (or special classes of forms) $(5, 5, -6)$, $(-5, -5, 6)$, $(29, 29, 6)$, and $(-29, -29, -6)$, of which the first two are reduced.

When $\Delta > 0$, if an ambiguous class has zero or two reduced ambiguous ideals, then the norm of the fundamental unit of the order is $+1$. For example, the order for $d = 34$, $f = 1$, has one ambiguous class without reduced ambiguous ideals and another ambiguous class with two reduced ambiguous ideals. The group $H_+(4 \cdot 34)$ is cyclic of order 4. The element of order 2 is the principal class generated by elements of negative norm. The ambiguous ideals in this class are $[17, \sqrt{34}]$ and $[34, \sqrt{34}]$, neither of which is reduced. These ideals are generated by $17 + 3\sqrt{34}$ and $\sqrt{34}$. The principal class generated by elements of positive norm has two ambiguous ideals, $[1, \sqrt{34}]$ and $[2, \sqrt{34}]$, both

of which are reduced. These ideals are generated by $35 + 6\sqrt{34}$ and $6 + \sqrt{34}$.

In $H_+(4{\cdot}7)$, which is of order 2, the only primitive reduced ambiguous ideals are $[1, \sqrt{7}]$ and $[2, 1 + \sqrt{7}]$, both of which are in the principal class generated by elements of positive norm. The only other primitive ambiguous ideals are $[7, \sqrt{7}]$ and $[14, 7 + \sqrt{7}]$, both of which are in the principal class generated by elements of negative norm, and neither of which is reduced.

For an example with a greater number of ambiguous classes without reduced ambiguous ideals, the order for $d = 81770$, $f = 1$, has 16 ambiguous classes, five of which have no reduced ambiguous ideals, and five of which have two reduced ambiguous ideals. Each of the five classes with no reduced ambiguous ideals is weakly equivalent to a class with two reduced ambiguous ideals, and vice-versa. Each of the 16 ambiguous classes has two ambiguous ideals, four ambiguous forms, and two reduced ambiguous forms. This d factors as $2 \cdot 5 \cdot 13 \cdot 17 \cdot 37$, so is a sum of squares.

As another example for $d > 0$, consider $d = 87087$, $f = 1$. This order has 14 ambiguous classes without reduced ambiguous ideals (and 14 with two reduced ambiguous ideals). This d factors as $3{\cdot}7{\cdot}11{\cdot}13{\cdot}29$, so is *not* a sum of squares.

For $d = 82$, $f = 1$, $N(\epsilon_0) = -1$, and both kinds of class occur. For $d = 399$, $f = 1$, $N(\epsilon_0) = +1$, and all three kinds of class occur.

7. Singular ideals

The ratio of the two ambiguous ideals in an ambiguous class is the *singular* ideal. If $\Delta < 0$ then the singular ideal is $(f\sqrt{d})$. Also, if $\Delta > 0$ and $N(\epsilon_0) = -1$, the singular ideal is $(f\sqrt{d})$, where ϵ_0 is the fundamental unit in the order.

If $\Delta > 0$ and $N(\epsilon_0) = +1$, $(f\sqrt{d})$ is not in the principal class of ideals generated by elements of positive norm, so the singular ideal is not $(f\sqrt{d})$. Let $t + u\omega$ be a fundamental unit in $\mathcal{O}$, so $N(t + u\omega) = +1$. Set $g = \gcd(1 + t, u), v = (1 + t)/g, w = u/g$. Then $(v + w\omega)$ is the singular ideal. This ideal is ambiguous and might or might not be reduced.

If J is the singular ideal, and I is ambiguous, then IJ is the other ambiguous ideal in the proper class. Both I and IJ can be reduced, or neither, or just one of them. The order $d = 81770$, $f = 1$ has examples of all 3.

