ACTA ARITHMETICA
XXI (1972)

A quadratic field of prime discriminant requiring three generators for its class group, and related theory

by

DANIEL SHANKS (Washington, D. C.) and
PETER WEINBERGER (Ann Arbor, Mich.)

Introduction. The quadratic field of the title is $Q(\sqrt{p})$ for the prime

$$p = 3^6 + 4 \cdot 19^6 = 188184253. \tag{1}$$

It has class number 27: $h(p) = 27$, and its class group is a product of 3 groups of order 3: $C(3) \times C(3) \times C(3)$. This field is of interest for its implications concerning two conjectures.

Šaferevič [13] raised the question whether there is a bound for the number of generators of the class group that is valid for all quadratic fields $Q(\sqrt{\pm p})$ of prime discriminant. If the discriminant of a quadratic field has sufficiently many divisors, he found that its class field tower is infinite, and it follows that almost all quadratic fields have an infinite tower. Now suppose the discriminant is prime. If the class group requires sufficiently many generators, then the tower is, once again, infinite.

But, as well-studied as quadratic fields are, no $Q(\sqrt{\pm p})$ has heretofore been discovered that required more than two generators, and even these latter prime discriminants are quite rare. To name several, cf. [5], [10], [11]: $Q(\sqrt{32009})$ and $Q(\sqrt{-4027})$ have the group $C(3) \times C(3)$ while $Q(\sqrt{-12451})$ and $Q(\sqrt{-37363})$ have the group $C(5) \times C(5)$. Several investigators conjectured (verbally, cf. [14]) that not only is the answer to Šaferevič's question "yes", but, in fact, that the bound in question is 2. By (1), we now know that this is false.

A second (opposite) conjecture, cf. [6], states that every finite Abelian group occurs as the class group for some quadratic field. For example, there are 40 distinct Abelian groups of order < 27, and, for each of them, at least one imaginary quadratic field is known to have this group as its class group. But the conjecture is nonetheless known to be false if one confines oneself to imaginary fields. Chowla [2] proved that there are

a limited number of imaginary fields having one class per genus and that implies that, for all $n >$ some n_0, each group

$$C(2) \times C(2) \times \ldots \times C(2) \quad (n \text{ factors})$$

must be missing. It is probable, in fact, that the group

$$C(2) \times C(2) \times C(2) \times C(2) \times C(2),$$

with class number 32, is already so missing; i.e., it is probable that $n_0 = 4$.

What is the smallest Abelian group that does not occur for imaginary fields? That is unknown, but probably it is

$$C(3) \times C(3) \times C(3). \tag{2}$$

Up to $\Delta = 103387$, all cases of class number 27, $h(-\Delta) = 27$, either have the group $C(27)$, or the group $C(3) \times C(9)$. It is very likely that $\Delta = 103387$ is the largest Δ such that $h(-\Delta) = 27$; there are no other examples [3] for $\Delta < 465072$, and any sufficiently large example would imply a violation of the generalized Riemann hypothesis. Therefore, if every Abelian group nonetheless occurs for some quadratic field, it follows that we must have a real field for (2), and, with (1), we now do.

We discuss below our reasons for investigating the primes

$$p(A, B) = A^6 + 4B^6, \tag{3}$$

and the quadratic fields

$$Q\left(\sqrt{p(A, B)}\right) \quad \text{and} \quad Q\left(\sqrt{-3p(A, B)}\right), \tag{4}$$

and we give the results of these investigations. The case (1) is $p(3, 19)$, and besides the already-mentioned fact:

$$Q\left(\sqrt{p(3, 19)}\right) \text{ has a group } C(3) \times C(3) \times C(3),$$

we can add that

$$Q\left(\sqrt{-3p(3, 19)}\right) \text{ has a group } C(3) \times C(3) \times C(3) \times C(604).$$

Similarly,

$$Q\left(\sqrt{p(29, 18)}\right) \text{ has a group } C(3) \times C(3),$$

and

$$Q\left(\sqrt{-3p(29, 18)}\right) \text{ has a group } C(3) \times C(3) \times C(3) \times C(464).$$

In Section 3, we give a table of such $p(A, B)$ together with the class groups of both fields (4), and in this table one readily notices consistent patterns in their class numbers, $h(p)$ and $h(-3p)$, and class groups. We then prove that these observations remain true for all primes $p(A, B)$ and even for all square-free discriminants:

$$\Delta(A, B) = A^6 + 4B^6. \tag{5}$$

Excluding $p(1, 1) = 5$, we prove that $3 | h(\Delta)$ in Theorem 3 and $3 | h(-3\Delta)$ in Theorem 1. Surprisingly, the implied element of order 3

in the latter theorem can be given explicitly in a completely elementary way. One notes that whenever $3 \nmid B$, as in $p(3, 19)$ above, the two 3-Sylow subgroups involved have an equal number of factors, and this is proven in Theorem 2. But, when $3 | B$, as in $p(29, 18)$, the corresponding subgroup for the imaginary field has precisely one extra factor than that for the real field. This is proven in Theorem 4.

