A type of class group for imaginary quadratic fields

by

MAURICE CRAIG (Ann Arbor, Mich.)

1. Introduction. Let $C(n)$ denote the cyclic group of order n, $C(n)\times C(n)$ the direct product of two such groups. In [5], Yamamoto constructs imaginary quadratic fields for which the ideal class group contains a subgroup isomorphic with $C(n)\times C(n)$, while showing that for each value of n, the cardinality of fields of this type is infinite. The construction rests upon a polynomial, of degree $2n-1$ in a parameter t, which can be arranged in two different ways in the form B^2-4A^n. Here A, B denote polynomials in t with rational integer coefficients.

A further result of the same type is the

THEOREM. *Infinitely many imaginary quadratic fields have a subgroup of the class group isomorphic to* $C(3)\times C(3)\times C(3)$.

The proof is by applying Yamamoto's methods to a polynomial of degree 24, which has five different representations in the form B^2-4A^3.

Making use of a theorem of Scholz, another of Yamamoto's conclusions is obtained as the

COROLLARY. *Infinitely many real quadratic fields have a subgroup of the class group isomorphic to* $C(3)\times C(3)$.

2. Preliminaries. (a) Let $Q(\sqrt{d})$ denote the quadratic field of discriminant d. As shown in [5], results concerning the ideal class group of $Q(\sqrt{d})$ may be inferred from certain solutions of the diophantine equation

$$B^2-4A^n = C^2 d. \tag{1}$$

For the case $d<-4$ and n an odd prime, the following two propositions summarize the procedures.

PROPOSITION 1. *Let* (A, B, C) *be a solution of* (1) *with* A *and* B *relatively prime. Suppose there is a rational prime* l *dividing* A, *such that* B *is not an* n*-th power residue of* l. *Then the ideal*

$$\mathfrak{A}_A = \left(A, \frac{B+C\sqrt{d}}{2}\right)$$

belongs to a class of order n.

We refer to $\mathfrak{A}_A$ as the ideal *corresponding* to the solution (A, B, C) and write f_A to denote the class containing it.

PROPOSITION 2. *Let*

$$B^2-4A^n = C^2d = B'^2-4A'^n \tag{2}$$

where

$$(A, B) = 1 = (A', B').$$

Suppose l, l' are distinct primes dividing A, A' respectively and that

$$B \not\equiv n\text{-th power} \pmod{l}, \qquad B' \not\equiv n\text{-th power} \pmod{l'}.$$

Suppose in addition the following "trace condition" holds:

$$\frac{B+B'}{2} \equiv \text{non-zero } n\text{-th power} \pmod{l'}.$$

Then the corresponding ideals $\mathfrak{A}_A, \mathfrak{A}_{A'}$ determine independent classes of order n.

Note that by Proposition 1, each of the cyclic groups $\langle f_A\rangle$, $\langle f_{A'}\rangle$ has order n. The role of the trace condition is to ensure that the subgroup $\langle f_A, f_{A'}\rangle$, generated by both classes taken together, is a direct product of two cyclic groups of order n.

By an immediate extension of the ideas used in proving Proposition 2, we obtain

PROPOSITION 3. *If $B^2-4A^n = B'^2-4A'^n = B''^2-4A''^n$, with $(A, B) = (A', B') = (A'', B'') = 1$, and for primes l, l', l'' dividing A, A', A'' respectively,*

$$B \text{ (resp. } B', B'') \not\equiv n\text{-th power} \pmod{l \text{ (resp. } l', l'')},$$

$$\frac{B+B'}{2} \equiv \text{non-zero } n\text{-th power} \pmod{l'},$$

$$\frac{B+B''}{2} \equiv \text{non-zero } n\text{-th power} \pmod{l''},$$

$$\frac{B'+B''}{2} \equiv \text{non-zero } n\text{-th power} \pmod{l''},$$

then

$$\langle f_A, f_{A'}, f_{A''}\rangle \cong \boldsymbol{C}(n)\times\boldsymbol{C}(n)\times\boldsymbol{C}(n).$$