8. I AND $(f\sqrt{d})I$

There is another way to pair up ambiguous ideals, namely select pairs so that the ratio of one to the other is $(f\sqrt{d})$. If I is ambiguous, then $(f\sqrt{d})I$ is ambiguous and exactly one of I and $(f\sqrt{d})I$ is reduced. As a result, exactly half of all ambiguous ideals are reduced. Note that $(f\sqrt{d})$ is ambiguous (it is equal to its conjugate), and the product of ambiguous ideals is ambiguous. If $\Delta > 0$ and $N(\epsilon_0) = +1$, then I and $(f\sqrt{d})I$ are in separate narrow classes; otherwise , i.e., if $\Delta < 0$ or $\Delta > 0$ and $N(\epsilon_0) = -1$, then I and $(f\sqrt{d})I$ are in the same narrow class. The ideals I and $(f\sqrt{d})I$ are always in the same wide class.

The preceding comments are easily proved, and it is useful to have simple characterizations of reduced ambiguous ideals. There are four cases to consider: whether d is congruent to 1 modulo 4 or not, and for each of these there are two kinds of ambiguous ideal—those associated with forms $(a, 0, c)$, and those associated with forms (a, a, c).

First consider the case where $d \not\equiv 1 \pmod 4$, and the ambiguous ideal is $[a, f\omega]$ (which is associated with the form $(a, 0, c)$). Here $\omega = \sqrt{d}$. For $[a, f\sqrt{d}]$ to be an ideal, we must have $a|N(f\sqrt{d})$, or $a|f^2d$. The ideal $[a, f\sqrt{d}]$ is reduced if and only if $a < f\sqrt{d}$ (otherwise for $\alpha = f\sqrt{d}$ both $|\alpha| < a$ and $|\overline{\alpha}| = |\alpha| < a$). Consider the ideal J

$$J = (f\sqrt{d})[a, f\sqrt{d}] = [af\sqrt{d}, f^2d] = a[(f^2d)/a, f\sqrt{d}].$$

If $a > f\sqrt{d}$, then $(f^2d)/a < f\sqrt{d}$, so J is reduced.

Second, consider the case where $d \not\equiv 1 \pmod 4$, and the ambiguous ideal is $I = [a, -a/2 + f\omega]$ (which is associated with the form (a, a, c)). Again $\omega = \sqrt{d}$. We must have that a is even, so that the discriminant is even. For $[a, -a/2 + f\sqrt{d}]$ to be an ideal, we must have $a|N(-a/2 + f\sqrt{d}) = (a^2 - 4f^2d)/4$, so $a|2f^2d$ (because a divides $(a/2)^2 - f^2d$ and $(a/2)$ divides $(a/2)^2$, so $a/2$ divides f^2d). The ideal I is reduced if and

only if $a < a/2 + f\sqrt{d}$, or $a < 2f\sqrt{d}$. Consider the ideal J,

$$J = (f\sqrt{d})[a, -a/2 + f\sqrt{d}] = [af\sqrt{d}, (-a/2)f\sqrt{d} + f^2 d]$$
$$= \frac{a}{2}[-f\sqrt{d} + 2(f^2 d)/a, 2f\sqrt{d}]$$
$$= \frac{a}{2}[(4f^2 d)/a, (-2f^2 d)/a + f\sqrt{d}].$$

If $a > 2f\sqrt{d}$, then $(4f^2 d)/a < 2f\sqrt{d}$, so J is reduced.

Third, consider the case where $d \equiv 1 \pmod 4$, and the ambiguous ideal is $I = [a, -f/2 + f\omega]$ (which is associated with the form $(a, 0, c)$). Here $\omega = (1 + \sqrt{d})/2$. We must have that f is even, because the discriminant is even. Also, $-f/2 + f\omega = f\sqrt{d}/2$, so $I = [a, f\sqrt{d}/2]$ and a divides $f^2 d/4$. The ideal I is reduced if $a < f\sqrt{d}/2$, or $2a < f\sqrt{d}$. For I to be an ideal, we must have $a | N(f\sqrt{d}/2)$, or $4a | f^2 d$. Consider the ideal J,

$$J = (f\sqrt{d})[a, f\sqrt{d}/2] = [af\sqrt{d}, f^2 d/2] = 2a[(f^2 d)/(4a), f\sqrt{d}/2].$$

If $a > f\sqrt{d}/2$ then $(f^2 d)/(4a) < f\sqrt{d}/2$, so J is reduced.