One also notes that $8 | h(-3p)$ if and only if $3 | B$, and this is proven in Theorem 5. We deduce this Theorem 5 from a more general result that gives an analogue to a recent theorem of Barrucand and Cohn [1]. In effect, they showed

THEOREM BC. *For primes $p = 8k+1$, these three conditions are equivalent*:

(a) $$p = a^2 + 32b^2,$$

(b) $$\left(\frac{-4}{p}\right)_8 = +1,$$

(c) $$8 | h(-4p).$$

We proved

THEOREM A. *For primes $p = 12k+1$, these three conditions are equivalent*:

(a) $$p = a^2 + 36b^2,$$

(b) $$\left(\frac{-3}{p}\right)_4 = +1,$$

(c) $$8 | h(-3p).$$

Subsequently, we learned that a special case of Rédei's Theorem II [7] implies most of Theorem A, and so we omit most of our own proof.

Finally, for those interested, we give in an appendix further detail concerning $Q\left(\sqrt{p(3, 19)}\right)$, such as its fundamental unit, a list of equivalence classes and their multiplication table. Corresponding data, and some discussion, is included for other fields of interest such as $Q\left(\sqrt{-3\Delta(17, 9)}\right)$ which has the remarkable class group:

$$C(3) \times C(3) \times C(81) \times C(2) \times C(2) \times C(2).$$

2. The plan of the search. The class group of $Q(\sqrt{d})$ is the group of ideal classes under ideal multiplication. More elementary is Gauss's original version: it is the group of equivalence classes of primitive binary quadratic forms of discriminant d under composition. If p^a is the largest power of p dividing the class number, the corresponding subgroup is the p-Sylow subgroup. We wished to find quadratic fields whose 3-Sylow subgroups contain at least 3 factors.

Our plan for this search combined a technique for finding numerous real fields having at least 2 factors with a use of Scholz's theorem [9]. A version of this can read

SCHOLZ'S THEOREM. *For square-free d satisfying $d > 0$, $3 \nmid d$, the two quadratic fields*

$$Q(\sqrt{d}) \quad \text{and} \quad Q(\sqrt{-3d})$$

have class groups whose 3-Sylow subgroups are related. If, for the imaginary field, this subgroup is a product of r cyclic groups $C(3^{\alpha_i})$, and if, for the real field, this subgroup is a product of s cyclic groups $C(3^{\beta_i})$, then

$$r = s \text{ or } s+1.$$

The class group for the imaginary fields can be readily computed by a new technique [12], and, given sufficiently promising candidates, one can now easily test them for

$$r \geqslant 3$$

(in Scholz's notation). The sufficiently promising candidates are the

$$Q(\sqrt{-3p(A,B)})$$

since the real fields

$$Q(\sqrt{p(A,B)})$$

have a strong tendency towards satisfying

$$s \geqslant 2$$

(in Scholz's notation).

The reason [11] for this asserted tendency is that for the discriminant

$$p(A,B) = A^6 + 4B^6$$

there is a quadratic form

$$F(u,v) = B^3u^2 + A^3uv - B^3v^2 \tag{6}$$

which represents both B^3 (by $u=1$, $v=0$) and A^3 (by $u=1$, $v=1$). This form:

$$F = (B^3, A^3, -B^3), \tag{7}$$

is equivalent to

$$(-B^3, -A^3, B^3),$$

and so, by composition, F^2 represents -1. Therefore,

$$F^4 = I, \tag{8}$$

the principal form, and F is of order 1, 2, or 4. But $Q(\sqrt{p})$ has an odd class number since p is prime. Therefore,

$$F = I, \tag{9}$$

and I, the principal form, represents both A^3 and B^3. That "encourages", but does not force, two forms that represent A and B:

$$F_1 = (A, B_1, C_1), \quad F_2 = (B, B_2, C_2) \tag{10}$$

to both be of order 3, and, possibly, independent.

The following impressive fact illustrates both the efficacy of the foregoing construction, and its necessity. The first 5000 primes $P \equiv 1 \pmod 4$ are $5, 13, \ldots, 105269$. *All but two* of the corresponding real fields $Q(\sqrt{P})$ have cyclic groups. The two exceptions are $32009 = p(5,4)$, found by Shanks [11], and $62501 = p(1,5)$ found much earlier by Schaffstein [8]. These two fields have the group $C(3) \times C(3)$ with $s = 2$.

3. The results of the search. In Tables 1 and 2 we list all $p(A,B)$ having $A, B \leqslant 30$ together with the class groups of the fields (4). Table 1 lists those having $3 \mid B$. Table 2 lists those with $3 \nmid B$ except that we omit 35 cases having $r = s = 1$ since they are of lesser interest. We show each 3-Sylow subgroup and its cofactor. For example, $Q(\sqrt{-3p(9,17)})$ in Table 2 has the (unusual) group

$$C(9) \times C(9) \times C(172).$$

We should add that the cofactor is cyclic in every case listed even if, e.g., see $p(19,20)$, the $C(550)$ shown has an order that is not square-free.

As was indicated, one readily observes patterns here concerning

$$3 \mid h, \quad 8 \mid h, \quad r = s \text{ or } s+1.$$

We give the theory in the following sections but first some remarks about the exceptional $p(3,19)$ of the title.