(b) Consider the diophantine equation

$$B^2-4A^n = B'^2-4A'^n$$

encountered above. Writing it as

$$\frac{B+B'}{2}\,\frac{B-B'}{2} = A^n-A'^n$$

and setting $A = xz$, $A' = xw$, $\dfrac{B+B'}{2} = x^n$, a parametric solution is obtained in the form of the identity

$$(x^n+z^n-w^n)^2-4(xz)^n = (x^n-z^n+w^n)^2-4(xw)^n.$$

From symmetry, each side equals

$$(-x^n+z^n+w^n)^2-4(zw)^n.$$

Suppose now that for integer values of x, z, w the common value of the three expressions above is C^2d, where d is a quadratic field discriminant, $d < -4$. We evidently have solutions of (2), so from Proposition 2 it is to be expected that for values of d which arise in this way, the field $\boldsymbol{Q}(\sqrt{d})$ will in some cases have a subgroup of the class group isomorphic to $\boldsymbol{C}(n)\times\boldsymbol{C}(n)$.

While this is the case, we do not obtain in this manner as many as three factors $\boldsymbol{C}(n)$, which might be expected from the existence of the third expression above. (This is because the classes of the three corresponding ideals satisfy an identical relation.) Suppose, however, that x, y, z, w could be selected with x and y unequal, but so that

$$(-x^n+z^n+w^n)^2-4(zw)^n = (-y^n+z^n+w^n)^2-4(zw)^n.$$

By means of the identities already noted, we should have not merely three, but five expressions of the same quantity in the form B^2-4A^n, the values for the five pairs $[A, B]$ being given by

$$\begin{aligned} &[xz,\ X+Z-W],\\ &[xw,\ X-Z+W],\\ &[yz,\ Y+Z-W],\\ &[yw,\ Y-Z+W],\\ &[zw,\ -X+Z+W], \end{aligned} \tag{3}$$

where $X = x^n$ and so on. It suffices to take

$$-x^n+z^n+w^n = -(-y^n+z^n+w^n)$$

or

$$x^n+y^n = 2(z^n+w^n). \tag{4}$$

Now when $n = 3$, the solutions of (4) in integers are known (cf. [1]). We make use of the solution given by the formulae

$$\begin{aligned} x &= s^4, \qquad y = s(18t^3-s^3),\\ z &= 18t^4, \qquad w = 3t(s^3-6t^3) \end{aligned} \tag{5}$$

and conclude the Preliminaries by noting the following

LEMMA 0. *Let x, y, z, w be as in (5), where s and t are integers. Then for each of the five pairs $[A, B]$ in (3) we have*

$$(A, B) = 1,$$

provided s and t satisfy the conditions

(i) $(t, 2) = 2$,
(ii) $(s, 3t) = 1$,
(iii) $(s+2^\alpha t,\ 7) = 1$ *for* $\alpha = 0, 1, 2$ (*this being the same as for all* $\alpha \geqslant 0$).

Proof. Using (4), it is readily verified that requiring all pairs in (3) to be relatively prime is equivalent to the requirements

$$(x, Z-W) = (y, Z-W) = (z, X-W) = (w, X-Z) = 1.$$

Take, for example, the last of these. Supposing there is a prime p dividing $(w, X-Z)$, then with congruences to the modulus p, we have

$$w \equiv 0, \quad X-Z \equiv 0.$$

From the former relation, either $3t \equiv 0$ or else $s^3 \equiv 6t^3$. If $3t \equiv 0$ then $Z \equiv 0$, so $X \equiv 0$. Thus p divides $(s, 3t)$, contradicting (ii). If $s^3 \equiv 6t^3$, then

$$X-Z = (s^4)^3 - (18t^4)^3 \equiv (6t^3)^4 - (18t^4)^3 = -21(6t^4)^3.$$

By virtue of (i), $6t \equiv 0$ is equivalent to $3t \equiv 0$ and leads to the same contradiction as before. On the other hand, if $p = 7$, then $s^3 \equiv -t^3$. We cannot have $t \equiv 0$, for in that case 7 divides (s, t). Thus

$$\left(\frac{s}{t}\right)^3 \equiv -1 \pmod 7 \quad \text{or} \quad \frac{s}{t} \equiv -1, -2 \text{ or } -4 \pmod 7,$$

contradicting (iii). The other cases are treated similarly.

