

# Computation of the Ideal Class Group of Certain Complex Quartic Fields

By Richard B. Lakein

**Abstract.** The ideal class group of quartic fields  $K = F(\sqrt{\mu})$ , where  $F = \mathbf{Q}(i)$ , is calculated by a method adapted from the method of cycles of reduced ideals for real quadratic fields. The class number is found in this way for 5000 fields  $K = F(\sqrt{\pi})$ ,  $\pi \equiv \pm 1 \pmod{4}$ ,  $\pi$  a prime of  $F$ . A tabulation of the distribution of class numbers shows a striking similarity to that for real quadratic fields with prime discriminant. Also, two fields were found with noncyclic ideal class group  $C(3) \times C(3)$ .

**1. Introduction.** In a famous paper of 1842, Dirichlet [1] extended Gauss' theory of binary quadratic forms to forms whose coefficients are Gaussian integers. In modern terms, he studied quadratic extension fields  $K$  of the Gauss field  $F = \mathbf{Q}(i)$ . The high point of the paper is the beautiful theorem that when  $K$  is the composite of quadratic fields, so  $K = \mathbf{Q}(\sqrt{m}, \sqrt{-m})$ , the class number of  $K$  equals the product of the class numbers of the quadratic subfields  $\mathbf{Q}(\sqrt{m})$ ,  $\mathbf{Q}(\sqrt{-m})$ , or one-half this product, with a simple criterion to distinguish the two cases.

In case  $K$  is not of this special form—so  $K = F(\sqrt{\mu})$ ,  $\mu$  a squarefree Gaussian integer which is neither real nor purely imaginary—then  $K/\mathbf{Q}$  is a quartic, non-Galois extension with no quadratic subfield except  $F$ . In this paper, a modified version of the classical method for real quadratic fields, counting periods of reduced ideals, is adapted to the relative quadratic extension  $K/F$  and used to calculate the class number  $h$  of  $K$ .

In a previous paper [8], I calculated, for 1000 fields  $K$ , the class number  $h$ —or rather a close approximation to  $h$ , by estimating the Dirichlet  $L$ -series in the analytic class number formula. Here, the class number is calculated exactly, by finding the ideal class group. The results of the earlier (approximate) computation are here confirmed and extended to 5000 cases. The remarkable empirical distribution of class numbers for real quadratic prime discriminants—80% have  $h = 1$ , 10% have  $h = 3$ , etc.—occurs in this quartic situation, as first reported in [8]. At the end of the paper, we tabulate the distribution for the 5000 cases, along with the corresponding data for real quadratic fields. Finally, we note that, in 1006 cases with  $h > 1$ , the computation found just 2 cases with noncyclic ideal class group:  $C(3) \times C(3)$ .

In Section 2, we discuss the fields  $K$  and explain why the method for the quadratic case must be modified. The method is given in Section 3, and, in Section 4, the numerical results are discussed.

**2. The Quartic Field  $K$ .** Let  $F = \mathbf{Q}(i)$ , the Gauss field, and  $G = \mathbf{Z}[i]$ , the Gaussian integers. Let  $K = F(\sqrt{\mu})$ , where  $\mu \in G$ , squarefree, and let  $\mathbf{I}$  be the ring of algebraic integers of  $K$ . Then (see [2]),  $\mathbf{I}$  has a relative integral basis  $1, \Omega$  over  $G$ ,

---

Received May 16, 1973.

AMS (MOS) subject classifications (1970). Primary 12A30, 12A50; Secondary 10F20, 12A05.

Copyright © 1974, American Mathematical Society

$I = G[\Omega]$ , where

$$\begin{aligned}\Omega &= \tfrac{1}{2}(\epsilon + \sqrt{\mu}), \epsilon = 1, i, & \text{if } \mu \equiv \epsilon^2 \equiv \pm 1 \pmod{4}, \\ &= (1 + \sqrt{\mu})/(1 + i), & \text{if } \mu \equiv \pm 1 + 2i \pmod{4}, \\ &= \sqrt{\mu}, & \text{otherwise.}\end{aligned}$$

