

## Class Groups of Quadratic Fields. II

By Duncan A. Buell\*

*Dedicated to Daniel Shanks on the occasion of his 70th birthday*

**Abstract.** A computation has been made of the noncyclic class groups of imaginary quadratic fields  $Q(\sqrt{-D})$  for even and odd discriminants  $-D$  from 0 to  $-25000000$ . Among the results are that 95% of the class groups are cyclic, and that  $-11203620$  and  $-18397407$  are the first discriminants of imaginary quadratic fields for which the class group has rank three in the 5-Sylow subgroup. The latter was known to be of rank three; this computation demonstrates that it is the first odd discriminant of 5-rank three or more.

**1. Introduction.** In [2] is described a computation of class numbers and class groups of imaginary quadratic fields  $Q(\sqrt{-D})$  for even and odd discriminants  $-D$  from 0 to  $-4000000$ . This computation has been used in various contexts [1], [3], [4], [7]. Due to interest in a new factoring technique which utilizes the nature and structure of imaginary quadratic class numbers and class groups [8], a further computation and statistical analysis was made of these numbers and groups [5]. To further define the nature of class groups, we have rewritten the programs of [2] and computed all noncyclic class groups of imaginary quadratic fields  $Q(\sqrt{-D})$  for even and odd discriminants  $-D$  from 0 to  $-25000000$ . This computation and its results are summarized in this paper.

We have followed the convention of [2] with regard to the 2-Sylow subgroup. Since the rank of that subgroup is determined by the number of prime factors in the discriminant  $-D$  (theorem of Gauss) for the purposes of our computation, the 2-Sylow subgroup of a class group is called "noncyclic" if the 2-Sylow subgroup of the subgroup of squares in the class group is noncyclic.

All programming was done in C on a VAX 11/780\*\* owned by the Computer Science Department, Louisiana State University, running 4.2BSD UNIX\*\*. Some of the statistical summaries were obtained using S.

### 2. The Computation.

**2.1. General Description.** The basic computation is similar to that of [2]. Even and odd discriminants were dealt with separately. Separate computations were done for discriminants in ranges of integers in blocks of 200000, using one long array. (Thus, one such computation would be for odd discriminants between  $-600000$  and  $-800000$ .) A first pass through the array removed integers which were not discriminants of quadratic fields by flagging integers with odd prime squares as factors or of

---

Received August 1, 1984; revised September 18, 1984 and August 8, 1985.

1980 *Mathematics Subject Classification*. Primary 10-04, 12A25, 10C07.

\*Research supported in part by NSF grant DCR-8311580.

\*\*VAX is a trademark of Digital Equipment Corporation, UNIX is a trademark of Bell Laboratories.

the wrong congruence class modulo 4. Then, for each remaining discriminant, a triple loop counted the binary quadratic forms of that discriminant, obtaining the class number, the class number of the group of forms and of the field being identical for imaginary fields.

The class numbers having thus been computed, a list was made of discriminants with “possibly noncyclic” groups by removing from the existing list those discriminants whose class numbers were not divisible by the square of at least one odd prime (or, for the 2-Sylow subgroup, the discriminants with fewer than 4 genera or without a factor of 4 in the number of norms per genus). Each of the possibly noncyclic  $p$ -Sylow subgroups of the remaining groups was then tested. The maximal order of any element in a class group being  $FPG/p$ , where  $FPG$  is the number of forms per genus for the discriminant, forms were generated “at random” and their  $FPG/p$ th powers computed. If any of these was not the identity, the group was known to be cyclic. If, in testing 15 “randomly generated” forms, only the identity was found for the  $FPG/p$ th powers, the group was determined to be “probably noncyclic” and the  $p$ -Sylow subgroup explicitly computed. Data for groups determined to be noncyclic were written to a disk file, and statistics and summaries produced after the computation was completed.

The “random generation” of binary quadratic forms was this: A form  $(a, b, c)$  of discriminant  $-D$  exists if the congruence  $x^2 \equiv -D \pmod{4\alpha}$  is solvable. For odd primes  $\alpha$ , this is equivalent to having the Jacobi symbol  $[-D/\alpha]$  equal to  $+1$ . Our program simply ran through the primes in sequence as possible first coefficients  $a$  and found and reduced the possible forms for the discriminant in question.

