manuscripta math. 37, 357 - 381 (1982)

manuscripta mathematica

AN ARTIN CHARACTER AND REPRESENTATIONS OF PRIMES BY BINARY QUADRATIC FORMS II

Franz HALTER-KOCH, Pierre KAPLAN and Kenneth S. WILLIAMS*

For any squarefree positive m there exists exactly one solvable antipellian equation, which can be used to construct a certain dihedral extension L/Q, cyclic of degree 4 above $k = Q(\sqrt{-m})$. We calculate the conductor of L/k and the value of the Artin character of L/k on the corresponding congruence ideal classes of order 2 of k. From this, we deduce results for the representations of powers of primes by binary quadratic forms, in the case where the norm of the fundamental unit of $Q(\sqrt{m})$ is $+1$.

1. Introduction. Let m be a squarefree positive rational integer. It is known (see, for instance, [6], §1, a): for a proof, see [2, §258] or [1, §153]) that amongst the antipellian equations

$$X^2 - mW^2 = dt \,, \tag{1.1}$$

where d is a positive divisor of m, $dt \neq 1$ and

* Research supported by Natural Sciences and Engineering Research Council Canada Grant No. A-7233

0025-2611/82/0037/0357/$05.00

$$(1.2)\qquad \begin{cases} t = 1, & \text{if } m \not\equiv -1 \pmod 4, \\ t = 1 \text{ or } 2, & \text{if } m \equiv -1 \pmod 4, \end{cases}$$

exactly one is solvable in rational integers.

Clearly (1.1) can be written as

$$(1.3)\qquad dV^2 - eW^2 = t\ ,$$

where $de = m$. In (1.3), we will suppose that V and W are positive and minimal; then V and W, as well as d, e and t are uniquely determined by m.

We define

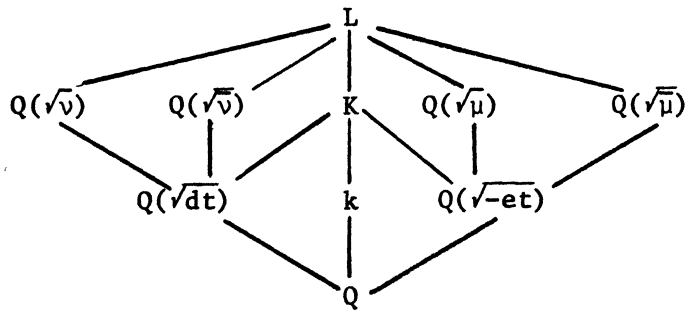
$$(1.4)\qquad \begin{cases} \mu = t - W\sqrt{-et}\ , & \bar{\mu} = t + W\sqrt{-et}\ , \\ \nu = 2t + 2V\sqrt{dt}\ , & \bar{\nu} = 2t - 2V\sqrt{dt}\ , \end{cases}$$

$$(1.5)\qquad \mu' = 2\mu,\quad \bar{\mu}' = 2\bar{\mu}\ ,\quad \nu' = \frac{\nu}{2}\ ,\quad \bar{\nu}' = \frac{\bar{\nu}}{2}\ ,$$

and consider the following fields

$$k = Q(\sqrt{-m}),\ K = Q(\sqrt{dt}, \sqrt{-et}),\ L = K(\sqrt{\mu}),\ L' = K(\sqrt{\mu'})\ .$$

Then, as $\mu\bar{\mu} = V^2 dt$, L and L' are dihedral extensions of Q whose subfield structure is as shown.



The extensions L/k and L'/k are cyclic of degree 4. As $(dt,et) = 1$ or 2 and as μ and ν have in K only divisors of 2 in common, the only ideals which can ramify in L/k and L'/k lie above 2. Therefore (cf. [3], satz 7) the conductors f and f' of L/k and L'/k are powers of 2.

The first main result of this paper is the calculation of at least one of f and f' in all cases (theorem 1, section 2).

The Artin reciprocity maps of the extensions L/k (resp. L'/k) define characters χ (resp. χ') on composition class groups C_f (resp. $C_{f'}$) of binary quadratic forms

$$F = aX^2 + bXY + cY^2 = [a,b,c]$$

of discriminant $\Delta = b^2 - 4ac = -mf^2$ (resp. $-mf'^2$) or $-4mf^2$ (resp. $-4mf'^2$) according as $-m \equiv 1 \pmod 4$ or not. The second main result of this paper gives the values of the characters χ and χ' on the classes of order 2 (ambiguous classes) of C_f and $C_{f'}$ (theorem 2, section 3).

We now define ε by

$$\varepsilon = \frac{V\sqrt{dt} + W\sqrt{-et}}{t} \quad . \tag{1.6}$$

In section 2, we shall see that ε is a unit of K and we relate it to the fundamental unit ε_m of $Q(\sqrt{m})$. On the other hand, ε and ν satisfy the following easily checked relation

$$\varepsilon\nu = t(\varepsilon + 1)^2 \quad . \tag{1.7}$$

In section 5, appealing to section 2 of [7], we give applications of the results of sections 3 and 4 to the representations of powers of certain primes q by ambiguous classes of C_f. As particular cases, we are able to prove some conjectures of [8].