The relative discriminant  $\delta$  of  $K/F$  is  $\delta = \mu$ ,  $2\mu$ , or  $4\mu$ , respectively, while the absolute discriminant of  $K$  is  $D = 16N\delta$ . ( $N\delta = |\delta|^2 = \text{norm}$ .) An integral ideal has a canonical  $G$ -basis

$$\alpha = [\alpha, \beta + \gamma\Omega], \quad \nu(\beta + \gamma\Omega) \equiv 0 \pmod{\alpha},$$

where  $\nu$  denotes the relative norm from  $K$  to  $F$ . Any ideal is equivalent to (in the same ideal class as) a *primitive* ideal (no factor in  $F$ ) having  $\gamma = 1$ . A primitive ideal  $\alpha = [\alpha, \beta + \Omega]$  has relative norm  $\alpha$  and absolute norm  $N\alpha = N\alpha = |\alpha|^2$ . As in the quadratic case, we make the correspondence

$$(1) \quad \alpha = [\alpha, \beta + \Omega] \leftrightarrow A = (\beta + \Omega)/\alpha,$$

where  $A$  is a quadratic irrational over  $F$ .

In analogy to the quadratic case, two ideals  $\alpha_1, \alpha_2$  are equivalent if and only if the corresponding quadratic irrationals  $A_1, A_2$  are equivalent complex numbers:

$$A_2 = (aA_1 + b)/(cA_1 + d), \quad a, b, c, d \in G, ad - bc = \pm 1, \pm i.$$

Recall that, in the quadratic case, one calculates the periodic continued fractions (CF's) of the quadratic irrationals, each pure period representing an ideal class of the quadratic field. Thus, one simply counts the number of distinct periods to obtain the class number. This is essentially the method used to construct the tables of Ince [5] and others. A complex CF will be introduced for our quartic fields, after we note some other analogies to the quadratic case.

The decomposition of a prime  $\pi$  of  $F$  in  $K$  is quite similar to the quadratic case—see [2]. In particular,  $\pi$  splits in  $K$ ,  $\pi = \wp\wp'$ , if and only if  $\delta$  is a quadratic residue of  $\pi$  (for  $\pi \neq 1 + i$ ). If  $\pi = 1 + i$  and  $\delta = \mu \equiv \pm 1 \pmod{4}$ ,  $\pi$  splits if and only if  $\delta \equiv \pm 1 \pmod{4 + 4i}$ . The group of units of  $K$  has one fundamental unit  $E_0$ . Finally, if  $\delta = \mu = \pi$  is a Gaussian prime, we say  $K$  has *prime discriminant*; as in the quadratic case, for such a field the class number is odd.

There is a complex generalization of continued fractions due to Hurwitz [3]. It generalizes not the usual CF but the “nearest integer” CF (which can be used for the real quadratic calculations). The complex CF is defined by partitioning the complex plane into unit squares  $U(a)$  centered at points  $a \in \mathbb{Z}[i]$ :

$$U(a) = \{a + u + vi \mid u, v \text{ real}, -\tfrac{1}{2} \leq u < \tfrac{1}{2}, -\tfrac{1}{2} \leq v < \tfrac{1}{2}\}.$$

If  $z \in U(a)$ , we say that  $a$  is the nearest Gaussian integer to  $z$ . Now, given a complex number  $x$ , we expand it in a simple CF:

$$(2) \quad x = x_0 = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots + \frac{1}{a_n + \frac{1}{x_{n+1}}}}} = (a_0, a_1, \dots, a_n, x_{n+1})$$

where  $x_n = a_n + 1/x_{n+1}$ , and the partial quotient  $a_n$  is the nearest Gaussian integer to  $x_n$ .

As expected, the CF for  $x$  terminates (some  $x_n = a_n \in \mathbf{Z}[i]$ )  $\Leftrightarrow x \in F$ ; and the CF for  $x$  is periodic  $\Leftrightarrow x$  is quadratic irrational over  $F$ . Furthermore, for a given discriminant  $\delta$ , there are only a finite number of distinct periods. However, unlike the situation in the real quadratic case, it is not the case that distinct periods always correspond to distinct ideal classes. A preliminary computation produced a field with two distinct periods representing the same class. Details will be given in Section 4.

