MATHEMATICS OF COMPUTATION, VOLUME 30, NUMBER 135
JULY 1976, PAGES 610–623

Class Groups of Quadratic Fields

By Duncan A. Buell

Abstract. The author has computed the class groups of all complex quadratic number fields $Q(\sqrt{-D})$ of discriminant $-D$ for $0 < D < 4000000$. In so doing, it was found that the first occurrences of rank three in the 3-Sylow subgroup are $D = 3321607$ = prime, class group $C(3) \times C(3) \times C(9.7)$ ($C(n)$ a cyclic group of order n), and $D = 3640387 = 421.8647$, class group $C(3) \times C(3) \times C(9.2)$. The author has also found polynomials representing discriminants of 3-rank ≥ 2, and has found 3-rank 3 for $D = 6562327 = 367.17881$, 8124503, 10676983, 193816927, all prime, $390240895 = 5.11.7095289$, and 503450951 = prime. The first five of these were discovered by Diaz y Diaz, using a different method. The author believes, however, that his computation independently establishes the fact that 3321607 and 3640387 are the smallest D with 3-rank 3.

The smallest examples of noncyclic 13-, 17-, and 19-Sylow subgroups have been found, and of groups noncyclic in two odd p-Sylow subgroups. $D = 119191$ = prime, class group $C(15) \times C(15)$, had been found by A. O. L. Atkin; the next such D is $2075343 = 3.17.40693$, class group $C(30) \times C(30)$. Finally, $D = 3561799$ = prime has class group $C(21) \times C(63)$, the smallest D noncyclic for 3 and 7 together.

Introduction. Throughout this paper, $-D < 0$ will denote the discriminant of an imaginary quadratic number field, and "smallest" will refer to D, not to $-D$, so that "smallest D" means "largest discriminant."

The author has computed the class groups of all quadratic number fields $Q(\sqrt{-d})$, $d > 0$, of discriminant $-D$, for $0 < D < 4000000$. By a theorem of Gauss, if D has k distinct prime factors, the 2-Sylow subgroup of the class group has rank $k - 1$. Apart from this, the groups tend to be cyclic. Even the 2-Sylow subgroup tends to be $k - 2$ elementary 2-groups and one large cyclic factor collecting the other powers of two in the class number, so that the 2-Sylow subgroup of the subgroup of squares is cyclic. In computing the 2-Sylow subgroup, then, we actually computed that subgroup of the subgroup of squares, and shall, by abuse of language, call this the 2-Sylow subgroup, calling the group cyclic if the subgroup of squares is. The subgroup of squares is, in the terminology of Gauss, the principal genus, and a discriminant for which the principal genus is noncyclic is called irregular. Thus, what we call a discriminant with a noncyclic 2-Sylow subgroup is a discriminant which Gauss would call irregular.

Statistics were kept on the frequency of occurrence of noncyclic groups, and of the noncyclic p-Sylow subgroups for $p = 2, 3, 5, 7$. Special listings were also made of the noncyclic p-Sylow subgroups for $p \geq 11$, of the p-Sylow subgroups $C(p^a) \times C(p^b)$ with a and $b \geq 2$, and of the class groups noncyclic in more than one p-Sylow subgroup. We note here that 95.74% of the class groups turned out to be cyclic. The

Received June 3, 1975; revised October 14, 1975.
AMS (MOS) subject classifications (1970). Primary 12–04, 12A25.

method of computation is outlined in Appendix A; the results are listed and discussed in Appendix B.

In the process of computation, we found that $D = 3321607 =$ prime has class group $C(3) \times C(3) \times C(9.7)$, and $D = 3640387 = 421.8647$ has class group $C(3) \times C(3) \times C(9.2)$. These are the smallest D for which the class group has p-rank greater than two, for $p \geqslant 3$. That an infinity of discriminants with 3-rank 3 exists has been proved by Craig [1], and numerous examples were given by Shanks and his collaborators [2]–[5], the smallest D being 63199139.

We developed a method for obtaining quartic polynomials representing, for all squarefree negative integer values within certain bounds, discriminants with 3-rank $\geqslant 2$. With this method, we found six more discriminants with 3-rank 3. The method and these immediate results are detailed in Section 1.

Subsequent to our investigation, we learned that Diaz y Diaz [6], [6a] had made, by an entirely different method, an extensive search for discriminants with 3-rank $\geqslant 3$, and had found, in addition to our five smallest D, ninety-four others smaller than 63199139. We feel, however, that our computation is the first complete verification of the fact that 3321607 and 3640387 are the smallest D with 3-rank 3.

In Section 2, we investigate an identical relation between forms obtained by the method of Section 1, and obtain a connection between the group composition of forms of discriminant $-D$ and the group law of the elliptic curve $Y^2 = 4X^3 - D$. Finally, in Section 3, we consider problems and conjectures of our method.

All of the computations were made on the IBM 370/158 computer at the University of Illinois at Chicago Circle, Chicago, Illinois; we thank the University for making the computer facilities available.