2. Relation between ε and the fundamental unit ε_m of $Q(\sqrt{m})$

LEMMA 1. Let (R,S) be the minimal positive solution of the pellian equation $R^2 - mS^2 = 1$ and set $\eta = R + S\sqrt{m}$. Then

$$\eta = \varepsilon^2 . \tag{2.1}$$

PROOF. From (1.3) one finds that

$$\left(\frac{V\sqrt{dt} + W\sqrt{et}}{t}\right)^2 = R' + S'\sqrt{m} , \tag{2.2}$$

where R', S' are positive integers such that $R'^2 - mS'^2 = 1$. For a given m, the numbers d, e, t are fixed and the numbers R' and S' increase with the positive solution (V,W) of (1.3). Thus to prove Lemma 1 it is enough to show that one can solve (1.3) and (2.2) when (R',S') is the minimal positive solution (R,S) of $R^2 - mS^2 = 1$. We write (1.2) as $R^2 - 1 = mS^2$. If S is even, R is odd and, as $\frac{R+1}{2}$ and $\frac{R-1}{2}$ are coprime, we have

$$R+1 = 2dV^2 , \quad R-1 = 2eW^2 , \quad S = 2VW ,$$

giving (1.3) and (2.2) with $t = 1$. If S is odd, then R is even, so that $m \equiv -1 \pmod 4$. Then

$$R+1 = dV^2 , \quad R-1 = eW^2 ,$$

giving (1.3) and (2.2) with $t = 2$. This completes the proof.

We now consider the fundamental unit ε_m of $Q(\sqrt{m})$. If $N(\varepsilon_m) = -1$, the antipellian equation $V^2 - mW^2 = -1$ is solvable so that $d = m$, $e = 1$, $t = 1$, $\varepsilon = V + W\sqrt{m}$. It is known (cf. [1], §151) that $\varepsilon = \varepsilon_m^3$ or ε_m according as the equations $r^2 - mS^2 = 4$ has or has not odd integral solutions (r,s). If $N(\varepsilon_m) = +1$ then $\varepsilon^2 = \varepsilon_m^3$ or ε_m according as the equation $r^2 - mS^2 = 4$ has, or has not, odd integral solutions (r,s).

Let now q be a prime such that

$$(2.3) \qquad (\frac{-1}{q}) = (\frac{dt}{q}) = (\frac{-et}{q}) = 1 .$$

Then the Legendre symbol $(\frac{\varepsilon}{q})$ is well defined and also, by (2.1), the biquadratic symbol $(\frac{\varepsilon_m}{q})_4$ in the case where $N(\varepsilon_m) = +1$, and we have

$$(2.4) \qquad \begin{cases} (\frac{\varepsilon}{q}) = (\frac{\varepsilon_m}{q}), \text{ if } N(\varepsilon_m) = -1, \\ (\frac{\varepsilon}{q}) = (\frac{\varepsilon_m}{q})_4, \text{ if } N(\varepsilon_m) = +1 . \end{cases}$$

3. Calculation of the conductors f and f'. We first consider the conductor f_1 of the extension K/k. Let D, D_1, D_2 be the discriminants of the fields k, $k_1 = Q(\sqrt{dt})$, $k_2 = Q\sqrt{-et})$ respectively. By a formula of [3], p. 431, we have

$$f_1^2 = \frac{D_1 D_2}{D} \quad . \tag{3.1}$$

From (3.1), we deduce

$$f_1 = 1, \text{ if } \begin{cases} m \equiv 1 \pmod 4, \\ m \equiv -1 \pmod 4,\ t = 1,\ d \equiv -e \equiv 1 \pmod 4, \\ m \equiv 2 \pmod 4,\ d \text{ or } -e \equiv 1 \pmod 4, \end{cases}$$

$$f_1 = 4, \text{ if } \begin{cases} m \equiv -1 \pmod 4,\ t = 1,\ d \equiv -e \equiv -1 \pmod 4, \\ m \equiv 2 \pmod 4,\ d \text{ or } -e \equiv -1 \pmod 4, \end{cases}$$

$$f_1 = 8, \text{ if } \quad m \equiv -1 \pmod 4,\ t = 2 \quad .$$

If $f_1 = 4$ or 8, satz 12 and satz 13 of [3], give the values of f and f'. We have

PROPOSITION 1. If $m \equiv -1 \pmod 4$, $t = 2$ or $t = 1$, $d \equiv -e \equiv -1 \pmod 4$, then $f = f' = 16$.

If $m \equiv 2 \pmod 4$, d or $-e \equiv -1 \pmod 4$, then $f = f' = 4$.

Let δ_1 and δ_2 be the relative discriminants of the extensions $Q(\sqrt{\nu})/Q(\sqrt{d})$ and $Q(\sqrt{\mu})/Q(\sqrt{-e})$ respectively and Δ_1, Δ_2 the discriminants of the fields $Q(\sqrt{\nu})$, $Q(\sqrt{\mu})$ respectively.

By [3], satz 24, we have

$$\Delta_1 = DD_1 f^2 \ , \quad \Delta_2 = DD_2 f^2 \ . \tag{3.2}$$

We also have (see for instance [9], p. 148)

$$\Delta_1 = N_{k_1/Q}(\delta_1) D_1^2 \ , \quad \Delta_2 = N_{k_2/Q}(\delta_2) D_2^2 \ . \tag{3.3}$$

From (3.2) and (3.3), we deduce

$$(3.4) \qquad f^2 = N_{k_1/Q}(\delta_1)\,\frac{D_1}{D} = N_{k_2/Q}(\delta_2)\,\frac{D_2}{D}\ .$$

As f is a power of 2, we have only to consider the 2-parts of the intervening factors. The 2-parts of D_1, D_2 and D are well-known. The 2-parts $N_2(\delta_i)$ of $N_{k_i/Q}(\delta_i)$ $(i=1,2)$ are given in the following lemma.