Thus, it is preferable to calculate with ideals, making use of the structure of the ideal class group. There is a helpful analogue to the well-known "Gauss bound" for the fields  $K$  ([6],[7]). In every ideal class of the field  $K = F(\sqrt{\delta})$  with relative discriminant  $\delta$ , there is an integral ideal  $\mathfrak{a}$  with norm  $N\mathfrak{a} \leq B = D^{1/2}/8 = \frac{1}{2}\sqrt{N\delta}$ . (The corresponding "Gauss bound" for the real quadratic fields is  $\frac{1}{2}\sqrt{d}$ .) So it is sufficient to find all primitive ideals of  $K$  with norm  $\leq B$  and determine how many ideal classes are represented. A further simplification comes from observing that such ideals are products of prime ideals  $\mathfrak{p} = [\pi, \rho + \Omega]$  with norm  $N\mathfrak{p} = N\pi \leq B$ , so the class group can be generated starting with these prime ideals.

**3. The Method for Fields  $K$  with Prime Discriminant.** These fields are obtained by generating successive rational primes  $P \equiv 1 \pmod{8}$ , with  $P = N\delta = a^2 + b^2$ ,  $a, b > 0$ ,  $4|b$ , so  $\delta = a + bi \equiv \pm 1 \pmod{4}$ . Then  $K = F(\sqrt{\delta})$ . Since  $\delta$  itself is the only prime that ramifies, using the "Gauss bound," we need only consider primes  $\pi$  which split in  $K$ .

(I) Given  $\delta$ , determine which  $\pi$  with  $N\pi \leq B = \frac{1}{2}\sqrt{P}$  split in  $K$ , which we denote by  $\chi(\pi) = +1$ . First,  $\chi(1+i) = +1 \Leftrightarrow \delta \equiv \pm 1 \pmod{4} + 4i$ . For  $\pi \neq 1+i$ , we calculate a "Gaussian Jacobi symbol"  $\chi(\pi)$ :

$$\chi(\pi) = [\delta/\pi] = +1 \Leftrightarrow \delta \equiv x^2 \pmod{\pi}, \quad x \in G.$$

The calculation of this symbol is like that of the ordinary rational Jacobi symbol, except of course for using the quadratic reciprocity law in  $F$  ([1, p.556],[6, p.390]). Note that if  $N\pi = \pi\bar{\pi} = p$ , we need compute only  $\chi(\pi)$ ; then  $\chi(\bar{\pi}) = \chi(\pi)(P/p)$ , the last a Legendre symbol in  $\mathbf{Q}$ . Those primes  $\pi$  for which  $\chi(\pi) = +1$  are stored in an array  $S$ ; they split in  $K$ ,  $\pi = \mathfrak{p}\mathfrak{p}'$ , where  $\mathfrak{p} = [\pi, \rho + \Omega]$ , and the ideals  $\mathfrak{p}$  generate the class group. In particular,  $h = 1$  if and only if these ideals  $\mathfrak{p}$  are all principal.

(II) Next, the basis number  $\Omega = \frac{1}{2}(\epsilon + \sqrt{\delta})$ , which corresponds by (1) to the unit ideal  $[1, \Omega]$ , is expanded in a CF, (2) until the end of the partial period is reached, where a complete quotient recurs, possibly with a unit factor  $i^e$ . That is, we set  $x_0 = \Omega$  and let the complete quotients and corresponding ideals be

$$(3) \quad x_n = \Omega_n = (b_n + \Omega)/a_n \leftrightarrow [a_n, b_n + \Omega].$$

In all cases computed,  $x_1 = \Omega_1$  is purely periodic; it may always be the case. So, eventually,  $x_m = (b_m + \Omega)/i^e$ ,  $x_{m+1} = i^e x_1$ , and the primitive partial period is  $\Omega_1 = x_1 = (c_1, c_2, \dots, c_m, i^e x_1)$ . After this, the ideals in (3) repeat since  $[i^k \alpha, \beta + \Omega] = [\alpha, \beta + \Omega]$ .

We should point out that, calculating just the denominators  $q_n$  of the convergents of the CF for  $\Omega_1$ , we have a unit  $E = q_m x_{m+1} + q_{m-1}$  which is the fundamental

unit  $E_0$  for all the cases computed, except only for  $\delta = 1 + 4i, 5 + 4i$ , when  $E = E_0^2$ .

Of course, all the ideals in (3) are principal. Therefore, each  $a_n$  in (3) is compared with each  $\pi \in S$ ; if  $a_n = i^k \pi$ ,  $\pi \in S$ , then the prime divisors  $\mathfrak{p}$ ,  $\mathfrak{p}'$  of  $\pi$  are principal and make no contribution to the class group. Accordingly,  $\pi$  is eliminated from  $S$ . In a very few cases, all  $\pi \in S$  are eliminated this way and it follows that  $h = 1$ .