3. Local considerations. (a) Let distinct primes m, n be chosen subject to the conditions

$$\left.\begin{matrix} 2,\ 3 \equiv \text{cubes} \\ 7 \not\equiv \text{cube} \end{matrix}\right\} \pmod m \text{ and } \pmod n.$$

(The smallest examples are given by 307, 499. Cf. [2].) For the rest of the discussion, m and n are fixed. Suppose now that for integers s and t satisfying the conditions of Lemma 0, we have

$$\begin{aligned} s &\equiv 0 \pmod 7, \\ 18t^3 - s^3 &\equiv 0 \pmod m, \\ s^3 - 6t^3 &\equiv 0 \pmod n. \end{aligned} \tag{6}$$

Our purpose is to show that, with the further provision $d < -4$, the field $Q(\sqrt{d})$ has three independent ideal classes of order three.

The first step is to associate with each pair $[A, B]$ in (3) a prime l dividing A, such that

$$B \not\equiv \text{cube} \pmod l.$$

From this it follows, by Proposition 1, that the corresponding ideal lies in a class of order three. The relevant information is displayed in a table below.

Class f_A	Pair $[A, B]$	Prime l dividing A	$B \pmod l$
f_{xz}	$[xz, X+Z-W]$	7	$2(18t^4)^3$
f_{xw}	$[xw, X-Z+W]$	7	$-2(18t^4)^3$
f_{yz}	$[yz, Y+Z-W]$	m	$-7(18t^4)^3$
f_{yw}	$[yw, Y-Z+W]$	m	$7(18t^4)^3$
f_{zw}	$[zw, -X+Z+W]$	n	$21(6t^4)^3$

Taking the third line, for example, we have

$$y = s(18t^3 - s^3) \equiv 0 \pmod m,$$

so that m divides $yz = A$. Then

$$z = 18t^4, \quad w = 3t(s^3 - 6t^3) \equiv 36t^4 \pmod m,$$

so

$$Y+Z-W \equiv (18t^4)^3 - (36t^4)^3 \pmod m$$

or

$$B \equiv -7(18t^4)^3 \pmod m.$$

Now

$$(18t^4, 18t^3 - s^3) = 1,$$

by the conditions on s and t given in Lemma 0. Thus B is a non-zero residue of m. By the assumption on the cubic character of 7 involved in the choice of m, we conclude that B is a non-cubic residue.

Secondly, Proposition 3 is applied. We select for this the subgroup $\langle f_{xz}, f_{yz}, f_{zw} \rangle$, so that referring to the table,

$$l = 7, \quad l' = m, \quad l'' = n.$$

Then as

$$\begin{aligned} B &= X+Z-W, \\ B' &= Y+Z-W, \\ B'' &= -X+Z+W, \end{aligned}$$

we have (using (4) when necessary),

$$\frac{B+B'}{2} = 2Z \equiv 2(18t^4)^3 \pmod{m},$$

$$\frac{B+B''}{2} = Z \equiv (18t^4)^3 \pmod{n},$$

$$\frac{B'+B''}{2} = Y-W \equiv 6(12t^4)^3 \pmod{n}.$$

Since these are non-zero cubic residues of their respective moduli, it follows

$$\langle f_{xz}, f_{yz}, f_{xw} \rangle \cong \boldsymbol{C}(3) \times \boldsymbol{C}(3) \times \boldsymbol{C}(3).$$

(b) We consider next how the integers s and t may be taken, so that the various conditions needed for (a) (with the exception of $d < -4$) are fulfilled. In terms of the primes m and n introduced above, let integers m_0 and n_0 be chosen, for which (considering the cubic character of 2, 3)

$$m_0^3 \equiv 18 \pmod{m},$$

$$n_0^3 \equiv 6 \pmod{n}.$$

Further, choose k satisfying

$$7k \equiv \begin{cases} 1 \pmod 2, \\ m_0 \pmod m, \\ n_0 \pmod n. \end{cases}$$