LEMMA 2. Let k be a number field, z a prime ideal divisor of 2 in k, e_o the exponent of z in 2, α a number of k such that $[k(\sqrt{\alpha}):k] = 2$, $v_z(x)$ the exponent of z in the prime ideal decomposition of the ideal or number x of k, δ the relative discriminant of the extension $k(\sqrt{\alpha})/k$.

Then

a) if $v_z(\alpha) \equiv 1 \pmod 2$, then $v_z(\delta) = 2e_o + 1$;

b) if $v_z(\alpha) \equiv 0 \pmod 2$, let u be the greatest positive integer such that

$$\alpha \overset{\times}{\equiv} 1 \pmod{z^u}\ ,$$

then $u \geq 1$ and, if $u \geq 2e_o$, $v_z(\delta) = 0$; if $1 \leq u < 2e_o$, $v_z(\delta) = 2e_o - u + 1$.

PROOF. a) If $v_z(\alpha) \equiv 1 \pmod 2$, [5], satz 118 shows that $v_z(\delta) > 0$. Therefore [4], satz 3_2 applies to give $v_z(\delta) = v+1$, where the number v is equal to $2e_o$ by [4], satz 10, beweis 2a).

b) If $v_z(\alpha) \equiv 0 \pmod 2$ and $u \geq 2e_o$, [5], satz 119 shows that z is not ramified in the extension $k(\sqrt{\alpha})/k$, so that $v_z(\delta) = 0$.

c) If $v_z(\alpha) \equiv 0 \pmod 2$ and $u < 2e_o$, by [5], satz 119, $v_z(\delta) > 0$; then [a], satz 3_2 gives $v_z(\delta) = v+1$, where the integer v is equal to $2e_o - u$ by [4], satz 10, 2. The fact that $u > 0$ is proved in the course of the proof of satz 119 of [5]. (III, p.153).

REMARKS. a) If k is galois over Q, then e_o is the same for all $z|2$.

b) The meaning of $\alpha \overset{x}{\equiv} 1 \pmod{z^u}$ is that there exists $x \in k$ such that $v_z(\frac{\alpha}{x^2} - 1) \geq u$.

COROLLARY. If k is a quadratic field and $\alpha \equiv 1 \pmod 4$, $v_z(\delta) = 0$ for any $z|2$; that is 2 is unramified in the extension $k(\sqrt{\alpha})/k$.

Applying the lemma, we obtain the following results (formulated to include proposition 1).

THEOREM 1. The values of f and f' are given by the following table 1.

The symbol f_- in the case where $m \equiv 2 \pmod 4$ is the value of the conductor of L/k where instead of μ, ν one takes $-\mu$, $-\nu$ to construct the field extensions.

PROOF. We note that, when $f_1 = 1$, the equation (1.3) can be written as

$$1 = dV^2 + (-e)W^2 . \tag{3.5}$$

This equation is symmetrical in (d,V) and

TABLE 1

m , t , d , e	W , f	V , f'
$m\equiv 1 \pmod 4$		
$d\equiv 1 \pmod 8, e\equiv 1 \pmod 4$	$W \equiv 0 \pmod 4$, f=1	V odd, f' = 4
$d\equiv 5 \pmod 8, e\equiv 1 \pmod 4$	$W \equiv 2 \pmod 4$, f=2	
$d\equiv -1 \pmod 4, -e\equiv 1 \pmod 8$	W odd, f = 4	$V \equiv 0 \pmod 4$, f' = 1
$d\equiv -1 \pmod 4, -e\equiv 5 \pmod 8$		$V \equiv 2 \pmod 4$, f' = 2
$m \equiv -1 \pmod 4$		
t = 2	f = 16	f' = 16
$t = 1,\ d \equiv -e \equiv -1 \pmod 4$	f = 16	f' = 16
$t = 1, d \equiv -e \equiv 1 \pmod 4$	W odd f = 8 $W\equiv 0 \pmod 4 \Rightarrow d\equiv 1 \pmod 8$, f=1 $W\equiv 2 \pmod 4 \Rightarrow d\equiv 5 \pmod 8$, f=4	$W\equiv 0 \pmod 4 \Rightarrow -e\equiv 1 \pmod 8$, f'=1 $W\equiv 2 \pmod 4 \Rightarrow -e\equiv 5 \pmod 8$, f'=4 V odd, f' = 8
$m\equiv 2 \pmod 4$		
$d\equiv 2,\ -e \equiv -1 \pmod 4$	f = 4	f' = 4
$d\equiv -1,\ e\equiv 2 \pmod 4$		
$d\equiv 2 \pmod 4, e\equiv 2 \pmod 4$	W odd	$V\equiv 0 \pmod 4$: f'=1, f_=2 $V\equiv 2 \pmod 4$: f'=2, f_=1
$d\equiv 1 \pmod 8,\ e\equiv 2 \pmod 4$	$W\equiv 0 \pmod 4$: f=1, f_=2 $W\equiv 2 \pmod 4$: f=2, f_=1	V odd

$(-e,W)$, so that, as the determination of f and f' is a 2-adic problem, it is enough to change (d,V) into $(-e,W)$ to obtain the value of f' knowing the value of f.

We give the proof in one case, $m \equiv 2 \pmod 4$; the other cases are similar.

Suppose $d \equiv 1 \pmod 4$, $e \equiv 2 \pmod 4$. By (2.4) we have

$$f^2 = \frac{1}{4} N_2(\delta_1) = N_2(\delta_2) .$$

Now, the relation $1 = dV^2 - eW^2$ shows that V is odd, therefore W is even and $d \equiv 1 \pmod 8$. Also $(2) = z^2$ in $Q(\sqrt{-e})$.