(III) If the principal period fails to exhaust  $S$ , we find the basis of  $\mathfrak{p}$  for each remaining  $\pi$ :

$$(4) \quad \mathfrak{p} = [\pi, \rho + \Omega], \quad \text{so} \quad \mathfrak{p}' = [\pi, (\pi - \rho - \epsilon) + \Omega].$$

This means solving the quadratic congruence  $\nu(\rho + \Omega) = \rho(\rho + \epsilon) + (\epsilon^2 - \delta)/4 \equiv 0 \pmod{\pi}$ . (Since  $N\pi < \frac{1}{2}\sqrt{P} < 250$  in this computation, no special tricks were used.)

Then each ideal  $\mathfrak{p}$  (4) is tested. It is principal if and only if the CF of  $A_\pi = (\rho + \Omega)/\pi$  falls into the principal period, so we need only test if a complete quotient  $(r + \Omega)/s$  has  $s = i^k$ . If so,  $\pi$  is eliminated from  $S$ . In case all  $\pi \in S$  are disposed of, again it follows that  $h = 1$ . Otherwise, for some  $\pi$ , the partial period of  $A_\pi$  is reached without any  $s = i^k$ , so the ideal  $\mathfrak{p}$  (4) is nonprincipal and so  $h > 1$ .

(IV) If  $h > 1$ , let  $\pi$  be the smallest prime remaining in  $S$ . The prime divisor  $\mathfrak{p}$  of  $\pi$  is in a nonprincipal ideal class  $C$ , and we calculate the cyclic group generated by  $C$ :  $\mathfrak{p} \in C$ ,  $\mathfrak{p}^2 \in C^2$ ,  $\dots$ ,  $\mathfrak{p}^n \in C^n = I$ , the principal class. However, we do not merely calculate powers of  $\mathfrak{p}$ ; the following simple modification is more suitable and has the advantage of avoiding any need for multiple-precision arithmetic when  $h$  is large.

Expand  $x = A_\pi = (\rho + \Omega)/\pi$  in a CF until the end of the partial period is reached, and choose an  $x_j$  in the period, which we denote  $A_1 = (\beta_1 + \Omega)/\alpha_1$ , and its corresponding ideal  $\mathfrak{a}_1$  (1), to represent the class  $C$  of  $\mathfrak{p}$ . Recursively, given a representative

$$(5) \quad \mathfrak{a}_m = [\alpha_m, \beta_m + \Omega] \leftrightarrow A_m = (\beta_m + \Omega)/\alpha_m$$

for the class  $C^m$ , calculate the ideal product  $\mathfrak{a}_m \mathfrak{p}$  (in essentially the same way as in a quadratic field). Then expand in a CF its corresponding quadratic irrational as before and take  $\mathfrak{a}_{m+1} = [\alpha_{m+1}, \beta_{m+1} + \Omega]$  in the periodic part. Thus  $\mathfrak{p}^{m+1} \sim \mathfrak{a}_m \mathfrak{p} \sim \mathfrak{a}_{m+1}$ , so  $\mathfrak{a}_{m+1}$  represents  $C^{m+1}$ . Since  $N\mathfrak{p} = N\pi < \frac{1}{2}\sqrt{P}$ , and an ideal in the period has  $N\mathfrak{a} = N\alpha < \sqrt{P}$ , so  $N(\mathfrak{a}\mathfrak{p}) < P$ , which is easily single precision.

Now, each class  $C^m$  is represented by a "reduced" ideal (purely periodic)  $\mathfrak{a}_m$  in (5), with  $\alpha_m, \beta_m$  stored in a table. The procedure continues until, finally, the principal period is encountered, so  $\mathfrak{p}^n \sim 1$ ,  $C^n = I$ .

(V) Once the cyclic group generated by  $\mathfrak{p}$  has been produced, the other remaining primes  $\kappa \in S$  are considered. Each  $\kappa$  has a nonprincipal prime ideal and corresponding quadratic irrational

$$(6) \quad \mathfrak{a} = [\kappa, \lambda + \Omega] \leftrightarrow B_\kappa = (\lambda + \Omega)/\kappa.$$

We expand  $B_\kappa$  in a CF; at each step the complete quotient  $(r + \Omega)/s$  is compared with the list of representatives (5) of the classes  $C^m$ . When a match is found— $r$

$= \beta_m$ ,  $s = i^k \alpha_m$ —then  $q \sim a_m \sim p^m$ , and so  $q$  contributes nothing new to the class group.

