MATHEMATICS OF COMPUTATION VOLUME 30, NUMBER 133
JANUARY 1976, PAGES 173–178

Class Groups of the Quadratic Fields Found by F. Diaz y Diaz

By Daniel Shanks

Abstract. F. Diaz y Diaz has discovered 99 discriminants d between -3321607 and -60638515 inclusive for which $Q(\sqrt{d})$ have a 3-rank $r_3 = 3$. These 99 imaginary quadratic fields are analyzed here and the class groups are given and discussed for all those of special interest. In 98 cases, the associated real quadratic fields have $r_3 = 2$, but for $d = 44806173 = 3 \cdot 14935391$, $Q(\sqrt{d})$ has a class group $C(3) \times C(3) \times C(3)$; and this is now the smallest known d for which a real quadratic field has $r_3 = 3$.

By selecting discriminants generated by certain quartic and sextic polynomials, the author and several collaborators [1]–[4] constructed a large number of imaginary quadratic fields having 3-rank r_3 equal to 3 or 4. That is, their ideal class groups contain $C(3) \times C(3) \times C(3)$ or $C(3) \times C(3) \times C(3) \times C(3)$ as subgroups. The smallest of these discriminants d was

$$d = -63199139 = -D_6(28),$$

where

$$D_6(z) = 108z^4 - 148z^3 + 84z^2 - 24z + 3.$$

The smallest class number of these fields, which was $h = 1836 = 27 \cdot 68$, occurred for

$$d = -3(17^6 + 4 \cdot 6^6).$$

Since the polynomials used were very special, it did seem possible [2, p. 545] that a somewhat smaller $|d|$ than 63199139 might exist having $r_3 = 3$. Again, while an example of $h = 27$ for $r_3 = 3$ is most unlikely, it did seem very probable that examples with $h/27 < 68$ do exist [2, p. 539]. The reason for the latter is that all of these discriminants d, by construction, had $(d/3) = +1$ or 0, whereas, to minimize h, it is clear that one wants $(d/p) = -1$ for all small primes p.

In [5], F. Diaz y Diaz obtained both smaller $|d|$ and smaller h by systematically computing reduced solutions of

$$4m^3 = x^2 + y^2D \tag{1}$$

for fundamental discriminants $-D$. Sorting these on D, one then has $Q(\sqrt{-D})$ with $r_3 \geqslant 3$ if (1) has 5 or more inequivalent solutions. He thus found 99 values of $D < 63199139$ with $r_3 = 3$ but none with $r_3 > 3$. His procedure is analogous to that in the

Received June 27, 1975.
AMS (MOS) subject classifications (1970). Primary 12A25, 12A50, 12A65.

older work of R. J. Porter [6], [7], the distinction being that Porter computed *irregular determinants* $-D$, in Gauss's terminology, with D not necessarily square-free. Porter systematically computed reduced quadratic forms $Au^2 + 2Buv + Cv^2$ of order 3 under composition, and then sorted them on their negative determinants $D = AC - B^2$.

Of the 99 D in [5], the smallest is

$$D = 3321607, \tag{2}$$

while the smallest class number, which is

$$h = 162 = 27 \cdot 6, \tag{3}$$

occurs for $D = 3640387$. By this method, one only obtains r_3, not the class group, or even the class number. However, Diaz y Diaz included the class groups in [5] for (2), (3) and one other D as follows:

	D	*Group*
(4)	3640387	$C(3) \times C(3) \times C(18)$
(5)	4897363	$C(3) \times C(3) \times C(33)$
(6)	3321607	$C(3) \times C(3) \times C(63)$.

For several investigations, such as certain studies of cubic fields (see [8], [9], [10], [11, pp. 285–286]), it is useful to examine a number of such D and the class groups of their $Q(\sqrt{-D})$. I have examined all 99 D in [5], and in Table 1 I list all 35 of these that have $h \leqslant 27 \cdot 50$. Table 1 lists D; its factorization (p means prime); the ratio $h/27$; and the class group (with (4) above abbreviated as $3 \times 3 \times 18$, etc.). Also listed is the Dirichlet function $L(1, \chi) = \pi h/\sqrt{D}$, and each field is assigned an identification number #. Note that (4), (5), and (6) above are #'s 1, 2, and 10, respectively. Table 2 includes eight other fields selected from the remaining 64 because they are of special interest.