This may be done, seeing the moduli are relatively prime in pairs and prime to 7. Finally, consider the solution in integers u, of the system

$$(7) \qquad \begin{aligned} u &\equiv 1 \pmod 2, \\ 2mnu &\equiv 1-k \pmod{3(7k-2)}. \end{aligned}$$

Concerning the second congruence, we have

$$(2mn, 3(7k-2)) = 1.$$

For as k is odd,

$$(2, 3(7k-2)) = 1.$$

This implies, incidentally, that the moduli in (7) are relatively prime. Then

$$(mn, 3) = 1,$$

while if

$$7k-2 \equiv 0 \pmod m,$$

we have by choice of k,

$$m_0 \equiv 2 \pmod m.$$

Cubing,

$$18 \equiv 8 \pmod m.$$

However, neither of 2, 5 is equal to m. The same argument shows we cannot have

$$7k-2 \equiv 0 \pmod n.$$

Thus the congruences (7) have solution for u, and in fact the solutions comprise an infinite set, which we denote by Σ.

LEMMA 1. *Suppose*

$$s = 7(2mnu+k), \qquad t = 7mnu+1,$$

where $u \in \Sigma$. *Then both* (6) *and the conditions of Lemma* 0 *are satisfied.*

Proof. We have

$$s \equiv 0 \pmod 7.$$

Then

$$s \equiv 7k \equiv m_0 \pmod m, \qquad t \equiv 1 \pmod m,$$

so

$$18t^3 - s^3 \equiv 0 \pmod m.$$

Similarly,

$$s^3 - 6t^3 \equiv 0 \pmod n.$$

This establishes (6). Next, since $u \equiv 1 \pmod 2$, we have

(i) $$(t, 2) = (7mnu+1, 2) = 2.$$

As $2mnu+k \equiv 1 \pmod 3$, it is clear

$$(s, 3) = 1.$$

And if the prime p divides (s, t), from $s-2t = 7k-2$ we derive

$$(s, 7k-2) \equiv 0 \pmod p$$

or

$$(7(2mnu+k), 7k-2) \equiv 0 \pmod p.$$

However,

$$2mnu+k \equiv 1 \pmod{7k-2} \quad \text{and} \quad (7, 7k-2) = 1.$$

This proves

(ii) $$(s, 3t) = 1.$$

Lastly, $s \equiv 0 \pmod 7$, $t \equiv 1 \pmod 7$ imply

(iii) $$(s+2^\alpha t, 7) = 1 \quad \text{for} \quad \alpha = 0, 1, 2.$$

4. The polynomial $D(s,t)$. Let x, y, z, w be as in (5). If we make use of (4), the common value of the five expressions B^2-4A^3 coming from the pairs $[A,B]$ in (3) may be shown to be

$$D(s,t) = (z^3-w^3)^2-(xy)^3.$$

$D(s,t)$ is homogeneous of degree 24 in s and t. Further,

$$D(s,t) \equiv s^{24} \pmod{3t}. \tag{8}$$

This gives the first assertion of

LEMMA 2. *$D(s,1)$ is monic in $\mathbf{Z}[s]$ and has no factor of the first or second degrees.*

Proof. If $s-a$ were a linear factor, by (8) we see

$$a \equiv 0 \pmod 3.$$

However,

$$D(a,1) = [18^3-3^3(a^3-6)^3]^2-a^{15}(18-a^3)^3 \geqslant a^{15}(a^3-18)^3,$$

which is positive unless $0 \leqslant a^3 < 18$. These two facts imply $a = 0$. But $D(0,1) \neq 0$.