If for every  $\kappa \in S$  the ideal  $q \sim p^m$  for some  $m$ , then, since the class group is generated by these prime ideals, the group is *cyclic*, generated by the class  $C$  of  $p$ .

There are three cases when the group is not settled in this way:

(a) The class group is cyclic, but  $p$  generates a proper subgroup. Repeating the procedure in (IV), (V) for a prime ideal outside this subgroup eventually generates the whole group.

(b) The class  $C$  does indeed generate the whole group, but some prime ideal  $q$  is a “mismatch” —  $q \sim a_m \sim p^m$ , but the period of  $B_\kappa$  is distinct from that of  $A_m$ . We may check that  $a_m q' \sim 1$ , so  $q$  is in the cyclic group. This occurred only two times during the computation. Details will be given in Section 4.

(c) The class group is *noncyclic* and our procedure can only produce cyclic subgroups. This occurred in two cases where the group is  $C(3) \times C(3)$ , and all four cyclic subgroups of order 3 were obtained.

**4. Results.** Using the above method, we computed the ideal class group, and so the class number, for 5000 prime discriminants  $\delta \equiv \pm 1 \pmod{4}$ ,  $17 \leq N\delta \leq 226241$ . The case where  $\delta$  is a rational prime  $p \equiv 3 \pmod{4}$  was excluded, since Dirichlet's theorem applies to show  $h = h(p)h(-p)$ , the product of the quadratic class numbers. Also  $E_0 = \sqrt{i\epsilon_0}$ , where  $\epsilon_0$  is the fundamental unit of  $\mathbf{Q}(\sqrt{p})$ .

(A) Out of 5000 cases, 3994 have  $h = 1$ , 1006 have  $h > 1$ . We list in a table the cumulative distribution of class numbers, along with the corresponding data for the quadratic case (copied from [10]). The data provide empirical evidence that the mysterious distribution of class numbers previously noted in the real quadratic case is the same for this quartic case. (That is, of course, if there actually is a fixed asymptotic distribution.)

We conjecture the same distribution for the fields  $K$  quadratic over  $F = \mathbf{Q}(\sqrt{-m})$  having class number 1:  $m = 2, 3, 7, 11, 19, 43, 67$ , or 163. In the first 4 cases, where there is a CF over  $F$ , it may be possible to test the conjecture. The distribution might even occur for  $K$  quadratic over any fixed complex quadratic field  $F$ —although this is more speculative, since in this general case the computations are probably infeasible.

(B) Of the 1006 cases with  $h > 1$ , all but two fields have a cyclic class group. (Only the 64 cases with  $h = 9, 25, 27$  are in question.) The two noncyclic groups occur for

$$P = 54713, \quad \delta = 107 + 208i;$$

$$P = 201881, \quad \delta = 91 + 440i.$$

In both cases,  $h = 9$  and the class group is  $C(3) \times C(3)$ . We may note (see [11, p. 75]) that of the first 5000 real quadratic prime discriminants, exactly two have noncyclic class group:  $d = 32009, 62501$ , group  $C(3) \times C(3)$ .

(C) Recall that after stage (II) of the procedure, the array  $S$  contains Gaussian primes  $\pi$  which split in  $K$  into prime ideal factors  $p, p'$  which are not in the principal period. We denote the prime in  $S$  of smallest norm by  $\pi_1$ ; or if there are two such primes with the same smallest norm, then they are complex conjugates:  $\pi_1, \bar{\pi}_1$ . Then we denote a prime ideal factor of  $\pi_1$  [respectively  $\bar{\pi}_1$ ] in  $K$  by  $p_1$  [ $\bar{p}_1$ ].