Fourth, and finally, consider the case where $d \equiv 1 \pmod 4$, and the ambiguous ideal is $I = [a, -(a + f)/2 + f\omega] = [a, -a/2 + f\sqrt{d}/2]$ (which is associated with the form (a, a, c)). We must have that $a + f$ is even, because the parity of the discriminant is that of f. The ideal I is reduced if $a < a/2 + f\sqrt{d}/2$, or $a < f\sqrt{d}$. Here $a | f^2 d$. Consider the ideal J,

$$J = (f\sqrt{d})[a, -a/2 + f\sqrt{d}/2] = [af\sqrt{d}, -(a/2)f\sqrt{d} + f^2 d/2]$$
$$= a[f^2 d/a, -(f^2 d)/(2a) + f\sqrt{d}/2].$$

If $a > f\sqrt{d}$ then $f^2 d/a < f\sqrt{d}$, so J is reduced.

9. A conjecture

I conjecture that when $\Delta < 0$, the maximal order can have at most one ambiguous class without reduced ambiguous ideal. Some $d < 0$ for which the maximal order has one ambiguous class without reduced ambiguous ideal include $d = -15$, -21, -35, -55, -65, -77, -91, and -105. More generally, I think that the number of classes with no

reduced ambiguous ideals is less than or equal to the conductor of the order. These might be known; comments welcome.

10. Definitions of reduced ideal

Here are three ways of stating the definition of a reduced ideal, which are trivially equivalent.

> I is reduced if there is no a, α so $I = [a, \alpha]$, $|\alpha| < a$, and $|\overline{\alpha}| < a$.
> If there are a, α so $I = [a, \alpha]$, $|\alpha| < a$, and $|\overline{\alpha}| < a$ then I is not reduced.
> I is reduced if for every a, α so $I = [a, \alpha]$, either $|\alpha| \geq a$ or $|\overline{\alpha}| \geq a$.

11. Inverses

Improperly equivalent forms are in classes that are inverses in the narrow class group. The forms (a, b, c) and $(a, -b, c)$ are always improperly equivalent, under the transform $[[1, 0], [0, -1]]$, so their classes are inverses in the narrow class group.

If

> $\Delta < 0$, or
> $\Delta > 0$ and $H_+(\Delta) = H(\Delta)$

then every class is weakly equivalent to itself, so every class that is weakly equivalent to its inverse is its own inverse, and so is ambiguous.

If $\Delta > 0$ and $H_+(\Delta) = H(\Delta) \times \mathbf{Z}/2\mathbf{Z}$ then no class is weakly equivalent to its inverse. This is because between a class and its weak equivalent, exactly one has a "1" in $\mathbf{Z}/2\mathbf{Z}$, and so does their product. Look at the maximal orders for $d = 427$ or 399 for examples.

If $\Delta > 0$, $h_+(\Delta) = 2h(\Delta)$, and $H_+(\Delta) \neq H(\Delta) \times \mathbf{Z}/2\mathbf{Z}$ then at least one class is weakly equivalent to its inverse. Any class that is weakly equivalent to its inverse is of order 4 in the class group. To see this, let J be the ideal that is the inverse of the ideal I, and assume $I \sim J$. Then $I^2 \approx J^2$, so $I^4 \approx I^2 J^2 \approx (1)$. Since I is not weakly equivalent to itself, $I \not\approx J$, so I is not of order 2, and so must be of order 4.