1. Let D be a positive squarefree integer. The solutions in integers of the Diophantine equation

$$4a^3 = b^2 + c^2D, \qquad 0 < a < \sqrt{D/3},\ 0 < b,\ (b, c) \leqslant 2, \tag{1}$$

correspond to ideals $\mathfrak{a} = (a, (b + c\sqrt{-D})/2)$ in the ring of integers of $Q(\sqrt{-D})$ whose cube is principal: $\mathfrak{a}^3 = ((b + c\sqrt{-D})/2)$ [4]. More simply, if $(a, b) = 1$, there is a quadratic form (a, b, a^2) of discriminant $-c^2D$ whose cube is principal:

$$(a, b, a^2)^2 \sim (a^2, b, a) \sim (a, -b, a^2) \sim (a, b, a^2)^{-1}.$$

Let us assume $c = 1$ in (1), and drop the restriction on the size of a, and call this Eq. (1a). We seek to produce discriminants $-D$ with a large 3-rank in the class group by obtaining parametric representations

$$-D = \Delta(x) = S_1^2 - 4C_1^3 = S_2^2 - 4C_2^3 = S_3^2 - 4C_3^3 \tag{2}$$

where the S_i and C_i are polynomials in x:

$$S_i(x) = x^2 + a_ix + b_i, \qquad C_i(x) = c_ix + d_i.$$

Then (2) implies

$$(S_i + S_j)(S_i - S_j) = 4(C_i - C_j)(C_i^2 + C_iC_j + C_j^2), \qquad 1 \leqslant i, j \leqslant 3,\ i < j.$$

If we insist that the linear term on the right divides the linear term on the left, that is,

$$(3)\quad S_1 - S_2 = K(C_1 - C_2), \quad S_1 - S_3 = K(C_1 - C_3), \quad S_2 - S_3 = K(C_2 - C_3),$$

for K an integer, we obtain the equations:

$$\begin{aligned} &b_1^2 - 4d_1^3 = b_2^2 - 4d_2^3, \quad (b_1 - b_2)/(d_1 - d_2) = K, \quad (a_1 - a_2)/(c_1 - c_2) = K, \\ (4)\qquad &a_1 = (K/2)(c_1 - c_2) + (2/K)(d_2(2c_2 + c_1) + d_1(2c_1 + c_2)), \\ &2K = (2c_1 + c_2)^2 + 3c_2^2 \end{aligned}$$

and two other sets of equations from the latter two of Eqs. (3). Considering the last equation in each set, we get, by the theory of automorphs of the form (1, 1, 1), that $c_1 + c_2 + c_3 = 0$. Using this, we can reduce the relations among the coefficients to the following:

$$\begin{aligned} &b_1^2 - 4d_1^3 = b_2^2 - 4d_2^3 = b_3^2 - 4d_3^3, \\ &(b_1 - b_2)/(d_1 - d_2) = (b_1 - b_3)/(d_1 - d_3) = (b_2 - b_3)/(d_2 - d_3) = K, \\ (5)\qquad &2K = (2u + v)^2 + 3v^2, \quad (c_1, c_2, c_3) \text{ some permutation of } (u, v, -u - v), \\ &a_1 = c_1K + (2/K)(c_1d_1 + c_2d_2 + c_3d_3) = c_1K + M, \\ &a_2 = c_2K + M, \quad a_3 = c_3K + M. \end{aligned}$$

Thus, if we assume b_1, b_2, b_3, d_1, d_2, d_3, K, u, and v satisfy the first three of Eqs. (5), we obtain, except in certain special cases, six distinct polynomials $\Delta(x)$ for each solution $(u, v, -u - v)$, corresponding to the two 3-cycles of the solution. (If $K = 6u^2$ we have $u = v$, and if $K = 2u^2$, we have $u = -v$. In the former instance only one cycle results; in the latter, only one cycle up to a change of sign, which, as we shall note, does not affect the polynomials obtained.) It appears to be the case, though we have not yet proved it, that exactly one of the two 3-cycles yields integers a_i, while the other yields only rational solutions in general. In the special cases, the a_i appear to be integral. Since the triple (c_1, c_2, c_3) is determined only up to a sign change, we choose as a convention that the largest of the $|c_i|$ should be chosen negative, noting that $\Delta(c_1, c_2, c_3, x) = \Delta(-c_1, -c_2, -c_3, -x)$.

We show now that only the first two of Eqs. (5) are independent; for all K such that the first two equations are solvable, $2K = u^2 + 3v^2$ has integer solutions u and v. The first equation can be partly rewritten

$$(b_1 + b_2)(b_1 - b_2) = (d_1 - d_2)((2d_2 + d_1)^2 + 3d_1^2).$$

Dividing by $4(d_1 - d_2)$, we obtain

$$((b_1 + b_2)/2)(K/2) = ((2d_2 + d_1)^2 + 3d_1^2)/4.$$

The left-hand side is thus the norm of an integer in $Q(\sqrt{-3})$. The only reason, then,

that $2K = u^2 + 3v^2$ might not be solvable would be that $p|(K/2)$ and $p|((b_1 + b_2)/2)$, for p a prime which is $\equiv 2$ modulo 3. But then we must have $p|d_1$ and $p|(2d_2 + d_1)$; there are no *primitive* representations $p^2 = u^2 + 3v^2$ for such p. That $p|(K/2)$ and $((b_1 + b_2)/2)$, however, implies that $p|b_1$ and $p|b_2$, so that $p^2|-D = b_1^2 - 4d_1^3$. Thus if D is squarefree, $2K = u^2 + 3v^2$ has integer solutions u and v.

We now have a list of discriminants $\Delta(x)$, and we establish conditions for independence of the forms. If (Q, P, Q^2) and (S, R, S^2) lie in the same or in inverse classes, then we can find integers a, b, c, d, such that $ad - bc = +1$ and that

$$4QS = (2Qa + Pc)^2 - c^2\Delta(x), \qquad 4QS = (2Sd - Rc_1)^2 - c^2\Delta(x),$$

where c_1 equals c if the classes are the same, and $-c$ if they are inverse to each other. If $\Delta(x) < 0$ and $4QS < -\Delta(x)$, we must choose $c = 0$. This forces $S = Qa^2$ and $Q = Sd^2$, which imply $S = Q$. Thus, of the forms (C_i, S_i, C_i^2), if we can satisfy $4C_iC_j < -\Delta(x)$ for $\Delta(x) < 0$ and $i \neq j$, we are guaranteed that the 3-Sylow subgroup of the class group of $Q(\sqrt{\Delta(x)})$ has rank at least two. (That we cannot guarantee rank three by the existence of the third form will appear in Section 2.)

