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 $\mathbb{Q}(\sqrt{d})$ 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 $d = 44806173 = 3 \cdot 14935391$, $\mathbb{Q}(\sqrt{d})$ 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

$$(1) \ 4m^3 = x^2 + y^2D$$

for fundamental discriminants $-D$. Sorting these on $D$, one then has $\mathbb{Q}(\sqrt{-D})$ with $r_3 > 3$ 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
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

\[(2) \quad D = 3321607,\]

while the smallest class number, which is

\[(3) \quad h = 162 = 27 \cdot 6,\]

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:

<table>
<thead>
<tr>
<th>(D)</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>(4) 3640387</td>
<td>(C(3) \times C(3) \times C(18))</td>
</tr>
<tr>
<td>(5) 4897363</td>
<td>(C(3) \times C(3) \times C(33))</td>
</tr>
<tr>
<td>(6) 3321607</td>
<td>(C(3) \times C(3) \times C(63))</td>
</tr>
</tbody>
</table>

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 \(h \leq 27 \cdot 50\). 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

<table>
<thead>
<tr>
<th>(A)</th>
<th>(B)</th>
<th>(C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>87</td>
<td>459587</td>
<td>446</td>
</tr>
<tr>
<td>99</td>
<td>746681</td>
<td>586</td>
</tr>
<tr>
<td>117</td>
<td>483526</td>
<td>1444</td>
</tr>
</tbody>
</table>

Fields \#14, 39, 40, 42, and 43 also contain \(C(6) \times C(6) \times C(6)\).
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 $p \leq 19$. Field

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 $p \leq 19$. Field
Table 2

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

#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 \( \mathbb{Q}(\sqrt{D/3}) \) must, therefore, have \( r_3 = 2 \) or 3, cf. [1]. Here, \( r_3 = 2 \) in all 3 examples; in fact, the class groups are

<table>
<thead>
<tr>
<th>#</th>
<th>real field</th>
<th>group</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td>( \mathbb{Q}(\sqrt{9219469}) )</td>
<td>( 3 \times 3 )</td>
</tr>
<tr>
<td>40</td>
<td>( \mathbb{Q}(\sqrt{9577541}) )</td>
<td>( 3 \times 12 )</td>
</tr>
<tr>
<td>41</td>
<td>( \mathbb{Q}(\sqrt{2866247}) )</td>
<td>( 3 \times 15 )</td>
</tr>
</tbody>
</table>

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:

\[
\begin{array}{cccccccc}
D \pmod{9} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
\hline
\text{no. examples} & 4 & 4 & 0 & 42 & 43 & 3 & 0 & 3 \\
\end{array}
\]

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 \( \mathbb{Q}(\sqrt{-D}) \) 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 \( \mathbb{Q}(\sqrt{3D}) \) with \( r_3 = 2 \) or 3. A very simple criterion can decide this immediately for all 89 \( D \equiv 2, 4, \text{ or } 5 \). 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 \( \mathbb{Q}(\sqrt{3D}) \) will be 1 less than that of \( \mathbb{Q}(\sqrt{-D}) \) if \( D \equiv 4 \text{ or } 5 \pmod{9} \) 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 \( y \equiv 1 \) (mod 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 \( \mathbb{Q}(\sqrt{D}) \) also have \( r_3 = 2 \). By more subtle computations, the remaining \( D \), those congruent to 1 or 8, also have \( \mathbb{Q}(\sqrt{D}) \) with \( r_3 = 2 \) with one single exception for \( D \equiv 8 \). This exception we list as field #44:

\[
\begin{array}{cccccc}
D & \text{factorization} & h/27 & \text{group} & L(1, \chi) & \\
14935391 & p & 135 & 3 \times 3 \times 405 & 2.96305 & 44
\end{array}
\]

We thus discover that, for

(7) \( d = 44806173 = 3 \cdot 14935391 \),

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

The principal reduced quadratic form of discriminant (7) is

(8) \( u^2 + 6693uv - 2481v^2 \).

Under the unimodular transformation

\[
\begin{pmatrix}
43 \\
116
\end{pmatrix}
\begin{pmatrix}
96 \\
259
\end{pmatrix}
\]

(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

\( 13, -17, -11, -13 \cdot 17, -11 \cdot 13, 11 \cdot 17, \) 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

(9) \( G = \mathcal{C}(3) \times \mathcal{C}(3) \times \mathcal{C}(3) \)

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

(10) \( d = 3^6 + 4 \cdot 19^6 = 188184253 \),

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

(11) \( d = 21^6 + 4 \cdot 8^6 = 86814697 \)

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