Now, if $W \equiv 0 \pmod 4$, $\mu = 1 - W\sqrt{-e} \equiv 1 \pmod 4$, therefore $\delta_2 = (1)$ and $f = 1$.

If $W \equiv 2 \pmod 4$, $\mu \equiv 1 \pmod{z^3}$, so that $u \geq 3$.

But one sees easily that $\mu \not\equiv$ square $\pmod 4$, so that $u = 3$ and $v_z(\delta_2) = 2$, $f = 2$.

Also $-1 + W\sqrt{-e} \equiv$ square $\pmod 4$ if, and only if, $W \equiv 2 \pmod 4$ so that $f_- = 2$ or 1 according as $W \equiv 0$ or $2 \pmod 4$.

Changing the role of d and $-e$, we see that if $d \equiv 2 \pmod 4$ and $-e \equiv 1 \pmod 4$, then $-e \equiv 1 \pmod 8$ and W is odd, V even, $f' = 1$, $f'_- = 2$ if $V \equiv 0 \pmod 4$, $f' = 2$, $f'_- = 1$ if $V \equiv 2 \pmod 4$.

4. Determination of the Artin character of L/k on ambiguous classes

The ideal class group of conductor f of the

ring of integers of k is isomorphic to the composition class group C_f of primitive positive binary quadratic forms

$$F = aX^2 + bXY + cY^2 = [a,b,c]$$

of discriminant $\Delta = b^2 - 4ac = -mf^2$ if $-m \equiv 1 \pmod 4$, $-4mf^2$ if $-m \not\equiv 1 \pmod 4$.

Before stating theorem 2, we give a list of the ambiguous classes and the generic characters for each C_f. In table 2, each class is defined from a decomposition $m = rs$ or $m = 2rs$ (r and s odd) by one form or by two equivalent ($\approx$) forms in it; all decompositions $m = rs$ or $m = 2rs$ are to be taken. For a proof, we refer to [1], §153.

The generic characters $e_p(F)$ are the values of the Legendre symbols $(\frac{x}{p})$ for $p \mid rs$ and any x prime to p represented by F and also eventually the supplementary characters $e_2(F) = (\frac{-1}{x})$ and $e_2'(F) = (\frac{2}{x})$ for any odd x represented by F. We indicate in table 2 whether e_2 or e_2' (or both) appears.

If the ambiguous class A contains a form $[r,0,s']$ or $[r, r, \frac{r+s}{4}]$ where r is odd, we say that the class A is odd. Otherwise, we say that the class A is even. Concerning the even classes, we note the following:

If $m \equiv 1\ (4)$, f or $f' = 1$, the class of $[2r, 2r, \frac{r+s}{2}]$ is the product of the class of $[r,0,s]$ and of $[2, 2, \frac{1+m}{2}]$. In the other cases, any even class of $[4r,4r,r+2^n s]$ is the product of the classes

TABLE 2

	Ambiguous classes	Generic characters e_2, e_2'
$m\equiv 1 \pmod 4$, $m=rs$,	$\Delta=-4mf^2$	
$f = 1$	$\begin{cases}[r,0,s] \approx [s,0,r] \\ [2r,2r,\frac{r+s}{2}]\approx[2s,2s,\frac{r+s}{2}]\end{cases}$	e_2
$f = 2$	$[r,0,4s]$	e_2
$f = 4$	$[r,0,16s],[4r,4r,r+4s]$	e_2, e_2'
$m\equiv -1 \pmod 4$, $m=rs$,	$\Delta = -mf^2$	
$f = 1$	$[r,r,\frac{r+s}{4}]$	
$f = 2$	$[r,0,s]$	
$f = 4$	$[r,0,4s]$	e_2
$f = 8$	$[r,0,16s],[4r,4r,r+4s]$	e_2, e_2'
$f = 16$	$[r,0,64s],[4r,4r,r+16s]$	e_2, e_2'
$m\equiv 2 \pmod 4$, $m=2rs$,	$\Delta = -4mf^2$	
$f = 1$	$[r,0,2s]$	$\begin{cases}e_2' & \text{if } m\equiv 6 \pmod 8 \\ e_2e_2' & \text{if } m\equiv 2 \pmod 8\end{cases}$
$f = 2$	$[r,0,8s],[4r,4r,r+2s]$	e_2, e_2'
$f = 4$	$[r,0,32s],[4r,4r,r+8s]$	e_2, e_2'

of $[r,0,2^{n+2}s]$ and $[4,4,1-\frac{\Delta}{16}]$, so that it is enough to know the value of the Artin characters on the odd classes, on the class of $[2,2,\frac{1+m}{2}]$ if $m \equiv 1 \pmod 4$, f or $f'=1$ and on the classes of $[4,4,1-\frac{\Delta}{16}]$ when they appear. We have

THEOREM 2. (i) Let A be an odd ambiguous class containing $[r,0,s']$ or $[r,r,s']$, where r is odd. Let $r = uv$ where $u|d$, $v|e$. Then we have

if $t = 1$, $\chi(A) = (\frac{2}{u})$, $\chi'(A) = (\frac{2}{v})$;

if $t = 2$, $\chi(A) = (\frac{2}{v})$, $\chi'(A) = (\frac{2}{u})$.

(ii) For the even ambiguous class A_o, containing the form $[4,4,1-\frac{\Delta}{16}]$, the values of $\chi(A_o)$ and $\chi'(A_o)$ are both -1.