Next, if s^2-bs-c were a quadratic factor, then

$$D(s,1) \equiv s^{24} \pmod 3,$$
$$D(s,1) \equiv 0 \pmod{s^2-bs-c},$$
$$s^2 \equiv bs+c \pmod{s^2-bs-c}.$$

Therefore with congruences modulo the ideal $(3, s^2-bs-c)$ in the ring $\mathbf{Z}[s]$, unless another modulus is indicated,

$$s^{24} \equiv 0, \tag{9}$$

$$s^2 \equiv bs+c. \tag{10}$$

If $b \equiv 0 \pmod 3$, (10) implies $s^3 \equiv c^4 \equiv c^2$ (seeing $c^3 \equiv c \pmod 3$), so that $s^{24} \equiv c^2$. Otherwise, $b^2 \equiv 1 \pmod 3$, as we now suppose. Cubing both sides in (10), $s^6 \equiv bs^3+c$. However,

$$s^3 \equiv b(bs+c)+cs \equiv (1+c)s+bc.$$

Thus

$$s^6 \equiv b(1+c)s-c.$$

Cubing again,

$$s^{18} \equiv b(1+c)s^3-c \equiv b(1+c)^2s+c^2.$$

Multiplying these, $s^{24} \equiv b(1-c^2)s+c^2$, which remains correct on setting $b \equiv 0 \pmod 3$. Using (9), we thus have for all values of b and c,

$$b(1-c^2)s+c^2 \equiv 0 \pmod{(3, s^2-bs-c)}.$$

Hence

$$b(1-c^2) \equiv 0 \equiv c^2 \pmod 3,$$

giving

$$b \equiv 0 \equiv c \pmod 3.$$

Set $b = 3b'$, $c = 3c'$ and $\sigma = b's+c'$. Then with congruences modulo $(3^{13}, s^2-bs-c)$ unless otherwise indicated, $s^2 \equiv 3\sigma$. From this we have

$$18^3+3^3(6-s^3)^3 \equiv 3^6[2^3+(2-s\sigma)^3],$$
$$s^5(18-s^3) \equiv 3^3s\sigma^2(6-s\sigma).$$

Hence

$$[18^3+3^3(6-s^3)^3]^2 \equiv 3^{12},$$
$$s^{15}(18-s^3)^3 \equiv 3^{10}s\sigma^7(-s\sigma)^3 \equiv -3^{12}\sigma^{12}.$$

Subtracting, $D(s,1) \equiv 3^{12}(1+\sigma^{12})$. But $\sigma^3 \equiv b's^3+c' \equiv c' \pmod 3$. Thus

$$\sigma^{12} \equiv c'^2 \pmod 3.$$

So finally, since $D(s,1) \equiv 0$, we obtain

$$3^{12}(1+c'^2) \equiv 0 \pmod{(3^{13}, s^2-bs-c)},$$

which means

$$3^{12}(1+c'^2) \equiv 0 \pmod{3^{13}}.$$

However, $1+c'^2 \equiv 0 \pmod 3$ is impossible for any integer c'. This completes the proof.

LEMMA 3. *Let*

$$D(s,1) = g(s)^2h(s)$$

be the factorization of $D(s,1)$ in $\mathbf{Z}[s]$, where $h(s)$ is square-free. Then $h(s)$ has at least three distinct (complex) roots.

Proof. The degree of $h(s)$ must be positive, since

$$D(2,1) = -2^8 \cdot 4799.$$

By the preceding lemma, any irreducible factor of $h(s)$ has degree at least three. Any three roots of this factor then furnish three distinct roots of $h(s)$.

Suppose now s and t are as in Lemma 1. Writing $v = mnu$ (where $u \in \Sigma$), this is to say

$$s = 7(2v+k), \quad t = 7v+1.$$

$D(s,t)$ becomes a polynomial in v and may be denoted by $D(v)$. Further, we write

$$D(v) = C(v)^2d(v),$$

with $d(v)$ a quadratic field discriminant. (This defines the function $d(v)$.)