It remains to be seen that solutions (d_i, b_i), $i = 1, 2, 3$, and K exist for the first two of Eqs. (5). The smallest D for which $3|h(Q(\sqrt{-D}))$ is $D = 23$, and we do indeed find solutions. However, since $\Delta(x)$ is a quartic polynomial, it assumes only finitely many negative integer values, and for these $\Delta(x)$ the discriminants less than zero are much too small to be interesting.

The appearance of $D = 3321607$, however, with thirteen pairs of solutions to (1a), provided numerous useful polynomials $\Delta(x)$. From (94, 27), (152, 3275), (538, 24891), $K = 56$, $(c_1, c_2, c_3) = (4, 2, -6)$, we get

$$\Delta(x) = (x^2 + 133x + 27)^2 - 4(4x + 94)^3 = (x^2 + 21x + 3275)^2 - 4(2x + 152)^3$$
$$= (x^2 - 427x + 24891)^2 - 4(-6x + 538)^3.$$

This $\Delta(x)$ is negative for integers x, $-8 \leqslant x \leqslant 75$, and $\Delta(70) = -6562327 = -367.17881$ has class group $C(3) \times C(3) \times C(9.2.7)$.

From (152, -3275), (284, 9397), (1868, 161461), $K = 96$, $(c_1, c_2, c_3) = (4, 4, -8)$, we get a $\Delta(x)$ which is negative for integers x, $-1 \leqslant x \leqslant 201$. $\Delta(60) = -193816927 =$ − prime has class group $C(3) \times C(3) \times C(3.5.53)$. $\Delta(108) = -390240895 = -5.11.7095289$ has a class group whose 3-Sylow subgroup is $C(3) \times C(3) \times C(27)$.

From (128, -2251), (202, 5445), (2374, 231333), $K = 104$, with $(c_1, c_2, c_3) = (6, 2, -8)$ (which has nonintegral a_i), we find that $\Delta(169) = -503450951$ − prime has class group $C(3) \times C(3) \times C(27.103)$.

We now take the constant in $\Delta(x)$ to be -6562327, and choose (118, 99), (248, 7379), (418, 16899), for which $K = 56$. If we let $(c_1, c_2, c_3) = (2, -6, 4)$, $\Delta(7) = -8124503 =$ − prime has class group $C(3) \times C(3) \times C(9.29)$; if we let $(c_1, c_2 c_3) = (4, 2, -6)$, we find that $\Delta(7) = -10676983 =$ − prime has class group $C(3) \times C(3) \times C(3.5.7)$.

2. The group law on an elliptic curve may be described simply by saying that collinear points sum to zero. That is, if the three (counting multiplicities) points of intersection of the curve with a straight line are P_1, P_2, and P_3, then $P_1 + P_2 + P_3 = 0$.

The composition of binary quadratic forms is considerably more complicated, in part because the elements of the group are not the forms themselves, but the classes of forms equivalent under the transformations of the modular group. One algorithm for composition is as follows:

To compound (a, b, c) with (a', b', c'), both of discriminant $-D$, let $b'' = (b + b')/2, m = (a, b'')$, and $n = (a', m)$. Solve the equation $ax + b''y = m$ for x and y, and then the congruence

$$mz/n \equiv (b'' - b)x - cy \pmod{a'/n}$$

for z. If we then let $A = aa'/n^2$, $B = b + 2az/n$, and $C = (B^2 + D)/4A$, the class of (A, B, C) is that compounded of the classes of (a, b, c) and (a', b', c'). In general, (A, B, C) will not be reduced.

Now, let $D \equiv -1 \pmod 4$ be a squarefree positive integer, and let (d_i, b_i), $i = 1, 2, 3$, be the points of intersection of the elliptic curve $Y^2 = 4X^3 - D$ with the line $Y = KX + L$. We assume that d_1, b_1, d_2, b_2, and K are integers, and let $F_1 = (d_1, b_1, d_1^2)$ and $F_2 = (d_2, b_2, d_2^2)$ be the corresponding forms. We note, as symmetric functions of the roots, that

$$K^2/4 = d_1 + d_2 + d_3 \quad \text{and} \quad L^2 + D = 4d_1d_2d_3. \tag{6}$$

By the first of these, K is even if and only if d_3 (and hence b_3) is integral. In this case, we have a third form $F_3 = (d_3, b_3, d_3^2)$.

If K is odd, then $d_3 = t/4$ and $b_3 = u/4$, for t and u odd integers. We notice $4t^3 = (2u)^2 + 64D$; barring the restriction on the size of a, we have a solution of (1). The ideal which we obtain is $\mathfrak{a} = (t, u + 4\sqrt{-D})$. Dividing (1) by 4, we notice that $t \equiv 1 \pmod 8$, and we rewrite the basis of $\mathfrak{a}$ as follows:

$$\mathfrak{a} = (t, u + 4\sqrt{-D}, u(1 - t)/4 + (1 - t)\sqrt{-D}) = (t, u + 4\sqrt{-D}, u(1 - t)/4 + \sqrt{-D})$$
$$= (t, u(1 - t)/4 + \sqrt{-D}) = (t, u(1 - t)/4 + rt + \sqrt{-D}) = (t, U),$$