We mention that in this computation all “probably noncyclic” groups were completely determined. This was not the case in the previous computation [2]. In that computation, a “probably noncyclic” group with a  $p$ -Sylow subgroup of order  $p^k$  was declared to be noncyclic of the form  $C(p) \times C(p^{k-1})$  if a form of order  $p^{k-1}$  was found. Similarly, “probably noncyclic”  $p$ -Sylow subgroups of order  $p^2$  and  $p^3$  were simply declared to be  $C(p) \times C(p)$  and  $C(p) \times C(p^2)$ , respectively. No differences were found between the results of the previous computation and the results of this one, however.

**2.2. The Group Computation.** The algorithm for computing class groups is derived from that of Shanks [10], is essentially the same as that of [2], and is given as Algorithm A below. The decomposition of an Abelian  $p$ -Sylow subgroup (written multiplicatively) begins as follows.

- a. Obtain a form,  $f_1$ , of order a power of  $p$ .
- b. Compute the  $p$ -exponent  $\text{ord}_1$  such that  $p^{\text{ord}_1}$  is the order of element  $f_1$ .
- c. Save the penultimate  $p$ -powers  $\{f_1^{i(p^{\text{ord}_1-1})}; 1 \leq i \leq (p-1)\}$  of  $f_1$ .
- d. Obtain a form  $f_2$  and compute  $\text{ord}_2$  similarly.
- e. If  $\text{ord}_2 > \text{ord}_1$ , exchange  $f_1$  and  $f_2$  and store the penultimate  $p$ -powers of the new  $f_1$ .
- f. If

$$f_2^{p^{\text{ord}_2-1}} = f_1^{i(p^{\text{ord}_1-1})},$$

for some  $i$ , then a dependence exists between  $f_1$  and  $f_2$ . This is removed by

replacing  $f_2$  with

$$f_2 \cdot f_1^{-i(p^{\text{ord}_1 - 1})},$$

and recomputing  $\text{ord}_2$ , repeating the test for dependence in this step until we find we have independent elements.

g. Having found two independent elements, if the  $p$ -orders sum to the  $p$ -power in the order of the group, we are, of course, done. If not, we find a third element, remove the dependence of this element on elements  $f_1$  and  $f_2$ , and continue until we have exhausted the  $p$ -Sylow subgroup. We note that removing dependence requires comparing the third element's penultimate  $p$ -power against the penultimate powers of the first and second elements of the cross products of those powers.

For quadratic class groups, several facts were taken into account in implementing the algorithm. First, our previous computation showed that 95.74% of the class groups for discriminants from 0 to  $-4000000$  were cyclic. Further, those noncyclic groups were in general "almost" cyclic, in the sense that the noncyclic  $p$ -Sylow subgroups were usually  $C(p) \times C(p^k)$ . Very few groups had rank three. Thus, we assumed that it would be normal for the groups to be easily computed and to be of rank two. Once the program established the fact that a group had rank three, therefore, it simply wrote this fact to the disk file, and went on to the next discriminant. In a very few cases, the entire decomposition had not at this point been found, and we performed a separate computation to finish the decomposition and "patch" the disk file of data on noncyclic groups. This happened for about 40 discriminants. No groups were found of rank larger than three for an odd prime Sylow subgroup. Although a detailed analysis was not undertaken, it is our general impression that this decomposition algorithm works well on quadratic class groups of this size.

**3. Results.** We present in Tables 1–4 a summary of the frequencies of occurrence of noncyclic  $p$ -Sylow subgroups and the first occurrences of those groups. In Table 1 we include counts of both noncyclic class groups and noncyclic subgroups, although

TABLE 1  
*Summary of noncyclic groups*

	A	B	C	D	E	F
Even	2533009	1084644	142224	143833	13.1	5.61
Odd	5066042	1758766	239409	241845	13.6	4.73
Total	7599051	2843410	381633	385678	13.4	5.02