Now, if  $h = 1$ , then, of course,  $\mathfrak{p}_1 [\bar{\mathfrak{p}}_1]$  becomes principal. It is remarkable that in all 1006 cases with  $h > 1$ ,  $\mathfrak{p}_1$  [and  $\bar{\mathfrak{p}}_1$ ] *remains nonprincipal*. That is,  $\mathfrak{p}_1$  [and  $\bar{\mathfrak{p}}_1$ ] becomes principal exactly when  $h = 1$ . A check of the first 5000 real quadratic prime discriminants found the identical situation: the analogous prime ideal  $\mathfrak{p}_1$  (that is, the splitting prime ideal of the smallest norm that remains after the primes in the principal period have been eliminated) becomes principal only when  $h = 1$ . Here is either a remarkable coincidence or a new conjecture.

We may also note that of the 1004 cyclic (quartic) cases with  $h > 1$ , in all but 23 cases, the class group is generated by  $\mathfrak{p}_1$  or by  $\bar{\mathfrak{p}}_1$ .

(D) There were other interesting results, all due to peculiarities of the CF. First, in real quadratic fields [5] conjugate ideal classes are always represented by conjugate periods of ideals. Such is frequently not the case here (nor for the quadratic case if the nearest integer CF is used). An example is  $P = 2137$ ,  $\delta = 29 + 36i$ , where  $h = 7$  and  $\mathfrak{p}_1 = [1 + i, \Omega]$ . Using the notation of [5], we represent the ideal  $[a, b + \Omega]$  by just  $a, b$ . The periods of (equivalent) ideals for the conjugate classes  $C, C^6$  are as follows:

$$C: 3 + 2i, 3 + 2i \sim 1 + i, 2 + 2i,$$

$$C^6: 3 + i, 3 + i \sim 1 + i, 2 + i.$$

(E) A second point of interest concerns the length of the *preperiod* of a periodic CF. In the quadratic case, given any ideal  $[a, b + \omega]$  with  $\text{norm} = a < \frac{1}{2}\sqrt{d}$ , it is easy to see that the (usual) CF for  $\alpha = (b + \omega)/a$  has at most a one-term preperiod. Using the nearest integer CF, it is easy to find 2-term preperiods. In the present complex quartic case, we encountered, for analogously restricted ideals  $\alpha$ , preperiods up to 9 terms long. No extensive check was made, but it seems possible that there is no bound on the length of the preperiod,\* even for ideals with norm below the "Gauss bound." Of course the uncertainty about the preperiod length makes it more tedious to check for the end of the period.

(F) A final, more serious peculiarity occurs for  $P = 2633$ ,  $\delta = 43 + 28i$ , which also has  $h = 7$ ,  $\mathfrak{p}_1 = [1 + i, \Omega]$ . The ideals

$$\alpha = [4, 3 + 2i + \Omega], \quad \mathfrak{b} = [4 - i, 5 - i + \Omega]$$

are equivalent, both in  $C^3$ . Let their corresponding quadratic irrationals be  $A = (3 + 2i + \Omega)/4$ ,  $B = (5 - i + \Omega)/(4 - i)$ . We find that  $B = (2A - i)/(A - i)$ , so  $A$  and  $B$  are equivalent numbers, as expected. However, the CF's, which are purely periodic, give distinct cycles:

$$(7) \quad \begin{aligned} A: 4, 3 + 2i &\sim -3 - 2i, 5 + i \sim -2 - 2i, 3 - i, \\ B: 4 - i, 5 - i &\sim 1 - 3i, 4 + 2i \sim -2 - 4i, 5. \end{aligned}$$

It turns out that the conjugate class  $C^4$  is also represented by two distinct cycles, each conjugate to one of the above cycles.

The class group of this field is of course cyclic, generated by  $\mathfrak{p}_1$ , but the prime  $\mathfrak{q}$  dividing  $3 + 2i$  is a "mismatch," since its period (that of  $A$  in (7)) has no match with the representative of  $C^3$  (in the period of  $B$  in (7)). It is easy to check that  $\alpha_3 \mathfrak{q}'$  is principal so that  $\mathfrak{q} \in C^3$ . This mismatch is clearly a rare event, occurring only twice

in the computation, and it is easily distinguished from the case where  $p_1$  generates a proper subgroup of the class group. For in the latter case, if the subgroup has index  $k$ , only about  $1/k$  of the primes in  $S$  will have their prime factors (6) in the subgroup. So one of the remaining primes in  $S$  is used and (except in the two noncyclic cases) eventually we obtain the whole cyclic group. On the other hand, in the case of a mismatch there will be only a very few primes of  $S$  left out of the group—just one prime in the case  $P = 2633$  above; two primes in the only other case encountered,  $P = 210209$ . For a mismatch  $q$ , we simply test if  $a_m q'$  is principal for  $1 \leq m < n$  to find the class  $C^m$  to which  $q$  belongs.