where r can be any integer. We choose r to be an odd integer such that $t \nmid (u - 4r)$. Then the norm of U is ts, where s is prime to t, and t is the norm of $\mathfrak{a}$. Since t is odd, we can choose as basis t and $U/2$: $\mathfrak{a} = (t, U/2)$. We note that since $t \equiv 1 \pmod 8$, and r is assumed odd, U is odd, and $(U + \sqrt{-D})/2$ is an integer in $Q(\sqrt{-D})$. By the correspondence between classes of ideals and classes of forms [7], $\mathfrak{a}$ induces a form (t, U, v) of discriminant $-D$, and has t and $U/2$ as an *integral* basis. We choose an equivalent form for F_3:

$$F_3 = (t, u(1 - t)/4 + t, v_1).$$

We now state and prove the following

THEOREM. *With the above notation,*

$$F_1 \circ F_2 \circ F_3 \sim (1, 1, (D + 1)/4) = \textit{group identity}.$$

Thus, the composition of classes of forms coincides with the group law of the elliptic curve.

Proof. We rewrite the first of Eqs. (5):

$$(b_1 + b_2)K = 4(d_1^2 + d_1 d_2 + d_2^2). \tag{7}$$

If $p|d_1$ and $p|(b_1 + b_2)$, for an odd prime p, then $p|d_2$. This, however, implies that $p|(b_1 - b_2)$, hence $p|b_1$, and $p^2|D$. Thus, in compounding, m and n are powers of 2 (or are 1). Simple congruences modulo 8 show that d_1 and d_2 (and d_3, if it is integral) are even if and only if $D \equiv -1 \pmod 8$ and odd if and only if $D \equiv -5 \pmod 8$. We now distinguish three cases:

(i) *K is even.* We know that $d_1 - d_2$ is even, and that b_1 and b_2 are odd. We write $b_1 = 4k + r$, $b_2 = 4j + s$, with $r, s = +1$ or $+3$. Then

$$b_1 - b_2 = 4(k - j) + (r - s) = K(d_1 - d_2) \equiv 0 \pmod 4.$$

Hence $r = s$, and $b'' = 2(k + j) + r$, which is odd. Thus $n = 1$.

We now compound the first and second forms, defining b'', m, and n as above, and solving $d_1 x + (b_1 + b_2)y/2 = m$ for x and y. Then

$$\begin{aligned} mz &\equiv (b'' - b_1)x - d_1^2 y \pmod{d_2} \\ &\equiv (b_2 - b_1)x/2 - d_1^2 y \equiv (-K/2)x(d_1 - d_2) - d_1^2 y \\ &\equiv (-K/2)xd_1 - d_1^2 y \equiv (-K/2)(m - y(b_1 + b_2)/2) - d_1^2 y \\ &\equiv (-Km/2) + yK(b_1 + b_2)/4 - d_1^2 y. \end{aligned}$$

But $K(b_1 + b_2)/4 = d_1^2 + d_1 d_2 + d_2^2 \equiv d_1^2 \pmod{d_2}$, hence

$$mz \equiv -Km/2 \pmod{d_2},$$

$$z \equiv -K/2 \pmod{d_2}, \quad \text{since } (m, d_2) = 1.$$

The compounded form is thus $(d_1 d_2, b_1 - Kd_1, C)$, for some integer C. From Eqs. (6), we see that $C = d_3$, so the composition is, remembering $b_1 - Kd_1 = b_2 - Kd_2 = b_3 - Kd_3 = L$,

$$(d_1 d_2, b_3 - Kd_3, d_3) \sim (d_3, -b_3, d_3^2) \sim (d_3, b_3, d_3^2)^{-1}.$$

(ii) *K is odd, and $D \equiv -1 \pmod 8$.* From (7), $4|(b_1 + b_2)$, hence $b_1 \equiv -b_2 \pmod 4$. Write $b_1 = 4k + r$, and $b_2 = 4j + r + 2$. Then $K = (4(k - j) - 2)/(d_1 - d_2)$, which implies that exactly one of $d_1/2$ and $d_2/2$ is odd. We assume, without loss of generality, that $d_1/2$ is odd. Then $m = n = 2$. We solve for x, y, and z as before, and find that $z \equiv -K \pmod{d_2/2}$. The compounded form is then $(d_1 d_2/4, b_1 - Kd_1, t)$ where we again use (6) to find the third term of the form. Since $t \equiv 1 \pmod 8$, and $(u - Kt)/4 = L$, which is odd, we see that $(K - u)/4$ is odd. This implies that

$$(u - Kt)/4 \equiv (1 - t)u/4 + t \pmod{2t};$$

hence

$$F_1 \circ F_2 \sim (d_1 d_2/4, L, t) \sim (t, -(1-t)u/4 + t, v_1) \sim F_3^{-1}.$$

(iii) *K is odd, and* $D \equiv -5 \pmod 8$. Since d_1 is odd, $m = n = 1$. Again, we solve for x, y, and z, and find this time that $z \equiv (d_2 - K)/2 \pmod{d_2}$. Then $F_1 \circ F_2 \sim (d_1 d_2, L + d_1 d_2, J)$, where $J = ((L + d_1 d_2)^2 + D)/4 d_1 d_2$. Using (6), we find $-L - d_1 d_2 + 4J = L + t$, so $(d_1 d_2, L + d_1 d_2, J) \sim (J, L + t, t)$. Now, $(u - Kt)/4 = L$ is even, and $t \equiv 1 \pmod 8$; we see $K \equiv u \pmod 8$. This is sufficient to prove that

$$L + t \equiv u(1-t)/4 + t \pmod{2t};$$

hence

$$(J, L + t, t) \sim (t, -(1-t)u/4 + t, v_1) \sim F_3^{-1},$$

and the theorem is proved.