A—number of discriminants

B—number of possibly noncyclic discriminants

C—number of noncyclic class groups

D—number of noncyclic subgroups

E— $100 \cdot C/B$

F— $100 \cdot C/A$

TABLE 2  
*Summary for individual  $p$ -Sylow subgroups*

A	B	C	D	E	F
2-Even	670838	26.48	103036	4.07	15.36
2-Odd	859385	16.96	157523	3.11	18.33
2-Total	1530223	20.14	260559	3.43	17.03
3-Even	372238	14.70	34992	1.38	9.40
3-Odd	749306	14.79	72211	1.43	9.64
3-Total	1121544	14.76	107203	1.41	9.56
5-Even	118144	4.66	4462	0.18	3.78
5-Odd	242187	4.78	9365	0.18	3.87
5-Total	360331	4.74	13827	0.18	3.84
7-Even	54338	2.15	1096	0.04	2.02
7-Odd	113926	2.25	2162	0.04	1.90
7-Total	168264	2.21	3258	0.04	1.94
11-Even	16883	0.67	142	0.01	0.84
11-Odd	40007	0.79	339	0.01	0.85
11-Total	56890	0.75	481	0.01	0.85
13-Even	10531	0.42	71	0.00	0.67
13-Odd	26737	0.53	160	0.00	0.60
13-Total	37268	0.49	231	0.00	0.62
17-Even	4302	0.17	17	0.00	0.40
17-Odd	13252	0.26	44	0.00	0.33
17-Total	17554	0.23	61	0.00	0.35
19-Even	2783	0.11	12	0.00	0.43
19-Odd	9756	0.19	28	0.00	0.29
19-Total	12539	0.17	40	0.00	0.32
23-Even	1206	0.05	3	0.00	0.25
23-Odd	5475	0.11	10	0.00	0.18
23-Total	6681	0.09	13	0.00	0.19
29-Even	320	0.01	2	0.00	0.63
29-Odd	2634	0.05	1	0.00	0.04
29-Total	2954	0.04	3	0.00	0.10
31-Even	239	0.01	0	0.00	0.00
31-Odd	2063	0.04	1	0.00	0.05
31-Total	2302	0.03	1	0.00	0.04
41-Even	22	0.00	0	0.00	0.00
41-Odd	638	0.01	1	0.00	0.16
41-Total	660	0.01	1	0.00	0.15

A—prime  $p$

B—number of possibly noncyclic discriminants

C—possibly noncyclic discriminants as a % of the total

D—number of noncyclic  $p$ -Sylow subgroups

E—actually noncyclic  $p$ -Sylow subgroups as a % of total

F—actually noncyclic  $p$ -Sylow subgroups as a % of possible

TABLE 3  
*Count of possibly noncyclic  $p$ -Sylow subgroups  
 ( for primes  $p$  with no noncyclic groups found )*

$p$	Even $D$	Odd $D$	Total
37	69	1050	1119
43	19	556	575
47	5	367	372
53	0	213	213
59	0	102	102
61	0	97	97
67	0	59	59
71	0	36	36
73	0	23	23
79	0	25	25
83	0	9	9
89	0	4	4
97	0	1	1

TABLE 4  
*First occurrences of noncyclic  $p$ -Sylow subgroups*

A	B	C	D	E
3	3896	$3 \times 12$	3299	$3 \times 9$
5	17944	$5 \times 10$	11199	$5 \times 20$
7	159592	$7 \times 14$	63499	$7 \times 7$
11	580424	$22 \times 22$	65591	$11 \times 22$
13	703636	$13 \times 26$	228679	$13 \times 26$
17	4034356	$17 \times 34$	1997799	$34 \times 34$
19	3419828	$19 \times 38$	373391	$19 \times 38$
23	11137012	$23 \times 46$	7472983	$23 \times 46$
29	16706324	$58 \times 58$	20113607	$29 \times 116$
31	—	—	11597903	$31 \times 62$
41	—	—	6112511	$41 \times 82$

- A—prime  $p$
- B—first even discriminant with noncyclic  $p$ -Sylow subgroup
- C—decomposition of class group
- D—first odd discriminant with noncyclic  $p$ -Sylow subgroup
- E—decomposition of class group

only a very small fraction of class groups turned out to be noncyclic in more than one  $p$ -Sylow subgroup. In Table 5 we list all the class groups found with a noncyclic  $p$ -Sylow subgroup for  $p > 19$ . In Tables 6–8 we detail information about noncyclic groups with  $p^3 | h$  for  $p \geq 5$ .

The most unique groups found were those for discriminants  $-11203620$ , with class group  $C(10) \times C(10) \times C(10)$ , and  $-18397407$ , with class group  $C(5) \times C(10) \times C(40)$ . The latter was given in a list of rank-three groups by Schoof [9], but the former is apparently new.