(G) Finally, we mention two old papers. J. Hurwitz [4] used a complex continued fraction to classify binary quadratic forms over  $\mathbb{Z}[i]$ . However, his CF has only *even* Gaussian integers as partial quotients, and his forms are always  $ax^2 + 2bxy + cy^2$ . For the fields in our computation with  $\delta \equiv \pm 5 \pmod{4} + 4i$ , J. Hurwitz' CF usually gives as class number  $3h$ , where  $h$  is the actual class number, so this method is unsuitable. G. B. Mathews [9] used, as we do, A. Hurwitz' CF, and his forms need not have an even middle coefficient. However, his basic definition of a reduced form is faulty, although it is not clear how much of his results are thereby invalidated.

The computation was done between November, 1972, and March, 1973, on a CDC 6400 at SUNY at Buffalo. In the final run, 12 minutes of CP time were

TABLE

*Cumulative distribution of class numbers for first 5000 prime discriminants*

<i>Quartic</i>						<i>Quadratic</i>					
$h =$	1000	2000	3000	4000	5000	cases	1000	2000	3000	4000	5000
1	830	1635	2427	3225	3994		816	1622	2420	3198	3987
3	100	208	310	410	525		101	213	306	422	522
5	35	65	113	155	198		35	70	111	145	183
7	14	31	47	69	85		22	36	58	79	98
9	5	13	25	37	56		9	16	34	50	66
11	6	14	19	22	28		6	10	13	19	29
13	3	11	19	22	30		5	8	14	20	28
15	2	8	13	15	21		2	7	13	16	20
17	3	6	10	15	19		1	2	7	9	11
19	—	—	2	5	6		—	2	5	8	11
21	—	1	1	3	6		1	1	2	5	7
23	1	1	3	4	5		—	2	2	3	4
25	1	1	1	2	3		—	1	4	7	10
27	—	3	3	4	5		1	3	3	4	4
29	—	1	2	2	3		—	—	1	2	4
>30	—	2	5	10	16		1	4	7	13	16

required to generate 5000 fields and to determine the 3994 cases with  $h = 1$ ; 10 minutes more were required to calculate the class group for the remaining 1006 cases. A copy of the complete table has been deposited in the UMT file of this journal.

Mathematics Department  
State University of New York at Buffalo  
Amherst, New York 14226

1. P. G. L. DIRICHLET, "Recherches sur les formes quadratiques à coefficients et à indéterminées complexes," *Werke* I, pp. 533-618.

2. D. HILBERT, "Über den Dirichletschen biquadratischen Zahlkörper," *Math. Ann.*, v. 45, 1894, pp. 309-340. (*Werke* I, pp. 24-52)

3. A. HURWITZ, "Über die Entwicklung komplexer Grössen in Kettenbrüche," *Acta Math.*, v. 11, 1887-1888, pp. 187-200. (*Werke* II, pp. 72-83)

4. J. HURWITZ, "Über die Reduction der binären quadratischen Formen mit complexen Coefficienten und Variabeln," *Acta Math.*, v. 25, 1902, pp. 231-290.

5. E. L. INCE, *Cycles of Reduced Ideals in Quadratic Fields*, British Association Tables, vol. 4, London, 1934.

6. S. KURODA, "Über den Dirichletschen Körper," *J. Fac. Sci. Imp. Univ. Tokyo Sect. I*, v. 4, 1943, pp. 383-406. MR 9,12.

7. R. B. LAKEIN, "A Gauss bound for a class of biquadratic fields," *J. Number Theory*, v. 1, 1969, pp. 108-112. MR 39 #1427.

8. R. B. LAKEIN, "Class numbers and units of complex quartic fields," in *Computers in Number Theory*, Academic Press, London, 1971, pp. 167-172.

9. G. B. MATHEWS, "A theory of binary quadratic arithmetical forms with complex integral coefficients," *Proc. London Math. Soc.* (2), v. 11, 1913, pp. 329-350.

10. D. SHANKS, "Review of table: Class number of primes of the form  $4n+1$ ," *Math. Comp.*, v. 23, 1969, pp. 213-214.

11. D. SHANKS & P. 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.