Commentary on These Fields. Field #1 has the smallest h, the smallest $L(1, \chi)$, and its *exponent* 18 is minimal although it is duplicated in #3 and #14. The 18th power of each of its integral ideals is principal, cf. [12], [13]. The next smallest exponent is 24 and occurs in #22 and #42. D is minimized in #10, and this is also the smallest prime D. But note that in #5 $Q(\sqrt{-1204729})$ also has $r_3 = 3$, so -1204729 is the smallest prime *determinant* in Gauss's terminology. The smallest determinant is -1118090 and is found in #29. Surprisingly, its class group contains $C(6) \times C(6) \times C(6)$. Accordingly,

$$A^6 = B^2 + C^2 1118090$$

has an exceptionally large number of small solutions A such as

A	B	C
87	459587	446
99	746681	586
117	483526	1444, etc.

Fields #14, 39, 40, 42, and 43 also contain $C(6) \times C(6) \times C(6)$.

TABLE 1

D	*factorization*	$h/27$	*group*	$L(1, \chi)$	#
3640387	421 · 8647	6	3 × 3 × 18	0.26674	1
4897363	p	11	3 × 3 × 33	0.42162	2
5048347	89 · 131 · 433	12	3 × 6 × 18	0.45302	3
15476323	37 · 418279	14	3 × 3 × 42	0.30186	4
4818916	4 · 1204729	16	3 × 3 × 48	0.61824	5
8992363	71 · 126653	16	3 × 3 × 48	0.45258	6
9778603	263 · 37181	16	3 × 3 × 48	0.43401	7
28114627	191 · 147197	18	3 × 3 × 54	0.28795	8
25012003	p	19	3 × 3 × 57	0.32225	9
3321607	p	21	3 × 3 × 63	0.97737	10
5067967	p	23	3 × 3 × 69	0.86661	11
5288968	8 · 661121	24	3 × 3 × 72	0.88520	12
19941763	29 · 687647	24	3 × 3 × 72	0.45587	13
26156083	23 · 43 · 53 · 499	24	6 × 6 × 18	0.39805	14
42895603	53 · 73 · 11087	24	3 × 6 × 36	0.31083	15
29482627	p	25	3 × 3 × 75	0.39054	16
17496643	47 · 372269	26	3 × 3 × 78	0.52724	17
16006307	157 · 269 · 379	28	3 × 6 × 42	0.59364	18
16784851	59 · 284489	30	3 × 3 × 90	0.62112	19
11324296	8 · 359 · 3943	32	3 × 6 × 48	0.80660	20
35269627	241 · 146347	32	3 × 3 × 96	0.45705	21
55458643	29 · 59 · 32413	32	3 × 12 × 24	0.36448	22
7016747	p	33	3 × 3 × 99	1.05672	23
10348907	p	35	3 × 3 × 105	0.92286	24
10676983	p	35	3 × 3 × 105	0.90857	25
36323563	p	35	3 × 3 × 105	0.49259	26
12201979	983 · 12413	36	3 × 3 × 108	0.87418	27
36399667	47 · 137 · 5653	36	3 × 6 × 54	0.50614	28
4472360	8 · 5 · 17 · 6577	40	6 × 6 × 30	1.60437	29
7060148	4 · 109 · 16193	40	3 × 6 × 60	1.27693	30
19969763	11 · 1109 · 1637	40	3 × 6 × 60	0.75925	31
6562327	367 · 17881	42	3 × 3 × 126	1.39070	32
30580763	347 · 88129	42	3 × 3 × 126	0.64423	33
30470603	p	49	3 × 3 × 147	0.75296	34
54433787	613 · 88799	50	3 × 15 × 30	0.57484	35

Note that #22 contains $C(4) \times C(8)$ and #35 contains $C(5) \times C(5)$ so their principal genera are irregular not only in their 3-Sylow subgroup but in an additional p-Sylow subgroup besides. Field #36 is the third smallest D but has a relatively large h. Field #37 has the largest $L(1, \chi)$; one finds that its $(d/p) = +1$ for all $p \leqslant 19$. Field