(iii) If $m \equiv 1 \pmod 4$ and A is the class of $[2,2,\frac{1+m}{2}]$, then if $f = 1$, $\chi(A) = (-1)^{\frac{W}{4}}$ and if $f'=1$, $\chi'(A) = (-1)^{\frac{W}{4}}$.

PROOF OF (i). Clearly it suffices to calculate the values of χ and χ' on a class A_p containing the form $[p,0,\frac{-\Delta}{p}]$ (or $[p,p,\frac{p+m}{4}]$ in the case $m \equiv -1 \pmod 4$, $f = 1$). The class A_p corresponds to the ideal class of conductor f of the ideal P of k such that $p = P^2$ in k. Therefore $\chi(A_p)$ (respectively $\chi'(A_p) = 1$ or -1) according as the ideal P is completely decomposed or not in the extension L/k (respectively L'/k). In K we have $P = P_1P_2$.

Suppose that $p|d$. Then, as $d'V^2 = t - e'W^2 = \mu\bar{\mu}$ and as μ and $\bar{\mu}$ have no common odd divisor we have, say, that $P_2|\bar{\mu}$ and $P_2|\bar{\mu}'$. As $L = K(\sqrt{\bar{\mu}})$ and $P_1|\mu$ so that $W\sqrt{-e'} \equiv t \pmod{P_1}$ we have, denoting by $[\ ]_K$ the quadratic residue symbol in K :

$$(4.1)\quad \begin{cases} \chi(A_p) = \left[\frac{\bar{\mu}}{P_1}\right]_K = \left[\frac{t+W\sqrt{-e'}}{P_1}\right]_K = \left[\frac{2t}{P_1}\right]_K = \left(\frac{2t}{p}\right), \\ \chi'(A_p) = \left(\frac{4t}{p}\right) = \left(\frac{t}{p}\right), \end{cases}$$

as $N(P_1) = p$ and $\bar{\mu}' = 2\mu'$.

If $p|e$ we find, using ν instead of μ

$$(4.2)\qquad \chi(A_p) = \left(\frac{t}{p}\right),\quad \chi'(A_p) = \left(\frac{2t}{p}\right),$$

which, together with (4.1), is our result.

PROOF OF (ii). Inclusion induces a natural homomorphism of the ideal class group of conductor f on the ideal class group of conductor $\frac{f}{2}$ whose kernel consists of the classes I and A_o. If $\chi(A_o)$ had the value 1 on A_o, χ would take the value 1 on the whole principal ideal class of conductor $\frac{f}{2}$, contradicting the fact that the conductor is f.

PROOF OF (iii). Here $m \equiv 1 \pmod 4$, f or $f' = 1$ (see table 1).

We treat the case $f = 1$, the case $f' = 1$ will be obtained by interchanging (d,V) and $(-e,W)$.

Therefore $d \equiv 1 \pmod 8$, $e \equiv 1 \pmod 4$. The ideal (2) decomposes as $(2) = \bar{2}^2$ in k and as

$(2) = z^2$ in $Q(\sqrt{-e})$. The ideal class of $\bar{2}$ corresponds to the class of the form $[2,2,\frac{1+m}{2}]$.

As $d \equiv 1 \pmod 8$ the ideal $\bar{2}$ is decomposed in K, therefore it is completely decomposed in L if, and only if, the ideal z is decomposed in $Q(\sqrt{\mu})$, that is, by [5], satz 119, if, and only if, the congruence

$$1 - W\sqrt{-e} \equiv Z^2 \pmod{z^5} \tag{4.3}$$

is solvable with Z in the ring of integers of $Q(\sqrt{-e})$. It is clear that, if $W \equiv 0 \pmod 8$, (4.3) is solvable. Conversely, suppose (4.3) solvable. We note that $z^4 = (4)$ and that z is the set of the integers of $Q(\sqrt{-e})$ congruent to $1 + \sqrt{-e}$ modulo 2.

Thus, if (3.3) is solvable, there exist rational integers a, b, x, y such that

$$1 - W\sqrt{-e} \equiv (a+b\sqrt{-e})^2 + 4(1+\sqrt{-e})(x+y\sqrt{-e}) \pmod 8$$

that is,

$$1 \equiv a^2 - eb^2 + 4(x-ey) \pmod 8, \tag{4.4}$$

$$W = 2ab + 4(x+y) \pmod 8. \tag{4.5}$$

From (4.4) we see that a is odd, b even, say $b = 2c$, so that

$$0 \equiv -ec^2 + x - ey \equiv c+x+y \pmod 2, \tag{4.5}$$

$$\frac{W}{4} \equiv c + (x+y) \pmod 2, \tag{4.6}$$

showing that $W \equiv 0 \pmod 8$.

5. Applications. We begin by letting r_{2^k} (respectively r'_{2^k}) denote the 2^k-rank of the group C_f (respectively $C_{f'}$). We note that for any ambiguous class, we have $\chi(A) = \pm 1$, $\chi'(A) = \pm 1$ and that $r_4 \geq 1$.

A prime q such that $(\frac{-m}{q}) = +1$ is represented by two inverse classes Q and Q^{-1} or by one self-inverse (ambiguous) class of forms of C_f, as well as of $C_{f'}$. If

$$(\frac{-et}{q}) = (\frac{dt}{q}) = +1 , \tag{5.1}$$

q is completely decomposed in K. Then q is completely decomposed in L (resp. L') if, and only if, $(\frac{\nu}{q}) = +1$ (resp. $(\frac{2\nu}{q}) = 1$).

The primes q satisfying (5.1) are those for which $\chi(Q) = \pm 1$, $\chi'(Q) = 1$, so that for such q we have $(\frac{\nu}{q}) = \chi(Q)$, $(\frac{2\nu}{q}) = \chi'(Q)$.