That $Q(\sqrt{p(3,19)})$ contains $C(3) \times C(3) \times C(3)$ may be verified without excessive computation. The principal reduced binary quadratic

Table 1, $3 \mid B$

A	B	$Q(\sqrt{p(A,B)})$	$Q(\sqrt{-3p(A,B)})$
1	3	3	$3 \times 3 \times 8$
5	3	3	$3 \times 3 \times 16$
5	12	3	$3 \times 3 \times 136$
19	3	3×5	$3 \times 3 \times 1072$
17	15	3	$3 \times 3 \times 808$
23	6	3	$3 \times 3 \times 568$
25	6	3	$9 \times 3 \times 152$
13	21	3×7	$9 \times 3 \times 1360$
17	21	3×5	$9 \times 3 \times 1280$
25	18	3	$3 \times 3 \times 608$
5	24	3×7	$3 \times 3 \times 680$
11	27	9	$27 \times 3 \times 616$
25	27	3	$27 \times 3 \times 352$
29	27	3	$3 \times 3 \times 5408$
1	30	27×239	$9 \times 3 \times 608$
13	30	9	$3 \times 3 \times 1856$
17	30	3	$3 \times 3 \times 1816$
19	30	3	$3 \times 3 \times 1760$
29	18	3×3	$3 \times 3 \times 3 \times 464$

Table 2, $3 \nmid B$

A	B	$Q(\sqrt{p(A,B)})$	$Q(\sqrt{-3p(A,B)})$
1	1	1	2
1	2	3	3×2
19	28	9×5	9×2666
5	4	3×3	$9\times 3\times 2$
1	5	3×3	$3\times 3\times 26$
5	7	3×3	$3\times 3\times 70$
5	8	9×3	$3\times 3\times 34$
9	10	$3\times 3\times 7$	$3\times 3\times 76$
13	10	3×3	$3\times 3\times 106$
5	13	3×3	$3\times 3\times 362$
17	1	$3\times 3\times 13$	$9\times 3\times 170$
3	16	3×3	$3\times 3\times 316$
21	10	9×3	$27\times 3\times 44$
17	16	3×3	$9\times 3\times 134$
9	17	$9\times 3\times 5$	$9\times 9\times 172$
23	10	3×3	$3\times 3\times 374$
21	17	3×3	$9\times 3\times 932$
25	2	3×3	$3\times 3\times 694$
25	8	9×3	$3\times 3\times 422$
25	11	3×3	$9\times 3\times 410$
1	20	$81\times 3\times 7$	$3\times 3\times 506$
7	20	3×3	$9\times 3\times 254$
19	20	3×3	$3\times 3\times 550$
23	19	9×3	$3\times 3\times 2542$
25	17	9×3	$3\times 3\times 1582$
27	10	9×3	$9\times 3\times 140$
27	14	3×3	$81\times 3\times 44$
27	19	9×3	$9\times 3\times 1484$
9	23	3×3	$3\times 3\times 3220$
11	23	$3\times 3\times 11$	$9\times 3\times 1274$
29	8	9×3	$3\times 3\times 866$
29	17	3×3	$3\times 3\times 3706$
13	25	3×3	$27\times 3\times 334$
29	22	3×3	$3\times 3\times 1366$
1	28	$3\times 3\times 355$	$27\times 3\times 314$
25	28	9×3	$9\times 3\times 554$
3	29	3×3	$9\times 3\times 2044$
15	29	3×3	$3\times 3\times 3740$
3	19	$3\times 3\times 3$	$3\times 3\times 3\times 604$

* 35 examples of $r = s = 1$ omitted here.

form having this discriminant is

$$(1, 13717, -7041),$$

and its *period* of reduced forms continues as

$$(-7041, 365, 6677), \quad (6677, 12989, -729), \text{ etc.}$$

until one reaches its midpoint at

$$(19^3, 3^3, -19^3)$$

as in equation (7). *En route*, one encounters

$$(17^3, 12729, -11^3) \quad \text{and} \quad (-3^3, 13691, 6859)$$

so the principal form represents

$$3^3, \ 11^3, \text{ and } 17^3.$$

On the other hand,

$$\pm 3, \ \pm 11, \ \pm 17$$

do not occur as end coefficients and the forms

$$\begin{aligned} J &= (3, 13717, -2347), \\ K &= (11, 13715, -1887), \\ L &= (17, 13715, -1221) \end{aligned} \tag{11}$$

are therefore all of order 3.

But, one also finds that

$$\pm 33, \ \pm 51, \ \pm 187$$

do not occur as end coefficients, so none of the forms (11) is either equivalent or conjugate to any other. Finally, ± 561 does not occur so L is not equivalent to any product generated by J and K. Therefore, each form (11) is an independent generator of order 3, and $C(3)\times C(3)\times C(3)$ is contained in the class group. Further computation shows that 27 is the class number and therefore $C(3)\times C(3)\times C(3)$ is the whole group, as was stated.