TABLE 2

D	*factorization*	$h/27$	*group*	$L(1, \chi)$	#
4019207	p	69	$3 \times 3 \times 207$	2.91939	36
16434239	$587 \cdot 27997$	282	$3 \times 3 \times 846$	5.90049	37
21658407	$3 \cdot 7219469$	82	$3 \times 3 \times 246$	1.49456	38
24952655	$5 \cdot 7 \cdot 13 \cdot 173 \cdot 317$	208	$2 \times 6 \times 6 \times 78$	3.53198	39
28732623	$3 \cdot 113 \cdot 131 \cdot 647$	112	$6 \times 6 \times 84$	1.77233	40
34394964	$4 \cdot 3 \cdot 2866247$	80	$3 \times 6 \times 120$	1.15706	41
42132596	$4 \cdot 11 \cdot 17 \cdot 23 \cdot 31 \cdot 79$	128	$2 \times 2 \times 6 \times 6 \times 24$	1.67269	42
55247159	$11 \cdot 71 \cdot 127 \cdot 557$	288	$6 \times 6 \times 216$	3.28663	43

#42 is truly remarkable: it has 6 ramifying primes but none greater than 79, and an exponent of 24 in spite of its relatively large D. It will have an infinite class tower because of its 2-rank = 5, cf. [3, p. 187].

Finally, we note that #38, 40, and 41 are the only three among the 99 D in [5] where D is divisible by 3. The associated real fields $Q(\sqrt{D/3})$ must, therefore, have $r_3 = 2$ or 3, cf. [1]. Here, $r_3 = 2$ in all 3 examples; in fact, the class groups are

#	*real field*	*group*
38	$Q(\sqrt{9219469})$	3×3
40	$Q(\sqrt{9577541})$	3×12
41	$Q(\sqrt{2866247})$	3×15

The real fields for #38 and #41 may have the smallest discriminant and determinant, respectively, having $r_3 = 2$ and an associated imaginary field with $r_3 = 3$.

The 99 D in [5] are distributed (mod 9) in the following interesting way:

D (mod 9)	1	2	3	4	5	6	7	8
no. examples	4	4	0	42	43	3	0	3

We note, in passing, that $D \equiv 3$ does exist; in fact,

$$D = 3(3^6 + 4 \cdot 19^6) \equiv 3 \pmod 9$$

was actually the first known case [1] where $Q(\sqrt{-D})$ had $r_3 = 3$. It is unknown to the author whether an example of $D \equiv 7$ exists.

A Smaller Real Field with $r_3 = 3$. The 96 D not divisible by 3 will have associated real fields $Q(\sqrt{3D})$ with $r_3 = 2$ or 3. A very simple criterion can decide this immediately for all 89 $D \equiv 2$, 4, or 5. It may be deduced from Scholz's second criterion [14] by much the same argumentation as in [2, p. 549], and so we state it without proof:

THEOREM. *The 3-rank of $Q(\sqrt{3D})$ will be 1 less than that of $Q(\sqrt{-D})$ if $D \equiv$ 4 or 5 (mod 9) and (1) has a solution with*

$$y \equiv 1, x \not\equiv 0 \pmod 9.$$

This is also true if $D \equiv 2$ *has any solution* (1) *with* $y \equiv 1 \pmod 9$.

For every $D \equiv 2$, 4, and 5 in [5], the solutions of (1) given there readily yield such examples with $y = 1$ for one of the smallest values of m. Therefore, all of their $Q(\sqrt{3D})$ also have $r_3 = 2$. By more subtle computations, the remaining D, those congruent to 1 or 8, also have $Q(\sqrt{3D})$ with $r_3 = 2$ with *one single exception* for $D \equiv 8$. This exception we list as field #44:

D	*factorization*	$h/27$	*group*	$L(1, \chi)$	#
14935391	p	135	$3 \times 3 \times 405$	2.96305	44

We thus discover that, for

$$d = 44806173 = 3 \cdot 14935391, \tag{7}$$

the real field $Q(\sqrt{d})$ has $r_3 = 3$.