3. The odd discriminants of complex quadratic number fields are congruent either to -1 or -5 modulo 8. We have so far applied the method of Section 1 only to the former type, beginning with -3321607 as the constant term. The odd discriminants thus obtained are always congruent to -1 modulo 8 because the a of Eq. (1a) are always even. One could also begin with the constant term $-3640387 \equiv -5 \pmod 8$, but the series which arise are inherently less useful, half of the discriminants being even and not fundamental. (It follows from (6) and the representation of $2K$ that the c_i are even if $D \equiv 1 \pmod 8$ and that exactly two of the c_i are odd if $D \equiv 5 \pmod 8$. Thus, for $D \equiv 5 \pmod 8$, the a_i are even, if they are integral, hence $S_i(x)$ is even for odd integers x.)

Using Scholz's theorem [8], we can deduce the 3-rank of the real fields $Q(\sqrt{3D})$ from that of the complex fields $Q(\sqrt{-D})$. However, in all of the eight discriminants found the 3-rank of the corresponding real field is, by the theorem, only two.

The major question which we have not been able to answer has already been raised: Why should one 3-cycle of solutions to $2K = u^2 + 3v^2$ yield integer coefficients a_i, and one 3-cycle not do so? We have noted further that when four 3-cycles exist, as for $K = 728$, only one of these yields integer values a_i.

The fact that quartic polynomials represent discriminants of complex quadratic fields only finitely many times is a limiting condition on the method we have developed. We considered cubic and sextic polynomials first, as they do not have this property. If, in (2), one lets the S_i and C_i be linear, one finds easily that there are no solutions with rational integer coefficients. We were successful in solving (2) with the S_i and C_i monic cubic and quadratic polynomials, respectively, so that $\Delta(x)$ has leading term $-3x^6$. However, $\Delta(x)$ was inherently not squarefree except in rare instances. For this reason we concentrated our attention on the quartic polynomials of Section 1.

Appendix A. The basic method of computation of the class numbers and class groups was suggested by Atkin, who used it to compute some tables of his own. The method of computing the class group was published by Shanks in [9]. The program was written entirely in FORTRAN, and was run in segments, each segment computing the class numbers, groups, and statistics for a block of discriminants of length 200000,

even and odd discriminants comprising different segments. (Thus, one such segment contained the odd discriminants $-D$, $600000 < D < 800000$.) An array of length 50000, CLANO, was used to store the needed information on the discriminants, CLANO(N) corresponding to $D = D(N) = 4N + i + S$, where S is the appropriate multiple of 200000 for the program segment being computed, and i is 0 or -1, depending on the parity of the discriminants in that segment.

The discriminants were first factorized, adding 10000 to CLANO for each prime factor, and adding -1000000 if a factor appeared twice. This allowed an easy separation of the fundamental from the nonfundamental discriminants, as neither the number of factors nor the class number would be large enough to make the entry of CLANO positive later. Also, since the actual class number is only about $\sqrt{D}$, the number of genera could be computed from the number of factors of D by using FORTRAN arithmetic to separate the digits of CLANO from one another.

The class numbers for all discriminants in a segment were computed together by executing a triple loop on the coefficients b, a, and c (from the outermost to the innermost loop) of the binary quadratic form (a, b, c) and then incrementing the counter CLANO(N) for the appropriate $-D(N) = b^2 - 4ac$. That is, instead of fixing a value for D and then computing the reduced forms for that D, we computed all reduced forms with discriminants in the range of the segment and kept a count for each D. Some care was taken to optimize these loops and remove all unnecessary multiplication; D was computed each time by adding to the previous D, rather than by direct computation.

The primary list of discriminants, number of genera, and number of forms per genus was now computed and printed, and a secondary list of "possibly noncyclic" groups was extracted. (In what follows, we describe the computation for an odd p-Sylow subgroup; the suitable changes for the case $p = 2$ are easy, but the description in words is cumbersome.) A group was "possibly noncyclic" in the p-Sylow subgroup if $p^2 | h$, where h is the order of the group (the class number). Each group in the list of possibles was then tested in the following manner: If $h = p^i m$, $(m, p) = 1$, one chooses "at random" (to be described in the next paragraph) up to eleven forms of the group and computes the hp^{1-i}th power of each. Should any of these not be the identity, the group is cyclic, and we proceed to the next discriminant. If that power of each of the eleven forms in the identity, the group is assumed to be noncyclic, and an actual computation of the p-Sylow subgroup is made, under the assumption that the group is noncyclic.

We now describe the "random" method for obtaining forms of a given discriminant: If, for a given $-D$, there is an a such that $-D$ is a quadratic residue modulo a, then there exists a form of discriminant $-D$ and leading coefficient a. We checked through the odd primes under 1000, in increasing order, to find one for which $-D$ was a residue. Taking this prime for the coefficient a, we searched for the smallest b such that $b^2 \equiv -D \pmod{a}$, obtaining a form (a, b, c), which we then reduced. A reasonably thorough testing of this method and a continued use of it have not revealed any obvious patterns in the forms produced, so we have assumed that it was sufficiently random for our purposes.

Appendix B. The smallest D for which the class group of $Q(\sqrt{-D})$ is noncyclic in the p-Sylow subgroup are listed in Table 1, even and odd discriminants being listed where known. No even discriminants with a noncyclic 17-Sylow subgroup were found. We note also that D = 1016083, 1438483, 1663747, 2407267, and 2942227, all (necessarily) prime, have class group *exactly* $C(13) \times C(13)$.