In order to apply theorems 1 and 2, we need some results from [7]. The results needed are stated as propositions 2 and 3 below.

We state them for C_f. In order to apply them to $C_{f'}$, it is enough to replace $(\frac{\nu}{q})$ by $(\frac{2\nu}{q})$.

PROPOSITION 2. *Suppose that* $r_8 = 0$. *Let* q *be a prime represented by a class* Q *in a genus of ambiguous classes of* C_f. *Then the class* Q^ℓ, *where*

$$\text{ord } Q = 2^x \ell, \quad \ell \text{ odd} \tag{5.2}$$

is an ambiguous class such that

$$\chi(Q^\ell) = (\frac{\nu}{q}) .$$

PROPOSITION 3. Suppose that $r_4 = 1$. Let J denote the ambiguous class different from the principal class I in the principal genus of C_f. Then

(5.3) $$r_8 = 1 \iff \chi(J) = 1 .$$

Let q be a prime represented by a class Q in the genus of the ambiguous classes A and AJ. Then we have

(5.4) The class QA is a fourth power if, and only if, $(\frac{\nu}{q}) = \chi(A)$,

(5.5) If $r_8 = 0$, then $Q^{\ell} = A$ or AJ according as $(\frac{\nu}{q}) = \chi(A)$ of $-\chi(A)$ respectively, where ℓ is defined by (5.2).

(5.6) If $r_8 = 1$, then $Q^s = I$ or J according as $(\frac{\nu}{q}) = \chi(A)$ or $-\chi(A)$ respectively, where

(5.7) $$s = h/2^{r_2+1} , \quad h = \operatorname{ord} C_f .$$

We remark that $Q^{\ell} = Q^s$ when $r_8 = 0$. If Q is the principal genus, we can take $A = I$ in proposition 3 to obtain the following corollary.

COROLLARY. Suppose that $r_4 = 1$. If Q is in the principal genus, then Q is a fourth power, if, and only if, $(\frac{\nu}{q}) = 1$; and q^s is represented by I or J according as $(\frac{\nu}{q}) = +1$ or -1 .

If the prime q satisfying (5.1) is $\equiv 1 \pmod 4$, then

(5.8) $$(\frac{-1}{q}) = (\frac{dt}{q}) = (\frac{et}{q}) = 1 .$$

For such a prime, the Legendre symbols $(\frac{\varepsilon t}{q})$ and

$(\frac{2\varepsilon t}{q})$ are well defined and by (1.7), we have:

$$(5.9) \qquad (\frac{\nu}{q}) = (\frac{\varepsilon t}{q}); \quad (\frac{2\nu}{q}) = (\frac{2\varepsilon t}{q}) .$$

EXAMPLE 1. We treat the case $m = pp'$, where $p \equiv p' \equiv 3 \pmod 4$, proving conjectures 1.6 of [8].

We may suppose $(\frac{p'}{p}) = 1$ and we set $\alpha = (\frac{2}{p})$, $\alpha' = (\frac{2}{p'})$.

It is easy to see that in this case the equation (1.3) is

$$1 = p'V^2 - pW^2 ,$$

so that $d = p'$, $e = p$ and by theorem 1, we have

$f = 4$, $f' = 1$ if $p \equiv 7 \pmod 8$, $f' = 2$ if $p \equiv 3 \pmod 8$.

a) Suppose $p \equiv 3 \pmod 8$, that is $\alpha = -1$. For $C_{f'} = C_2$, the generic characters are $(\frac{-1}{x})$, $(\frac{x}{p})$, $(\frac{x}{p'})$. We list representatives of the ambiguous classes, the values of the generic characters (G.C) and of the Artin character χ' :

	[1,0,4pp']	[p,0,4p']	[p',0,4p]	[pp',0,4]
G.C.	1 , 1 , 1	-1,+1,-1	-1,+1,-1	1, 1, 1
χ'	1	$\alpha = -1$	1	$\alpha = -1$.

We see that $r_2' = 2$, $r_4' = 1$, $J = \{[pp',0,4]\}$ and $r_8' = 0$, as $\chi'(J) = -1$. Also $s = \frac{h'}{8} = \frac{h}{4}$ where h is the class number of $Q(\sqrt{-pp'})$. Therefore, we obtain by (5.5) and (5.9)

A) Let q be such that $(\frac{-1}{q}) = (\frac{q}{p}) = (\frac{q}{p'}) = 1$. Then $q^{\frac{h}{4}}$ is represented by $[1,0,4pp']$ or $[4,0,pp']$ according as $(\frac{\varepsilon}{q})(\frac{2}{q}) = 1$ or -1.

B) If q is such that $(\frac{-1}{q}) = (\frac{q}{p'}) = -1$, $(\frac{q}{p}) = 1$, then $q^{\frac{h}{4}}$ is represented by $[p',0,4p]$ or by $[p,0,4p']$ according as $(\frac{2\nu}{q}) = 1$ or -1.

Numerical example. $m = 21$, $h = 4$, $p = e = 3$, $p' = d = 7$.

Clearly $1 = 7.2^2 - 3.3^2$ so that $V = 2$, $W = 3$ and

$$\varepsilon = 2\sqrt{7} + 3\sqrt{3} \; ; \quad 2\nu = 4 + 4\sqrt{7} \; .$$

$q = 37$, $(\frac{-1}{q}) = (\frac{q}{3}) = (\frac{q}{7}) = 1$. We find $7 \equiv 9^2$, $3 \equiv 15^2 \pmod{37}$ so that $(\frac{2}{37}) = (\frac{\varepsilon}{37}) = -(\frac{2\sqrt{7} + 3\sqrt{3}}{37}) = -(\frac{18 + 45}{37}) = -1$.