For examples of Δ meeting the criteria of the preceding paragraph, consider $d = 34$, 146, 410, 898, 4810 (all $f = 1$). The maximal order

for $d = 81770$ has 8 classes weakly equivalent to their inverses. Not all classes of order 4 are weakly equivalent to their inverses, for example some of the classes in the maximal orders when $d = 4658$, 4810, 5986, 8738, 9266, 9554, 11713, 12002, 12505, or 12994. But, all of these orders also have classes weakly equivalent to their inverses.

For $\Delta > 0$, the forms (a, b, c) and $(-a, b, -c)$ map to weakly equivalent classes under the standard maps.

12. A comment in the literature

Occasionally you will find a statement similar to, "An ambiguous class can have no ambiguous ideals, but at most one ambiguous class in an order can have no ambiguous ideals." No matter how you try to interpret this statement, it is wrong.

First, most authors consider ambiguous classes to be classes in the narrow (strict) ideal group (or, via any of the usual isomorphisms, proper group of forms). An ambiguous strict ideal class always has exactly two ambiguous ideals.

Some authors consider classes of order 2 in the wide class group to be ambiguous classes. If you use this definition, then ambiguous wide classes can have no ambiguous ideals. But there can be more than one ambiguous class without ambiguous ideals. For example, for the maximal order of $\mathbf{Q}(\sqrt{410})$ (so $d = 410$, $f = 1$, and $\Delta = 1640$) there are two wide classes of order 2 without ambiguous ideals, namely the classes of the ideals $[7, 2 + \sqrt{410}]$ and $[11, 5 + \sqrt{410}]$. For the maximal order of $\mathbf{Q}(\sqrt{9490})$ (so $\Delta = 37960$), there are four wide classes of order 2, namely those with the ideals $[9, 2 + \sqrt{9490}]$, $[18, 2 + \sqrt{9490}]$, $[29, 6 + \sqrt{9490}]$, and $[45, 20 + \sqrt{9490}]$. No ambiguous ideals are strictly or weakly equivalent to any of these four ideals, so these are four classes without ambiguous ideals.

I don't think calling classes of order 2 in the wide class group ambiguous classes is either useful or in the spirit of Gauss's original use of the term ambiguous. For one thing, the ambiguous classes without ambiguous ideals do not have ambiguous forms under the usual isomorphisms.

The reason for interest in ambiguous classes is that they are the obstruction to there being a class group under proper and improper equivalence of forms. Ambiguous classes are improperly equivalent to themselves, while classes that are not ambiguous are improperly equivalent to some other class.

13. Appendix–Reduction step for forms

The *reduction step* for positive definite forms is as follows. Given a form (a, b, c) we will produce a (not necessarily distinct) form (a', b', c') and the transformation T between these forms.

If (a, b, c) is reduced, take $a' = a$, $b' = b$, $c' = c$ and

$$T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

i.e., do nothing.

Otherwise, if $a > c$ then take $a' = c$, $b' = -b$, $c' = a$ and

$$T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

If the above conditions did not apply, look at

$$k = \left\lfloor \frac{a-b}{2a} \right\rfloor.$$

If $k \neq 0$ then take $a' = a$, $b' = 2ak + b$, $c' = ak^2 + bk + c$, and

$$T = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}.$$

Finally, if none of the above applied, we must have $b < 0$ and $a = c$ in which case take $a' = a$, $b' = -b$, $c' = c = a$ and

$$T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Cohen [1, p. 258] gives the following reduction step for $d > 0$. Recall that neither a nor c can be zero for any forms we consider.

First define $r(-b, c)$ to be the unique integer r so that $r \equiv -b \pmod{2|c|}$ and $-|c| < r \leq |c|$ if $|c| > \sqrt{\Delta}$, or $\sqrt{\Delta} - 2|c| < r < \sqrt{\Delta}$ if $|c| < \sqrt{\Delta}$.