Of interest also are the groups which are noncyclic in more than one Sylow subgroup. There were 418 of these in all. Most of these were $C(12) \times C(12)$, the first (even and odd D) being 64952 and 104255. The first $C(20) \times C(20)$ subgroups occurred for D = 472196 and 280847; the first $C(28) \times C(28)$ subgroups were for D = 858296 and 465719. The class group $C(15) \times C(15)$ for D = 119191 had been found some time ago by A. O. L. Atkin; surprisingly, the next examples are quite large. We list them in Table 2. Throughout Tables 1–10, column A is the discriminant $-D$, column B the factorization of D, and column C the class group of $Q(\sqrt{-D})$, where, for example, 15 × 15 signifies the group $C(15) \times C(15)$.

The question of which finite Abelian groups occur as class groups of quadratic fields has been discussed at length in the literature (for example, [15], [16], and [17]). In Tables 11–13 we list some of the more unusual groups that occurred. Columns A through D are, respectively, the group, the smallest D for which that group occurred, the factorization of D, and the number of occurrences of that group. In Table 11 are listed, for $p \geqslant 3$, the groups which are themselves, or whose principal genera are, p-groups $C(p^a) \times C(p^b)$ with a and $b \geqslant 2$. Note the single example of $p \geqslant 5$. In Table 12 are the 2-groups which contain a $C(4) \times C(4) \times C(4)$ subgroup, that is, the 2-groups whose principal genus has rank 3. There were no groups found with a subgroup $C(p^a) \times C(p^b)$, a and $b \geqslant 3$ and $p > 2$; we list in Table 13, however, the class groups whose principal genus contained a subgroup $C(2^a) \times C(2^b)$, a and $b \geqslant 3$.

Finally, in Tables 14 and 15 we collect some statistics on the frequency of occurrence of noncyclic groups.

TABLE 1

p	A	B	C	A	B	C
3	-3299	prime	3x9	-3896	8.487	3x12
5	-11199	3.3733	5x20	-17944	8.2243	5x10
7	-63499	prime	7x7	-159592	8.19949	7x14
11	-65591	107.613	11x22	-580424*	8.13.5581	22x22
13	-228679*	11.20789	13x26	-703636*	4.175909	13x26
17	-1997799*	3.59.11287	34x34	----------	----------	----------
19	-373391*	67.5573	19x38	-3419828*	4.854957	19x38

TABLE 2

A	B	C	A	B	C
-119191	prime	15x15	-3150391	prime	15x105
-2075343	3.17.40693	30x30	-3358427	349.9623	15x30
-2403659	prime	15x45	-3492051	3.941.1237	30x30
-2690455	5.37.14543	30x30	-3561799	prime	21x63
-2766392	8.59.5861	30x30	-3860484	4.3.321707	30x30
-2982783	3.809.1229	30x30	-3862148	4.67.14411	30x30
-3072743	83.37021	15x60	-3874699	467.8297	15x30

TABLE 3

Groups with a 20 × 20 *subgroup*

A	B	C	A	B	C
-280847	7.53.757	20x20	-2540344	8.17.18679	20x20
-458695	5.199.461	20x20	-2664955	5.29.18379	20x20
-472196	4.97.1217	20x20	-2713144	8.7.48449	20x20
-1323896	8.7.47.503	2x20x20	-2729255	5.19.28729	20x60
-1567495	5.251.1249	20x40	-2814299	17.19.8713	20x40
-1627451	7.29.8017	20x20	-2910615	3.5.61.3181	2x20x20
-1633487	19.149.577	20x40	-2922488	8.401.911	20x40
-1663023	3.457.1213	20x40	-2925944	8.7.52249	20x40
-1751335	5.23.97.157	2x20x20	-2985995	5.199.3001	20x40
-1847795	5.101.3659	20x20	-3044455	5.41.14851	20x40
-2007172	4.337.1489	20x20	-3174951	3.13.81409	20x80
-2025560	8.5.79.641	2x20x20	-3256568	8.7.58153	20x40
-2176955	5.11.39581	20x20	-3270307	17.47.4093	20x20
-2295736	8.31.9257	20x20	-3390483	3.457.2473	20x20
-2326904	8.239.1217	20x60	-3401615	5.7.17.5717	2x20x40
-2452439	11.113.1973	20x120	-3642743	13.17.53.311	2x20x40
-2524247	11.29.41.193	2x20x40	-3972344	8.97.5119	20x80

TABLE 4

Groups with a 28 × 28 *subgroup*

A	B	C	A	B	C
-465719	37.41.307	28x28	-3055571	37.269.307	28x28
-632687	11.113.509	28x28	-3158111	11.53.5417	28x84
-858296	8.17.6311	28x28	-3326771	7.137.3469	28x28
-2471624	8.521.593	28x28			

TABLE 5

Noncyclic 5-Sylow subgroups for $D < 100000$

A	B	C	A	B	C
-11199	3.3733	5x20	-67063	199.337	5x30
-12451	prime	5x5	-67128	8.3.2797	10x10
-17944	8.2243	5x10	-69811	7.9973	5x10
-30263	53.571	5x30	-72084	4.3.6007	10x10
-33531	3.11177	5x10	-74051	prime	5x35
-37363	prime	5x5	-75688	8.9461	5x10
-38047	prime	5x15	-81287	29.2803	5x50
-39947	43.929	5x10	-83767	211.397	5x30
-42871	43.997	5x30	-84271	11.47.163	10x20
-50783	43.1181	5x50	-85099	7.12157	5x10
-53079	3.13.1361	10x20	-85279	107.797	5x40
-54211	23.2357	5x10	-87971	13.67.101	10x10
-58424	8.67.109	10x10	-89751	3.29917	5x60
-61556	4.11.1399	10x20	-90795	3.5.6053	10x10
-62632	8.7829	5x10	-90868	4.22717	5x10
-63411	3.23.919	10x10	-92263	257.359	5x30
-64103	13.4931	5x40	-98591	19.5189	5x90
-65784	8.3.2741	10x10	-99031	167.593	5x30
-66328	8.8291	5x10	-99743	7.14249	5x60
-67031	17.3943	5x80			