TABLE 5  
*Groups noncyclic in a  $p$ -Sylow subgroup for  $p > 19$*

Disc	Group	Disc	Group
6112511	$41 \times 82$	14969711	$2 \times 46 \times 46$
7472983	$23 \times 46$	16706324	$58 \times 58$
7814559	$46 \times 46$	18359043	$23 \times 46$
11137012	$23 \times 46$	20113607	$29 \times 116$
11597903	$31 \times 62$	20859463	$23 \times 69$
11836723	$23 \times 23$	21360324	$46 \times 446$
12919471	$23 \times 92$	22287687	$46 \times 46$
13034696	$23 \times 92$	23855464	$29 \times 58$
14115151	$46 \times 46$	24482399	$23 \times 207$

TABLE 6  
*Noncyclic groups for which  $125 \mid h$*

Group	First odd $D$	First even $D$	Total number
$5 \times 25$	258563	—	11
$5 \times 125$	1287491	—	33
$5 \times 625$	258563	—	7
$5 \times 50$	50783	178004	78
$5 \times 250$	1287491	2189204	74
$25 \times 50$	258563	—	2
$10 \times 50$	309263	702456	243
$10 \times 250$	2177951	9059636	68
$50 \times 50$	—	9623444	1
$5 \times 10 \times 40$	18397407	—	1
$2 \times 10 \times 50$	1337479	2340680	236
$2 \times 10 \times 250$	15945095	—	3
$10 \times 10 \times 10$	—	11203620	1
$2 \times 2 \times 10 \times 50$	4798335	10865256	55

TABLE 7  
*Noncyclic groups for which  $343 \mid h$*

Group	First odd $D$	First even $D$	Total number
$7 \times 49$	480059	—	13
$7 \times 343$	4603007	—	4
$7 \times 98$	1984715	890984	55
$14 \times 98$	2249295	3617480	73
$2 \times 14 \times 98$	9599159	13944644	12

TABLE 8

*Groups with  $p^3 | h$  with  $p \geq 11$* 

$D$	Group	$D$	Group
7948999	$11 \times 121$	19461503	$11 \times 242$
9055019	$11 \times 121$	24557096	$11 \times 121$
9670583	$11 \times 121$	14127343	$13 \times 169$
12139691	$11 \times 121$	17803439	$19 \times 361$
19380719	$11 \times 363$		

TABLE 9

*Groups with high powers of 2 in two cyclic factors*

Disc	Group	Disc	Group
6342959	$16 \times 256$	21025623	$32 \times 64$
12993671	$32 \times 128$	22128095	$64 \times 64$
13263095	$32 \times 192$	22209799	$16 \times 256$
14060036	$32 \times 64$	22947695	$16 \times 256$
16834223	$16 \times 256$	23144495	$32 \times 192$
17317119	$16 \times 256$	23429156	$32 \times 64$
18961895	$16 \times 256$	24475919	$32 \times 256$

One question which occasionally arises is that of which groups appear as class groups of quadratic fields. Although an exhaustive search did not seem worthwhile, we did consider the groups of odd order (which correspond to prime discriminants) of order less than 1000. Of these, the only groups of rank two which did not appear were  $C(p) \times C(p)$  for  $p = 11, 19, 29,$  and  $31,$  and  $C(25) \times C(25)$ . The only groups of rank three which did occur were  $C(3) \times C(3) \times C(33), C(3) \times C(3) \times C(69), C(3) \times C(3) \times C(99),$  and  $C(3) \times C(3) \times C(105)$ .

We present in Table 9 the groups for which the 2-Sylow subgroup (of the subgroup of squares) had order at least 512 and the first cyclic factor was of order at least 8. And finally, in Table 10, we present all class groups which were noncyclic in two different  $p$ -Sylow subgroups for odd primes  $p$ .

It is to be noted that the frequency of noncyclic 3-Sylow and 5-Sylow subgroups (1.14% and 0.18%, respectively, from Table 2) are not substantially different from the heuristically conjectured frequencies of Cohen and Lenstra [6], which are 1.167% and 0.158%, respectively, for subgroups  $C(3) \times C(3)$  and  $C(5) \times C(5)$ , to which must be added percentages of lower order for more complex subgroups.

*Remark.* In our computation, we called a class group “noncyclic” in the 2-Sylow subgroup if the 2-Sylow subgroup of the subgroup of squares was noncyclic. In all our tables, however, when groups are explicitly presented, the group that is presented is the full class group, not just the subgroup of squares.