That $Q(\sqrt{-3p(3,19)})$ also contains $C(3)\times C(3)\times C(3)$ is easier to verify. The reduced forms

$$\begin{aligned} J &= (1110, 81, 127153), \\ K &= (1812, 1509, 78205), \\ L &= (2082, 411, 67810) \end{aligned} \tag{12}$$

may be seen to satisfy $J^2 = J^{-1}$, $K^2 = K^{-1}$, $L^2 = L^{-1}$ by squaring them using composition. As before, their products under composition constitute the 27 cube-roots of the identity:

$$I = (1, 1, 141138190). \tag{13}$$

In the Appendix, we give further details concerning these two fields for those interested. We also give this data for the previously-mentioned $p(29, 18)$ and for a smaller, composite discriminant

$$\Delta(17, 9) = 101 \cdot 457 \cdot 569$$

that also has $s = 2$, and therefore $r = 3$.

As an example of Theorem 1 we shall see that the form J of (12) could have been easily computed a priori from $A = 3$, $B = 19$.

4. The elementary, explicit cube roots. The generalization of this J is given in

THEOREM 1. *For natural numbers A, B, a square-free $\Delta = A^6 + 4B^6$, and a discriminant $-3\Delta < -15$, the quadratic form*

$$J = (3[A^2+B^2], 3A^3, A^4 - A^2B^2 + B^4) \tag{14}$$

is a primitive form of order 3. Thus, $3 \mid h(-3\Delta)$ and $r \geqslant 1$.

Proof. Since Δ is square-free, $(A, 2B) = 1$ and J is primitive. Now J may be factored as $J = GH$, where

$$G = (A^2+B^2, 3A^3, 3[A^4 - A^2B^2 + B^4]), \quad H = (3, 3, [3+\Delta]/4).$$

Then $J^2 \sim G^2$ since H is ambiguous: $H^2 \sim I = (1, 1, [3\Delta+1]/4)$. But

$$G \sim (A^2+B^2, 3A^3 - 6A[A^2+B^2], 3[A^2+B^2]^2), \tag{14a}$$

and so, by composition,

$$\begin{aligned} G^2 &\sim ([A^2+B^2]^2, 3A^3 - 6A[A^2+B^2], 3[A^2+B^2]) \\ &\sim (3[A^2+B^2], -3A^3 + 6A[A^2+B^2], [A^2+B^2]^3) \\ &\sim (3[A^2+B^2], -3A^3, A^4 - A^2B^2 + B^4) = J^{-1}. \end{aligned}$$

Therefore, $J^3 \sim I$ and the theorem follows if we can exclude $J \sim I$.

For the excluded case $A = B = 1$, $\Delta = 5$, we do, indeed, have $J = (6, 3, 1) \sim (1, 1, 4) = I$. But, from (14), if

$$(3[A^2+B^2])^2 < 3\Delta/4, \tag{15}$$

then either J is already a reduced form, or, when it is reduced, the left coefficient $3[A^2+B^2]$ remains unchanged. Then $J \nsim I$ since $3[A^2+B^2] \neq 1$. Assume $A < B$. Then (15) holds if

$$(3[A^2+B^2])^2 < 36B^4 \leqslant 3B^6 < 3\Delta/4$$

or $B > 3$. But (15) also holds if $B = 3$. And if $B = 2$, $A = 1$,

$$J = (15, 3, 13) \sim (13, -3, 15) \nsim I.$$

Assume $A > B$. Then (15) holds if $48A^4 \leqslant A^6$ or $A > 6$. One may verify that (15) holds if $A = 5$ also. Finally, if $A = 3$, $B = 1$,

$$J = (30, 81, 73) \sim (22, -21, 30) \nsim I,$$

while if $A = 3$, $B = 2$,

$$J = (39, 81, 61) \sim (19, -3, 39) \nsim I,$$

which completes the proof.

5. The real fields $Q(\sqrt{\Delta})$. Let A, B, Δ be as before, and let ε be the fundamental unit of K, the ring of integers of $Q(\sqrt{\Delta})$. Scholz [9] gives the following criterion for his theorem:

One has $r = s+1$ if, and only if, ε, and all integers γ that are cubes of ideals $\mathfrak{c}$ in the ring of integers of $Q(\sqrt{d})$:

$$(\gamma) = \mathfrak{c}^3,$$

are cubic residues modulo 9.

Define two ideals of K:

$$\mathfrak{a} = (A, \delta_1 - \gamma), \quad \mathfrak{b} = (B, \delta_2), \tag{16}$$

where

$$\delta_1 = 2B^3 + \sqrt{\Delta}, \quad \delta_2 = (A^3 + \sqrt{\Delta})/2, \quad \gamma = (2B^3 + A^3 + \sqrt{\Delta})/2, \tag{17}$$

and where (α, β) means that α and β are a Z-basis for the ideal. Then their product

$$\mathfrak{c} = \mathfrak{a}\mathfrak{b} \tag{18}$$

is given by

$$\mathfrak{c} = (AB, \gamma) \tag{19}$$

and one may verify that $\mathfrak{c}^3$, $\mathfrak{a}^6$, and $\mathfrak{b}^6$ are all principal ideals:

$$\mathfrak{c}^3 = (\gamma), \quad \mathfrak{a}^6 = (\delta_1), \quad \mathfrak{b}^6 = (\delta_2). \tag{20}$$

We need the cubic residues (mod 9) in the three cases that occur. They are

$3 \mid B$, $\Delta \equiv 1 \pmod 9$: $0, \pm 1, \pm\sqrt{\Delta}, \pm 4 \pm 4\sqrt{\Delta}$.