We have also $37 = 4.2^2 + 21.1^2$, which shows that 37 is represented by the form $[4,0,pp']$, in accordance with A).

$q = 19$, $(\frac{-1}{q}) = (\frac{q}{7}) = -1$, $(\frac{q}{3}) = 1$. We find $7 \equiv 8^2 \pmod{19}$ so that $(\frac{2\nu}{q}) = (\frac{4 + 4\sqrt{7}}{19}) = (\frac{4 + 4.8}{19}) = (\frac{36}{19}) = 1$, but here $19 = 7.1^2 + 3.2^2$, that is 19 is represented by the form $[p',0,4p]$, in accordance with B).

We now show how A) implies conjectures 1.6 of [8]. Here $(\frac{-1}{q}) = (\frac{p}{q}) = (\frac{q}{p'}) = 1$.

If $(\frac{\varepsilon}{q}) = (\frac{2}{q})$, then $q^{\frac{h}{4}} = X^2 + 4pp'Y^2$. As $\frac{h}{4}$ is odd, $(\frac{2}{q}) = (-1)^Y$, so that

$$(\frac{\eta}{q})_4 = (\frac{\varepsilon}{q}) = (-1)^Y .$$

If $(\frac{\varepsilon}{q}) = -(\frac{2}{q})$, then $q^{\frac{h}{4}} = 4X^2 + pp'Y^2$, therefore $q \equiv 4X + 3p' \pmod 8$, so that $(-1)^X = (\frac{2}{q})(\frac{-2}{p'})$ giving

$$(\frac{\eta}{q})_4 = (\frac{\varepsilon}{q}) = -(\frac{2}{q}) = (-1)^{X+1}(\frac{-2}{p'}) .$$

b) Suppose $p \equiv 7 \pmod 8$, that is $\alpha = 1$; then $f' = 1$. The generic characters are $(\frac{-1}{x})$, $(\frac{x}{p})$, $(\frac{x}{p'})$. We give the ambiguous classes

$$[1,0,pp'] \; ; \; [p,0,p'] \; ; \; [2,2,\tfrac{1+pp'}{2}] \; ; \; [2p,2p,\tfrac{p+p'}{2}]$$

G.C.	1,1,1	; -1,1,-1	; α',1,α'	; $-\alpha'$,1,$-\alpha'$
χ'	1	; 1	; $(-1)^{\frac{V}{4}}$	; $(-1)^{\frac{V}{4}}$

Here $r_2' = 2$, $r_4' = 1$, $r_8' = 1$ if $V \equiv 0 \pmod 8$, $r_8' = 0$ if $V \equiv 4 \pmod 8$ and the class J is the class of $[2,2,\frac{1+pp'}{2}]$ or of $[2p,2p,\frac{p+p'}{2}]$ according as $\alpha' = 1$ or -1. We obtain the following result.

A) Let $q \equiv 1 \pmod 4$ be such that $(\frac{q}{p}) = (\frac{q}{p'}) = 1$. Then $q^{\frac{h}{8}}$ is represented by I or J according as $(\frac{\varepsilon}{q})(\frac{2}{q}) = 1$ or -1.

Let $q \equiv -1 \pmod 4$ be such that $(\frac{q}{p}) = -(\frac{q}{p'}) = 1$.

If $r_8' = 1$, $q^{\frac{h}{8}}$ is represented by I or J according as $(\frac{2\nu}{q}) = 1$ or -1 .

If $r_8' = 0$, $q^{\frac{h}{8}}$ is represented by A_p or JA_p according as $(\frac{2\nu}{q}) = 1$ or -1 where A_p is the class of $[p,0,p']$.

The conjectures 1.7 of [8] can be proved by the same method. The conjectures 3.6 and 3.7 cannot be obtained, but we note that the case 3.6 is included in 1.6.

We now treat the case of conjectures 3.7 of [8].

EXAMPLE 2. $m = 2pp'$, $p \equiv 5 \pmod 8$, $p' \equiv 3 \pmod 4$, $(\frac{p'}{p}) = -1$.

Considering the class group of forms of discriminant $+8pp'$, we see that in this case (1.3) is

$$1 = 2p'V^2 - pW^2 .$$

Therefore $d = 2p'$, $e = -p \equiv -1 \pmod 4$, so that $f = f' = 4$.

We consider C_f. The generic characters are $(\frac{-1}{x})$, $(\frac{2}{x})$, $(\frac{x}{p})$, $(\frac{x}{p'})$.

The ambiguous classes in the principal genus are the unit class I and the class J of $[4,4,1+8pp']$, for which $\chi(J) = -1$, so that $r_2 = 3$, $r_4 = 1$, $r_8 = 0$.

Let h be the ideal class number of $Q(\sqrt{-m})$;

$s = \frac{4h}{16} = \frac{h}{4}$. Then we obtain

A) Let $q \equiv 1 \pmod 8$ be such that $(\frac{q}{p}) = (\frac{q}{p'}) = 1$. Then $q^{\frac{h}{4}}$ is represented by I or J according as $(\frac{\varepsilon}{q}) = 1$ or -1.

A') Let $q \equiv 5 \pmod 8$ be such that $(\frac{q}{p}) = 1$, $(\frac{q}{p'}) = -1$. Then $q^{\frac{h}{4}}$ is represented by $[p,0,32p']$ or $[4p,4p,p+8p']$ according as $(\frac{\varepsilon}{q}) = 1$ or -1.