For the reduction step, take $a' = c$, $b' = r(-b, c)$, and $c' = ((b')^2 - \Delta)/4c$. The transform T is

$$T = \begin{pmatrix} 0 & 1 \\ -1 & -(b+b')/2c \end{pmatrix}.$$

Repeated application of the reduction step eventually produces a reduced form. When the reduction step is applied to a reduced form, the result is a reduced form. When $d < 0$, application of the reduction step to a reduced form returns the original form. When $d > 0$ application of the reduction step to a reduced form returns a different form. After a "period" or "cycle" of reduced forms, the original form will eventually reappear after an even number of applications of the reduction step.

14. Appendix–Reduction step for ideals

Jacobson and Williams [2, p. 95] give the following reduction step for primitive ideals. Write I as $I = [a, b + f\omega]$ and write $\alpha = b + f\omega$. Define the *trace* of α as $T(\alpha) = \alpha + \overline{\alpha}$, so $T(\alpha) = 2b + f$ when $d \equiv 1 \pmod 4$, and $T(\alpha) = 2b$ otherwise. Now put

$$q = \begin{cases} \lfloor T(\alpha)/(2a) \rceil & \text{when } d < 0 \\ \lfloor \alpha/a \rfloor & \text{when } d > 0 \end{cases} \tag{1}$$

and $\beta = \alpha - qa$. Here $\lfloor * \rceil$ denotes the nearest integer function. Now define ρ as the operator that takes I as input and returns the ideal $\rho(I) = [-N(\beta)/a, -\overline{\beta}]$.

The ideals I and $\rho(I)$ are always weakly equivalent and might or might not be strictly equivalent.

Repeated application of the reduction step eventually produces a reduced ideal. When $d < 0$, application of the reduction step to a reduced ideal returns a different ideal (with the one exception, $d = -3$, $f = 1$, $\rho([1, \omega]) = [1, \omega]$). If $d < 0$ and I is reduced then $\rho^2(I) = I$. The ideal $\rho(I)$ might or might not be reduced. When $d > 0$ application of the reduction step to a reduced ideal returns a reduced ideal (which might or might not be different from the original ideal). Regardless of the sign of d, if I is reduced, $\rho^n(I) = I$ for some $n > 0$.

When $d < 0$, an ideal I is reduced if $N(\rho(I)) \geq N(I)$.

When $d > 0$, to see whether an ideal $I = [a, b + f\omega]$ is reduced set $k = \lfloor (-1)(b + f\overline{\omega})/|a| \rfloor$ and $\beta = k|a| + b + f\omega$. The ideal I is reduced if $\beta > |a|$.

If $d < 0$ and I is a reduced ideal, then $N(I) < \sqrt{\Delta/3}$. If $d > 0$ and I is a reduced ideal, then $N(I) < \sqrt{\Delta}$.

Every class has a reduced ideal (whether $d < 0$ or $d > 0$).

When $d > 0$, an ideal $[a, b + f\omega]$ with $a > 1$ has a cycle length of at least 2, and otherwise can be any integer. If $a = 1$, the cycle length can be any positive integer, including 1. For example, the lengths of the cycles for the following ideals is 1 (where the ideals are written as $[1, f\omega]$: $[1, \sqrt{2}]$, $[1, 5\sqrt{2}]$, $[1, (1 + \sqrt{5})/2]$, $[1, 2(1 + \sqrt{5})/2]$, $[1, 5(1 + \sqrt{5})/2]$, $[1, 13(1 + \sqrt{5})/2]$, $[1, \sqrt{10}]$, $[1, (1 + \sqrt{13})/2]$, $[1, 10(1 + \sqrt{13})/2]$, $[1, 2(1 + \sqrt{17})/2]$, $[1, \sqrt{26}]$, $[1, (1 + \sqrt{29})/2]$,$[1, 2(1 + \sqrt{37})/2]$, $[1, 10(1 + \sqrt{41})/2]$,$[1, (1+\sqrt{53})/2]$, $[1, 13\sqrt{58}]$. The length of the cycle for $[1, \sqrt{46}]$ is 12.

References

[1] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.

[2] Michael J. Jacobson Jr. and Hugh C. Williams, *Solving the Pell Equation*, Springer-Verlag, 2008.