LEMMA 4. *At least three roots of $D(v)$ occur with odd multiplicities.*

Proof. Let $Q_H[s, t]$ denote the homogeneous ring of forms in s and t with rational coefficients. There is a natural one-to-one correspondence $Q_H[s, t] \to Q[s]$ under which $t \to 1$. Analogously, we have the map $Q_H[v, w] \to Q[v]$ (where w is not to be confused with our earlier use of this symbol).

The substitution

$$\begin{bmatrix} s \\ t \end{bmatrix} = \begin{bmatrix} 14 & 7k \\ 7 & 1 \end{bmatrix} \begin{bmatrix} v \\ w \end{bmatrix}$$

has determinant $7(2-7k) \neq 0$, so gives an isomorphism between the homogeneous rings $Q_H[s, t]$, $Q_H[v, w]$. The composite map

$$Q[s] \to Q_H[s, t] \to Q_H[v, w] \to Q[v]$$

then provides a Q-isomorphism of the rings $Q[s]$, $Q[v]$, in which $D(s, 1)$ is carried to $D(v)$. We conclude that on factoring $D(v)$ in $Z[v]$, we obtain an expression whose square-free part has at least three distinct roots, this property of $D(s, 1)$ in $Z[s]$ being carried over from Lemma 3 by the isomorphism.

LEMMA 5. *For all sufficiently large $|v|$, $D(v)$ is negative. Further, the cardinality of the set $\{d(v) |\ v = mnu, u \in \Sigma\}$ is infinite.*

Proof. We have

$$s = 2.7v + O(1), \qquad t = 7v + O(1).$$

Recalling that $D(s, t)$ is homogeneous of degree 24, we infer

$$D(s, t) = D(2, 1) \cdot (7v)^{24} + O(|v|^{23}).$$

That is,

$$D(v) = -2^8 \cdot 4799\,(7v)^{24} + O(|v|^{23}).$$

This gives the first part. The second follows from the well-known result of Siegel [4], that for a polynomial $D(v)$ in $Z[v]$ satisfying the statement of Lemma 4, for each fixed integer d the equation

$$C^2 d = D(v)$$

has at most finitely many solutions in integers v, C.

5. Conclusion. (a) The theorem of the Introduction is obtained if we summarize our results. According to Section 3, for each $v = mnu$, $u \in \Sigma$, the field $Q(\sqrt{d(v)})$ has three independent classes of order three, provided $d(v) < -4$. On the other hand, as shown in Section 4, $d(v)$ is negative for all sufficiently large $|v|$, and unbounded as $|v|$ tends to infinity. Letting u tend to infinity in Σ, infinitely many distinct imaginary quadratic fields of the form $Q(\sqrt{d(mnu)})$ are obtained, each with three independent ideal classes of order three.

(b) A theorem of Scholz [3] states that if $d < 0$, then $Q(\sqrt{-3d})$ has either the same number of cyclic factors as $Q(\sqrt{d})$ or one less, when the 3-primary components of their class groups are compared. Using (a), the Corollary is obtained.

(c) Infinitely many imaginary quadratic fields also occur, for which the class group contains the more elaborate structure $C(3) \times C(3) \times C(3) \times C(3)$ (four factors). It follows that the Theorem above is true for real quadratic fields, as well as for imaginary. These matters will form the subject of a later article.

Acknowledgements. The author wishes to thank Professor D. Lewis and Dr. P. Weinberger for their help and suggestions.

References

[1] L. J. Mordell, *Diophantine Equations*, Pure and Applied Mathematics Series, Volume 30, Academic Press, 1969.

[2] T. Nagell, *Sur quelques problèmes dans la théorie des restes quadratiques et cubiques*, Arkiv för Mat. 3 (1956), pp. 211–222.

[3] A. Scholz, *Über die Beziehung der Klassenzahlen quadratischer Körper zueinander*, Crelle's Journal 166 (1932), pp. 201–203.

[4] C. L. Siegel, *Über einige Anwendungen Diophantischer Approximationen*, Gesammelte Abhandlungen, Band I, pp. 209–266.

[5] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka Journ. Math. 7 (1970), pp. 57–76.

THE UNIVERSITY OF MICHIGAN

Received on 1. 3. 1972