TABLE 10  
*Groups noncyclic in two odd-Sylow subgroups*

Group	1st even $D$	1st odd $D$	Group	1st even $D$	1st odd $D$
$15 \times 15$	—	119191	$21 \times 84$	24924488	—
$15 \times 30$	—	3358427	$21 \times 126$	—	4620215
$15 \times 45$	—	2403659	$21 \times 147$	—	24565367
$15 \times 60$	7773124	3072743	$21 \times 168$	24594884	—
$15 \times 75$	—	10064191	$21 \times 189$	—	20532511
$15 \times 90$	11044456	7153015	$21 \times 231$	—	24294143
$15 \times 105$	—	3150391	$21 \times 378$	—	21657191
$15 \times 120$	4587656	7932539	$30 \times 30$	2766392	2075343
$15 \times 135$	—	12057919	$30 \times 60$	6006356	4425351
$15 \times 150$	11358104	21307739	$30 \times 90$	11912984	6567311
$15 \times 165$	—	10181471	$30 \times 120$	24481784	17414135
$15 \times 180$	—	5046527	$30 \times 150$	—	9763511
$15 \times 210$	—	18016831	$30 \times 180$	—	16911191
$15 \times 225$	—	8396639	$30 \times 210$	—	23996759
$15 \times 240$	—	8196191	$33 \times 33$	—	22479739
$15 \times 270$	—	14348903	$33 \times 66$	22297448	—
$15 \times 285$	—	9609071	$33 \times 99$	—	14898623
$15 \times 300$	—	13017119	$35 \times 35$	—	19399067
$15 \times 360$	—	19260095	$42 \times 42$	16053944	7192015
$15 \times 450$	—	23224151	$70 \times 70$	—	21428391
$15 \times 480$	—	17896199	$126 \times 126$	—	8209319
$15 \times 525$	—	23906711	$2 \times 30 \times 30$	11905176	5486327
$21 \times 21$	—	8847427	$2 \times 30 \times 60$	21140216	7814015
$21 \times 42$	16574248	6481447	$2 \times 30 \times 90$	—	17535791
$21 \times 63$	—	3561799	$2 \times 42 \times 42$	—	19701647

**4. Note.** The data which form the output of the group computation currently exist online on the Computer Science Department's VAX computer. The author is willing to respond to limited requests from interested parties, or to provide copies of the data if supplied with a magnetic tape.

Computer Science Department  
Louisiana State University  
Baton Rouge, Louisiana 70803

1. JOSEPH BLASS & RAY STEINER, "On the equation  $y^2 + k = x^7$ ," *Utilitas Math.*, v. 13, 1978, pp. 293–297.
2. DUNCAN A. BUELL, "Class groups of quadratic fields," *Math. Comp.*, v. 30, 1976, pp. 610–623.
3. DUNCAN A. BUELL, "Small class numbers and extreme values of  $L$ -functions of quadratic fields," *Math. Comp.*, v. 31, 1977, pp. 786–796.
4. DUNCAN A. BUELL, H. C. WILLIAMS & KENNETH S. WILLIAMS, "On the imaginary bicyclic bi-quadratic fields of class-number 2," *Math. Comp.*, v. 31, 1977, pp. 1034–1042.
5. DUNCAN A. BUELL, "The expectation of success using a Monte Carlo factoring method—some statistics on quadratic class numbers," *Math. Comp.*, v. 43, 1984, pp. 313–327.



6. H. COHEN & H. W. LENSTRA, JR., "Heuristics on class groups of number fields," in *Number Theory* (H. Jager, ed.), Lecture Notes in Math., vol. 1068. Springer-Verlag, Berlin, 1984, pp. 33–62.
7. FRANZ-PETER HEIDER & BODO SCHMITHALS, "Zur Kapitulation der Idealklassen in unverzweigten primzyklischen Erweiterungen," *J. Reine Angew. Math.*, v. 336, 1983, pp. 1–25.
8. C. P. SCHNORR & H. W. LENSTRA, JR., "A Monte Carlo factoring algorithm with linear storage," *Math. Comp.*, v. 43, 1984, pp. 289–312.
9. R. J. SCHOOF, "Class groups of complex quadratic fields," *Math. Comp.*, v. 41, 1983, pp. 295–302.
10. DANIEL SHANKS, *Class Number, A Theory of Factorization and Genera*, Proc. Sympos. Pure Math., vol. 20, Amer. Math. Soc., Providence, R.I., 1969, pp. 415–440.