The principal reduced quadratic form of discriminant (7) is

$$u^2 + 6693uv - 2481v^2. \tag{8}$$

Under the unimodular transformation

$$\begin{pmatrix} 43 & 96 \\ 116 & 259 \end{pmatrix}$$

(8) becomes another reduced form

$$f(U, V) = 2197U^2 + 3117UV - 3993V^2,$$

and one finds that

$$f(1, 0) = 13^3, \quad f(1, -1) = (-17)^3, \quad f(0, 1) = 3(-11)^3.$$

But the ideal class number is odd, since $d/3$ is prime, and so the ramified 3 is principal. Therefore, (8) represents the three cubes: 13^3, $(-17)^3$, $(-11)^3$. Since the period of reduced forms is only twenty-six forms long until we reach its symmetric midpoint: $(-827, 6693, 3)$, we readily verify that (8) does *not* represent

$$13, \ -17, \ -11, \ -13 \cdot 17, \ -11 \cdot 13, \ 11 \cdot 17, \text{ or } 11 \cdot 13 \cdot 17,$$

since none of these numbers equals an end-coefficient in a reduced form. As in [1, p. 77], one thus finds that

$$G = C(3) \times C(3) \times C(3) \tag{9}$$

is a subgroup of the class group. In fact, as in the earlier case [1], where

$$d = 3^6 + 4 \cdot 19^6 = 188184253, \tag{10}$$

G is the entire ideal class group. The new d in (7) is smaller; in fact, it is also smaller than the

$$d = 21^6 + 4 \cdot 8^6 = 86814697 \tag{11}$$

of [2, p. 539], and so it gives the smallest known real $Q(\sqrt{d})$ with $r_3 = 3$. The new

$Q(\sqrt{d})$ also differs from that with (10) in that its fundamental unit now has norm $+1$.

Correspondingly, there will be thirteen distinct totally real cubic fields of discriminant $d = 44806173$, and that is the smallest known such d. The thirteen cubic polynomials are readily obtained from the thirteen solutions (1) with $D = 14935391$, cf. [10].

Computation and Mathematics Department
Naval Ship Research and Development Center
Bethesda, Maryland 20084

1. DANIEL SHANKS & PETER WEINBERGER, "A quadratic field of prime discriminant requiring three generators for its class group, and related theory," *Acta Arith.*, v. 21, 1972, pp. 71–87. MR **46** #9003.

2. DANIEL SHANKS, "New types of quadratic fields having three invariants divisible by 3," *J. Number Theory*, v. 4, 1972, pp. 537–556. MR **47** #1775.

3. DANIEL SHANKS & RICHARD SERAFIN, "Quadratic fields with four invariants divisible by 3," *Math. Comp.*, v. 27, 1973, pp. 183–187; "Corrigenda," *ibid.*, p. 1012. MR **48** #8436a, b.

4. CAROL NEILD & DANIEL SHANKS, "On the 3-rank of quadratic fields and the Euler product," *Math. Comp.*, v. 28, 1974, pp. 279–291.

5. F. DIAZ Y DIAZ, "Sur les corps quadratiques imaginaires dont le 3-rang du groupe des classes est supérieur à 1", *Séminaire Delange-Pisot-Poitou*, 1973/74, no. G15.

6. R. J. PORTER, "On irregular negative determinants of exponent $9n$," *MTAC*, v. 10, 1956, pp. 22–25. MR **17**, 1140.

7. R. J. PORTER, *Tables in the UMT file, MTAC*, v. 7, 1953, p. 34; v. 8, 1954, pp. 96–97; v. 9, 1955, p. 26, p. 126, p. 198; v. 11, 1957, p. 275; v. 12, 1958, p. 225.

8. T. CALLAHAN, "The 3-class groups of non-Galois cubic fields. I," *Mathematika*, v. 21, 1974, pp. 72–89.

9. T. CALLAHAN, "The 3-class groups of non-Galois cubic fields. II," *Mathematika*, v. 21, 1974, pp. 168–188.

10. DANIEL SHANKS, "Review of Angell's table," *Math. Comp.*, v. 29, 1975, pp. 661–665.

11. DANIEL SHANKS, "Calculation and applications of Epstein zeta functions," *Math. Comp.*, v. 29, 1975, pp. 271–287.

12. DAVID W. BOYD & H. KISILEVSKY, "On the exponent of the ideal class groups of complex quadratic fields," *Proc. Amer. Math. Soc.*, v. 31, 1972, pp. 433–436. MR **44** #6644.

13. P. J. WEINBERGER, "Exponents of the class groups of complex quadratic fields," *Acta Arith.*, v. 22, 1973, pp. 117–124. MR **47** #1776.

14. A. SCHOLZ, "Über die Beziehung der Klassenzahlen quadratischer Körper zueinander," *Crelle's J.*, v. 166, 1932, pp. 201–203.