TABLE 6

Noncyclic 7-Sylow subgroups for $D < 500000$

A	B	C	A	B	C
-63499	prime	7x7	-268739	31.8669	7x28
-118843	prime	7x7	-272179	prime	7x21
-124043	163.761	7x14	-275636	4.68909	7x42
-149519	prime	7x91	-294935	5.61.967	14x28
-159592	8.19949	7x14	-299627	103.2909	7x28
-170679	3.56893	7x56	-301211	prime	7x21
-183619	139.1321	7x14	-308531	29.10639	7x28
-185723	prime	7x21	-318547	113.2819	7x14
-220503	3.31.2371	14x28	-346883	19.18257	7x28
-226691	prime	7x35	-361595	5.13.5563	14x14
-227387	prime	7x21	-366295	5.73259	7x56
-227860	4.5.11393	14x14	-373655	5.74731	7x84
-236931	3.78977	7x14	-465719	37.41.307	28x28
-240347	prime	7x21	-480059	prime	7x49
-240655	5.48131	7x28	-489576	8.3.20399	14x28
-247252	4.61813	7x14	-491767	37.13291	7x42
-260111	prime	7x77			

TABLE 7

Noncyclic 11-Sylow subgroups

A	B	C	A	B	C
-65591	107.613	11x22	-2659099	23.115613	11x22
-126407	19.6653	11x22	-2661639	3.17.52189	22x44
-175031	383.457	11x66	-2668715	5.7.76249	22x22
-272231	prime	11x33	-2697779	7.385397	11x66
-423335	5.11.43.179	2x22x22	-2741799	3.913933	11x88
-527019	3.175673	11x22	-2747743	43.63901	11x66
-580424	8.13.5581	22x22	-2828680	8.5.70717	22x22
-593183	prime	11x77	-2913679	109.26731	11x132
-680767	prime	11x33	-2934312	8.3.122263	22x22
-694907	571.1217	11x22	-2946299	prime	11x55
-767147	prime	11x33	-3032179	prime	11x33
-857099	prime	11x33	-3037459	127.23917	11x44
-1161239	prime	11x99	-3130027	prime	11x33
-1314676	4.11.29879	22x22	-3131864	8.23.17021	22x44
-1451639	7.207377	11x132	-3152315	5.103.6121	22x22
-1471423	prime	11x33	-3251123	113.28771	11x44
-1654147	11.150377	11x22	-3301883	13.499.509	22x22
-1689371	509.3319	11x66	-3418507	149.22943	11x22
-1734395	5.13.26683	22x22	-3426456	8.3.11.12979	2x22x22
-1764687	3.588229	11x44	-3431179	prime	11x33
-1963419	3.167.3919	22x22	-3497892	4.3.291491	22x22
-2148079	307.6997	11x110	-3645907	883.4129	11x22
-2253971	prime	11x55	-3781607	173.21859	11x110
-2608212	4.3.217351	22x22	-3810631	11.346421	11x132
-2628123	3.876041	11x22	-3894239	prime	11x297

TABLE 8

Noncyclic 13-Sylow subgroups

A	B	C	A	B	C
-228679	11.20789	13x26	-2676383	prime	13x117
-703636	4.175909	13x26	-2708135	5.23.23549	26x78
-1016083	prime	13x13	-2772843	3.924281	13x26
-1022639	prime	13x91	-2793752	8.13.26863	26x26
-1043999	11.107.887	26x52	-2795939	17.163.1009	26x26
-1192367	11.61.1777	26x26	-2942227	prime	13x13
-1201667	503.2389	13x26	-2943271	19.97.1597	26x26
-1277843	7.182549	13x26	-3081748	4.770437	13x26
-1328359	41.179.181	26x26	-3220040	8.5.79.1019	2x26x26
-1384831	7.181.1093	26x26	-3519247	prime	13x65
-1438483	prime	13x13	-3544952	8.347.1277	26x26
-1440659	11.130969	13x52	-3715559	prime	13x143
-1582399	7.13.17389	26x26	-3730568	8.466321	13x52
-1663747	prime	13x13	-3756504	8.3.156521	26x26
-1968323	7.281189	13x26	-3799192	8.474899	13x26
-2074760	8.5.51869	26x26	-3805224	8.3.158551	26x26
-2407267	prime	13x13	-3991559	11.13.103.271	2x26x52
-2524487	7.43.8387	26x52			

TABLE 9

Noncyclic 17-Sylow subgroups

A	B	C	A	B	C
-1997799	3.59.11287	34x34	-2984171	47.63493	17x34
-2667895	5.17.31387	34x34	-3112639	prime	17x85
-2890903	1019.2837	17x34			

TABLE 10

Noncyclic 19-Sylow subgroups

A	B	C	A	B	C
-373391	67.5573	19x38	-3419828	4.854957	19x38
-1078919	prime	19x57	-3479127	3.1159709	19x38
-2505135	3.5.167009	38x38	-3837956	4.959489	19x76