It is also possible here to obtain results analogous to A of example 1 for $q \equiv -1 \pmod 4$.

Numerical example. $p = 5$, $p' = 3$; $V = W = 1$, $\varepsilon = \sqrt{5} + \sqrt{6}$, $h = 4$; $t = 1$.

The smallest $q \equiv 1 \pmod 8$ such that $(\frac{q}{5}) = (\frac{q}{3}) = 1$ is 241.

By the exclusion method [2], §319, we find easily that $\sqrt{5} \equiv 103$ and $\sqrt{6} \equiv 27 \pmod{241}$ so that $(\frac{\varepsilon}{241}) = (\frac{130}{241}) = -1$. Here, in accordance with A , 241 is represented by the form $4X^2 + 4XY + 121Y^2$ for $X = 5$, $Y = 1$ and not by $X^2 + 480Y^2$.

The smallest $q \equiv 5 \pmod 8$ such that $(\frac{q}{5}) = 1$, $(\frac{q}{3}) = -1$ is 29 .

Here, $\sqrt{6} \equiv 8$, $\sqrt{5} \equiv 11 \pmod{29}$, $(\frac{\varepsilon}{29}) = (\frac{19}{29}) = -1$, and, in accordance with A', 29 is represented by $[20,20,29]$ for $(0,1)$ and clearly not by $[5,0,96]$.

EXAMPLE 3. Let m be a positive squarefree odd integer such that the antipellian equation

$$V^2 - mW^2 = 2 \quad , \quad \delta = \pm 1 \, , \tag{5.10}$$

is solvable in integers V and W, implying that $m \equiv 3 \pmod 4$. Clearly V and W are both odd so that $m \equiv 7 \pmod 8$ if $\delta = +1$, $m \equiv 3 \pmod 8$ if $\delta = -1$.

Here $t = 2$, $f = 16$ and (1.3) becomes

$$2 = \delta V^2 - \delta m W^2 \, ,$$

so that $d = 1$, $e = m$ if $\delta = +1$ and $d = m$, $e = 1$ if $\delta = -1$. We choose L' if $\delta = 1$, L if $\delta = -1$; then the Artin character χ' or χ has the value 1 on the odd ambiguous classes and -1 on the even ambiguous classes of C_{16}. On the other hand, it is easy to check that C_{16} and C_1 have the same 8-rank so that we obtain, using proposition 1:

Suppose that m is a positive squarefree odd integer satisfying (5.10) and having 8-rank of the ideal class group of $Q(\sqrt{-m})$ equal to zero. Then, if q is a prime satisfying

$$(\frac{-1}{q}) = (\frac{2}{q}) = (\frac{m}{q}) = +1$$

and represented by a class in a genus of ambiguous classes of C_{16}, then q^{ℓ} is represented by an odd ambiguous class or by an even ambiguous class according as $(\frac{\varepsilon}{q}) = +1$ or -1, where ℓ denotes the largest odd divisor of the order of the ideal class group of

$Q(\sqrt{-m})$.

EXAMPLE 4. This example generalises example 3 of [7], p. 14-15. We suppose that m is a product of primes $\equiv 1 \pmod 8$. Then $f = 1$ and (1.3) can be written as

$$1 = dV^2 - eW^2$$

where $W \equiv 0 \pmod 4$.

If $r_8 = 0$, that is, if the 8-rank of $Q(\sqrt{-m})$ is 0 , we can prove as in [7], p. 14-15, that $W \equiv 4 \pmod 8$ and that if q is a prime $\equiv 1 \pmod 4$ represented by a class Q in the genus of an ambiguous class, then the class Q^{ℓ} is odd or even according as $(\frac{\varepsilon}{q}) = 1$ or -1.

REFERENCES

[1] P. G. L. DIRICHLET and R. DEDEKIND, Vorlesungen über Zahlentheorie, Chelsea Publishing Company, New York (1968)

[2] C. F. GAUSS, Disquisitiones Arithmeticae, translated into English by Arthur A. Clarke, Yale University Press, (1966)

[3] F. HALTER-KOCH, Arithmetische Theorie der Normalkörper von 2. Potenzgrad mit Dieder gruppe, J. Number Theory, 3, (1971), pp.412-443

[4] H. HASSE, Bericht über neuere Untersuchungen une Probleme aus der Theorie der algebraischen Zahlkörper, Physica-Verlag, Würzburg (1965)

[5] E. HECKE, Vorlesungen über die Theorie der algebraischen Zahlen, Chelsea Publishing Company, New York (1965)

[6] P. KAPLAN, Sur le 2-groupe des classes d'idéaux des corps quadratiques, J. Reine Angew. Math. 283/284 (1976), 313-363

[7] P. KAPLAN and K. S. WILLIAMS, An Artin character and representations of primes by binary quadratic forms, Manuscripta Mathematica, 33 (1981), 339-356

[8] P. A. LEONARD and K. S. WILLIAMS, The quadratic and quartic character of certain quadratic units II, Rocky Mountain J. Math. 9 (1979), 683-692

[9] W. NARKIEWICZ, Elementary and Analytic Theory of Algebraic Numbers, Polish Scientific Publishers, Warsaw (1974)

Institut für Mathematik
Karl-Franzens-Universität Graz
Halbärthgasse 1/1
A-8010 Graz
AUSTRIA

10, Allée Jacques Offenbach
54420 - Saulxures les Nancy
FRANCE

Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario, CANADA
K1S 5B6

(Received February 9, 1982)