$3 \mid \Delta$, $\Delta \equiv 4 \pmod 9$: $0, \pm 1, \pm 4\sqrt{\Delta}, \pm 4 \pm 2\sqrt{\Delta}$.

$3 \nmid AB$, $\Delta \equiv 5 \pmod 9$: $0, \pm 1, \pm 4\sqrt{\Delta}, \pm 2 \pm \sqrt{\Delta}$.

Thus, γ is a cubic residue (mod 9) if, and only if, $3 \mid B$. Therefore, we have

THEOREM 2. *If $3 \nmid B$, $r = s$.*

Proof. This follows at once from (20) and Scholz's criterion.

A number α of K is called primary if $\alpha > 0$ and

$$1 \leqslant |\alpha/\bar{\alpha}| < \varepsilon^2. \tag{21}$$

Every principal ideal of K is generated by a unique primary number, and, for (20) in particular, we record

LEMMA 1.

1. *γ is primary if $AB \neq 1$.*
2. *δ_1 is primary if $A \neq 1$.*
3. *δ_2 is primary if $B \neq 1$.*

Proof. We may rewrite (21) as

$$1 \leqslant a/|N(a)|^{1/2} < \varepsilon.$$

The lemma then follows from the inequalities:

$$A^3,\ 2B^3 < \sqrt{\Delta} < 2\varepsilon.$$

LEMMA 2. *If $AB \neq 1$, $(m+n\sqrt{\Delta})/2$ is not a cube in K for $n = 1$ or 2.*

Proof. If $(m+n\sqrt{\Delta})/2 = [(r+s\sqrt{\Delta})/2]^3$, one has

$$s\left(3r^2+s^2(A^6+4B^6)\right) = 4n$$

which has no solution for $n = 1$ and only $s = r^2 = A = B = 1$ for $n = 2$.

THEOREM 3. *For $\Delta > 5$, at least one of $\mathfrak{a}^2$ and $\mathfrak{b}^2$ is not principal in K and therefore is of order 3. Thus, $3 \mid h(\Delta)$ and $s \geqslant 1$.*

Proof. Assume the contrary:

$$\mathfrak{a}^2 = (a), \quad \mathfrak{b}^2 = (\beta), \tag{22}$$

with a and β primary. Since $\mathfrak{c}^3 = \mathfrak{a}^3\mathfrak{b}^3$ is principal, then so is $\mathfrak{c}$:

$$\mathfrak{c} = (\sigma) \tag{23}$$

for some primary σ. Then, from (20),

$$a^3 = \delta_1\varepsilon^i, \quad \beta^3 = \delta_2\varepsilon^j, \quad \sigma^3 = \gamma\varepsilon^k \tag{24}$$

for certain exponents i, j, k. But we also have

$$\sigma^2 = a\beta\varepsilon^m \tag{25}$$

from (18), and therefore must have

$$2k = i+j+3m. \tag{26}$$

Since $\Delta > 5$, γ is primary, and so $k = 1$ or 2 from (24) and Lemma 2.

Let us first dispose of the case $A = 1$ and the case $B = 1$. If $A = 1$,

$$a = 1, \quad \varepsilon = \delta_1, \quad i = -1,$$

and $j = 1$ or 2 since δ_2 is primary. If $B = 1$,

$$\beta = 1, \quad \varepsilon = \delta_2, \quad j = -1,$$

and $i = 1$ or 2 since δ_1 is primary. In either case, $m = 0$ or 1 and thus, from (26), we must have $k = 2$. Therefore,

$$(\sigma/\varepsilon)^3 = \gamma/\varepsilon \tag{27}$$

from (24). The two cases now require

$$(\sigma/\varepsilon)^3 = (1-2B^3+\sqrt{\Delta})/2 \text{ or } (2-A^3+\sqrt{\Delta})/2,$$

respectively. Both cases are thus excluded by Lemma 2.

In the main case, $A, B > 1$, both δ_1 and δ_2 are primary. Therefore, both i and j are 1 or 2, while $m = -1$, 0, or 1. The only solution of (26) is

$$m = 0, \quad i = j,$$

and it follows from (24) that

$$a^3\delta_2 = \beta^3\delta_1.$$

Multiplying both sides by $-\bar{\delta}_2$ gives

$$(B^2a/\beta)^3 = (\sqrt{\Delta}-A^3)(2B^3+\sqrt{\Delta})/2.$$

Since B^2a/β is an integer, say, $(u+v\sqrt{\Delta})/2$, we must have

$$v\left(3u^2+v^2(A^6+4B^6)\right) = 4A^3-8B^3$$

which is impossible if $v = 0$; and also if $v \neq 0$ since $A, B > 1$. That completes the proof.

This Theorem 3, and similarly, Theorem 1 above, can be generalized but this is of little interest for our present purpose. It is not necessary that Δ be square-free. It suffices if $(A, B) = 1$ and K is the *order* of $Q(\sqrt{\Delta})$.

Note that unlike Theorem 1, and its unequivocal form (14), here we can only point to the two forms corresponding to the two ideals $\mathfrak{a}^2$ and $\mathfrak{b}^2$:

$$(-A^2, 2B^3-A^3, AB^3), \quad (-B^2, A^3, B^4),$$

and assert that at least one of them is of order 3. The other may be equivalent to the principal form. In effect, we now return to this unequivocal form (14) to settle the escalatory case: $r = s+1$.