TABLE 11

A	B	C	D	A	B	C	D
9x9	-134059	prime	3	18x18	-727087	37.43.457	18
9x27	-351751	prime	4	18x54	-1871295	3.5.124753	7
9x81	-1332167	prime	1	2x18x18	-2442020	4.5.7.17443	5
9x18	-208084	4.52021	5	25x50	-1390367	11.126397	1
9x54	-690503	11.62773	9				

TABLE 12

A	B	C	D	A	B	C	D
4x4x8	-503659	13.17.43.53	4	4x8x8	-2209467	3.13.181.313	4
4x4x16	-550712	8.23.41.73	6	4x8x16	-1456131	3.61.73.109	1
4x4x32	-863455	5.19.61.149	5	2x4x4x16	-2172651	3.13.17.29.113	2
4x4x64	-3600632	8.7.113.569	1	2x2x4x4x8	-2188920	8.3.5.17.29.37	1

TABLE 13

A	B	C	D	A	B	C	D
16x16	-618947	7.29.3049	16	16x128	-3194495	5.29.22031	1
16x48	-936183	3.313.997	12	32x32	-2365599	3.421.1873	1
16x80	-1831031	29.103.613	3	2x16x16	-804639	3.11.37.659	17
16x112	-1602095	5.11.29129	1	2x16x48	-3228215	5.17.163.233	2
16x32	-971095	5.359.541	17	2x16x32	-1987215	3.5.17.7793	2
16x96	-2747399	43.181.353	1	2x2x16x16	-3909576	8.3.11.59.251	1
16x64	-1008095	5.11.18329	6				

TABLE 14

	A	B	C	D	E	F
Odd D	810578	265739	32.78	32507	12.23	4.01
Even D	405276	166296	41.03	19345	11.63	4.77
Total	1215854	432035	35.53	51852	12.00	4.26

A=number of fundamental discriminants
B=number of possibly noncyclic groups
C=100xB/A
D=number of actually noncyclic class groups
E=100xD/B
F=100xD/A

TABLE 15

Noncyclic p-Sylow subgroups

p=2	A	B	C	D	E	F
Odd D	810578	122971	15.71	20837	16.94	2.57
Even D	405276	101029	24.93	13862	13.72	3.42
Total	1215854	224000	18.42	34699	15.49	2.85

p=3	A	B	C	D	E	F
Odd D	810578	115904	14.30	10132	8.74	1.25
Even D	405276	57264	14.13	4832	8.44	1.19
Total	1215854	173168	14.24	14964	8.64	1.23

p=5	A	B	C	D	E	F
Odd D	810578	37485	4.62	1419	3.79	.18
Even D	405276	17639	4.35	648	3.67	.16
Total	1215854	55124	4.53	2067	3.75	.17

p=7	A	B	C	D	E	F
Odd D	810578	16877	2.08	295	1.75	.04
Even D	405276	7620	1.88	149	1.96	.04
Total	1215854	24497	2.01	444	1.81	.04

A=number of fundamental discriminants
B=number of possibly noncyclic p-Sylow subgroups
C=100xB/A
D=number of actually noncyclic p-Sylow subgroups
E=100xD/B
F=100xD/A

Department of Mathematics
University of Illinois at Chicago Circle
Chicago, Illinois 60680

1. MAURICE CRAIG, "A type of class group for imaginary quadratic fields," *Acta Arith.*, v. 22, 1973, pp. 449–459. MR 47 #6647.

2. 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.

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

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

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

6. 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.

6a. DANIEL SHANKS, "Class groups of the quadratic fields found by Diaz y Diaz," *Math. Comp.*, v. 30, 1976, pp. 173–178.

7. ERICH HECKE, *Vorlesungen über die Theorie der algebraischen Zahlen*, Chelsea, New York, 1970. MR 50 #4524.

8. ARNOLD SCHOLZ, "Über die Beziehung der Klassenzahlen quadratischer Körper zueinander," *J. Reine Angew. Math.*, v. 166, 1932, pp. 201–203.

9. DANIEL SHANKS, "Class number, a theory of factorization, and genera," *Proc. Sympos. Pure Math.*, v. 20, Amer. Math. Soc., Providence, R. I., 1971, pp. 415–440. MR 47 #4932.

10. R. A. LIPPMAN, "Note on irregular discriminants," *J. London Math. Soc.*, v. 38, 1963, pp. 385–386. MR 28 #1174.

11. E. T. ORDMAN, "Tables of class numbers for negative prime discriminants," UMT 29, *Math. Comp.*, v. 23, 1969, p. 458.

12. M. NEWMAN, "Table of the class number $h(-p)$ for p prime, $p \equiv 3 \pmod 4$, $101987 \leqslant p \leqslant 166807$," UMT 50, *Math. Comp.*, v. 23, 1969, p. 683.

13. RICHARD B. LAKEIN & SIGEKATU KURODA, "Tables of class numbers $h(-p)$ for fields $Q(\sqrt{-p})$, $p \leqslant 465071$," UMT 39, *Math. Comp.*, v. 24, 1970, pp. 491–493.

14. H. WADA, "A table of ideal class groups of imaginary quadratic fields," *Proc. Japan Acad.*, v. 46, 1970, pp. 401–403.

15. S. CHOWLA, "An extension of Heilbronn's class number theorem," *Quart. J. Math. Oxford Ser.*, v. 5, 1934, pp. 304–307.

16. W. NARKIEWICZ, "Class number and factorization in quadratic number fields," *Colloq. Math.*, v. 17, 1967, pp. 167–190. MR 36 #3750.

17. DANIEL SHANKS, "On Gauss's class-number problems," *Math Comp.*, v. 23, 1969, pp. 151–163. MR 41 #6814.