6. The escalatory case. Scholz [9] gives a second, complementary criterion for his theorem. Consider square-free $d > 0$ as before, and, for our present purpose, assume $d \equiv 1 \pmod 3$. The biquadratic field $P = Q(\sqrt{d}, \sqrt{-3d})$ has quadratic subfields $Q(\sqrt{-3}), Q(\sqrt{d}), Q(\sqrt{-3d})$, and, in this P, we may factor the principal ideal (3):

$$(3) = \mathfrak{p}^2\bar{\mathfrak{p}}^2 \tag{28}$$

into certain prime ideals $\mathfrak{p}$ and their conjugates $\bar{\mathfrak{p}}$. The criterion referred to is this:

One has $r = s$ if and only if all integers ω that are cubes of integral ideals $\mathfrak{c}$ of $Q(\sqrt{-3d})$:

$$(\omega) = \mathfrak{c}^3$$

are cubic residues modulo $\mathfrak{p}^3$.

LEMMA 3. *In P, if $d \equiv 1 \pmod 9$, all cubic residues $\pmod{p^3}$ are $\equiv 0, 1,$ or -1.*

Proof. Since $9 \equiv 0 \pmod{p^3}$, one has

$$d \equiv 1 \quad \text{and} \quad \sqrt{d} \equiv 1 \text{ or } -1 \pmod{p^3}. \tag{29}$$

Next, since $(\sqrt{-3}) = p\bar{p}$, $\sqrt{-3} \equiv 0 \pmod p$, and so

$$3\sqrt{-3} \equiv 3\sqrt{-3d} \equiv 9 \equiv 0 \pmod{p^3}. \tag{30}$$

Let α be an integer of P. Then

$$\alpha \equiv u + v\sqrt{d} + w\sqrt{-3} + x\sqrt{-3d} \pmod{p^3}$$

for rational integers u, v, w, x. Therefore, by (29) and (30),

$$\alpha^3 \equiv (u+v)^3 \text{ or } (u-v)^3 \pmod{p^3}. \tag{31}$$

Reduction of (31) modulo 9 proves the lemma.

THEOREM 4. *For square-free $d = \Delta(A, B) = A^6 + 4B^6$, and $3 \mid B$, $r = s+1$.*

Proof. From (14a) we obtain

$$3(A^2+B^2)^3 = N\left([-3A(A^2+2B^2)+\sqrt{-3\Delta}]/2\right),$$

and, squaring this,

$$(A^2+B^2)^6 = N(\omega) \tag{32}$$

with

$$\omega = [A^6 + 6A^4B^2 + 6A^2B^4 - 2B^6 - A(A^2+2B^2)\sqrt{-3\Delta}]/2. \tag{33}$$

Therefore, there is an integral ideal $\mathfrak{g}^2$ of $Q(\sqrt{-3\Delta})$ whose cube is principal: $\mathfrak{g}^6 = (\omega)$. If $3 \mid B$, and therefore $A \equiv \pm 1 \pmod 3$, $\Delta \equiv 1 \pmod 9$, one has

$$\omega \equiv [1 \pm \sqrt{-3}]/2 \equiv 5 \pm 5\sqrt{-3} \pmod{p^3}, \tag{34}$$

and, since ω is not a cubic residue $\pmod{p^3}$, by Lemma 3, we conclude that $r = s+1$ from Scholz's criterion.

It may be useful to add that the more general condition $d \equiv 1 \pmod 9$ does not suffice for $r = s+1$. For example, for $d = 2089$, one has $h(d) = 3$, $h(-3d) = 12$, and therefore $r = s = 1$. In contrast with (34), here we find

$$43^3 = N(152 + 3\sqrt{-3d}) \quad \text{and} \quad 152 + 3\sqrt{-3d} \equiv -1 \pmod{p^3}.$$

7. Analogue of a recent theorem. Returning to discriminants $-3p(A, B)$ with p prime, one easily finds that

$$h(-3p(A,B)) \equiv 0 \text{ or } 2 \pmod 4 \tag{35}$$

according as $3 \mid AB$ or not. This is because the ambiguous form $H = (3, 3, [3+p]/4)$ of Theorem 1 is in the principal genus or not according as $(3/p) = +1$ or -1. Thus, H is a square, and $4 \mid h(-3p)$, if and only if $3 \mid AB$ and thereby $p \equiv 1 \pmod 3$.

The distinction between $3 \mid A$ and $3 \mid B$ is more subtle. We found

THEOREM 5. *If, and only if $3 \mid B$, $8 \mid h(-3p(A,B))$. The subgroup of order 8 involved is cyclic.*

Proof. We prove this by using our Theorem A.

We have already shown that $4 \mid h(-3p(A,B))$ if and only if $3 \mid AB$. If $3 \mid AB$, $p(A,B) = 12k+1$ and Theorem A applies. Thus, $8 \mid h$ if and only if $p(A,B)$ is of the form a^2+36b^2. This condition holds for $p = A^6+4B^6$ if $3 \mid B$, and does not hold if $3 \mid A$ since $p(A,B)$ has a unique decomposition as a sum of two squares. That the subgroup of order 8 is cyclic is clear since the only reduced ambiguous form besides the identity is $H = (3, 3, [3+p]/4)$.

Now, in Theorem A, the equivalence of (a) and (b) is easy to prove. By the method, say, in Emma Lehmer [4], one shows that -3 is a quartic residue of $p = 12k+1$ if and only if $p = a^2+36b^2$. One could complete Theorem A either by proving (a) and (c) equivalent, or (b) and (c) equivalent. We did the former by analogy with the Barrucand–Cohn Theorem BC [1] mentioned in the introduction. Essentially, one shows that the $H = (3, 3, [3+p]/4)$ above is not only a square, but also a fourth power, if and only if (a) holds. We used the field $Q(\sqrt[6]{-1})$ instead of the $Q(\sqrt[4]{-1})$ used in [1].

We omit this proof since subsequently we learned that a special case of Rédei's Theorem II [7] implies the equivalence of (b) and (c). If one adds the equivalence of (a) and (b) mentioned above, that suffices to complete Theorem A, and thereby Theorem 5 also.

We may now utilize almost the entire theory by combining Theorems 3, 4, and 5 into the

COROLLARY. *For primes $p = A^6+4B^6$ and $3 \mid B$, one has*

$$72 \mid h(-3p).$$

More specifically,

$$C(8) \times C(3) \times C(3)$$

is a subgroup of the class group of $Q(\sqrt{-3p})$.

The smallest example is $Q(\sqrt{-3p(1,3)})$, and we observe in Table 1 that we have accounted for its entire structure.

8. Acknowledgments. We are pleased to make the following acknowledgments: To Professors D. H. and Emma Lehmer, for assistance

in computing the $h(-3p)$ and for helpful discussion of the Barrucand–Cohn and Rédei theorems; to Professor Robert Gold for helpful discussion of the Scholz theorem; and to Richard Serafin for programming and other computer work upon which Tables 1 and 2 are based.

Appendix. Here are further data on $Q(\sqrt{-3p(3,19)})$. The products of the three generators J, K, L in (12) are

$$\begin{aligned} JK &= (3211, 3065, 44686),\\ J^2K &= (4822, 3363, 29856),\\ J^2L^2 &= (3316, 2957, 43222),\\ J^2L &= (5095, 2681, 28054),\\ KL &= (6780, 5301, 28153),\\ KL^2 &= (9705, 8871, 16570),\\ JK^2L^2 &= (8362, 1931, 16990),\\ J^2KL^2 &= (3154, 25, 44749),\\ J^2K^2L &= (6033, 5349, 24580),\\ JKL &= (2110, 399, 66909). \end{aligned} \tag{36}$$

The 13 reduced forms (12) and (36), the 13 inverses:

$$J^2 = (1110, -81, 127153),$$

etc., and the identity (13) constitute the 27 cube-roots of the identity.

Similarly, for $Q(\sqrt{p(3,19)})$, one has the products of the J, K, L in (11):

$$\begin{aligned} JK &= (13, 13709, -4761),\\ J^2K &= (23, 13709, -2691),\\ JL &= (29, 13699, -4497),\\ J^2L &= (349, 13377, -6619),\\ KL &= (19, 13691, -9747),\\ K^2L &= (293, 13585, -3099),\\ JK^2L^2 &= (37, 13715, -561),\\ J^2KL^2 &= (557, 12677, -12333),\\ JKL^2 &= (103, 13663, -3657),\\ J^2K^2L^2 &= (89, 13589, -9897). \end{aligned} \tag{37}$$

In (37), as in (11), we have represented each equivalence class by that reduced form which has as its left coefficient the smallest prime represented by this class.

The fundamental unit ε of this real field is rather large. It is

$$\tfrac{1}{2}(T + U\sqrt{p})$$

where

$$\begin{aligned} T &= 1375789524*(92)*2925998389,\\ U &= 1002906297*(88)*1417062305 \end{aligned} \tag{38}$$

in which $*(N)*$ means that N digits are omitted. Since T and U are odd, that implies that the primitive forms of discriminant $4p$ (or, of what Gauss calls the *determinant* p), also have $h(4p) = 27$ and the same structure. These numbers T and U were computed by a new, abbreviated method that allows us to write (38) even if we do not know the missing $*(N)*$ digits. In fact, these missing digits are of little use since the high-order digits suffice for evaluating the regulator and $L(1, \chi)$ accurately, while the values of T and U (mod n) suffice for other theoretical purposes. Thus, above, with $n = 2$, we determined $h(4p)$. We may explain this new method elsewhere.

For $Q(\sqrt{-3p(29,18)})$ we have the $r = 3$ generators

$$\begin{aligned} J &= (3495, 3267, 157603),\\ K &= (2613, 2577, 210415),\\ L &= (4141, 207, 132375), \end{aligned} \tag{39}$$

and for $Q(\sqrt{p(29,18)})$ we have $s = 2$ and can obtain the 9 cube-roots from

$$\begin{aligned} J &= (29, 26993, -19398),\\ K &= (18, 27017, -13249). \end{aligned} \tag{40}$$

We omit these products and those of (39) for brevity. They are easy enough to compute by composition. The ε for this $Q(\sqrt{p(29,18)})$ is very large and it was not computed accurately, but since $p(29,18) \equiv 1 \pmod 8$ one can once again state that the determinant p has the same structure: $C(3) \times C(3)$.

Finally, for the composite $\Delta(17, 9)$, the real field $Q(\sqrt{\Delta})$ has a class group

$$C(3) \times C(3) \times C(2) \times C(4).$$

For the $s = 2$ generators of its 3-Sylow subgroup we may select the (unreduced) forms:

$$\begin{aligned} J &= (-81, 4913, 81^2),\\ K &= (-87, 4861, 87^2). \end{aligned} \tag{41}$$

Note that unlike $Q(\sqrt{p(29,18)})$ where the $\mathfrak{a}^2$ and $\mathfrak{b}^2$ of Theorem 3 are both nonprincipal, here only $\mathfrak{b}^2$ is of order 3 while $\mathfrak{a}^2$ is principal. Nonetheless,

$s = 2$ again owing the (unexpected) generator K of (41). This does suggest that we would also find cases $\Delta(A, B)$ with $3 \mid B$ and $s = 3$, and therefore $r = 4$, if only we searched long enough.

We also record the (modest) fundamental unit

$$\varepsilon = 13379443326 + 2610737\sqrt{\Delta}. \tag{42}$$

The imaginary field $Q(\sqrt{-3\Delta})$ has a class group

$$C(3) \times C(3) \times C(81) \times C(2) \times C(2) \times C(2).$$

We now have cube-roots

$$\begin{aligned} J &= (1110, 801, 17890), \\ K &= (660, 399, 29905), \\ L &= (682, 157, 28891) \end{aligned} \tag{43}$$

of order 3, and ambiguous forms

$$\begin{aligned} P &= (3, 3, 6565834), \\ Q &= (101, 101, 195050), \\ R &= (457, 457, 43216), \end{aligned} \tag{44}$$

of order 2. The six forms (43) and (44) generate a subgroup that constitutes the 216 sixth-roots of the identity

$$I = (1, 1, 19697500).$$

It follows that the diophantine equation

$$4n^6 = u^2 + 3\Delta v^2$$

has an exceptionally large number of relatively small solutions $n < \sqrt{\Delta}$.

One of these:

$$n = 370, \ u = 75042667, \ v = 7667,$$

is the elementary solution (32) upon which we based the proof of $r = s+1$, but there are any number of others here, such as

n	u	v
212	12555431	1615
220	4967333	2333
223	21259630	712

that would serve the same purpose for $\Delta(17, 9)$, except, of course, that they were unknown a priori. Alternatively, $r = s+1$ is also implied for $\Delta(17, 9)$ by (41), (42), and Scholz's other criterion (mod 9).

References

[1] Pierre Barrucand and Harvey Cohn, *Note on primes of type $x^2 + 32y^2$, class number, and residuacity*, Crelle's Journ. 238 (1969), pp. 67–70.

[2] S. Chowla, *An extension of Heilbronn's class-number theorem*, Quart. Journ. Math., Oxford series, 5 (1934), pp. 304–307.

[3] Richard B. Lakein and Sigekatu Kuroda, *Tables of class numbers $h(-p)$ for fields $Q(\sqrt{-p})$, $p \leqslant 465071$*, Math. Comp., UMT 38, 24 (1970), pp. 491–493.

[4] Emma Lehmer, *Criteria for cubic and quartic residuacity*, Mathematika 5 (1958), pp. 20–29.

[5] R. A. Lippman, *Note on irregular discriminants*, Journ. London Math. Soc. 38 (1963), pp. 385–386.

[6] W. Narkiewicz, *Class number and factorization in quadratic number fields*, Colloq. Math. 17 (2) (1967), pp. 167–190, esp. p. 174.

[7] L. Rédei, *Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe in quadratischen Zahlkörpern*, Crelle's Journ. 171 (1934), pp. 131–148.

[8] K. Schaffstein, *Tafel der Klassenzahlen, usw.*, Math. Annalen 98 (1928), pp. 745–748.

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

[10] A. Scholz and Olga Taussky, *Die Hauptideale der kubischen Klassenkörper imaginär quadratischer Zahlkörper: ihre rechnerische Bestimmung und ihr Einfluss auf den Klassenkörperturm*, Crelle's Journ. 171 (1934), pp. 19–41.

[11] Daniel Shanks, *On Gauss's class number problems*, Math. Comp. 23 (1969), pp. 151–163.

[12] — *Class number, a theory of factorization, and genera*, Vol. 20 of Proceedings of Symposia in Pure Mathematics, Amer. Math. Soc., 1971, pp. 415–440.

[13] I. R. Šaferevič, *Algebraic number fields* (in Russian), Proceedings of International Congress of Mathematicians, Stockholm, 1962, pp. 163–176.

[14] H. Wada, *A table of ideal class groups of imaginary quadratic fields*, Proc. Japan Acad. 46 (1970), pp. 401–403.

APPLIED MATHEMATICS LABORATORY
NAVAL SHIP R&D CENTER
Washington, D. C.

MATHEMATICS DEPARTMENT
UNIVERSITY OF MICHIGAN
Ann Arbor, Michigan

Received on 15. 1. 1971 (133)